REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-02-2012	Final	21-09-2010 to 30-09-2011

4. TITLE AND SUBTITLE

Interagency and Multinational Information Sharing Architectures and Solutions (IMISAS) Project

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

JS J-7
Joint Development, Solutions Evaluation Division
116 Lakeview Parkway
Suffolk, VA 23435

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Interagency and Multinational Information Sharing Architectures and Solutions (IMISAS) experiment project focused on developing proposed solutions with the potential to overcome challenges in unclassified information sharing, coordination and collaboration with non-military mission partners. This Joint Concept Development and Experimentation (JCD&E) Enterprise project explored the current unclassified information sharing environment to include existing policies, processes, procedures, local authorities and available tools at several United States Combatant Commander organizations. The IMISAS experiment utilized a humanitarian assistance/disaster relief scenario, but found that principles of unclassified information sharing are applicable across a range of operations. The project's community of interest included the US Department of Defense and other US Government agencies, multinational and coalition, international organizations and non-governmental organizations.
This report is comprehensive of the entire project and is separated into six sections and 18 annexes. The sections address project background, project experiment design and analysis, descriptions of proposed solutions, recommendation transition approaches and a summary conclusion. The annexes contain acronyms, terms, definitions, references, supplemental research and project documentation.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Kathryn J. Smith (kathryn.smith@js.mil)
Unclassified	Unclassified	Unclassified	Same as Report (SAR)	988	**19b. TELEPHONE NUMBER** *(include area code)* 757-203-3164

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project Final Report

1 February 2012

Deputy Director Joint Staff, Joint and Coalition Warfighting
116 Lake View Parkway, Suffolk, VA 23435-2697
Attn: Ms. Kathryn Smith
Solution Evaluation Division
(757) 203-5322

(THIS PAGE INTENTIONALLY BLANK)

Executive Summary

The Department of Defense (DOD) operates in an interconnected world, where operations routinely involve a wide variety of participating organizations operating outside of the military domain. This context has established a clear need for sustained and habitual information sharing and collaboration among military and non-military stakeholders. Responding to a high priority warfighting challenge submitted by United States Africa Command (USAFRICOM) and United States European Command (USEUCOM), the Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) project was undertaken in September 2010.

The IMISAS project through experimentation and analysis, focused on developing proposed solutions with potential to overcome challenges in unclassified information sharing (UIS) and collaboration with non-military mission partners. The project community of interest included DOD and other U.S. Government agencies, multinational and coalition, international organizations and non-governmental organizations. The project design and analytic framework included gap identification and prioritization; potential solution identification and development; and experimentation on potential solutions with opportunities for discovery. Both quantitative and qualitative content analysis techniques were used to generate relevant findings and recommendations. Project events included site visits, planning conferences, and technical spirals that culminated in a scenario-driven Analytic Seminar in August 2011. Participants in the Seminar included USAFRICOM and USEUCOM staff officers, United States Agency for International Development (USAID) and Department of Commerce (DOC) representatives assigned to USAFRICOM and USEUCOM, representatives from Department of State (DOS), DOD Chief Information Office (DOD CIO), NATO's Civil-Military Fusion Centre (NATO CFC), United Nations Satellite Imagery Office, UN Office for the Coordination of Humanitarian Affairs (UNOCHA), UN High Commissioner for Refugees (UNHCR), UN World Health Organization (WHO), the Assessment Capacities Project (ACAP) and the Bundeswehr Transformation Centre (BTC).

Using the existing All Partners Access Network (APAN) portal as the DOD unclassified information sharing capability (UISC) proxy, the Analytic Seminar event allowed participants to explore, discuss and evaluate potential solutions in a simulated humanitarian assistance/disaster relief (HA/DR) scenario. Five non-materiel and ten materiel solutions were examined through experimentation.

Non-Materiel Solutions: The non-materiel solutions examined ranged from a pre-planned unclassified information decision release matrix to a quick reference staff guide detailing non-military organizational roles, responsibilities, and information requirements. These were aggregated into an *Operational Guide for Unclassified Information Sharing (OGUIS).* The draft

Guide with the proposed solutions in the form of processes, techniques and procedures was used by the experimental audience during the Analytic Seminar.

Non-materiel findings included:

- Operators indicated confusion about the policies, procedures, and mechanisms for releasing information to mission partners despite a strong desire to share information.
- Operator habit patterns formed through training and a fear of reprimand or the breaking of legal barriers contribute to a culture of withholding information.
- Participants noted the importance of building relationships among prospective mission partners in order to set conditions for information sharing during subsequent crisis operations.
- Operators noted that leveraging the early engagement of non-military partners was seen as an important step for effective and efficient use of military planning time and resources.

Non-materiel recommendations and best practices:

- Staffs should use the *Operational Guide for Unclassified Information Sharing* to supplement training and provide reinforcement of command information management procedures to establish habit and behavior patterns.
- Commanders should implement a pre-planned release matrix to clearly define criteria for release of sharable unclassified information.
- Organization work site design should include unclassified information sharing storage sites that more closely resemble flatter and collaborative methods used by external partners.
- Staffs should establish and maintain a mission partner's guide to include comprehensive descriptions of likely partner organizations.
- Commanders should encourage the establishment of relationships with mission partners during in Phase 0.

Along with local policy changes, training, and exercises, the day to day mechanisms recommended in the *Guide* can be an important catalyst for inculcating a culture of risk management and enabling more active unclassified information sharing behaviors.

Materiel Solutions:

The ten materiel solutions examined focused primarily on platform capability. They represented a broad spectrum of unclassified information sharing (UIS) features and approaches to improve user familiarity and leverage existing DOD and commercial capabilities. Solutions included integration with commercially available social networking applications and other websites used by non-DOD partners as a means for improving unclassified information sharing and collaboration with external partners.

Materiel findings:

- Potentially large volumes of information and requests for information during crisis response operations dictated the need for dedicated Knowledge Management support.
- Unclassified information sharing tools most frequently used throughout the experiment periods were request for information (RFI)/request for assistance (RFA) forum, media galleries, and Adobe® Connect Online™.
- Participants recognized the positive value of mapping capabilities such as MapView and GeoCommons.
- A "learning curve" is associated with any suite of centralized and integrated collaborative tools.
- The experimental audience stated clear benefits to pushing information to social media sites, particularly as part of the humanitarian assistance and disaster relief scenario.

Materiel recommendations:

- The DOD unclassified information sharing service (UISS) must include:
  - A continued development process for an integrated template of multimedia collaboration tools to serve the needs military and non-military partners.
  - Tool definitions and descriptions eliminating military specific terminology.
  - Provision for robust knowledge management (KM) support.
  - A web-based collaboration venue accommodating active moderation.
  - A dedicated question and answer (RFI or "query") tool with features such as filterability, topic group, easily searchable and capable of organizing and linking RFIs.
  - A robust, easy to use mapping utility.

The sheer number of recommendations for future unclassified information sharing technical capabilities attests to the interest in this area. The entire list of recommendations is found in Section 4.2 of this report, and includes a recommendation for DOD CIO and Joint Staff J8 to create a configuration management governance body to maintain configuration management of the unclassified information sharing service tools and capabilities.

This report is comprehensive of the entire project and is separated into six sections and 18 annexes. Section 1 introduces the project background. Section 2 outlines the project design, including the research questions, hypotheses, and data collection methodologies. Section 3 outlines the project execution with associated lines of operation for research and analysis, solutions development, experimentation, and transition. Section 4 offers descriptions of the proposed non-materiel and materiel solutions evaluated during experimentation, with findings, and recommendations. Section 5 outlines transition approaches for products developed through this project: the *Operational Guide for Unclassified Information Sharing (OGUIS)*, Unclassified Information Sharing (UIS) Architecture, the *White Paper on Unclassified Information Sharing*,

and materiel recommendations. Section 6 offers a conclusion and the proposed way ahead. The Annexes contain acronyms, terms and definitions and references, as well as project documentation.

Analysis of observations and findings throughout the course of the project affirmed that aligning potentially conflicting aspects of technology, policy, processes, procedures, and organizational cultures may prove to be the largest challenge in developing DOD's future information sharing capabilities. An aspect of that challenge will involve achieving balance between the need to share and the need to protect information, both of which can addressed through active risk management. Current information sharing capabilities remain underutilized due to local policies, staff procedures, and the need for additional training and education in organizational engagement. Further exploration of the organizational culture aspects of information sharing will likely yield the greatest return on investment.

The IMISAS project addressed elements of real operational problems and provided the foundation for addressing the larger information sharing challenges expressed in the initial problem statement. The findings and products from the project will be used to inform the DOD Unclassified Information Sharing Enterprise. Joint Requirements Oversight Council Memorandum (JROCM) 109-11 tasked the Defense Information Systems Agency (DISA) to study and provide recommendations to the Command, Control, Communications/ Cyberspace (C4/Cyber) Functional Control Board (FCB) based on the findings from the IMISAS project. The DISA brief to the C4 Cyber FCB on 3 November 2011 incorporated the recommendations found in this report.

JROCM 109-11 also tasked DOD Chief Information Office to study the findings and recommendations from the project to inform Program Objective Management (POM) 14 submissions. DOD CIO and JS J8 have further acted on an IMISAS project recommendation to create a configuration management governance body and co-hosted along with JS J8 the initial Unclassified Information Sharing Governance Working Group in late November 2011.

In the near term, many of the procedures and solutions identified can be implemented immediately, used in training and other joint force development events and activities.

TABLE OF CONTENTS

1. Introduction 1
1.1. Background and Context 2
1.2. Problem Statement 5
1.3. Objectives and Desired Outcomes 6
1.4. Community of Interest 7
2. Project Design 8
2.1. Research Questions 9
2.2. Project Hypotheses 10
3. Project Execution 10
3.1. Research and Analysis 11
3.2. Solutions Development 11
3.3. Experimentation 12
3.3.1. Experimentation Data Collection and Analysis 13
3.3.2. Bundeswehr Transformation Centre Human Factors Analysis 14
3.4. Transition 15
4. Solution-based Findings and Recommendations 15
4.1. Non-Materiel Solutions, Findings and Recommendations 16
4.1.1. Pre-planned UIS Release Matrix (1-1a) 17
4.1.2. Unclassified Information Storage (1-1b) 17
4.1.3. Business Rules for Manual Cross Domain Transfer (1-2) 18
4.1.4. Guide to Enable Information Sharing with Mission Partners via the Unclassified Information Sharing Capability (1-5) 19
4.1.5. Information Management and Knowledge Management Business Rules for Unclassified Information Sharing (1-7) 20
4.1.6. Quick-Reference Guide to Potential Non-DOD Mission Partners (1-8) 21
4.2. Materiel Solutions 22
4.2.1. Work Site Template (1-3a) 23
4.2.2. Business Rules for UISC Work Site (1-3b) 26

4.2.3. Business Rules for Data and Metadata Standards and Tags (3-1) 27
4.2.4. Accommodating Disadvantaged Users (4-1) 27
4.2.5. Graduated User Accounts (4-6) 28
4.2.6. Rapid User Account Registration (4-7) 28
4.2.7. Pushing and Posting Data from Dynamic Sources (4-8) 29
4.2.8. Capturing, Sorting, and Categorizing Information (4-9) 29
4.2.9. Business Rules for Automatic Trust Center Capability (4-10) 30
4.2.10. Source Authenticity and Reliability Rating (4-11) 30
4.2.11. UISC Search Capabilities (4-12) 30
5. Solutions to Product - Transition 31
6. Conclusion 33
Annex A – Acronyms A-1
Annex B – Terms and Definitions B-1
Annex C – References C-1
Annex D – Experimentation Plan D-1
Annex E – Baseline Assessment Report (BAR) E-1
Annex F – After Action Reports F-1
Annex G – Analytic Framework G-1
Annex H – Data Collection and Analysis Plan (DCAP) – Technical Sprials H-1
Annex I - Data Collection and Analysis Plan (DCAP) – Analytic Seminar (AS) I-1
Annex J – Final Project Analysis J-1
Annex K – Bundeswehr Transformation Centre (BTC) Final Report K-1
Annex L – IMISAS Project Transition Plan L-1
Annex M – Operational for Unclassified Information Sharing M-1
Annex N – Unclassified Informaiton Sharing (UIS) Architectural Products N-1
Annex O – White Paper on Unclassified Information Sharing (UIS) O-1

LIST OF FIGURES

Figure 1 – Project Framework 9
Figure 2 – The IMISAS Project Campaign Lines of Operation 11

LIST OF TABLES

Table 1 – IMISAS Project Non-technical Solutions..... 16
Table 2 – IMISAS Project Technical Solutions..... 22

1. Introduction

"One would think we can share information by now. But Katrina again proved we cannot."[1]

In a 2009 report to the U.S. Congress, the Government Accountability Office (GAO) identified significant challenges to sharing and integrating information across agencies due to: "1) lack of standards for data collection, usage, storage, protection, or a combination of these; 2) cultural or political barriers that inhibit information sharing; 3) lack of interagency agreements on procedures for sharing information; and 4) security clearance requirements that are not harmonized."[2]

In September 2010, the Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) project was launched as a twelve-month effort approved as part of the fiscal year (FY) 10/11 Program of Work by the Joint Concept and Development Experimentation Executive Council, representing primary stakeholders from the operational community. The project was designed to identify and experimentally validate processes, policy changes, procedures, technologies and other modifications needed to address barriers to effective information sharing and collaboration in operational military environments. The project employed a scenario focused on Humanitarian Assistance/Disaster Relief (HA/DR) mission planning and execution activities to give a broad representation of real-world information sharing and collaboration challenges that face combatant commanders (CCDRs) and their staffs working with non-Department of Defense (DOD) mission partners.

Using a mix of face-to-face planning conferences, virtual collaborative planning sessions, technology spirals, and other experimentation activities, the community of interest (COI) identified and developed proposed solutions and recommendations for improving unclassified information sharing and collaboration.

For clarification of terminology used in this report, *Annex A* contains the document acronyms, *Annex B* contains terms and definitions, and *Annex C* contains the document references.

---

[1] Congressional reports: *H Rpt. 109-377 – A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*, February 15, 2006.
[2] U.S. Government Accountability Office Report, *Interagency Collaboration: Key Issues for Congressional Oversight of National Security Strategies, Organizations, Workforce, and Information Sharing*, GAO-09-904SP (Washington, D.C.: September 25, 2009).

1.1. Background and Context

"In the aftermath of the Indian Ocean Basin Tsunami in 2004, it became quite evident that the U.S. Department of Defense was in need of a mechanism to share unclassified information amongst a wide variety of non-traditional mission partners including international organizations, non-governmental organizations (NGO's), coalition militaries, and with multiple nations. It was not precisely known exactly what type of system, capability, or mechanism was required."[3]

In the past decade, the U.S. and the international community have witnessed and responded to human rights abuses, massive refugee movements and the endangerment and death of hundreds of thousands of civilians as a result of natural disasters, civil wars and major conflicts in countries like Somalia, the former Yugoslavia, Indonesia, Haiti, Iraq and Afghanistan. Bringing this global context home to the U.S., the experiences of September 11, 2001 and Hurricane Katrina resulted in a similar set of responses among DOD, other government agencies, non-governmental organizations (NGO), and private sector actors. The 2011 Tōhoku earthquake and tsunami as well as the erupting civil conflict in Libya saw a vast international response in the coordination of relief efforts. Each of these incidents reinforced and highlighted the need to embrace unclassified information sharing and collaboration.

In today's interconnected world, contingency operations routinely involve a wide variety of actors and participating organizations operating outside the military domain throughout the phases of an operation, including Phase 0.[4] Current USG organization, policies, and procedures and host nation cultural considerations generally point toward non-DOD actors as having the lead role in today's theater cooperation, stabilization, and HA/DR mission areas. The HA/DR mission environments generally involve a wide variety of historically independent and non-aligned NGOs as highly-capable responders who are generally trusted by the indigenous populations.[5] These organizations are generally actively engaged in the crisis before DOD organizations begin formal planning and operations. Current USG policy identifies the "United States Agency for International Development (USAID) as the 'lead agency' for development where it carries out programs complemented by DOD efforts in stabilization, disaster response,

---

[3] Chlebo, Christman, and Johnson. *Enhancing Collective Command and Control (C2) in the International Environment: Leveraging the Unclassified Information Sharing Enterprise Service*, June 2011.
[4] Phase 0 (shaping) involves pre-crisis and/or pre-contingency activities in order to "enhance bonds between future coalition partners." Reference Joint Pub 3-0, *Joint Operations*, page xix.
[5] Joint Publication 3-08, *Interorganizational Coordination During Joint Operations*, June 24, 2011, xiv.

foreign internal defense, and security force assistance."[6] Apart from these facts, recent events show an increasing use of technologically enabled capabilities, i.e., crowdsourcing, open-source social networks, and mobile technology among these non-DOD actors.[7] Taken together, these and other considerations indicate that CCDRs and their staffs require similar capabilities to be effective in their supporting role in HA/DR missions.

Over the past decade DOD has worked toward improving civil-military coordination and cooperation with a wide range of programs and initiatives. The 2006 *Quadrennial Defense Review (QDR)* called upon DOD to broadly improve "information sharing with other agencies and with international allies and partners" and develop a strategy guiding "operations with Federal, State, local and coalition partners".[8] Responding to the QDR, the DOD Chief Information Officer (CIO) on May 4, 2007 signed the *Department of Defense Information Sharing Strategy*, and in April 2009 promulgated the *Department of Defense Information Sharing Implementation Plan*, which established a set of near-term tasks to position DOD to progress toward implementation of the broader strategy. On November 15, 2010 the Director Joint Staff for Operations (J3) released the *Unclassified Information Sharing Capability (UISC) Concept of Operations (CONOPS)*, which "outlines the capability designed to assist joint, coalition and military organizations in their efforts to collaborate, plan and coordinate operations, exchange information and build situational awareness with both traditional and non-traditional mission partners across various mission sets."[9]

In concert with efforts to modernize DOD policy and approaches, a broad range of joint studies, experiments, advanced technology development efforts and joint tests filled the collective trade space for exploring information sharing and collaboration capability gaps and framing proposed solutions.[10] These efforts began in the early 2000s, with the United States Pacific Command's (USPACOM) use of a common website for sharing information with its multinational partners as a part of its Multinational Planning Augmentation Team (MPAT). Beginning as the Asia-Pacific Area Network in 2000 (later renamed the All Partner Access Network), it was an unclassified portal, including log-in and "password for access" control, reserving more operationally sensitive, yet still unclassified information, for trusted MPAT members. This portal was

---

[6] Joint Publication 3-08, *Interorganizational Coordination During Joint Operations*, June 24, 2011, xix. Also, see U.S. Agency for International Development (USAID), Bureau for Democracy, Conflict and Humanitarian Assistance (DCHA), Office of U.S. Foreign Disaster Assistance (OFDA) *Guidance for Disaster Planning and Response- FY 2011*.

[7] U.S. Southern Command Science and Technology Office, *Transnational Information-Sharing Cooperation (TISC) Concept of Operations, version 2.1.2*, 10, June 2010.

[8] QDR, 2006.

[9] U.S. Joint Chiefs of Staff, J36, *Unclassified Information Sharing Capability (UISC) Concept of Operations*, November 15, 2010.

[10] The IMISAS *Baseline Assessment Report*, Annex E of this report, provides further discussion of individual programs.

originally envisioned as a file sharing and military exercise tracking tool and publicly releasable information was published to keep exercise participants up-to-date on the current exercise status. In 2010, The Transnational Information Sharing Capability (TISC) Joint Concept Technology Demonstration (JCTD) successfully used the All Partners Access Network (APAN) to demonstrate its utility as an unclassified information sharing capability in support of three geographic COCOMs. In 2010, the communications system directorate of the Joint Staff (J6) concluded that "APAN's capability is operationally acceptable for implementation as the initial capability for unclassified information sharing" and APAN was designated as the Shared Enterprise Service.[11]

Related to information sharing, and with a civil-military information gathering focus, the Joint-Civil Information Management (J-CIM) Joint Test and Evaluation event produced a *Tactics, Techniques and Procedures (TTP) Handbook for Civil Information Management (CIM)* to standardize assessment methods and information management business processes. The Civil Information Fusion Concept (CIFC) "was designed to capture lessons learned from the various non-doctrinal organizations that *most successfully* prioritize civil information, to distill those best practices, and to address these emerging requirements and tasks against any joint task force (JTF) mission" and proposed a new framework to fuse and integrate Civil/Military information and intelligence.[12] The United States Special Operations Command (USSOCOM) established the CIM Data Processing System (DPS) as a program of record to aid in collection, management, and analysis in this domain. Further, the Mapping Human Terrain Quick Reaction Capability added analytical tools to aid in the in-depth examination of socio-cultural link analysis among key actors in social networks.[13]

In the context of further developing a comprehensive approach, the Interagency Shared Situational Awareness (IA SSA) limited objective experiment conducted in 2009 was designed to provide "joint force commanders with a better capability to share information with interagency, multinational and non-government agencies during crisis operations."[14] In concert with Multinational Experiment 6 (MNE 6), the Adaptive Logistics Network (ALN) project examined "potential solutions of how best to improve planning and coordination of international

---

[11] Joint Chiefs of Staff J-6 Memorandum for Acting Assistant Secretary of Defense for Networks and Information Integration. *Department of Defense (DOD) Enterprise Unclassified Information Sharing Service*, August 10, 2010

[12] Lindenmayer, Martin J. Civil Information and Intelligence Fusion: Making "Non-Traditional" into "New Traditional" for the JTF Commander. *Small Wars Journal*, June 22, 2011.

[13] Chlebo, Paul, Gerard J. Christman, and Roy A. Johnson. *Enhancing Collective C2 in the International Environment: Leveraging the Unclassified Information Sharing Enterprise Service*. Paper presented at 16th International Command and Control Research and Technology Symposium: Collective C2 in Multinational Civil-Military Operations, Quebec City, Canada: June 21-23, 2011.

[14] Parker, Katrina. *Situational awareness experiment prepares for real world crises*. USJFCOM Public Affairs news release, July 29, 2009.

logistic responses [toward] reducing inefficiencies and eliminating redundancies arising when multiple agencies and organizations respond simultaneously to crises."[15]

In studying these and other complementary efforts, the IMISAS project leveraged foundational and supporting work previously produced in order to scope this effort and optimize the project resources.

1.2. Problem Statement

> *"USEUCOM and USAFRICOM require the capability to share essential information with interagency partners, Coalition and Alliance partners, or emerging partner nations in bi-lateral or multinational efforts. The capability gap is the result of: restrictive network access and information sharing policies; restrictive and cumbersome accreditation procedures for coalition networks and systems; lack of a coherent/unified strategy for a whole-of-government (to include foreign government) approach to an information sharing/collaborative environment; and resourcing to support that environment and its associated network enterprise services."*[16]

Derived from the combined USEUCOM/USAFRICOM Warfighter Challenge submission (above), the IMISAS project problem statement was developed early, coordinated with the partners, and remained relatively unchanged throughout the project.

IMISAS Project Problem Statement

"COCOMs lack a coherent framework/capability to share information and collaborate across multiple domains with a broad range of mission partners (government / interagency, multinational, multilateral and private sector) due primarily to restrictive policies, conflicting authorities, ad hoc / non-existent procedures, business rules and non-interoperable networks and systems."

[15] USJFCOM J9, Final Report, *Adaptive Logistics Network/Multinational Experiment 6, Objective 4.5*, April 29, 2011.
[16] Warfighter Challenge Submittal, 2010

In its simplest form, information sharing between two parties is not without difficulties. In a comprehensive approach, with multiple partners, the challenges are formidable and involve dimensions of organizational, cultural, policy, process, procedural, and technological impediments. Information sharing is impeded by sensitivities associated with military security concerns, as well as the neutrality and independent policies of international organizations (IOs) and non-governmental organizations (NGOs). A lack of cultural and social situational awareness, the "political will" of participants and organizations, or differences in communication and authority structures complicates efforts to build trust and a shared understanding of expectations. Conflicts and shortfalls in policy, doctrine and tactics, techniques and procedures further complicate the situation.

Policy restrictions on information release, management and assurance requirements, and organizational authorities and resources for network and spectrum management also complicate the issues. Technical challenges include the necessity of integrating ad hoc, stove-piped capabilities, lack of a unifying architecture and concept of operations, large and complex problems in data management, the need to accommodate the disadvantaged user, and the need to address the problems of linguistic differences over a potentially vast set of languages and dialects.

Several compounding factors informed the project objectives, desired outcomes, project design and execution. These factors included:

- Outdated, conflicting and restrictive policies and authorities which impede efforts to establish habitual information sharing and collaboration.
- Ineffective information sharing procedures and business rules.
- Non-interoperable networks and a proliferation of specialized systems diffuse integrated information sharing and hinder collaboration.
- Exclusion of low technology users in favor of more advanced technology; current solutions, implemented in crisis response accommodate current users, are not designed to accommodate low technology users.
- Inadequate practices that do not foster the development of habitual relations for building trust and enabling enduring information sharing and collaboration.

1.3. Objectives and Desired Outcomes

The project objectives and outcomes were derived from planning conferences, virtual collaborative sessions, and supported by technology spirals, and experimentation activities. The project objectives were:

- Examine how DOD can share information with a range of global partners, including international organizations, NGOs, and private organizations, for HA/DR operations.

- Examine policy and recommend changes to facilitate information sharing with a range of partners in an HA/DR environment.
- Examine potential security and cross domain solutions for unclassified information sharing during the period of the project.
- Using APAN as the technical proxy, conduct technical spirals and an experiment to examine enhancement recommendations previously identified, focusing on those aligning with the capability gaps expressed in the warfighter challenge.

The desired project outcomes were:

- Project findings and observations increase participants' collective understanding of policies and procedures governing information sharing and collaboration.
- Consensus recommendations among participants on policy and procedure interpretations and/or changes improving information sharing and collaboration in the HA/DR mission environment (as appropriate, extending to other mission area domains).
- Project findings, observations, and recommendations contributing to a handbook of best practices, pitfalls to avoid, tactics, techniques, and procedures for optimizing information sharing and collaboration among the full range of partners in the HA/DR mission environment (as appropriate, extending to other mission area domains).
- Technological assessment of the UIS capabilities to reveal gaps to inform modernization requirements for unclassified information sharing and collaboration systems.

1.4. Community of Interest

Operational military forces routinely carry out missions in a complex, multi-actor operating environment characterized by a broad diversity of perspectives, interests, approaches, and objectives among participants. The COCOM participants and core project team cast a wide net to solicit participant organizations, and the effort generated an active Community of Interest (COI) comprised of core team partners, engaged actors, and generally interested participants:

- Bundeswehr Transformation Centre (BTC)
- Defense Information Systems Agency (DISA)
- Department of Defense Executive Agent for Maritime Domain Awareness
- Joint Irregular Warfare Center (JIWC)
- Joint Staff Force Structure, Resources, and Assessment Directorate, J8 (JCS J8)
- Joint Staff Joint Force Development Directorate, J7 (JCS J7)
- Joint Staff Force Structure, Resources and Capabilities Directorate, J8 (JCS J8)
- National Defense University (NDU)
- National Security Agency (NSA)

- North Atlantic Treaty Organization Civil-Military Centre of Excellence (NATO CCE)
- North Atlantic Treaty Organization Civil-Military Fusion Centre (NATO CFC)
- Office of the Assistant Secretary of Defense Networks and Information Integration/CIO (Now DOD Chief Information Office)
- United Nations (UN) Office for Coordination of Humanitarian Affairs (OCHA)
- UN High Commissioner for Refugees (HCR)
- UN World Health Organization (WHO)
- United States Agency for International Development (USAID)
- United States Department of Commerce (DOC)
- United States Department of State (DOS), Humanitarian Information Unit (HIU)
- United States Africa Command (USAFRICOM)
- United States European Command (USEUCOM)
- United States Northern Command (USNORTHCOM)
- United States Pacific Command (USPACOM), Pacific Warfighter Center APAN Team
- United States Special Operations Command (USSOCOM)
- United States Southern Command (USSOUTHCOM)

2. Project Design

The project examined concept and capability solutions at various levels of maturity using the general project design and analytic framework illustrated in Figure 1. It consisted of baseline research, gap identification and alignment, gap prioritization, identification of potential solutions and feasibility of experimentation and associated risk assessment, experiment design and execution, and recommendations resulting from the analysis of experimentation results. Details of the project design can be found in the *Experiment Plan*, Annex D and *Analytic Framework*, Annex G.

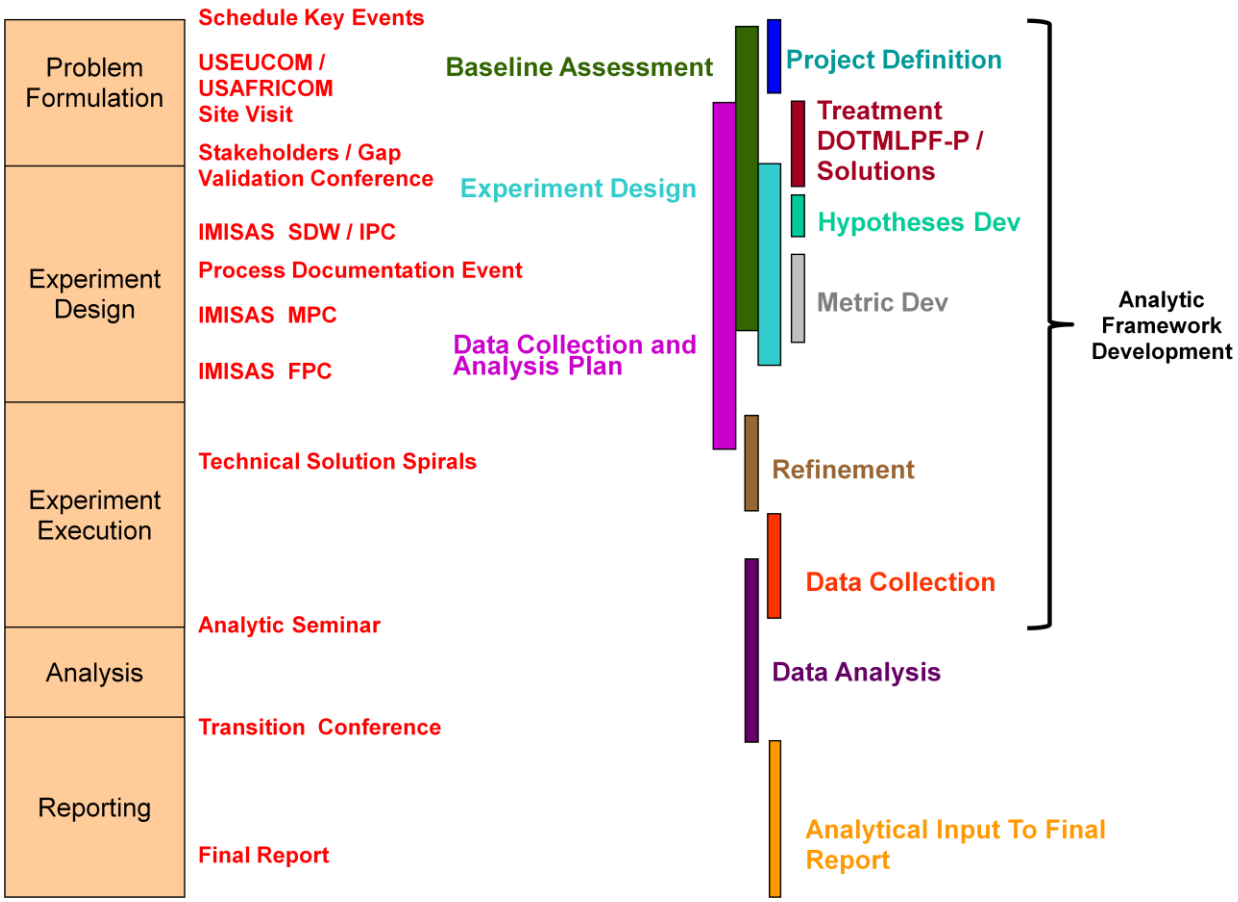


Figure 1 – Project Framework

2.1. Research Questions

The project design was grounded in the following research questions:

- What is the current state of primary HA/DR participants' collective understanding of policies and procedures governing information sharing and collaboration in the HA/DR mission environment?
- What system enhancements should be integrated into unclassified information sharing technologies and systems to maximize information sharing and collaboration among HA/DR participant organizations?
- What policy and procedure interpretations and/or changes would improve participants' information sharing and collaboration in the HA/DR mission environment?
- What best practices, pitfalls to avoid, tactics, techniques, and procedures optimize information sharing and collaboration among the full range of partners in the HA/DR mission environment?

2.2. Project Hypotheses

Three high level hypotheses were developed for the project.

- If the unclassified information sharing capability combines knowledge management methodologies with a minimum-demand user interface and carefully designed software composition including social media interfaces, then accessibility, completeness, responsiveness, and timeliness of information will increase, with attendant increases in relevance to the activity of responders and their situational understanding.
- If COCOMs foster coordination with, outreach to, and holistic comprehension of the span of HA/DR responders, then the coherence, agility, responsiveness, robustness, and speed of combined HA/DR responses will increase.
- If a risk-managed approach to information sharing is adopted, to include information release policy, mechanisms for identity establishment and source vetting, and methods for assuring confidentiality and anonymity, then within acceptable limits of information accuracy and security, improvements will be garnered in information accessibility and the agility, flexibility, responsiveness, speed, and timeliness of an HA/DR response.

3. Project Execution

The project incorporated four distinct but interrelated lines of operation (Figure 2). Research and analysis focused on developing a full and complete understanding of the unclassified information sharing operating environment and its inherent challenges. Solutions development built on these research findings to identify areas for further exploration in the experimental context. Experimentation focused on the generation of empirical data, observations, and findings in the context of real-world operations and hypothetical HA/DR scenarios. Transition planning began at the outset of the project, after prioritization of gaps and potential solutions, in order to identify potential change agents for implementing project recommendations.

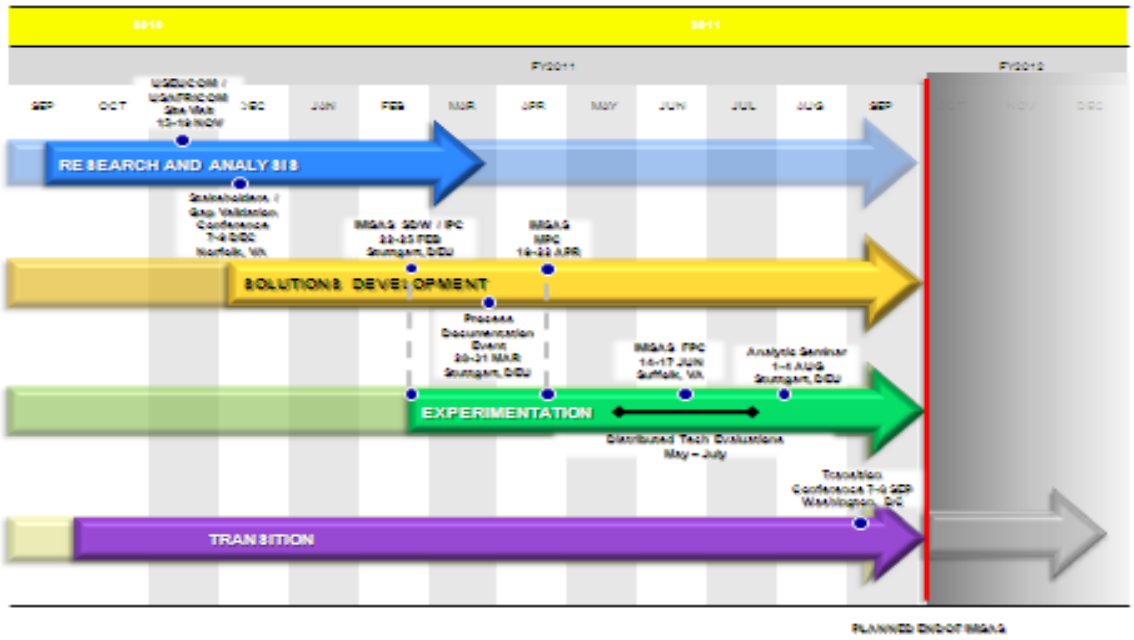


Figure 2 – The IMISAS Project Campaign Lines of Operation

3.1. Research and Analysis

Research and analysis included review of findings from earlier information sharing studies and reports, engagement with related ongoing efforts, as well as site visits, and conference activities to inform the baseline for the information sharing environment, inclusive of current USAFRICOM and USEUCOM unclassified information sharing procedures. During the November 2010 site survey visit, members of the project team interviewed staff representatives at USEUCOM and USAFRICOM. The site visit allowed for an in-depth discussion on the current processes, practices and local policies in place for unclassified information sharing with a range of military and non-military actors. In December 2010, gaps and initial potential solutions were validated and prioritized at the Stakeholder/Gap Validation Conference. The results of these efforts and the conference were incorporated into the *IMISAS Baseline Assessment Report (BAR)*. (See Annex E for further details.)

3.2. Solutions Development

Solutions development incorporated major process documentation and informed the development of a draft *Operational Guide for Unclassified Information Sharing*. In February 2011, a Solutions Development Workshop (SDW) and experiment Initial Planning Conference

(IPC) was held at USEUCOM. These events served to validate and prioritize capability gaps, and evaluate potential solutions for further development and to shape planning for the project experiment. The SDW/IPC marked a shift from research to solution refinement and focused planning for the scheduled August 2011 Analytic Seminar. Annex F, Appendix 1 contains the details of this workshop and conference.

Based on the research, analysis and the initial set of potential solutions, the drafting of a *White Paper on Unclassified Information Sharing (UIS)* was initiated. This paper was intended to further define the environment and provide context for the experiment. The *White Paper* was iteratively developed in concert with the project.

A Process Documentation Event was conducted at USAFRICOM and USEUCOM, 28-31 March 2010. The objective of the event was to further examine existing processes and potential solutions in support of continued event design and planning, and set the conditions for further refinement during the Mid-Planning Conference (MPC). Annex F, Appendix 2 contains the details of this event.

The MPC was held 19-22 April 2011 in Suffolk, VA. Participants validated the high-level potential solutions for examination, agreed on the foreign humanitarian assistance scenario focused on multi-organizational information sharing, and further refined planning of the key experiment design elements. Annex F, Appendix 3 contains the details of this planning conference.

At the Final Planning Conference (FPC), 14-17 June 2011 in Suffolk, VA, participants agreed to the solution elements to be examined during experimentation in the Analytic Seminar. The FPC provided the primary forum to finalize all planning and execution requirements for the Analytic Seminar. Annex F, Appendix 4 contains the details of this planning conference.

3.3. Experimentation

Experimentation began in May 2011, with a series of five technical spirals, using APAN as a UISC proxy to accomplish limited explorations and analysis. Technical spiral participants included representatives from the project team, the BTC, NATO CFC and anticipated Analytic Seminar experimentation audience participants, including representatives from USEUCOM and USAFRICOM. The group explored APAN capabilities collaboratively, using Adobe® Connect™ Online (ACO™) sessions to conduct each spiral.

In August 2010, the Analytic Seminar focused on information sharing procedures in the context of USAFRICOM support to a notional multinational, civilian-led humanitarian assistance/ disaster relief operation in Central Africa. The Analytic Seminar Experiment Audience represented a notional COCOM level Operational Planning Team (OPT) and various mission partners serving as experiment role players in the scenario. Participants included USAFRICOM

and USEUCOM staff officers, USAID and Department of Commerce representatives assigned to USAFRICOM and USEUCOM, representatives from the Department of State, DOD Chief Information Office, NATO's Civil-Military Fusion Centre, UN Satellite Imagery Office, UN Office for the Coordinator of Human Affairs, UN High Commissioner for Refugees, UN World Health Organizations, the Assessment Capacities Project, and the Bundeswehr Transformation Centre.

The Analytic Seminar presented the experiment participants with four vignettes developed to provide operationally relevant context for examining the potential solutions addressing information sharing issues among mission partners. Annex F, Appendix 5 contains further details.

By partnering directly with the stakeholders (USEUCOM and USAFRICOM), integrating a multinational experimentation partner (Germany), and inviting international organization (IO) and non-governmental organization (NGO) representatives for the execution phase, the potential solutions were evaluated in a more realistic environment.

3.3.1. Experimentation Data Collection and Analysis

To support the analysis of proposed solutions, data collection for the project was conducted primarily during the five technical spirals and in the culminating Analytic Seminar. The details of the data collection schemes and analysis plans are contained in the Analytical Framework found in Annex G, in the Data Collection and Analysis Plan (DCAP) for the Technical Spirals found in Annex H, and in the DCAP for the Analytical Seminar found in Annex I.

Both qualitative and quantitative data were collected using a variety of methods and tools to provide a balanced evaluation of the solutions. These methods included:

- Structured interviews with experiment participants.
- Direct observations of experiment participants.
- Responses to research questions.
- Responses to directed survey questions.
- Automated or instrumented time-stamped data collected from various tools and applications.

Survey questions to solicit participant responses for subsequent comparative and distribution analysis were generally administered either in the form of five-response Likert Scale[17] questions or in open-ended essay questions. Some of the Likert Scale questions included an option for the respondents to indicate that they did not have enough information to answer the question.

The primary data analysis method was intended to compare information sharing effectiveness between cases, i.e., simulated situations without using recommended solutions versus simulated situations using recommended solutions. Time constraints imposed on the event due to real-world mission requirements prevented the execution of a repetitive trials approach. These limitations, as well as significant differences between information sharing practices and equities at USEUCOM and USAFRICOM, rendered direct comparisons between the "as-is" and "to-be" information sharing architectures as infeasible.

For some solutions, by treating the Operational Planning Team (OPT) and Response Cell as independent entities, the analysts could draw significant conclusions by comparing the response of the two groups. In other cases, by treating participant responses as the binomial objects of analysis, the analysts were able to statistically evaluate the significance of responses and infer meaningful experimental findings.

Blending survey responses with amplifying data from open-format comments and direct observations, the analysts generated inferential findings and conclusions from the available data. These findings and recommendations are reported in Section 4 below, with the detailed observations and data included in Annex J (Analysis).

3.3.2. Bundeswehr Transformation Centre Human Factors Analysis

In addition to the primary data collection and analysis focused on the effectiveness of information sharing using the potential solutions, the BTC as partners in the experiment provided human factors analysts focused on quality aspects of the information sharing. The general objective of Human Factors Analysis is to observe the impact of work and organizational design on human performance and well being. The BTC team looked for related factors such as usefulness and relevance of information, deemed extremely important for mission partners. The human factors analysts had two research issues related to the IMISAS project:

[17] When responding to a Likert questionnaire item, respondents specify their level of agreement or disagreement on a symmetric scale for a series of statements. The scale range captures the intensity of the respondents' feelings for a given item.

- Exploring the impact of motivation and attitudes towards civil-military / interagency cooperation on information sharing requirements using web-based platforms / tools.
- Building and developing intra-group and inter-organizational shared situational awareness (SSA).

This approach complemented the U.S. solution evaluation. The human factors analysts interviewed and surveyed a majority of the experimental audience, and their findings principally supported general findings and observations of the primary analysis team. The Bundeswehr Transformation Centre Report is found at Annex K.

3.4. Transition

Transition planning commenced at the outset of the project and included the iterative development of a transition plan consistent with projected outcomes and anticipated non-materiel doctrinal, training, leadership and education, and policy solutions and recommendations. Materiel recommendations were focused on enhancements to the APAN platform and recommendations for consideration of requirements for the future DOD unclassified information sharing capability. A Transition Conference was held on 7-8 September 2011 in Washington, DC. Annex F, Appendix 6 contains details of the conference.

The Transition Conference brought together partner and key COI representatives to review findings from the experiment, the proposed recommendations, and to establish consensus for future implementation of products and recommendations as presented in the Transition Plan found in Annex L.

4. Solution-based Findings and Recommendations

The findings and recommendations resulting from experimentation can be traced to the initial gap analysis, which generated 138 potential solutions for consideration. When assessed against anticipated resource and scheduling constraints for experimentation, this list was further reduced to 56 potential solutions. The consolidated list was vetted with the USEUCOM and USAFRICOM staffs for prioritization, resulting in 22 potential solutions arranged into four categories:

- Standard operating procedures supporting tactics, techniques and procedures
- Knowledge, skills and abilities and training
- Data standards
- Unclassified information sharing capability enhancements

After further examination, five solutions were deferred as not experimentally verifiable within the scope of the project. Two solutions were combined with others, leaving five non-materiel and ten materiel (technical enhancement) solutions for analysis (Tables 1 and 2). This section of the Final Report outlines the non-materiel and materiel (technical enhancement) solution-based and findings and recommendations. Annex J contains additional details.

4.1. Non-Materiel Solutions, Findings and Recommendations

The five solutions focused on policy, process and procedures outlined in the *Operational Guide for Unclassified Information Sharing (UIS)*, found in Annex M, were evaluated (Table 1). Unless noted otherwise, the majority of findings were generated during the August 2011 Analytic Seminar.

Table 1 – IMISAS Project Non-Materiel Solutions

Solution		Elements	
1-1	Process and procedures for the expedited release of controlled unclassified information (CUI) in a crisis response situation	**1-1a**	Pre-planned release matrix • Linked to Commander's release guidance • Release matrix applies risk management • Additional release authorities
		1-1b	Unclassified information storage – UISC • Business rules for storage of unclassified information on the UISC
1-2	Business rules governing the expedited transfer of unclassified information from classified networks to non-classified networks.	**1-2a**	Business rules for manual cross domain transfer
1-5	Guides to enable UIS with mission partners via a UISC	**1-5a**	Processes and procedures to effectively engage mission partners for information sharing • U.S. Interagency, Host Nation (HN), multinational/coalition partners, Intergovernmental Organizations (IGOs) and NGOs • Use of staff embeds/liaison officers (LNOs) • Address all UIS capabilities (portal, e-mail, phone, etc.)
1-7	Guides for staff use of UISC in support of operations	**1-7a**	Best practices to maximize use of UISC • Information Management (IM)/Knowledge Management (KM) business rules
1-8	Quick reference guides for the roles, responsibilities and general information requirements of potential non-DOD mission partners	**1-8a**	Reference guide for mission partners • U.S. Interagency, HN, IGOs and NGOs • Roles, responsibilities and general information requirements • Electronically searchable

4.1.1. Pre-planned UIS Release Matrix (1-1a)

This solution involved processes and procedures for the expedited release of controlled unclassified information in a crisis response situation. This element of the solution entailed a pre-planned release matrix linked to Commander's release guidance and applied risk management in the context of additional release authorities.

Findings:

- OPT members exhibited a strong desire to share information. This finding was supported by the German Human Factors Analysis findings.
- OPT members were confused about the requirements for releasing information to mission partners. As a course of habit and due to this confusion, unclassified information is often withheld.
- Fear of reprimand or breaking legal barriers may significantly contribute to a "culture" of withholding information.

Recommendations:

- Staff use of the *Operational Guide for Unclassified Information Sharing (UIS)* to supplement reinforcement and training of command information management procedures to establish habit and behavior patterns.
- Commanders implement a pre-planned release matrix clearly defining review criteria for controlled unclassified information and distinguish between unclassified information having sensitivities defined by law and information "not for public release."
- Commanders implement guidance outlining review authorities for controlled unclassified information with clear definition of the roles and responsibilities of the Public Affairs Officer (PAO) and Foreign Disclosure Officer (FDO).
- Commanders and staffs use a pre-planned release matrix in training and exercises to encourage and develop a risk managed information sharing culture.

Note: During the Transition Conference, senior organizational representatives recommended OPT members tailor the release matrix to address the unique needs of the operational situation and release matrix authorities be documented in the Commanders' intent sections of the operations order and supporting organizations' planning documentation.

4.1.2. Unclassified Information Storage (1-1b)

This solution included processes and procedures for expedited release of controlled unclassified information in a crisis response situation. This solution element focused on information storage on an unclassified information sharing capability (UISC) and included associated business rules.

Findings:

- Non-military participants were more satisfied than military participants with their organization's information storage mechanisms, to include storage locations, management of the locations, and organization of the information.
- Military participants identified a lack of unclassified information storage for sharing with non-military partners.
- Military participants displayed inconsistent knowledge of command unclassified information storage locations.
- A need to selectively share stored information with a smaller sub-set of non-military partners.
- OPT members indicated that complex operations place a premium on tools with a more open approach to information storage and effective content organization.

Recommendations:

- DOD design and provide unclassified information storage sites that more closely resemble flatter and collaborative methods used by external partners.
- DOD ensure that information storage sites include a location for sharing information with a set of trusted partners.
- DOD consider that in the absence of a dedicated DOD information storage site, use of commercially available file sharing vehicles on the open internet as a potential means to accommodate users.

4.1.3. Business Rules for Manual Cross Domain Transfer (1-2)

This solution focused on business rules governing the expedited transfer of unclassified information from classified networks to non-classified networks, primarily via manual cross domain transfer processes. Due to security policy constraints at the site, this solution was not formally evaluated in the Analytic Seminar.

Findings:

- Many military organizations conduct day-to-day operations on classified networks, even when the information is unclassified or non-classified in nature.
- Participant survey responses during site visits and the Analytic Seminar indicated current processes are time consuming and can range from hours to weeks, depending on FDO work

flow priorities. A significant variance was noted among experiment participants when discussing administrative ownership of the cross domain transfer process.

- Participants moderately agreed the draft *Operational Guide for Unclassified Information Sharing* manual cross domain transfer procedure offered a method for accelerating the movement of information to unclassified networks while minimizing risk.

Recommendations:

- Staff use of the *Operational Guide for Unclassified Information Sharing* to supplement training and reinforcement of command information management procedures to establish habit and behavior patterns.
- Commanders implement centralized and standardized cross domain transfer policy and procedures, with training for reviewers.
- Commanders provide guidance encouraging the maximum use of unclassified networks in the conduct of unclassified work to improve information sharing.
- The DOD Unclassified Information Sharing Enterprise continue with further examination in determining specific methods for information sharing involving cross domain transfer.

4.1.4. Guide to Enable Information Sharing with Mission Partners via the Unclassified Information Sharing Capability (1-5)

This solution focused on the processes and procedures to effectively share information and collaborate with non-military mission partners (e.g., U.S. interagency, HN, multinational/coalition partners, IGOs and NGOs) as well as non-DOD staff and liaison personnel. Although similar in some degree to solution 1-8, this solution focused on the "how" of sharing information with partners.

Findings:

- During the experiment, participants saw the need for a guide to address the span of mission partners, type of information to be shared, and the rationale for sharing.
- During the Analytic Seminar, participants noted the importance of military organizations establishing relationships among prospective mission partners, especially during theater engagement and shaping (i.e., Phase 0) activities, in order to set conditions for collaboration and information sharing.
- Planning styles differ between the military and its non-military partners. While the military tends to organize and interact hierarchically and focus internally during the initial stages of planning, non-military organizations generally approach the problem through outreach.

- Leveraging the early engagement of non-military partners was seen as an important step for effective and efficient use of military planning time and resources.

Recommendations and best practices:

- Staff use of the *Operational Guide for Unclassified Information Sharing (UIS)* to supplement reinforcement and training of command information management procedures to establish habit and behavior patterns.
- Commanders implement and staff use of a mission partners guide that includes comprehensive partner organization descriptions, and a section that addresses DOD restrictions to information sharing, including access to non military websites.
- Commanders provide guidance to establish and develop relationships recognizing organizational differences in planning styles, the need to accommodate preferences for engagement timing and seek common partner goals and objectives.
- Commanders implement military training to include organizational differences in planning styles, preferences in engagement timing, and reinforcement of the importance of collaboration and reciprocation in information sharing.

4.1.5. Information Management and Knowledge Management Business Rules for Unclassified Information Sharing (1-7)

This solution involved staff procedures and best practices focusing on information management and knowledge management (IM/KM) business rules while working with partners in non-DOD collaboration environments.

Findings:

- Consistent application and constant reinforcement of information management plans are paramount.
- Each organization in the experimental audience had some form of information management plan.
- Using mission partner information sharing venues and tools may improve effective collaboration.
- Overuse and misuse of military jargon complicates even the most basic communications between partners.

Recommendations:

- Staff use of the *Operational Guide for Unclassified Information Sharing (UIS)* to supplement reinforcement and training of command information management procedures to establish habit and behavior patterns.
- DOD and Commanders establish policies to ensure access to and encourage use of mission partner information sharing venues.
- Commanders implement military training focusing on underlying organizational cultures in order to improve collaboration and information sharing.

4.1.6. Quick-Reference Guide to Potential Non-DOD Mission Partners (1-8)

This solution involves quick reference guides for the roles, responsibilities and general information requirements of potential non-DOD mission partners (e.g., U.S. interagency, HN, IGOs, NGOs). Although similar in some degree to Solution 1-5, this solution focused on detailed descriptions of non-military organizational roles, responsibilities and information requirements. During the experiment, perspectives on the "who, what, why, when, and where" of effective information sharing with external partners included the discussion of information exchange requirements.

Findings:

- Participants saw the need for a guide to address the span of mission partners, type of information to be shared, and the rationale for sharing.
- During the experiment, participants viewed the quality of current command reference material on potential mission partners as needing improvement,
- The Quick Reference Guide was viewed as an improvement that requires additional refinement.
- A Quick Reference Guide would serve to reduce the risk associated with high turnover on military staffs and the loss of corporate memory for partnering in particular mission areas, i.e., humanitarian assistance and disaster relief.

Recommendations:

- Commanders implement and staff use of a mission partners guide (electronically searchable) that includes comprehensive partner organization descriptions.
- Commanders implement a feedback and review process to maintain currency.

- Although not sufficiently explored during the Analytic Seminar, an information exchange requirement matrix is worthy of further study as a potential mechanism for integrating into the larger DOD Architectural Framework.

4.2. Materiel Solutions

The IMISAS project team explored ten materiel solutions (Table 2) during the technical spirals and Analytic Seminar.

Table 2 – IMISAS Project Materiel Solutions

Solution		Elements	
***1-3**	Pre-defined template and business rules for the establishment of UISC work sites	**1-3a**	UISC work site template • UISC collaboration tools (e.g., wikis, blogs and widgets)
		1-3b	Business rules to support UISC work site • Portal establishment • Work site management
3-1	Business Rules to define data types, standards, metadata requirements that facilitate posting, transfer and use of data	• Standardized metatags • Business rules to standardize the tagging of documents, blogs, and forums	
4-1	UISC to make automatic bandwidth recommendations in a restricted communications environment	• Redirect mobile or low bandwidth device users to site with limited rich content • Develop appropriate business rules and procedures	
4-6	Graduated user account permissions and procedures for anticipated and unanticipated users to facilitate allocating access to different levels of unclassified information based on trust	• Emulate a granular permission structure from within APAN • Develop business rules and procedures	
4-7	A rapid user registration system with the capability and capacity to support expansion of the UISC COI in crisis response	• Scaled down UISC registration process to limit the use of personally identifiable information (PII)	
4-8	UIS capability to push or post aggregated data from dynamic sources to mission partners	• UISC to push and receive really simple syndication (RSS) feed • Business rules and procedures for the tagging of RSS feed data • Social media, hotlines, news	
4-9	UIS capability to capture, sort, categorize, filter information in the public domain	• Business rules for data tagging to support filtering and categorizing public domain data that is brought into UISC	

Table 2 – IMISAS Project Materiel Solutions		
Solution		**Elements**
4-10	Business rules to maximize current automatic trust center capability including: rating, recommendations, and level of confidence	• APAN "Star" rating system • Telligent "points" system potential use • Business rules
4-11	Source authenticity and information reliability capability for UISC use in filtering and verification of real-time data from channels such as Twitter, short message service (SMS), e-mail and RSS feeds	• Source authenticity and information reliability capability (e.g., SwiftRiver) • Business rules and a set of protocols for determining the source authenticity and information reliability
4-12	UIS search capabilities (federated or integrated)	• Currently APAN has capability to search blogs, wikis, forums • Use of filters (e.g., Ifilter) to search Office 2003/2007 products and PDF files within the media gallery(if functional) • Standardized metatags

***** Note – Solution 1-3 is both a materiel and non-materiel related.

4.2.1. Work Site Template (1-3a)

This broad solution focused on defined templates and business rules for the establishment of work sites on unclassified information sharing capability platform. This solution element identified collaboration tools (e.g., wikis, blogs and widgets) and other key features that should be included in any unclassified information sharing capability (UISC) work site. While the format of the template used during the experiment was specific to APAN, the content recommendations are applicable to other information sharing portals.

Note: Throughout the course of the IMISAS project, the term "Unclassified Information Sharing Capability" (UISC) was used to describe the future DOD information sharing platform and service. In September 2011, DOD CIO and DISA officially adopted the term "Unclassified Information Sharing Service" (UISS). All previously documented references to the UISC in this report would refer to what is now termed the UISS.

Findings:

- The capability package demonstrated by APAN generated widely mixed responses with respect to usefulness and applicability in crisis response situations. The Human Factors Analysis corroborated this finding.
- APAN provided somewhat easy access to information although there were some instances of system latencies.
- Potentially large volumes of information and requests for information during crisis response operations dictated the need for dedicated KM support.

- UISC tools used most frequently used throughout the experiment periods were request for information (RFI)/request for assistance (RFA) forum, media galleries, and ACO.
- Document posting and collaboration functions were easy to use and useful in a crisis response environment, but additional capabilities are necessary to make them more useful to the operators.
- The chat capability was regularly used. Criticisms of the chat utilities were related to the user interface.
- Participants recognized the positive value of mapping capabilities such as MapView and GeoCommons.
- A "learning curve" is associated with any suite of centralized and integrated collaborative tools.
- The experiment audience used e-mail on a regular basis as a method for unclassified information sharing among mission partners.

Recommendations:

- The UISC/UISS must include:
  - A stable platform with a simplified user interface, optimized for speed.
  - A continued development process for an integrated template of multimedia collaboration tools to serve the needs of both military and non-military partners.
  - Ability to send alerts to users who subscribe to automated information feeds.
  - Tool definitions and descriptions that eliminate military specific terminology.
  - Provision for robust KM support to include active moderation of user roles and inputs.
  - A web-based collaboration venue (such as ACO™) that accommodates active moderation using rules of order.
  - A dedicated question and answer (RFI or "query") tool with the following features:
    - Filterable
    - Grouping by topic and easily searchable
    - Capable of organizing and linking RFIs
  - A forum tool allowing multiple instantiations for segregating discussion areas.
  - A file management capability with the following features:
    - A multi-tiered folder structure for the storage of data or files
    - A user friendly means to upload files
    - Version control with the capability to check-out, revert, and compare previous versions in history
    - Drag and drop functionality
    - A simple sort, search, and retrieval utility
    - Support for simple standard tagging and naming conventions

- A means of designating a single source point for authoritative documents (with links to other areas if required)

- A document collaboration capability enabling simultaneous, multi-user contributions with the following features:
  - Version control
  - History comparison
  - Moderation (as required)
  - Draft document work area and publish control capability
  - Publish capability
  - Graduated access
  - Subscription/alerts when content is updated/changed
  - Rich text editor with spell check
- An extensible markup and presence protocol (XMPP) chat capability with the following features:
  - Ability to run a chat process independently of the active UISC window
  - Automatic logging, archiving, and exporting of chat for historical use
  - Automatic alerts to annunciate when other participants are away, idle, and active
  - Automatic alerts for users of new messages via a visual and/or audible cue
  - Notification of user's "log-on" status
  - Ability to converse with an entire group or privately with an individual
  - Ability to create and use multiple chat rooms
  - Ability to restrict access to different chat rooms
- A robust, easy to use mapping utility with the following features:
  - Ability to pull and push data among other sites in a variety of formats (e.g., Keyhole Markup Language (KML), Really Simple Syndication (RSS), Geographic RSS (GeoRSS), Web Map Service (WMS))
  - Ability to activate and deactivate layers, change base maps, modify zoom levels, drill down into map elements, and attach time, date, imagery and video to map elements
  - Ability to sequence content in time
  - Compatible with current ".mil" security requirements
- Policies, processes and procedures to enable crisis responders to access resources on the open internet by facilitating the following:
  - A relaxed security environment
  - The capability to install required applications and browser plug-ins used to work with partners
  - Provision of commercial-off-the-shelf clients and commercial internet as an alternative to configurable clients and connectivity via the NIPRNet

  - Training interfaces to accelerate user familiarity.
- The UISC/UISS does not need an embedded e-mail capability, but must have the ability to send out e-mail alerts to users who subscribe to a UISC feed.
- Commanders implement procedures to limit "point-to-point" e-mails and encourage posting information to locations that are searchable by and available to the larger community.
- DOD CIO and JS J8 create a configuration management governance body to:
  - Maintain configuration management of the UISC/UISS tools and capabilities
  - Develop a continuous, feedback-based program of user training on provided tools
  - Implement business rules
  - Charter a user / operating system group forum
  - Establish enterprise control to include future planning and an international consortium or steering group

4.2.2. Business Rules for UISC Work Site (1-3b)

This solution involved business rules for the implementation and use of the unclassified information sharing site template. During the Analytic Seminar, participants primarily used the business rules when posting requests for information (RFIs).

Findings:

- The magnitude of the information management challenge quickly became apparent as experiment play progressed and emphasized the need for business rules to use the UISC tool suite.
- The business rules for use of the UISC require updating or adaption to meet the needs of each operation.

Recommendation:

- The UISC/UISS must include business rules:
  - Adaptable for the range of operations
  - Reinforced through training
  - That address the adjudication, managing or moderating of site transactions
  - Standardized naming conventions and other processes
  - That are continually reviewed to ensure both the warfighter and the mission partners' benefit from the information and collaboration practices on the UISC

4.2.3. Business Rules for Data and Metadata Standards and Tags (3-1)

This solution proposed business rules to define data types, standards, and metadata requirements facilitating posting, transfer and use of data (e.g., documents, blogs, and forums) through standardized content tags and search capabilities.

Finding:

- Accurate and standardized tagging of information is of great importance to those researching information as a method of categorizing data and arranging thematically related materiel.

Recommendations:

- The UISC/UISS must employ a tagging process to enable different organizations to locate information hosted at partner sites.
- The UISC/UISS must employ a robust tagging mechanism for all content, based upon a standard tag library, configurable at the group or site level at a minimum, and automatically available to every module or capability.
- Commanders provide military training focused on standardized tagging practices.

4.2.4. Accommodating Disadvantaged Users (4-1)

This solution focused on the disadvantaged (low bandwidth / technology) users, by making automatic bandwidth recommendations in a restricted communications environment and redirecting mobile or low bandwidth device users to a site with limited rich content.[18] This solution was evaluated only during the technical spirals.

Findings:

- Participants found the disadvantaged and low bandwidth site easy to access for posting information.
- Response time was adequate and users generally felt comfortable using the site, despite some concerns with limited functionality.
- The system worked well with multiple mobile platforms.

[18] "Limited Rich Content" can be defined as a subset of online information that contains text and non-text information (graphics, audio, video and animation) that has been taken from a larger, more comprehensive site and bounded to accommodate user bandwidth and technology limitations.

- The current capability does not support site searching and the ability to join a new group.

Recommendations:

- The UISC/UISS must include a disadvantaged, limited rich content user site, with:
  - The capability of searching and joining new groups/sites of interest
  - The capability to work with the latest internet browsers and client operating systems
  - SMS / MMS messaging capability
  - Continual site review for optimized speed and user experience

4.2.5. Graduated User Accounts (4-6)

This solution involved graduated user account permissions and procedures to facilitate allocating access to different levels of unclassified information based on trust. All users initially had "read-only" access to the site and after being granted full-site membership, participants were able to post information as well.

Finding:

- The experimental audience cited the need for a "fenced" area to allow limited access for work on documents in preparatory stages of development.

Recommendation:

- The UISC/UISS must have a graduated user access capability.

4.2.6. Rapid User Account Registration (4-7)

This solution explored a revised, rapid user registration system during one technical spiral with the capability and capacity to support expansion of the UISC COI in crisis response situations. This capability was identified during the early stages of the project and a revised registration system was put in place and tested during a technical spiral.

Finding:

- The user account registration was straightforward, asked appropriate questions requisite to access, and required minimal information.

Recommendation:

- The UISC/UISS must have streamlined registration.

4.2.7. Pushing and Posting Data from Dynamic Sources (4-8)

This solution involved the capability to push or post aggregated data from dynamic sources such as Facebook and Twitter to mission partners, using business rules and procedures for pushing content to social media sources.

Findings:

- The experimental audience stated clear benefits to pushing information to social media sites, particularly as part of the humanitarian assistance and disaster relief scenario.
- Some concerns about posting of information to social media sites, including the potential:
  - To confuse the public over DOD's role in crisis
  - For misinterpretation of information causing friction with mission partners.

Recommendations:

- The UISC/UISS must have the capability and associated procedures to push and post information to external social media sites in real-time.
- Commands and organizations use standardized, common disclaimers as a means for message shaping.

4.2.8. Capturing, Sorting, and Categorizing Information (4-9)

This solution involved the capability to capture, sort, categorize, and filter information in the public domain from social media sources.

Findings:

- Participants noted the potential utility of social media information sources.
- The current presentation of social media information does not support developing mission analysis and planning.
- There are currently no mechanisms to assess the validity of the information presented.
- Raw data from social media can help focus initial inquiries in order to gain verifiable information.

Recommendation:

- The UISC/UISS requires the capability to:
  - Subscribe, filter and present social media feeds
  - Generate alert notifications when external content is posted

- Improve confidence in social media information sources. Refer to Section 4.2.10 (Source Authenticity and Reliability).

4.2.9. Business Rules for Automatic Trust Center Capability (4-10)

This solution involved business rules to maximize an automatic trust center capability (e.g., rating, and a level of confidence).

Findings:

- The "star" rating capability available on the existing APAN platform was easy to use but was not universally trusted for attaining source reliability and trustworthiness.
- Participants found source attribution was the most accepted reliability mechanism for generating confidence level ratings.

Recommendation:

- The UISC/UISS requires a content rating capability that provides descriptions of how ratings are obtained, the number of ratings applied to content, and visibility into the profiles of content raters.

4.2.10. Source Authenticity and Reliability Rating (4-11)

This solution involved source authenticity, including a reliable information capability for the UISC to use in filtering and the verification of real-time social networking data. The source identification solution was not fully examined due to limited access to the "SwiftRiver" tool.

Finding:

- Data was collected for other technical solutions referencing the need for a source reliability mechanism.

Recommendation:

- Although the source reliability and verification system concept is promising, further research is needed in this area.

4.2.11. UISC Search Capabilities (4-12)

This solution involved searching across all UISC tools to include content and standard tags searches.

Findings:

- No single search capability may be able to satisfy the requirements of an OPT or other organizations.
- Guidelines, business rules and training could enhance the use of the search capability.
- The search capability was found to be easy to use during the technical spiral but was problematic during the Analytic Seminar.

Recommendations:

- The UISC/UISS requires a robust search capability that is capable of fixed, exact, approximate, and partial logic queries.

5. Solutions to Product - Transition

The overall transition strategy focused on solutions that hold the potential for improvements to existing capabilities and concepts. The primary transition pathway would use informal processes described in the *Manual for Joint Concept Development and Experimentation (CJCSM 3010.02)* to effect changes in the areas of doctrine, training, materiel, leadership and education, and policy. Although the project focused on operational requirements for the warfighter challenge sponsors, USEUCOM and USAFRICOM, the products are intended to inform the joint force as a whole.

The potential solutions identified and evaluated through experimentation and described in Section 4 of this report are incorporated in the below listed project products.

Operational Guide for Unclassified Information Sharing (Annex M)**.** This pre-doctrinal document provides fundamental guidance, planning considerations, techniques and procedures for implementing an effective, information sharing environment during military operations in support of a wide variety of civilian and other non-DOD partners, regardless of the particular mission.

During the Transition Conference, participants supported Joint Staff publication of the *Operational Guide for Unclassified Information Sharing* and its continued use and refinement during exercises and other training events. Participants supported the publication and broad distribution of the *Guide* as a potential catalyst for formal doctrine development activities.

A Joint Knowledge On-Line (JKO) course was developed based on the *Guide.* The course title is "J3OP-US1108 Operational Guide for Unclassified Information Sharing" and it was released in January 2012.

Unclassified Information Sharing (UIS) Architecture Products **(**Annex N)**.** DOD Architecture Framework (DODAF) views identify the architecture and provide general information describing the scope, purpose and perspective. The documents also identify the tools and file formats used

for the architecture description, including representative views. The UIS "as-is" architecture provides the context for the architecture in the 2011 time frame. The UIS "to-be" architecture provides general information describing the scope, purpose and perspective while providing the context for the architecture through the 2015 time frame.

During the Transition Conference, participants approved using the architecture products to inform the development of a DOD unclassified information sharing enterprise. In October 2011, the architecture products were provided to DISA and DOD CIO for that purpose. The architecture products have also been provided to the Joint Staff J8, Deputy Director for Command, Control, Communications, Computers (DDC4), Combat Capability Developer Division to inform efforts in developing the Future Mission Network (FMN).

White Paper on Unclassified Information Sharing (UIS) (Annex O)**.** This document describes an anticipated environment informing a vision for unclassified information sharing among mission partners and participant organizations. The document will serve to generate effective discourse, collectively explore tomorrow's "realm of the possible," and provide a conceptual foundation for subsequent capability development activities and joint experimentation.

During the Transition Conference, participants supported broad distribution of the document as a potential catalyst for formal concept development activities. This document has been released for distribution among the Community of Interest.

Materiel Recommendations. While materiel solutions were not the primary focus of this project, APAN (as proxy for a DOD unclassified information sharing platform) was used extensively for training, collaboration, conference facilitation, preparation for and in the execution of the Analytic Seminar. Through usage over a nine-month period, the project team and participants identified recommended changes to enhance the existing APAN platform. Experimentation and analysis activities provided recommendations for the DOD "to-be" unclassified information sharing service. Joint Requirement Oversight Council Memorandum (JROCM) 109-11 tasked DISA to study and provide recommendations to the Command, Control, Communications/ Cyberspace (C4/Cyber) Functional Control Board (FCB) based on the findings from the IMISAS project. JROCM 109-11 tasks DOD Chief Information Office to study the findings and recommendations from the project to inform Program Objective Management (POM) 14 submissions. Recommended capabilities for the future UISS are outlined in Section 4.2.1 through 4.2.11 of this report. Those recommendations specific to the existing APAN platform were also summarized and provided to the APAN development team under separate cover.

6. Conclusion

The IMISAS project explored the current unclassified information sharing environment to include existing policies, processes, procedures, local authorities and business rules, and available tools at several COCOMs. Through analysis of capability gaps, potential solutions were conceived, and developed to enable improve interorganizational information sharing and collaboration and then evaluated during experimentation. The APAN tool was used as a proxy for DOD's unclassified information sharing capability throughout the experiment. Through analysis of the experiment results, recommendations for changes in the areas of doctrine, training, materiel, leadership and education, and policy were developed.

Many of the procedures and recommendations from this project can be implemented now and will have immediate impact on improving unclassified information sharing between DOD and non-DOD partners. It is well recognized that inter-organizational information sharing is a highly complex issue; this effort should be seen as a positive step in providing immediate capability enhancement and informing the ongoing work on other contributing issues.

Aligning potentially conflicting aspects of technology, policy, processes, procedures, and organizational cultures may prove to be the largest challenge in developing DOD's future information sharing capabilities. The speed of technology predicates more frequent review of policies guiding use of this technology. Another challenge will be achieving balance between the "need to share" imperative and the "need to protect" information, but this balance can be addressed through active risk management. Current information sharing capabilities remain underutilized due to local policies, internal staff procedures, and the need for additional training and education in Interorganizational engagement. Further exploration of the cultural aspects of information sharing will likely yield the greatest return on investment. The proposed recommendations from Section 4, particularly the non-materiel solutions of Section 4.1, offer straightforward first steps to help the joint force adjust to the realities of the increasingly growing unclassified information sharing environment.

The IMISAS project provided a foundation for addressing the larger information sharing challenge expressed in the initial problem statement. The findings and products from the project will be used to inform the DOD Unclassified Information Sharing Service. The DISA brief to the C4 Cyber FCB on 3 November 2011 incorporated the recommendations found in this report. DOD CIO and JS J8 to have further acted on an IMISAS project recommendation to create a configuration management governance body and are co-hosting an Unclassified Information Sharing Governance Working Group in late November 2011.

In the near term, solutions identified can be implemented immediately, used in training and other joint force development events and activities.

(THIS PAGE INTENTIONALLY BLANK)

Annex A – Acronyms

Annex B – Terms and Definitions

Annex C – References

Annex D – Experimentation Plan

Annex E – Baseline Assessment Report (BAR)

Annex F – After Action Reports

Annex G – Analytic Framework

Annex H – Data Collection and Analysis Plan (DCAP) – Technical Sprials

Annex I - Data Collection and Analysis Plan (DCAP) – Analytic Seminar (AS)

Annex J – Final Project Analysis

Annex K – Bundeswehr Transformation Centre (BTC) Final Report

Annex L – IMISAS Project Transition Plan

Annex M – Operational Guide for Unclassified Information Sharing

Annex N – Unclassified Information Sharing (UIS) Architectural Products

Annex O – White Paper on Unclassified Information Sharing (UIS)

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions Project
(IMISAS)

Annex A - Acronyms

AC10	Austere Challenge 2010 (exercise)
ACO	Adobe® Connect™ online
ACT	Allied Command Transformation
ALN	Adaptive Logistics Network
AMB	ambassador
APAN	All Partners Access Network (formerly Asia-Pacific Area Network)
APEX	Adaptive Planning and Execution
ATL	acquisition, technology and logistics
AV	all viewpoint
BAR	baseline assessment report
BICES	Battlefield Information, Collection and Exploitation System
BP	building partnerships
BTC	Bundeswehr Transformation Centre
C2	command and control
C4	command, control, communications and computers
C4I	command, control, communications, computers and intelligence
CAP	crisis action planning
CARE	Cooperative for Assistance and Relief Everywhere
CARS	Collaborative Alert and Respond System
CCDD	combat capability developer division
CCDR	combatant commander
CCJO	Capstone Concept for Joint Operations
CCOE	CIMIC Center of Excellence
CDC	cross domain cell
CDCIE	Cross Domain Collaborative Information Environment
CD&E	concept development and experimentation
CDP	capability development package

CFBL	Combined Federated Battle Labs
CFD	Canadian First Defense
CIE	collaborative information environment
CIFC	Civil Information Fusion Concept
CIL	critical information list
CIM	civil information management
CIMIC	civil-military cooperation
CIO	chief information officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJOS	combined joint operations from the sea
CMOC	civil-military operations center
COA	course of action
COCOM	combatant command
COE	center of excellence
COI	community of interest
CONOPS	concept of operations
COOP	continuity of operations
COP	common operational picture
CPM	capability portfolio manager
C-PORTS	Coalition Portal for Situational Awareness
CPX	command post exercise
CRS	Catholic Relief Services
CS	civil support
CUI	controlled unclassified information
CWID	Coalition Warfighter Interoperability Demonstration
CWIP	Coalition Warrior Information Portal
DAA	designated approving authority
DART	disaster assistance response team (USAID)

DCAP	data collection and analysis plan
DCHA	Bureau for Democracy, Conflict, and Humanitarian Assistance (USAID)
DCO	Defense Connect Online
DCR	DOTMLPF-P change recommendation
DD	deputy director
DECC	Defense Enterprise Computing Center
DEU	Deutschland (Federal Republic of Germany)
DG	director general
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DIL	disconnected, interrupted, and low-bandwidth
DISA	Defense Information Systems Agency
DMS	Defense Message System
DNI	Director of National Intelligence
DNS	domain name services
DOC	Department of Commerce
DOD	Department of Defense
DODAF	Department of Defense Architecture Framework
DOS	Department of State
DOTMLPF-P	doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy
DPS	data processing system
DR	disaster relief
DSCA	Defense Support of Civil Authorities
DTRA	Defense Threat Reduction Agency
EA	executive agent
ECA	Economic Commission for Africa (UN)
ECHO	European Community Humanitarian Office

ED	event directive
EEA	essential elements of analysis
EMD	experiment manning document
ESB	enterprise service bus
EuroControl	European Organisation for the Safety of Air Navigation
EWTGLANT	Expeditionary Warfare Training Group, Atlantic
FAO	Food and Agriculture Organization (UN)
FCB	functional capability board
FDO	foreign disclosure officer
FHA	foreign humanitarian assistance
FLO	foreign liaison officer
FOIA	Freedom of Information Act
FOUO	for official use only
FPC	final planning conference
FY	fiscal year
GAO	Government Accountability Office
GCC	geographic combatant commander
GeoRSS	geographic really simple syndication
GES	Global Information Grid Enterprise Services
GIG	Global Information Grid
GIS	geospatial information systems
G-TSCMIS	Global Theater Security Cooperation Management Information System
HA	humanitarian assistance
HD	homeland defense
HN	host nation
HIC	humanitarian information center

HITL	human-in-the-loop
HIU	humanitarian information unit (DOS)
HOC	humanitarian operations center
HQ	headquarters
HSIN	Homeland Security Information Network
HSPD	homeland security Presidential directive
HTTP	hypertext transfer protocol
IA	interagency
IAP	information assurance platform
IA SSA	Interagency Shared Situational Awareness
IATO	interim authority to operate
ICD	initial capabilities document
ICRC	International Committee of the Red Cross
ICT	information and communications technology
IDA	Institute for Defense Analysis
IEAT	Information Exchange Architecture and Technology
IER	information exchange requirement
IFRC	International Federation of Red Cross and Red Crescent Societies
IGO	intergovernmental organization
IID	interoperability and integration division
IO	international organization
IM	information management
IMISAS	Interagency and Multinational Information Sharing Architecture and Solutions
IMP	information management plan
InterAction	The American Council for Voluntary International Action
IOC	initial operational capability
IP	internet protocol
IPC	initial planning conference

IPR	in-process review
IRIN	Integrated Regional Information Networks (UN)
ISAF	International Security Assistance Force
ISIP	Information Sharing Implementation Plan (DOD)
ISR	intelligence, surveillance and reconnaissance
IT	information technology
JAPCC	Joint Air Power Competence Center
JCA	joint capability area
JCD&E	joint concept development and experimentation
J-CIM	Joint-Civil Information Management
JCTD	joint capability technology demonstration
JCW	Joint and Coalition Warfighting
JFC	joint force commander
JFEC	Joint Faculty Education Conference
JIMDA	Joint Integration of Maritime Domain Awareness
JKO	Joint Knowledge Online
JOC	joint operating concept, joint operations center
JOT	JCW Observation Tool
JP	joint publication
JROCM	Joint Requirements Oversight Council Memorandum
JS	The Joint Staff
JS J6	Communications System Directorate of a Joint Staff; Command, Control, Communications, and Computer Systems Staff Section
JTF	joint task force
KM	knowledge management
KM L	keyhole markup language

KSA	knowledge, skills and abilities
LAN	local area network
LMR	land mobile radios
LNO	liaison officer
LOE	limited objective experiment
MDA	maritime domain awareness
MEU	Marine expeditionary unit
MINUSTAH	United Nations Stabilization Mission in Haiti
MMS	multimedia messaging service
MN	multinational
MNCC	multinational forces coordination center
MNE	multinational experiment
MNF	multinational forces
MNIS	Multinational Information Sharing
MNMP	Multinational and other Mission Partners
MPAT	multinational planning augmentation team
MPC	mid-planning conference
MRX	mission rehearsal exercise
MSEL	master scenario events list
MSF	Médecins Sans Frontières (Doctors Without Borders)
NATO	North Atlantic Treaty Organization
NECC	Net-Enabled Command Capability
NEIC	National Earthquake Information Center
NEPAD	New Partnership for Africa's Development
NGDC	National Geophysical Data Center
NGA	National Geospatial-Intelligence Agency

NGO	non-governmental organization
NII	networks and information integration
NIPRNet	Non-secure Internet Protocol Router Network
NJOIC	National Joint Operations Intelligence Center
NMCC	National Military Command Center
NOAA	National Oceanographic and Atmospheric Administration
NOFORN	not releasable to foreign nationals
NORAD	North American Aerospace Defense Command
NR	Noble Resolve (exercise)
NSPD	national security Presidential directive
NTCI	nontraditional community of interest
OBMEP	Officer Professional Military Education Policy
OFDA	Office of U.S. Foreign Disaster Assistance (USAID)
OMA	Office of Military Affairs
OPCON	operational control
OPORD	operation order
OPSEC	operations security
OPT	Operational Planning Team
OSAA	Office of the Special Adviser on Africa
OSD	Office of the Secretary of Defense
OV	operational viewpoint
Oxfam	Oxford Committee for Famine Relief
PAO	public affairs officer
POA&M	Plan of Actions and Milestones
PBO	post-bureaucratic organization
PBWS	performance based work statement
PCCIP	President's Commission on Critical Infrastructure

PDE	process documentation event
pdf	portable document format
PEI	partnership and emerging issues
PII	personally identifiable information
PIV	personal identity verification
PKI	public key infrastructure
PME	professional military education
POM	program objective memorandum
POTUS	President of the United States
POW	program of work
PRM	Bureau of Population, Resources and Migration (DOS)
PRT	provincial reconstruction team
PSI™	Portable Systems Interconnect™
PSO	private sector organization
PVO	private voluntary organization
PWC	Pacific Warfighting Center
QDR	quadrennial defense review
QoS	quality of service
QRC	quick reaction capability
RDA	regional domain awareness
RFA	request for assistance
RFI	request for information
ROI	return on investment
RSS	really simple syndication
SA	situational awareness
SBU	sensitive but unclassified

SDW	solutions development workshop
SecDef	Secretary of Defense
SHAPE	Supreme Headquarters Allied Powers Europe
SHIFT	Shared Information Framework and Technology
SIP	Service Improvement Plan
SIPRNET	SECRET Internet Protocol Router Network
SITREP	situation report
SLA	service level agreement
SLM	service level management
SME	subject matter expert
SMS	short message service
SMTP	simple mail transfer protocol
SNS	social network site
SOA	services oriented architecture
SOO	statement of objectives
SOP	standard operating procedure
SPAWAR	Space and Naval Warfare Systems Command
SSL	secure sockets layer
SSTR	stability, security, transition and reconstruction
SV	systems viewpoint
SvcV	services viewpoint
TCO	total cost of ownership
TISC	Transnational Information Sharing Cooperation
TLS	transport layer security
TRADOC	Training and Development Command
TRANSLI™	Translation of Information™
TSC	theater security cooperation
TTP	tactics, techniques, and procedures

TV	technical standards viewpoints
UDOP	user defined operational picture
UIS	unclassified information sharing
UISC	unclassified information sharing capability
UJTL	Universal Joint Task List
UN	United Nations
UNDAC	United Nations disaster assessment and coordination
UNDHA	United Nations Department of Humanitarian Affairs
UNDP	United Nations development programme
UNHCR	United Nations Office of the High Commissioner for Refugees
UNICEF	United Nations Children's Fund
UNOCHA	United Nations Office for the Coordination of Humanitarian Affairs
UNODIR	unless otherwise directed
USA	United States Army
USAF	United States Air Force
USAFRICOM	United States Africa Command
USAID	United States Agency for International Development
USCENTCOM	United States Central Command
USEUCOM	United States European Command
USFOR-A	United States Forces Afghanistan
USG	United States Government
USIP	United States Institute for Peace
USJFCOM	United States Joint Forces Command
USMC	United State Marine Corps
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
USSOCOM	United States Special Operations Command
USSOUTHCOM	United States Southern Command

VICOM	virtual intercom system
VoIP	voice over internet protocol
WFC	warfighter challenge
WFP	World Food Programme (UN)
WHO	World Health Organization (UN)
WJTSC	Worldwide Joint Training and Scheduling Conference
X24	Exercise 24
XML	extensible markup language
XMPP	extensible markup and presence protocol

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions Project

(IMISAS)

Annex B – Terms and Definitions

agility: The synergistic combination of robustness, resilience, responsiveness, flexibility, innovation, and adaptation. (Source: Alberts, David S. and Hayes, Richard E. *Code of Best Practice Experimentation*. Third Printing. Washington, DC: CCRP, 2005. See www.dodccrp.org)

alliance: The relationship that results from a formal agreement between two or more nations for broad, long-term objectives that further the common interests of the members. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

assumption: A statement related to the study that is taken as true in the absence of facts, often to accommodate a limitation. (Source: Department of the Army, FM 101-5, *Staff Organization and Operations*, 31 May 1997)

blog: A blog (a blend of the term web log) is a type of website or part of a website. Blogs are usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video. Entries are commonly displayed in reverse-chronological order. Blog can also be used as a verb, meaning to maintain or add content to a blog. (Source: Wikipedia)

capability: The ability to achieve a desired effect under specified standards and conditions through combinations of means. (Source: Adapted from definitions provided in Department of the Army, FM 101-5, *Staff Organization and Operations*, 31 May 1997, and Department of the Army/ U.S. Marine Corps Headquarters, FM 101-5-1/MCRP 5-2A, *Operational Terms and Graphics*, 30 September 1997)

capacity: The combination of all the strengths, attributes and resources available within a community, society or organization that can be used to achieve agreed goals. Capacity may include infrastructure and physical means, institutions, societal coping abilities, as well as human knowledge, skills and collective attributes such as social relationships, leadership and management. Capacity also may be described as capability. (Source: United Nations International Strategy for Disaster Reduction (UNISDR), *2009 UNISDR Terminology on Risk Reduction*, May 2009.)

capability gap: The inability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks. The gap may be the result of no existing capability, lack of proficiency or sufficiency in an existing capability, or the need to replace an existing capability. (Source: Adapted from definitions provided in Department of the Army, FM 101-5, Staff Organization and Operations, 31 May 1997, and Department of the Army/ U.S. Marine Corps Headquarters, FM 101-5-1/MCRP 5-2A, Operational Terms and Graphics, 30 September 1997)

civil-military operations center: An organization normally comprised of civil affairs, established to plan and facilitate coordination of activities of the Armed Forces of the United

States with indigenous populations and institutions, the private sector, intergovernmental organizations, non-governmental organizations, multinational forces, and other governmental agencies in support of the joint force commander. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

coalition: An arrangement between two or more nations for common action. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

collaboration: Collaboration can be described as a process where organizations work together to attain common goals by sharing knowledge, learning, and building consensus. (Source: Joint Publication 3-08, Interorganizational Coordination During Joint Operations, 24 Jun 11.)

collaborative information environment (CIE): The virtual aggregation of people and organizations, infrastructure, and policy and procedures to create and share the data, information, and knowledge needed to plan, execute, and assess operations and to enable a commander to make decisions better and faster than the adversary. (Source: U.S. Joint Staff, J-3, Unclassified Information Sharing Capability (UISC) Concept of Operations, 15 November 2010.)

combatant command: A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

combatant commander: A commander of one of the unified or specified combatant commands established by the President. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

community of interest: COIs is the inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange. (Source: DOD CIO, Department of Defense Net-Centric Data Strategy, 9 May 2003.)

conceptual model: A graphical representation of the phenomenon that is being studied; assists in visualizing the requirements for the experimentation environment. (Source: Alberts, David S. and Hayes, Richard E. *Code of Best Practice Experimentation*. Third Printing. Washington, DC: CCRP, 2005.)

constraint: A restriction imposed by the study sponsor that limits the study team's options in conducting the study. (Source: U.S. Army Training and Doctrine Command (TRADOC) Analysis Center, *The TRADOC Analysis Center's Definitions for Analysts*, May 2005.)

crowd sourcing: Crowd Sourcing is a term that has has been used recently with businesses, authors, and journalists as shorthand for the trend of leveraging the mass collaboration enabled by Web 2.0 technologies to achieve business goals. (Source: Wikipedia)

Department of Defense Architecture Framework (DODAF): The DODAF defines a set of products that act as mechanisms for visualizing, understanding, and assimilating the broad scope and complexities of an architecture description through graphic, tabular, or textual means. These products are organized under the following views; each viewpoint depicts certain perspectives of the architecture.

- Overarching All Viewpoint (AV)
- Operational Viewpoint (OV)
- Services Viewpoint (SvcV)
- Systems Viewpoint (SV)
- Technical Standards Viewpoint (TV)

(Source: DOD CIO, Department of Defense Architecture Framework (DODAF) Version 2.0, Manager's Guide, 28 May 2009)

disaster: A serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope using its own resources. Disasters are often described as a result of the combination of: the exposure to a hazard; the conditions of vulnerability that are present; and insufficient capacity or measures to reduce or cope with the potential negative consequences. Disaster impacts may include loss of life, injury, disease and other negative effects on human physical, mental and social well-being, together with damage to property, destruction of assets, loss of services, social and economic disruption and environmental degradation. (Source: United Nations International Strategy for Disaster Reduction (UNISDR), 2009 UNISDR Terminology on Risk Reduction, May 2009.)

disaster assistance response team: A team of specialists, trained in a variety of disaster relief skills, rapidly deployed to assist U.S. embassies and United States Agency for International Development missions with the management of U.S. Government response to disasters. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

extended enterprise: All internal and external participants required to ensure mission success. Extended enterprise includes Federal, State, local, tribal, coalition partners, foreign governments and security forces, international organizations, non-governmental organizations, and the private sector. (Source: Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, *Department of Defense Information Sharing Implementation Plan*, April 2009.)

federation: The process of associating separated organizational servers into one operational domain. (Source: U.S. Joint Staff, J-3, Unclassified Information Sharing Capability (UISC) Concept of Operations, 15 November 2010.)

foreign humanitarian assistance: Department of Defense activities, normally in support of the United States Agency for International Development or Department of State, conducted outside the United States, its territories, and possessions to relieve or reduce human suffering, disease, hunger, or privation. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

group administrator: Technical facilitator who enables through basic access control the ability of individuals to interact through specific media, potentially crossing many boundaries (geographical, national, political, economic, social, financial, and linguistic, etc.) in order to pursue mutual interests or goals. (Source: U.S. Joint Staff, J-3, Unclassified Information Sharing Capability (UISC) Concept of Operations, 15 November 2010.)

group owner: Administrative lead of a group of individuals who interact through specific media, potentially crossing many boundaries (geographical, national, political, economic, social, financial, and linguistic, etc.) in order to pursue mutual interests or goals. (Source: U.S. Joint Staff, J-3, Unclassified Information Sharing Capability (UISC) Concept of Operations, 15 November 2010.)

high-level operational concept graphic: High level graphical and textual description of an operational concept (high level organizations, missions, geographic configuration, connectivity, etc). The DODAF defines a set of products that act as mechanisms for visualizing, understanding, and assimilating the broad scope and complexities of an architecture description through graphic, tabular, or textual means. These products are organized under four views: overarching all view (AV), operational view (OV), systems view, and the technical standards view. Each view depicts certain perspectives of an architecture.

host nation: A nation which receives the forces and/or supplies of allied nations and/or NATO organizations to be located on, to operate in, or to transit through its territory. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

humanitarian assistance coordination center: A temporary center established by a geographic combatant commander to assist with interagency coordination and planning. A humanitarian assistance coordination center operates during the early planning and coordination stages of foreign humanitarian assistance operations by providing the link between the geographic combatant commander and other United States Government agencies, non-governmental organizations, and international and regional organizations at the strategic level. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

humanitarian operations center: An international and interagency body that coordinates the overall relief strategy and unity of effort among all participants in a large foreign humanitarian assistance operation. It normally is established under the direction of the government of the affected country or the United Nations, or a U.S. Government agency during a U.S. unilateral operation. Because the humanitarian operations center operates at the national level, it will normally consist of senior representatives from the affected country, assisting countries, the United Nations, non-governmental organizations, intergovernmental organizations, and other major organizations involved in the operation. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

interagency: Of or pertaining to United States Government agencies and departments, including the Department of Defense. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

information environment: The aggregate of individuals, organizations, and systems that collect, process disseminate, or act on information. (Source: U.S. Joint Staff, J-3, Unclassified Information Sharing Capability (UISC) Concept of Operations, 15 November 2010.)

information sharing: Making information available to participants (people, processes, or systems). Information sharing includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant. (Source: Department of Defense Information Sharing Executive, Office of the Chief Information Officer, Department of Defense Information Sharing Strategy, 4 May 2007.)

intergovernmental organization: An organization created by a formal agreement between two or more governments on a global, regional, or functional basis to protect and promote national interests shared by member states. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

joint capability area: Collection of "like" DOD capabilities functionally grouped to support capability analysis, strategy development, investment decision making, capability portfolio management, and capabilities-based force development and operational planning. (Source Chairman Joint Chiefs of Staff Manual (CJCSM) 3010.02, Manual for Joint Concept Development and Experimentation, 25 June 2010.)

joint concept: Links strategic guidance to the development and employment of future joint force capabilities and serve as "engines for transformation" that may ultimately lead to doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) and policy changes. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

joint force commander: A general term applied to a combatant commander, sub-unified commander, or joint task force commander authorized to exercise combatant command

(command authority) or operational control over a joint force. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

joint task force: A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a sub-unified commander, or an existing joint task force commander. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

limitation: An inability of the study team to fully meet the study objectives or fully investigate the study issues. (Source: Adapted from definitions provided in Department of the Army, FM 101-5, Staff Organization and Operations, 31 May 1997, and Department of the Army/ U.S. Marine Corps Headquarters, FM 101-5-1/MCRP 5-2A, Operational Terms and Graphics, 30 September 1997)

master scenario event list: A chronological timeline of expected actions and scripted events that controllers inject into exercise (or experiment) conduct to generate or prompt participant activity. It ensures that necessary events happen so that all objectives are met. Each MSEL record contains a designated scenario time; an event synopsis; the name of the controller responsible for delivering the MSEL record; and, if applicable, special delivery instructions, the task and objective to be demonstrated, the expected action, the intended player, and a note-taking section. (Sources: DOD Instruction 3020.47, DOD Participation in the National Exercise Program (NEP), January 29, 2009. The Technical Cooperation Program, *Guide for Understanding and Implementing Defense Experimentation (GUIDEx)*, ver. 1.1, February 2006.

mission partners: External partners as defined in the DOD Information Sharing Strategy: Federal, State, local, tribal, coalition partners, foreign governments and security forces, international organizations, non-governmental organizations, and the private sector. (Source: Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, Department of Defense Information Sharing Implementation Plan, April 2009.)

multinational coordination center: A multinational coordination center that facilitates coordination and cooperation of foreign military forces with the affected nation to support humanitarian assistance and disaster relief (HA/DR) missions. (Source: U.S. Pacific Command, Multinational Force Standard Operating Procedure, HA/DR Mission Extract, ver. 2.5, January 2010.)

non-governmental organization: A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging the establishment of democratic institutions and civil society. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

operational viewpoint: The operational viewpoint (OV) captures the organizations, tasks, or activities performed, and information that must be exchanged between them to accomplish DOD missions. It conveys the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges. (Source: DOD CIO, Department of Defense Architecture Framework (DODAF) Version 2.0, Manager's Guide, 28 May 2009)

operations security (OPSEC): A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities including:

- Identifying those actions that can be observed by adversary intelligence systems.
- Determining indicators that hostile adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical intelligence information in time to be useful to adversaries.
- Selecting and executing measures that eliminate or reduce, to an acceptable level, the vulnerabilities of friendly actions to adversary exploitation.

(Source: U.S. Joint Staff, J-3, Unclassified Information Sharing Capability (UISC) Concept of Operations, 15 November 2010.)

organizational culture: what a group learns over a period of time as that group solves its problems of survival in an external environment and its problems of internal integration. (Source: Schein, Edgar H. *Organizational Culture & Leadership*, Oct 1997)

portal: A portion of an asynchronous collaborative environment which provides web-based, single point of access to a variety of information and application tools. (Source: U.S. Joint Staff, J-3, Unclassified Information Sharing Capability (UISC) Concept of Operations, 15 November 2010.)

peace operations: A broad term that encompasses multiagency and multinational crisis response and limited contingency operations involving all instruments of national power with military missions to contain conflict, redress the peace, and shape the environment to support reconciliation and rebuilding and facilitate the transition to legitimate governance. Peace operations include peacekeeping, peace enforcement, peacemaking, peace building, and conflict prevention efforts. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

private sector: An umbrella term that may be applied in the United States and in foreign countries to any or all of the nonpublic or commercial individuals and businesses specified nonprofit organizations, most of academia and other scholastic institutions, and selected non-governmental organizations. (Source: Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.)

services viewpoint: The services viewpoint (SvcV) captures system, service, and interconnection functionality providing for, or supporting, operational activities. DOD processes include warfighting, business, intelligence, and infrastructure functions. The SvcV functions and service resources and components may be linked to the architectural data in the OV. These system functions and service resources support the operational activities and facilitate the exchange of information. (Source: DOD CIO, Department of Defense Architecture Framework (DODAF) Version 2.0, Manager's Guide, 28 May 2009)

social network sites (SNSs): Collaborative networked environments such as MySpace, Facebook, LinkedIn that have attracted millions of users, many of whom have integrated these sites into their daily practices. There are thousands of SNSs, with various capabilities and attributes, supporting a wide range of interests and practices. While their key technological features are fairly consistent, the cultures that emerge around SNSs are varied. Most sites support the maintenance of pre-existing social networks, but others help strangers connect based on shared interests, views, activities, goals and objectives. (Source: U.S. Joint Staff, J-3, Unclassified Information Sharing Capability (UISC) Concept of Operations, 15 November 2010.)

sponsoring agency: The U.S. Government entity that has responsibility for area where the UISC is being implemented. This organization may provide the group administrator and/or technical support for UISC users/groups. (Source: U.S. Joint Staff, J-3, Unclassified Information Sharing Capability (UISC) Concept of Operations, 15 November 2010.)

stakeholder participant organizations: NGOs and members of the public and private sectors involved with the same community of interest (COI) or issue who would reject affiliation as a DOD mission partner. (Proposed new term)

systems viewpoint: systems viewpoint (SV) captures the information on supporting automated systems, interconnectivity, and other systems functionality in support of operating activities. (Source: DOD CIO, Department of Defense Architecture Framework (DODAF) Version 2.0, Manager's Guide, 28 May 2009)

unclassified information sharing capability (UISC): A "community of communities" capability that combines the benefits of unstructured collaboration (wikis, blogs, forums) and structured collaboration (file sharing, calendar) with the personalization of social networking to facilitate unclassified information sharing with multinational partners, non-governmental organizations, and among various U.S. Federal and State agencies. (Source: U.S. Joint Staff, J-3, Unclassified Information Sharing Capability (UISC) Concept of Operations, 15 November 2010.)

value network: Any web of relationships that generates both tangible and intangible value through complex dynamic exchanges between two or more individuals, groups or organizations. Any of these engaged in both tangible and intangible exchanges can be viewed as a value network, whether private industry, government or public sector. The nodes in a value network

may represent people (or roles), groups or organizations. The nodes are connected by interactions that represent tangible and intangible deliverables. Intangible deliverables may take forms such as; information, knowledge, or awareness and tangibles may be in forms such as; financial value, goods, or services. (Source: U.S. Joint Staff, J-3, Unclassified Information Sharing Capability (UISC) Concept of Operations, 15 November 2010.)

virtual collaboration: The use of communications and computer technology to enable dispersed individuals and organizations to interactively work together on similar goals or shared interests. This capability is enabled within a collaborative information environment by the use of high-speed telecommunications networks and a common suite of enterprise multimedia planning, conferencing, and assessment tools. (Source: U.S. Joint Staff, J-3, Unclassified Information Sharing Capability (UISC) Concept of Operations, 15 November 2010.)

virtual community: A social network of individuals who interact through specific media, potentially crossing many boundaries (geographical, national, political, economic, social, financial, and linguistic, etc.) in order to pursue mutual interests or goals. One of the most pervasive types of virtual communities includes social networking sites, which consist of various online communities. Virtual communities are used for a variety of social and professional groups. (Source: U.S. Joint Staff, J-3, Unclassified Information Sharing Capability (UISC) Concept of Operations, 15 November 2010.)

warfighter challenge (WFC): An expression of a joint experimentation requirement articulated as a joint force problem to be considered for examination through JCD&E. WFCs are normally submitted by the Combatant Commands and Services annually via the Comprehensive Joint Assessment (CJA). (Source: Chairman Joint Chiefs of Staff Manual (CJCSM) 3010.02, Manual for Joint Concept Development and Experimentation, 25 June 2010.)

Web 2.0: A concept based on the participants' abilities to exploit emergent group-forming behaviors and collaborate with others online in a web-scalable environment. (Source: U.S. Joint Staff, J-3, Unclassified Information Sharing Capability (UISC) Concept of Operations, 15 November 2010.)

widget: In computer programming, a widget (or control) is an element of a graphical user interface (GUI) that displays an information arrangement changeable by the user, such as a window or a text box. The defining characteristic of a widget is to provide a single interaction point for the direct manipulation of a given kind of data. In other words, widgets are basic visual building blocks which, combined in an application, hold all the data processed by the application and the available interactions on this data. (Source: Wikipedia)

wiki: A wiki is a website that allows the creation and editing of any number of interlinked web pages via a web browser using a simplified markup language or a WYSIWYG text editor. Wikis are typically powered by wiki software and are often used collaboratively by multiple users. Examples include community websites, corporate intranets, knowledge management systems, and note services. (Source: Wikipedia)

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions Project

(IMISAS)

Annex C – References

Annex C – References

Aall, Pamela: Miltenberger, Lt. Col. Daniel; Weiss, Thomas G: Guide to IGOs, NGOs and the Military in Peace and Relief Operations. United States Institute for Peace, Washington, DC. 2000.

Alberts, David S. and Richard E. Hayes. *Code of Best Practice for Experimentation*, DOD Command and Control Research Program, 2002.

Alberts, David S., John J. Garstka, Richard E. Hayes, and David T. Signori. *Understanding Information Age Warfare*. Washington, DC: CCRP, 2001.

Alberts, David S., Reiner K. Huber, and James Moffat. *NATO Network Enabled Capability (NEC) Command and Control (C2) Maturity Model*, Command and Control Research Program, Jan 2010.

All Partners Access Network (APAN) - Information System Security Framework. United States Pacific Command. 2010.

All Partner Access Network (APAN) Specs. (n.d.).

APAN Capablities. United States Pacific Command. 2010.

APANv4 Overview HADR. United States Pacific Command. 2009.

APANv4 Overview VCJS. United States Pacific Command. 2009.

Arias, R. Beyond Command and Control: USSOUTHCOM'S Use of Social Networking to "Connect and Collaborate". *Air Land Sea Bulletin*, January 2000.

Ariely, D. G. Operational Knowledge Management As an International Interagency Interoperability Vehicle. *2009 NATO Information Systems and Technology Panel (IST) Symposium*, 2009.

Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Department of Defense Regulation 5200.1-R; Information Security Program, January 14, 1997.

Assistant Secretary of Defense for Networks and Information Integration, DOD Memorandum. DoD Enterprise Services Designation, Collaboration, Content Discovery, and Content Delivery. Feb 02, 2009.

Bain, B., Beizer, D., Weigelt, M., & Lipowicz, A. *Agencies harness social media for Haiti relief efforts.* Retrieved November 21, 2010, from Federal Computer Week: http://fcw.com/articles/2010/01/14/social-media-haiti-earthquake-relief.aspx

Brundidge, G. L. *Unclassified/ Non-Classified Information Sharing*. June 4, 2010.

Burke, H. *Enabling COIs with Open Technology Development (COTD).* SPAWAR. 2008.

CARE USA, Milkah Kihunah. (2003, Sep). "Non-Governmental Organizations (NGOs) in Development and Relief Settings".

Center for Law and Military Operations; *U.S. Government Interagency Complex Contingency Operations Organizational and Legal Handbook*. The Judge Advocate General's Legal Center and School, United States Army. Charlottesville, Virginia (24 February 2004)

Chairman Joint Chiefs of Staff Instruction (CJCSI) 1800.01D, Officer Professional Military Education Policy (OBMEP), 15 July 2009.

Chairman Joint Chiefs of Staff Instruction (CJCSI) 3010.02C, Joint Concept Development and Experimentation (JCD&E), 25 June 2010.

Chairman Joint Chiefs of Staff Instruction (CJCSI) 6212.01E. Interoperability and Supportability of Information Technology and National Security Systems. December 15, 2008.

Chairman Joint Chiefs of Staff Instruction (CJCSI) 6285.01B, Multinational Information Sharing (MNIS) Operational Systems Requirements Management Process, 13 Sep 2010.

Chairman Joint Chiefs of Staff Manual (CJCSM) 3010.02, Manual for Joint Concept Development and Experimentation, 25 June 2010.

Chairman Joint Chiefs of Staff Notice 3500.01, 2011-2014 Chairmans Joint Training Guidiance, December 3, 2010.

Charter for Command and Control Profolio Data and Services Steering Commitee. ver. 3.1, December 10, 2008.

Chlebo, Paul, Gerard J. Christman, and Roy A. Johnson. *Enhancing Collective C2 in the International Environment: Leveraging the Unclassified Information Sharing Enterprise Service.* Paper presented at 16th International Command and Control Research and Technology Symposium: Collective C2 in Multinational Civil-Military Operations, Quebec City, Canada: 21-23 June 2011.

Clarke, C. Case Study: Haiti: Revisiting a Relief Contingency, October 14, 2010.

Coalition Warrior Interoperability Demonstration Joint Management Office. October 2010.

Collaboration in the National Security Arena: *Myths and Reality -- What Science and Experience can Contribute to its Success, Strategic Multi-layer Assessment (SMA) Multi-agency/Multi-disciplinary White Papers in Support of Counter-Terrorism and Counter-WMD*, Jun 09.

Communities of Interest (COI). 2009.

Congress, U. (2010). *"Interagency National Security Professional Education, Administration, and Development System Act of 2010 (INSPEAD System Act of 2010)"*.

Contract SOW N00189-09-D-Z046-0004. (n.d.).

Contract SOW N00189-10-Q-2499-0001. (n.d.).

Cooperative Implementation Planning, Management and Evaluation (CIP/CIME) Major Integrating Event. April 2008.

Council, E. *Joint Concept Development and Experimentation (JCD&E)*. August 25, 2010.

CWID 2010 Final Report Assessment Briefs Booklet. Hampton, VA, USA: Coalition Warrior Interoperability Demonstration Joint Management Office.

Data Strategy for Command and Control Capabilities Update. *JROCM 110-10*. July 06, 2010.

Defense Information Systems Agency (DISA), C.-T. *Transnational Information Sharing Cooperation (TISC) Joint Capability Technology Demonstration (JCTD) (Brief)*, May 05, 2010.

Defense Information Systems Agency (DISA). *Transnational Information Sharing Cooperation (TISC) Joint Capablity Technology Demonstration (JCTD)*. DISA CTO T02. 2010.

Defense Security Cooperation Agency (DSCA). *Humanitarianand Civic Assistance (HCA) Program*. December 2006.

Department of Defense Chief Information Officer, *Department of Defense Architecture Framework (DODAF) Version 2.0, Manager's Guide*, 28 May 2009

Department of Defense Chief Information Officer, *Department of Defense Net-Centric Data Strategy*, 9 May 2003.

Department of Defense (DoD) Enterprise Unclassified Information Sharing Service. 2010.

Department of Defense Information Sharing Executive, Office of the Chief Information Officer, *Department of Defense Information Sharing Strategy*, 4 May 2007.

Department of Defense Directive 3000.07, Irregular Warfare. December 1, 2008.

Department of Defense Directive 5205.2, DOD Operations Security Program, March 6, 2006.

Department of Defense Directive 5230.09; Clearance of DOD Information for Public Release, August 22, 2008

Department of Defense Directive 5230.11; Disclosure of Classified Military Information to Foreign Governments and International Organizations, June 16, 1992.

Department of Defense Instruction 2205.02. Humanitarian And Civic Assistance (HCA) Activities. December 12, 2008.

Department of Defense Instruction 2205.3. Implementing Procedures for the Humanitarian and Civic Assistance (HCA). January 27, 1995.

Department of Defense Instruction 2205.05, Humanitarian and Civic Assistance (HCA) Activities, Dec 02, 2008.

Department of Defense Instruction 3000.05, Stability Operations, September 16, 2009.

Department of Defense Instruction 3020.47, DOD Participation in the National Exercise Program (NEP), January 29, 2009.

Department of Defense Instruction 5200.01, incorporating Change 1: DOD Information Security Program and Protection of Sensitive Compartmented Information, June 13, 2011.

Department of Defense Instruction 5230.29, Security and Policy Review of DOD Information for Public Release, January 8, 2009.

Department of Defense Instruction 6000.15. Joint Medical Executive Skills Development Program. April 19, 1999.

Department of Defense Instruction 8110.01, Multinational and Other Mission Partner (MNMP) Information-Sharing Capability Framework, 9 Jun 2010.

Department of Defense Instruction 8220.02, Information and Communications Technology (ICT) Capability for Support of Stabilization and Reconstruction, Disaster Relief, and Humanitarian and Civic Assistance Operations, 30 Apr 2009.

Department of Defense Instruction 8510.01. DoD Information Assurance Certification and Accreditation Process (DIACAP). November 28, 2007.

Department of State. (n.d.). *Leadership at State*. Retrieved November 5, 2010, from U.S. Department of State: http://www.state.gov/m/irm/ediplomacy/c23841.htm.Department of the Army, FM 101-5, Staff Organization and Operations, 31 May 1997

Department of the Army/U.S. Marine Corps Headquarters, FM 101-5-1/MCRP 5-2A, Operational Terms and Graphics, 30 September 1997

Department of the Navy Chief Information Officer. *Department of the Navy Knowledge Management Strategy*. 2005.

Deputy Secretary of Defense Directive-Type Memorandum 09-026, *Responsible and Effective Use of Internet-based Capabilities*, February 25, 2010.

Endorserment of All Partners Access Network. July 20, 2010.

1st Marine Expeditionary Force (n.d.). 1MEF Case Study.

Fletcher, B. *Cross Domain Collaborative Information Environment (CDCIE) : Collaboration Tool Overview.* USJFCOM & SPAWAR. 2007.

Grey, C. and Garsten, C. (2000). Trust, Control and Post-Bureaucracy. *Organization Studies*, 22(1), 229-250.

Haimes, Yacov Y; Kaplan, Stan; and Lambert, James H., *Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling*. Society for Risk Analysis; McLean, Virginia. Risk Analysis, Volume 22, No. 2, and (2002)

Hall, T., & Giles, J. *All Partner Access Network (APAN) - Service Scope.* PACOM, 2010.

Hanchard, D. *Haiti: High- and Low-Tech Disaster Reflief.* ZDNET, 2010.

HarmonieWeb - Info Brief v4. United States Joint Forces Command.

Heckscher, C. (1994). Defining the Post-Bureaucratic Type. *In The Post-Bureaucratic Organization*, Charles Heckscher and Anne Donnellon (Eds.). Thousand Oaks, CA: Sage, 14-62.

Hodge, N. *Wired*. January 20, 2010. Retrieved November 21, 2010, from http://www.wired.com/dangerroom/2010/01/disaster-relief-20-haitis-virtual-surge/

Homeland Security Exercise and Evaluation Program (HSEEP), Vol II, *Exercise Planning and Conduct*, February 2007.

Information Exchange Architecture and Technology Concept in the MNE5 environment. September 30, 2008.

Infostate of Africa 2009. Appfrica Labs, 2009.

Institute for Defense Analysis (IDA). *A Snapshot of Emerging U.S. Government Civilian Capabilities to Support Foreign Reconstruction and Stabilization Contingencies*. August 2006.

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Planning Package Summary, 2010.

Interagency Shared Situational Awareness Guide (IA SSA). (n.d.)

IT/Knowledge Management Officer wanted at Save The Children. (n.d.). Retrieved November 5, 2010, from Gblcareers: Global Careers and Job Vacancies: http://gblcareers.com/2010/10/itknowledge-management-officer-wanted-at-save-the-children.html

Jain, Abby. (2004). *Using the Lens of Max Weber's Theory of Bureaucracy to Examine E-Government Research*. Paper presented at 37th Hawaii International Conference on System Sciences.

Jerauld, J.G., CAPT. FY-11 Warfighter Challenge 1: Multi-National and Inter-Agency Information Sharing. February 17, 2010.

Joint Chiefs of Staff J-6 Memorandum for Acting Assistant Secretary of Defense for Networks and Information Integration. *Department of Defense (DOD) Enterprise Unclassified Information Sharing Service*, 10 August 2010.

Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010, as amended through 15 Aug 2011.

Joint Publication 3-0, Joint Operations, 11 Aug 2011.

Joint Publication 3-06, Joint Urban Operations, 08 November 2009.

Joint Publication 3-08, Interorganizational Coordination During Joint Operations, 24 June 11.

Joint Publication 3-16, Multinational Operations, 07 March 2007.

Joint Publication 3-29, Foreign Humanitarian Assistance, 17 March 2009.

Joint Technology Assessment Activity, *Transnational Information Sharing Cooperation Joint Capability Technology Demonstration Integrated Assessment Plan*, Revision 2, Oct 2009.

Jumper, C. Cursor on Target . *CoT Narrative, 2002.*

Keen, P. K., Maj Gen, USEUCOM Chief of Staff. Preface remarks to *Collaboration in the National Security Arena: Myths and Reality -- What Science and Experience can Contribute to its Success*, Strategic Multi-layer Assessment (SMA) Multi-agency/Multi-disciplinary White Papers in Support of Counter-Terrorism and Counter-WMD, Jun 09.

Kiernan, Kathleen, and Carl Hunt. *The Law Enforcement Perspective in U.S. Interagency Collaboration: Leveraging the Whole of Government Approach*, in Collaboration in the National Security Arena: Myths and Reality -- What Science and Experience can Contribute to its Success, Strategic Multi-layer Assessment (SMA) Multi-agency/Multi-disciplinary White Papers in Support of Counter-Terrorism and Counter-WMD, Jun 09.

King, Dennis. *The Haiti Earthquake: Breaking New Ground in the Humanitarian Information Landscape*. Humanitarian Exchange Magazine, October 2010.

Knowles, D. *Twitter Message Sparks Big Rescue Effort.* Retrieved November 21, 2010, from AOL News: http://www.aolnews.com/tech/article/twitter-message-sparks-big-rescue-effort-in-haiti/19337648, January 10, 2010.

Kuusisto, R. *"SHIFT" THEORETICALLY PRACTICALLY Modivated Framework*. 2009.

Lake, Anthony; Whitman, Christine Todd; et al, *More than Humanitarianism; A strategic U.S. Approach Toward Africa*. Council on Foreign Relations, Independent Task Force Report No. 56. New York (2006)

Leadership, J. S. *DoD Net-Centric Data Strategy (DS) and Community of Interest (COI) Training*. October 27, 2008.

Li, F. (2003). Implementing e-Government Strategy in Scotland: Current Situation and Emerging Issues. *Journal of Electronic Commerce in Organizations* (1:2), 44-65.

Lindenmayer, Martin J. *Civil Information and Intelligence Fusion: Making "Non-Traditional" into "New Traditional" for the JTF Commander*. Small Wars Journal, 22 June 2011.

Marahrens, Soenke, Lt Col, (n.d.). *Aspects of Military Command and Control for the 21st Century*.

Marche, S., and McNiven, J. (2003). *E-government and E-governance: the future isn't what it used to be*, Canadian Journal of Administrative Sciences (20:1), 74-86.

McNabb, M. Case Study: Haiti: Revisiting a Relief Contingency. *13-14 October 2010 Office of the Director of National Intelligence Partner Engagement Conference* . Washington, DC: Office of the Director of National Intelligence. October 14, 2010.

Merton, R.K. (1957). *Social Theory and Social Structure*. New York: Free Press, 1957.

MicroLink. *HarmonieWeb - A Case Study*. MicroLink, LLC. 2009.

MicroLink, Mr. Todd Neff. *HARMONIEWeb: A Collaboration Portal for U.S. Joint Forces Command that Supports Humanitarian Assistance and Disaster Relief*. 2008.

Mills, James H., CDR, Net-Centric Security Pilot Proposed Way Ahead. April 4, 2008.

MNE-5 Major Integrating Event 2010. (n.d.).

NATO Network Enabled Capability Interaction Maturity. (n.d.).

NGO Global Network. (n.d.). Retrieved February 06,2011,from http://www.ngo.org/ngoinfo/define.html:2011

Office of the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, *Department of Defense Information Sharing Implementation Plan*, April 2009.

Office of the Director of National Intelligence Partner Engagement Conference . Washington, D.C. Office of the Director of National Intelligence, 13-14 October 2010.

Office of the Under Secretary of Defense for Intelligence, Mr. Kevin West. *Defense Intelligence Information Enterprise - Enabling Mission Powered Partnerships*, September2010.

Office of the Under Secretary of Defense for Policy, Global-Theater Security Cooperation Management Information System (G-TSCMIS) Roadmap, Version 1.0 (Pre-decisional draft). March 5, 2009.

Parker, Katrina. *Situational awareness experiment prepares for real world crises*. USJFCOM Public Affairs news release, 29 July 2009, retrieved from http://www.jfcom.mil/newslink/storyarchive/2009/pa072909.html.

Paulsen, J. E. *Joint Training Directorate/Joint Warfighting Center (J7/JWFC*, September 7, 2010. Retrieved November 21, 2010, from USJFCOM Portal: https://us.jfcom.mil/sites/J7/Ops/JTD/ac11/Preparation%20Material/RE%20AC%2010%20Lessons%20Learned%20VTC.txt

Perito, Robert M. (Ed.); *Guide for Participants in Peace, Stability and Relief Operations*. United States Institute for Peace, Washington, DC (2007)

Pierce, D. Pentagon's Social Network Becomes Hub for Haiti Relief, January 21, 2010. Retrieved Nov 21, 2010, from Wired: http://www.wired.com/dangerroom/2010/01/pentagons-social-network-becomes-hub-for-haiti-relief/

President of the United States. Executive Order 13556 "Controlled Unclassified Information". November 4, 2010.

Raduege, C., GIG 2.0, Web 2.0 & Information Sharing: a Perspective from the Joint Staff, September 23, 2009. Retrieved November 18, 2010, from https://www.ncoic.org: https://www.ncoic.org/apps/group_public/download.php/13748/Raduege%20GIG%202%200%20and%20Web%202%200%20Keynote%20to%20NCOIC%2020090923.ppt

Reference Architecture for MNE5 technical system. May 30, 2007.

Referentia, Mr. Tim Williams. *Agile Coalition Environment (ACE) "Capability Gap Analysis" (Report).* Jan 27, 2010.

Ross, P., Joint C2 Data Strategy, March 6, 2009.

Schein, E. H. (1990). *Organizational culture*. American Psychologist, *45*(2), 110.

Schein, Edgar H. *Organizational Culture & Leadership*, Oct 1997

Schein, E. H. (1996). *Culture: The missing concept in organizational studies*. Administrative Sciences Quarterly, *41*(2), 229.

Schmitt, John F., *A Practical Guide for Developing and Writing Military Concepts. Defense Analysis Red Team (DART)*, Dec 2002.

Secretary of Defense Report, *Quadrennial Defense Review Report*, Feb 2010.

Secretary of the Army. *Army Knowledge Management Principles.* Washington, DC: Government Printing Office. 2008.

Selznik, P. (1980). *TVA and the Grass Roots: A Study of Politics and Organization*. Berkeley: University of California Press.

Shared Information Framework and Technology (SHIFT) Technical Solution for MNE 5. January 20, 2009.

SHIFT Handbook Shared Information Framework and Technology. February 2009.

(n.d.). *SHIFT Shared Information Framework and Technology Enabling focus area MNE5 High Level Overview Document*.

SHIFT Shared Information Framework and Technology Concept Ver 9, February 2009.

Smith, Kathryn, *All Partners Access Network (APAN) Support to the Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project Feedback.* Memorandum to USPACOM/J73, 19 September 2011.

Space & Naval Warfare Systems Command, Michele McGuire. *Agile Coalition Environment (ACE) "Freedom within a Framework"*. 2004.

Staff, V. C., Data Strategy for Command and Control Capabilites. July 6, 2010.

The Technical Cooperation Program, *Guide for Understanding and Implementing Defense Experimentation (GUIDEx)*, Version 1.1, March 2006.

United Nations International Strategy for Disaster Reduction (UNISDR), *2009 UNISDR Terminology on Risk Reduction*, May 2009.

U.S. Agency for International Development (USAID). *Civilian – Military Cooperation Policy*, Jul 28, 2008.

U.S. Agency for International Development (USAID), *Economic Growth, Agriculture & Trade (EGAT)*; Bureau Primer. Washington, DC (2007)

U.S. Agency for International Development (USAID). *USAID Haiti Earthquake Web Page*, October 1, 2010. Retrieved November 21, 2010, from http://www.usaid.gov/helphaiti/

U.S. Agency for International Development (USAID), Bureau for Democracy, Conflict and Humanitarian Assistance (DCHA), Office of U.S. Foreign Disaster Assistance (OFDA) *Guidance for Disaster Planning and Response- FY 2011*.

U.S. Army Test and Evaluation Command Quick Reaction Test, Foreign Humanitarian Assistance/Disaster Relief, *DOD Support to Foreign Disaster Relief Handbook for Joint Task Force Commander and Below,* version 4.0, 2010.

U.S. Army Training and Doctrine Command (TRADOC) Analysis Center, *The TRADOC Analysis Center's Definitions for Analysts*, May 2005.

U.S. Center for Research and Education on Strategy and Technology, *Multinational Experiment 5 (MNE 5),* December 2008. Retrieved November 28, 2010, from U.S. Center for Research and Education on Strategy and Technology (U.S. CREST): http://www.uscrest.org/files/mne5.pdf

U.S. Department of Defense *Quadrennial Report (QDR),* 2006.

USEUCOM/USSOUTHCOM TISC JCTD Integrated Management Team. *Transnational Information Sharing Cooperation (TISC) Joint Capability Technology Demonstration (JCTD): A Roadmap to an Operationally Validated.* Crane, Indiana: Joint Technology and Assessment Activity (JTAA), NSWC Crane, Code 606. 2009.

U.S. Government Accountability Office briefing, *Interagency Collaboration: Implications of a Common Alignment of World Regions among Select Federal Agencies*. 11 July 2011.

U.S. Government Accountability Office Report, *Interagency Collaboration: Key Issues for Congressional Oversight of National Security Strategies, Organizations, Workforce, and Information Sharing,* GAO-09-904SP (Washington, D.C.: Sept. 25, 2009).

U.S. Joint Chiefs of Staff, J36, *Unclassified Information Sharing Capability (UISC) Concept of Operations*, 15 November 2010.

U.S. Joint Chiefs of Staff, J8, DDC4 CCD, *Department Of Defense (DOD) Multinational And Other Mission Partners (MNMP) Information Sharing Capability (ISC) Concept of Operations*, Draft v. 1.8.

U.S. Joint Chiefs of Staff, Joint and Coalition Warfighting (JCW), *Handbook for Unclassified Information Sharing (UIS)*, 30 September 2011.

U.S. Joint Chiefs of Staff, Joint and Coalition Warfighting (JCW), *Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Analytic Wargame (AWG), Draft Data Collection and Analysis Plan (DCAP),* 16 May 2011, v1.5.

U.S. Joint Chiefs of Staff, Joint and Coalition Warfighting (JCW), *Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Technical Evaluations, Draft Data Collection and Analysis Plan (DCAP),* 01 July 2011, v1.3.

U.S. Joint Chiefs of Staff, Joint and Coalition Warfighting (JCW), *Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) End-to-End Experiment Plan (EP),* 20 September 2011, v 2.0.

U.S. Joint Chiefs of Staff, Joint and Coalition Warfighting (JCW), *Unclassified Information Sharing (UIS) Unofficial Joint Operating Concept (JOC)*, 19 September 2011, v 1.0.

U.S. Joint Forces Command, *Adaptive Logistics Network/Multinational Experiment 6, Objective 4.5*, Final Report, 29 April 2011.

U.S. Joint Forces Command, Cross Domain Collaborative Information Environment (CDCIE). 2007.

U.S. Joint Forces Command, *Cross Domain Collaborative Information Environment (CDCIE) - Joint Capability Technology Demostration (JCTD) CONOPS,* 2010.

U.S. Joint Forces Command, *Cross Domain Collaborative Information Environment (CDCIE) Joint CapabilityTechnology Demonstration (JCTD)FY08 (Rolling Start)-09, Transition FY10 Annual Review for DDRE (RFD).* 2007.

U.S. Joint Forces Command. *Cross Domain Collaborative Information Environment (CDCIE) - Joint Capability Technology Demostration (JCTD) : Management Transition Plan,* 2009.

U.S. Joint Forces Command, Guidelines for Conducting A Baseline Assessment, June 10, 2010.

U.S. Joint Forces Command, *HarmonieWeb - A Basic User Handbook v2.0,* 2009.

U.S. Joint Forces Command, Joint Futures Lab. Interagency Shared Situational Awareness (IA SSA) Guide. Sep 30, 2009.

U.S. Joint Forces Command, J9 Directorate. *Interagency Shared Situational Awareness (IA SSA) Project (Final Report).* September 28, 2009.

U.S. Joint Forces Command, J9 Directorate. Joint Distributed Operations (JDO) Limited Objective Experiment (LOE) – Human Factors Analysis (HFA). August 2010.

U.S. Joint Forces Command, *JCD&E Solution Transition Standard Operating Procedures (SOP)*, ver. 1, 24 February 2011.

U.S. Joint Forces Command, *Multinational Information Sharing (MNIS) Initial Capabilities Document (ICD) Version v1.0*, 18 September 2006.

U.S. Joint Forces Command, *Multinational and other Mission Partners (MNMP) C2 Information Sharing Capability Definition Package*, 12 October 2010.

U.S. Joint Forces Command, *Required Capablities for HarmonieWeb.* United States Joint Forces Command, 2007.

U.S. Joint Forces Command, *The Civil Information Fusion Concept of Operations*, 3 Jun 2011.

U.S. Pacific Command, *Asia Pacific Area Network (APAN) CONOPS*, June 2009.

U.S. Pacific Command, Multinational Force Standard Operating Procedure, HA/DR Mission Extract, ver. 2.5, January 2010.

U.S.Pacific Command, *Transnational Information Sharing Cooperation (TISC) Joint Capability Technology Demonstration (White Paper).* 2009.

U.S. Joint Forces Command, Joint Center for Operational Analysis; *Case Study: U.S. Southern Command and JTF-Haiti, Some Challenges and Considerations in Forming a Joint Task Force*, 24 June 2010.

U.S. Southern Command Science and Technology Office, *Transnational Information-Sharing Cooperation (TISC) Concept of Operations*, version 2.1.2, 10 Jun 2010.

U.S. Special Operations Command, Joint Civil Information Management Joint Test and Evaluation, *Tactics, Techniques and Procedures (TTP) Handbook for Civil Information Management (CIM)*, 2010.

Warfighter Challenges FY09 inputs for Joint Interagency and Multi-National Interoperability.

Weber, Max. (1968). *Economy and Society*. Roth, Guenther and Claus Wittich (Eds.). New York: Bedminister Press, 956-958.

Wiki. (n.d.). In Wikipedia. Retrieved September 29, 2011, from http://en.wikipedia.org/wiki/Wiki

Widget. (n.d.). In Wikipedia. Retrieved September 29, 2011, from http://en.wikipedia.org/wiki/GUI_widget

World Cares Center (2010). Designing an Inclusive Simulation Environment: Understanding the Landscape of Non-military Humanitarian Assistance and Disaster Relief Actors. New York, NY.

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions Project

(IMISAS)

Annex D – Experimentation Plan

Table of Contents

1.0 Background and Context D-3
1.1 Key Partners/Forces Involved D-4
1.2 Problem Statement D-5
1.3 Baseline Assessment Process D-6
1.4 Solution Development Process D-6
2.0 Outcomes, Objectives, Products, and Activities D-7
2.1 Outcome 1 ..... D-7
2.2 Outcome 2 ..... D-8
2.3 Campaign Plan and Experimentation Activities Schedule D-10
3.0 Experiment Environment and Procedures D-14
3.1 Design D-14
3.2 Control Function D-14
3.3 Scenario D-15
3.4 Security D-16
3.5 Experimentation Ethics Compliance D-16
4.0 Analysis and Data Collection D-16
5.0 Experiment Design Assessment D-17
6.0 Transition Planning D-23
References D-23

1.0 Background and Context

The IMISAS project's intent is to improve information sharing between the U.S. Department of Defense (DOD) and a wide variety of non-military mission partners, who may include civilian U.S. government agencies, other nations, inter-governmental organizations, and nongovernmental organizations.

In this last decade, we have recognized an increasing need for improved civil-military coordination and cooperation. The U.S. and the international community have witnessed and responded to human rights abuses, massive refugee movements and the endangerment and death of hundreds of thousands of civilians as a result of natural disasters, civil wars and major conflicts in countries like Somalia, the former Yugoslavia, Rwanda, Haiti, Iraq and Afghanistan.

Two quintessential events (9/11 and Katrina) within our own borders reinforced and highlighted the need for the enhanced information sharing with non-DOD mission partners. The extension of information sharing to a broader multinational context for a "Whole of Government" approach possesses even greater challenges.

Non-governmental organizations (NGOs) such as the International Federation of Red Cross and Red Crescent Societies, Doctors without Borders, CARE, OXFAM and church relief organizations have delivered vast amounts of emergency humanitarian assistance, medical supplies, water purification equipment and shelters during humanitarian assistance/disaster relief (HA/DR) operations. Although NGOs have sometimes worked together with militaries in the past, the extremely harsh environments now faced by humanitarian missions in often lawless frontiers have argued for new working relationships. One touch point which has gained some traction is in the arena of information sharing.

Information sharing is not without difficulties. The challenges are formidable and include:

- The "political will" of participants and organizations
- Organizational culture differences
- International organization and NGO neutrality and independence sensitivities
- Conflicts and shortfalls in policy, doctrine, tactics, techniques and procedures
- Security restrictions, necessity of integrating ad hoc stove-piped capabilities; language differences
- Cultural and social situation awareness
- Complex and large data problem sets
- Information management and assurance requirements
- Unifying architecture and concept of operations

- Network and spectrum management, organizational authority and resources
- Building trust and a shared understanding of expectations

The 2006 Quadrennial Defense Review (QDR) called upon the Department of Defense (DOD) to broadly improve "information sharing with other agencies and with international allies and partners" and develop a strategy that guides "operations with Federal, State, local and coalition partners." Responding to the QDR, on May 4, 2007 the DOD Chief Information Officer signed the DOD Information Sharing Strategy and in April 2009 promulgated the DOD Information Sharing Implementation Plan which established a set of near-term tasks to position DOD to progress toward implementation of the broader Strategy.

It is within this overall context that the IMISAS Project is chartered. Specifically, IMISAS seeks to identify the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) solutions providing the Commander, U.S. Africa Command (USAFRICOM) and the Commander, U.S. European Command (USEUCOM) the ability to effectively collaborate with a range of mission partners in order to synchronize potential U.S. DOD contributions in a supported or supporting role across the operational aspect of potential missions. The changes in DOTMLPF-P shall lead to an operating concept and methods to enable information sharing, collaboration and transactions between interagency (IA) groups, multinational partners, international sovereign partners and organizations (IOs), NGOs, and private partners. In order to reduce redundancies and inefficiencies of any potential U.S. DOD contribution, IMISAS will identify solutions to overcome restrictive policies, and reduce the effect of or eliminate conflicting authorities in a supporting or supported role.

The IMISAS project was reviewed and approved as part of the FY 10/11 Joint Experimentation Program of Work (PoW) by the Joint Experimentation Executive Council representing primary stakeholders from USEUCOM, USAFRICOM, U.S. Joint Forces Command (USJFCOM) Joint Concept Development and Experimentation (JCD&E) J9 in consensus with the broader JCD&E Enterprise. This EP is designed to provide an end to end synopsis of activities designed to complete the project successfully. A Baseline Assessment was conducted to establish the current state of practice in order to determine and prioritize gaps, develop solutions to overcome the prioritized gaps, and determine which solutions are most valid via experimentation.

1.1 Key Partners/Forces Involved

The Warfighter Challenge is sponsored by USEUCOM and USAFRICOM; however other DOD agencies play key roles in the development and subsequent transition of solutions. The key partners are listed below:

- USAFRICOM,

- USEUCOM, and
- Office of the Secretary of Defense Networks and Information Integration/Chief Information Officer (OSD NII/CIO).

Due to the need to share information across the whole of government, host nation, NGO, and IOs, participation from non-DOD entities is of the utmost importance. The following agencies and organizations that currently have interest or have committed to contributing to the IMISAS campaign are below:

Key participants

- USAFRICOM
- USEUCOM
- North Atlantic Treaty Organization/Allied Command Transformation
- U.S. Department of State (DOS)
- U.S. Agency for International Development (USAID)
- NGO Community; World Care Center
- Academia
- United Nations Office for the Coordination of Humanitarian Affairs
- OSD NII/CIO
- Defense Information Systems Agency (DISA)
- DISA Europe
- JS J6

1.2 Problem Statement

As stated previously, USEUCOM and USAFRICOM's highest priority warfighter challenge is:

"USEUCOM and USAFRICOM require the capability to share essential information with interagency partners, Coalition and Alliance partners, or emerging partner nations' in bi-lateral or multinational efforts. The capability gap is the result of: restrictive network access and information sharing policies; restrictive and cumbersome accreditation procedures for coalition networks and systems; lack of a coherent/unified strategy for a whole of government (to include foreign government) approach to an information sharing/collaborative environment; and resourcing to support that environment and its associated network enterprise services."

The IMISAS problem statement is derived from the USEUCOM and USAFRICOM Warfighter Challenge:

"COCOMs lack a coherent framework/capability to share information and collaborate across multiple domains with a broad range of mission partners (government/interagency, multi-

national, multi-lateral & private sector) due primarily to restrictive policies, conflicting authorities, ad-hoc/non-existent procedures, business rules and non-interoperable networks and systems."

All work regarding the IMISAS project emanates from this problem statement.

1.3 Baseline Assessment Process

The baseline assessment process is extensively explained in the IMISAS Baseline Assessment Report (BAR). In summary, the baseline assessment process commenced with an extensive literature review, coupled with telephone conversations with principal stakeholders and the IMISAS Community of Interest (COI), a site visit with USEUCOM and USAFRICOM staffs (17-19 November 2010), and the Stakeholders/Gap Validation Conference.

In the course of the literature review, several hundred documents were examined and evaluated for relevance. Over one hundred were identified and tagged for further assessment and evaluation. A listing and assessment of those documents, most pertinent to the baseline assessment and the project as a whole, are consolidated in the Source Review Spreadsheet in Appendix 4 of the IMISAS BAR. The Source Review Spreadsheet along with the aforementioned discovery initiatives provide the basis for discovery and discovery assessment leading to identification and evaluation of requirements, gaps and potential solutions.

1.4 Solution Development Process

A gap analysis was performed as part of the baseline assessment. The gap analysis process followed the approach outlined in the USJFCOM BAR Guidelines, beginning with identification of capabilities supporting stakeholder and partner requirements. That list was then evaluated against existing current joint capabilities to determine the existence of gaps. Gaps were decomposed by individual DOTMLPF-P areas and characterized as capability, capacity, or authority shortfalls.

The resulting gaps were prioritized by the experiment team and the stakeholders, and an initial list of potential solutions generated by the IMISAS analysis team for those gaps not addressed by current experimental efforts. Potential solutions are to be evaluated in terms of gap mitigating strategies by DOTMLPF-P area, projected sufficiency and effectiveness of incremental improvements, potential change agent(s)/organization(s), time to deliver the solution to the warfighter, cost of the complete solution, methods to determine value added, and potential sponsors for solution implementation and risk. Those solutions whose projected value added (positive impact) are not justified in terms of cost, time, or other project resource constraints will be excluded from further consideration, as will those solutions not having joint applicability or not observable in an experimentation venue (war game, seminar, or limited objective

experiment). The feasible set of solutions will then be submitted to the Experiment Design Project Lead for development.

2.0 Outcomes, Objectives, Products, and Activities

The project will use an analytic wargame (AWG) and/or analytic seminar as the culminating event to the IMISAS campaign. The AWG shall evaluate the effectiveness, suitability, and limitations of an enterprise collaboration capability in supporting ongoing operations. Experimental results will include observations, surveys, and hypothesis tests based on both numerical and categorical data. These will form the basis for creation of the IMISAS final products:

1) Unclassified information sharing handbook/guide.
2) Unclassified information sharing architectural products.
3) White paper on unclassified information sharing (unofficial joint operating concept).
4) DOTMLPF-P Change Recommendations (DCR) (if any), most likely focused upon:
    a. Doctrinal recommendations on how DOD can better work with the U.S. Government (USG) internally and provide and share information with IOs, NGOs, coalition, and private partners, and
    b. Policy and procedural changes on how to best facilitate information sharing with a range of partners in a HA/DR environment.
5) Offer potential upgrades or additions to the existing All Partners Access Network (APAN) capability.

The format for this section is separated into two outcomes with associated objectives for each outcome. Each outcome will directly lead to a product and activities to be utilized in order to reach the objective.

2.1 Outcome 1

Inform the development of the 'To Be' Unclassified Information Sharing Capability (UISC) employing Technical Spirals and an Analytic Wargame (AWG) focused on using/integrating available portal and cross domain technologies.

2.1.1 Objective 1.1: Identify requirements and potential operational solutions and technical enhancements using All Partners Access Network (APAN) as the technical proxy for experimentation.

2.1.1.1 Products:

Baseline Assessment

Requirements, Gaps, and Solutions

Description of 'As Is' capability and Operational View (OV)-1

Description of ‘To Be’ capability and OV-1

2.1.1.2 Activities:

Research

Stakeholders/Gaps Conference

Solution Development Workshop (SDW)

2.1.2 Objective 1.2: Pursue, as feasible, required authority and/or certifications required to test or demonstrate a cross-domain capability to USEUCOM/USAFRICOM.

(NOTE: This objective will not be part of the experiment activities. If anything of value is gleaned from the experiment activities it can be noted in the Analysis Report.)

2.1.3 Objective 1.3: Define and design an experiment employing a Humanitarian Assistance/Disaster Relief (HA/DR) scenario to validate information sharing and collaboration capability enhancements and policy and procedure variables addressing capability gaps.

2.1.3.1 Products:

Process and Procedures Handbook

Architectural Framework

UIS Unofficial Joint Concept (white paper)

2.1.3.2 Activities:

Site visits / Process Documentation

Stakeholders/Gap Validation Conference

SDW

IPC

Mid-Planning Conference (MPC)

Final Planning Conference (FPC)

2.2 Outcome 2

Improved processes, procedures and enabling policies to establish information sharing collaborative networked environment that can work across organizational and security boundaries for mission partners.

2.2.1 Objective 2.1: Develop an unofficial joint operating concept (white paper) based on the UISC Concept of Operations to include processes, procedures, and an organizational construct reflecting required roles, responsibilities, authorities and policies.

2.2.1.1 Products:

Policy and Procedures Handbook

AWG User Guide

AWG Standard Operating Procedures (SOP)

2.2.1.2 Activities:

Build partnerships

Stakeholders/Gaps Validation Conference

SDW

2.2.2 Objective 2.2: Develop and verify operationally focused processes and procedures required to implement information sharing and collaboration for HA/DR operations.

2.2.2.1 Products:

Policy and Procedures Handbook

2.2.2.2 Activities:

SDW

AWG

2.2.3 Objective 2.3: Examine policies, processes, and procedures, and recommend changes to facilitate information sharing with a range of partners in a HA/DR environment.

2.2.3.1 Products:

Policy and Procedures Handbook

2.2.3.2 Activities:

Site visits / Process Documentation

AWG

Transition Conference

2.2.4 Objective 2.4: Conduct user validation of potential UISC to provide enhancement recommendations for current UISC.

2.2.4.1 Products:

IMISAS Recommended APAN Enhancements

2.2.4.2 Activities:

AWG

Transition Conference

2.2.5 Objective 2.5: Develop a handbook and experimentally validated recommendations for doctrinal recommendations on how the DOD can better work with and engage the USG internally and how to provide and share information with IO/NGO/private partners for HA/DR.

2.2.5.1 Products:

Staff Handbook for Unclassified Information Sharing

2.2.5.2 Activities:

AWG

Transition Conference

2.3 Campaign Plan and Experimentation Activities Schedule

The Campaign Plan detailed below is an initial outline of events, their individual purposes, and expected outputs. The major events (workshops, conferences, technical spirals, and analytic wargame) coupled with ongoing research and Combatant Command site surveys; build upon each other. Due to the nature of this design and experimentation in general, initial events may result in findings that may necessitate a different course of action. These changes could result in an adjustment to the purposes and outputs listed below or require the addition of events or even remove the need for a given event. The aforesaid findings will be based on a set of consistent, complementary observations or evidence of a potential trend or pattern. The results will be grouped for each major area of research and will include research objective, research question/study issue as appropriate. Information sources that lead to each observation/insight will be provided with quantifiable, objective results.

Events will provide the stakeholders, mission partners and the COI the ability to contribute to and help shape the final project output.

High Level Timeline of Major Activities and Milestones for the IMISAS events are as follows:

- 13 October 2010: Interim Authority to Operate Certification Meeting
  - Purpose
    - Government and Contractor Team Roles and responsibilities, timeline review, objectives, scope. Present contractor manning plan, (organization, contractor work locations, and contact information). Intent was to open communications with and establish methods of communication with the Government leads. Discuss In-Process Review preparations and frequency. Review expectations and desired formats for contract deliverables. Present communication/interaction plan and receive feedback.
  - Output

        - Contact lists, draft experimentation plan; project timeline, manning plan, Strategic Communication/Stakeholder Engagement Plan.

[NOTE: This was preparatory work conducted early in the project when prototype and cross-domain capabilities were still considered viable products. This is no longer a requirement to the project.]

- 15-19 November 2010: USEUCOM/USAFRICOM Site Visit
  - Purpose
    - Investigate the proposed site where IMISAS experiment will occur.
  - Output
    - Requirements documentation
    - Technical Review
- 06-09 December 2010: Stakeholders/Gaps Validation Conference
  - Purpose
    - Bring stakeholders together to review Gaps and Solutions; investigate the technical solution; investigate procedures to be implemented. Provide the Solution Development Team the opportunity to review, discuss and incorporate Subject Matter Expert (SME) inputs to the initial draft of the operating concept.
    - Prioritize gaps and determine which gaps can be addressed in the timeframe of this experiment.
    - Determine what events are required in order to test potential solutions.
    - Determine timeline, to include dates, locations, and responsibilities for the events.
  - Output
    - Agreement on gaps and requirements
    - Identified potential solutions
    - Baseline Assessment Report
    - Technical review
- 22-23 February 2011: IMISAS SDW
  - Purpose:
    - To inform the IMISAS COI of capability gaps identified in the BAR, to evaluate potential solutions for experimentation, and to solicit additional viewpoints for solution development and refinement.
  - Output
    - A comprehensive prioritized list of potential solutions for experimentation and their supporting requirements and their supporting requirements and insights for the Operating Concept and the Handbook.
- 24-25 February 2011: IMISAS IPC
  - Purpose
    - To initiate planning for the experiment scheduled for August 2011.

- Output
  - Refine the Experimentation Plan for the experiment.
  - Initial plans for the MPC

- 28-31 March 2011: Process Documentation Event
  - Purpose
    - Collect data of the processes of information sharing, collecting and disseminating during creation of an OPT
    - Determine barriers to information sharing
    - Determine the 'as is' process for information sharing
  - Output
    - Baseline process for the experiment
    - Data to create the MSEL for the experiment
    - Data to assist in design of the experiment
- 19-21 April 2011: IMISAS MPC
  - Purpose
  - The purpose of the MPC is to further define the shape and scope of the IMISAS Analytic Wargame scheduled for 1 – 4 August 2011.
  - Output
    - Experiment design
    - Agreement on solutions for evaluation
    - Obtain all inputs required to complete a draft ED.
    - Complete a draft Experiment Manning Document (EMD).
    - Refine scenario requirements.
    - Draft MSEL / Use Cases
    - Develop requirements for draft training, control and OPSEC plans.
    - Draft technical requirements and associated business rules.
    - Project schedule of events and milestones leading up to the Technical Evaluation & Demonstration and the Analytic Wargame.
    - Updated IMISAS Experimentation Project DCAP.
    - Draft of the FPC objectives.
- 14-18 June 2011: IMISAS FPC
  - Purpose
    - Final check/last opportunity for course correction prior to execution of the Analytic wargame scheduled for 1-4 August 2011. Validate the completion of required products and work.
  - Output
    - Details ready for execution.
      - MSEL
      - Manning Document

  - Control Plan
  - KM Plan
  - DCAP
  - Technical review

- May – July 2011 Technical Spirals
  - Purpose
    - Five events to demonstrate technical enhancements and prepare APAN experimental site for Analytic Wargame.
- 1 – 4 August 2011: Analytic Wargame
  - Overall Purpose
  - Analytic Wargame to examine policy, process and procedures.
  - Overall Output
    - Recommendations for changes to existing policy, process and procedures.
    - Inputs to support Transition Conference
- 07-09 September 2011: Transition Conference
  - Purpose
    - Provide stakeholders with results of the Analytic Wargame; prepare all deliverables to be transitioned to stakeholders.
  - Output
    - DCR input, system to be transitioned, process, procedures, and enabling policies.

Figure D-1 offers a graphic overview of the campaign timeline.

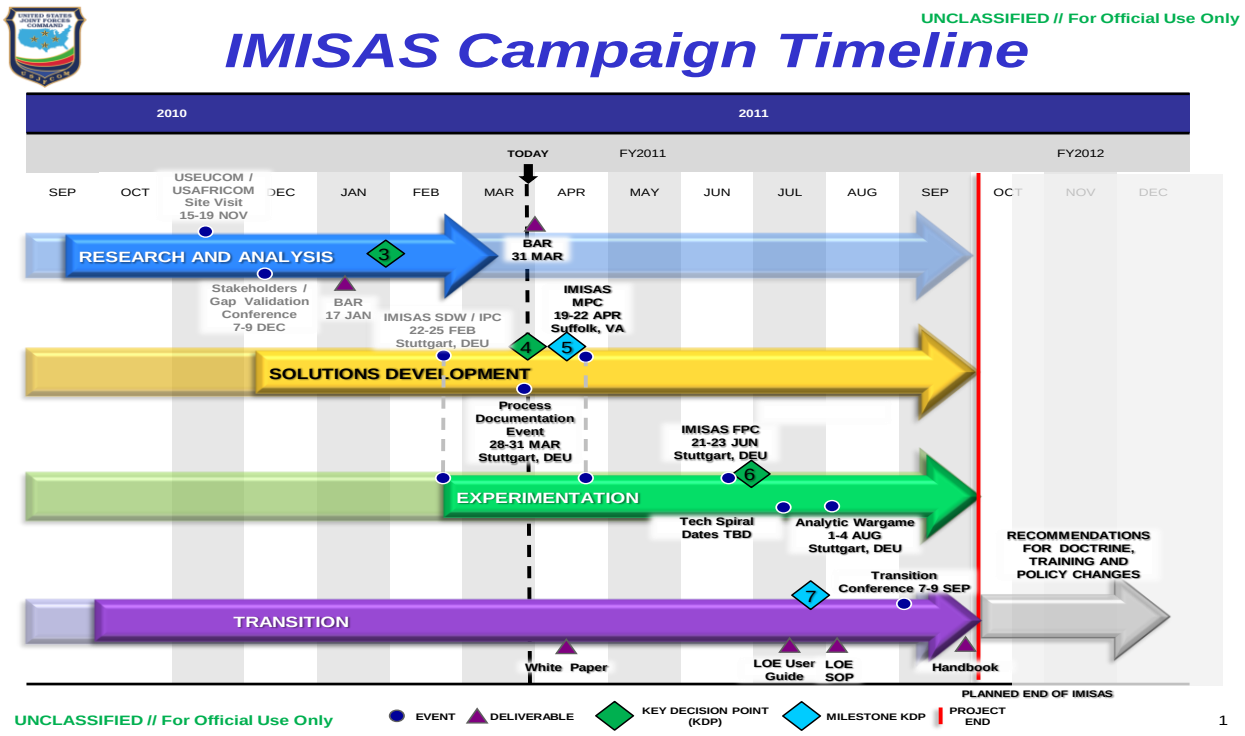


Figure D-1 – IMISAS Campaign Time Line

3.0 Experiment Environment and Procedures

3.1 Design

All IMISAS events will be conducted at the unclassified level. The design requirements for the Analytic wargame are being shaped by outputs from the Stakeholders/Gaps Validation Conference, three upcoming planning conferences (IPC, MPC, FPC), and outputs from trial events. Additionally, scheduled weekly teleconferences are allowing IMISAS partners and stakeholders an open forum to express ideas, opinions and points of view. Partner and stakeholder requirements will be used to determine the final evaluation event designs which will replicate the functionality of a combatant command operational planning team during a HA/DR mission.

3.2 Control Function

The IMISAS evaluation events will be controlled by an Event Directive (ED) (to be developed in a separate document). The ED will provide specific details, guidance and processes to be used in the execution of the event. USJFCOM has the overall lead for control and will establish a Control Group, led by the Chief Controller. Controllers or trusted agents will be used at each site to keep the Control Group apprised of any situation that might require the Control Group to

alter the day's activity or the activity of a specific execution period in order to meet the experiments objectives. Control is transparent and will go unnoticed by participants. The Control Group is not an active participant in the event but serves solely to provide the means to ensure the event runs smoothly and the experimental objectives are met.

The Chief Controller is responsible for ensuring that the event is conducted in accordance with the experiment design and in a fashion that attains the event objectives and study issues. The Controller will work closely with the Director of Experiment Design, with the Lead Analyst, and with the Concept Leads to ensure the environment in which the concepts are being examined is as realistic as possible and that it is meeting experimental requirements.

The Chief Controller will use the following principles in order to establish the proper environment:

- "Control" as an entity does not exist (from an Experiment Audience perspective).
- Interaction with the Experiment Audience must be as "real world" as possible.
- Experiment control and monitoring will be centralized via the Chief Controller and his staff.
- All inputs into the Experiment Audience must be filtered through the Chief Controller.
- The Experiment Audience and the Chief Controller will be collocated.
- Some key Experiment Audience leaders will act as Trusted Agents (the Chief Controller/Concept linkage).
- A full-time Analysis representative will be present as part of experiment control to monitor the event's progress (the Lead Analyst and Chief Controller work very closely together).

3.3 Scenario

Proposed solutions will be evaluated in the appropriate context to ensure USEUCOM's and USAFRICOM's experimental objectives are addressed. A scenario will be used in the Analytic Wargame to address HA/DR activities in a coordinated and controlled process and will be driven by a Master Scenario Event List (MSEL). The MSEL and the specific injects therein will be developed in concert with mission partners to force action and drive communications.

The basic scenario is to be presented for stakeholder buy in during the MPC. MSEL development will continue to the FPC. At the FPC, the final scenario and specific MSEL injects will be presented for approval by the experiment stakeholders.

USJFCOM has the lead for scenario development.

3.4 Security

The experiment will use unclassified information only. Care must be taken to ensure that information is given the appropriate protection, to include Controlled Unclassified Information. This information must be protected by dissemination restrictions, and all persons receiving this information must protect it in accordance with those restrictions. Proper procedures, to include approved marking standards, will be briefed at the opening of each event. IMISAS SMEs and the IMISAS Risk Management Coordinator will review briefings and materials as appropriate in order to prevent an escalation in the sensitivity of such materials through the aggregation of data that are less sensitive on their own.

In order to protect against inadvertent disclosure of material that the government considers sensitive, all personnel who participate in IMISAS activities will be familiar with the Critical Information List (CIL) prepared by the IMISAS Risk Management Coordinator for each event (and included as Annex B of this document). The preliminary CIL provided in Annex B will be updated as appropriate as additional documents are introduced into use. The CIL identifies potential sensitive and classified information so that participants can take appropriate measures to prevent the unauthorized dissemination of sensitive information.

Based on DODI 5200.1-R and DODD 5205.2, the following guidelines shall be implemented at all IMISAS events.

- Briefs from all organizations shall be labeled to indicate dissemination restrictions or public releasability, as appropriate.
- Administrative remarks at the beginning of each IMISAS event will remind participants that all information discussed during an event must be releasable to the IMISAS COI.
- In addition to other topics, these administrative remarks will remind personnel of the classification and releasability requirements of the information used, and all security requirements associated with that information.

3.5 Experimentation Ethics Compliance

As a U.S. led event, the IMISAS Analytic Wargame will comply with all applicable provisions of U.S. regulations and directives regarding the protection of human subjects in research experimentation and the safeguarding of experiment data. If individual partner nation rules and directives require additional provisions for their own events, participants or sites they will be implemented on a case by case basis only for those events, individuals and sites.

4.0 Analysis and Data Collection

Data collection will occur at experiment evaluation and other events. Each event collection plan will be a stand-alone document. For experimentation events the plan will contain a minimum of

observations and analyst notes, surveys, interviews, constructive simulation output, APAN system logs, multimedia output, screen captures, after action reports and hot washes. Both quantitative and qualitative data will be collected as best captures the effects to be observed in testing solutions.

The analysis strategy has been designed to achieve the specific experiment objectives; however, through the course of the experiment, the analysis team will avail itself of all opportunities to capture additional information that may lead to other lines of investigation both during and after the experiment.

Annex G, Analytic Framework, provides a details of data collection and analysis for the experiment.

5.0 Experiment Design Assessment

The experiment design has been assessed against the 21 threats to valid experimentation[1] shown in Figure D-2. In Table D-1 each threat is rated for its applicability to, or impact on, this experiment (rated as high, medium or low). The risk of each threat is then rated as red (significant problem or shortfall), yellow (area of concern or experiment limitation) or green (no known problems). Techniques planned for mitigating the risk of any threat evaluated as red or yellow are described in the column that follows.

[1] (Kass, 2006)

	Ability to Use Capability	Ability to Detect Results	Ability to Isolate Reason for Results		Ability to Relate Results to Operations
			Single Group	Multiple Groups	
1 Treatment	**1. Capability not workable:** Do the hardware and software work?	**5. Capability variability:** Are systems (hardware and software) and use in like trials the same?	**11. Capability changes over time:** Are there system (hardware or software) or process changes during the test?	N/A	**18. Nonrepresentative capability:** Is the experimental surrogate functionally representative?
2 Players	**2. Player non-use:** Do the players have the training and TTP to use the capability?	**6. Player variability:** Do individual operators/units in like trials have similar characteristics?	**12. Player changes over time:** Will the player unit change over time?	**15. Player differences:** Are there differences between groups unrelated to the treatment?	**19. Nonrepresentative players:** Is the player unit similar to the intended operational unit?
3 Effect	**3. No potential effect in output:** Is the output sensitive to capability use?	**7. Data collection variability:** Is there a large error variability in the data collection process?	**13. Data collection changes over time:** Are there changes in instrumentation or manual data collection during the experiment?	**16. Data collection differences:** Are there potential data collection differences between treatment groups?	**20. Nonrepresentative measures:** Do the performance measures reflect the desired operational outcome?
4 Trial	**4. Capability not exercised:** Does the scenario and Master Scenario Event List (MSEL) call for capability use?	**8. Trial conditions variability:** Are there uncontrolled or unmonitored changes in trial conditions for like trials? Look for intervening variables not recorded.	**14. Trial condition changes over time:** Are there changes in trial conditions (such as weather, light, start conditions, and threat) during the experiment?	**17. Trial condition differences:** Are the trial conditions similar for each treatment group?	**21. Nonrepresentative scenario:** Are the Blue, Green, and Red conditions realistic?
5 Analysis	N/A	**9. Low statistical power:** Is the analysis efficient and the sample sufficient? **10. Violation of statistical assumptions:** Are correct analysis techniques used and error rate avoided?	• The purpose of an experiment is to verify that A causes B. • A valid experiment allows the conclusion "A causes B" to be based on evidence and sound reasoning… - by reducing or eliminating the 21 known threats to validity.		

Figure D-2 – Threats to Valid Experimentation

Table D-1 – Risk Evaluation Matrix

Challenge	Impact on this Event	Risk	Risk Mitigation Measures
Ability to use capability			
1. Capability not workable: Does the hardware and software work?	High	Yellow	APAN software is already a fielded capability and the Analytic Wargame involves no physical modifications to the hardware or software. The experiment may introduce new mature applications not previously integrated on the APAN network. The newly introduced applications will be tested individually and as a system before use in the experiment. There is some concern over APAN help desk support due to time differences between the APAN server and experiment location. Coordination is currently underway to provide dedicated server, software, and APAN administrative support during and off APAN help desk hours.

Table D-1 – Risk Evaluation Matrix			
Challenge	**Impact on this Event**	**Risk**	**Risk Mitigation Measures**
2. Player non-use: Do the players have the training and TTP to use the capability?	**High**	**Low**	**During the Technical Spirals, recommendations will be gathered for streamlining the procedures and approval process for APAN site instantiation. For the experiment audience, training will be conducted for the processes, procedures, and APAN enhancements they will utilize during the experiment. Additionally, support personnel will be trained on the processes, procedures, and APAN enhancements to fully enable them to support the experiment.**
3. No potential effect in output: Is the output sensitive to capability use?	**High**	**Yellow**	**"As-is" and "to-be" capabilities are captured in separate events. The Process Documentation Event will document and quantify, as applicable, existing capabilities, processes, and procedures as well as barriers. Technical Spirals will establish and verify APAN (UIS) processes to be utilized during the experiment. The experiment will examine performance under solution-enabled environment with results captured for comparison purposes with those from the Process Documentation Event.** **The number of potential solutions and still undetermined scope of the scenario may strain the resources necessary for a full-factorial design, creating the possibility of "as-is" and "to- be" comparisons that lack discriminating power.**
4. Capability not exercised: Does the scenario and Master Scenario Event List (MSEL) call for capability use?	**High**	**Yellow**	**The MSEL is not yet created but intent is to use a fully developed MSEL during the Analytic Wargame. Challenges are expected in scripting vignettes stressing non-technical (particularly cultural) solutions as their effects are inherently more difficult to quantify and stimuli more difficult to craft.** **Controllers, solution developers, and analysts will be involved in developing the MSEL to ensure the appropriate objectives and data collection from the experiment can be collected.** **Technical Spirals will not have a fully developed MSEL, but will use scripted use cases to be developed.**
Ability to Detect Results: Correctly detect a true effect			
5. Capability variability: Is systems (hardware and software) and use in like trials the same?	**Low**	**Green**	**The "as-is" is documented from interview and research. The "to-be" will be performed in a laboratory environment with only a series of vignettes vice trials; thus this issue is of minimum consequence. Technical Spirals will be checking that APAN enhancements operate properly. APAN will be managed from its home server with someone who has been given administrative**

Table D-1 – Risk Evaluation Matrix			
Challenge	**Impact on this Event**	**Risk**	**Risk Mitigation Measures**
			credentials.
6. Player variability: Do individual operators/units in like trials have similar characteristics?	**Medium**	**Green**	**The "as-is" is documented from interview and research. The "to-be" will be performed in a laboratory environment with only a series of vignettes vice trials; thus this issue is of minimum consequence.** **Training will be conducted on the experiment audience in the days immediately prior to experiment execution; thus, the individual operators will be the same.**
7. Data collection variability: Is there large error variability in the data collection process?	**High**	**Green**	**A large proportion of data is expected to be captured through observations, surveys and interviews and collated in a central location. The use of a standard survey tool, such as Vovici, will be utilized if available. Training for data collectors, observers, and analysts will be held prior to the experiment. All data collectors, observers, and analysts are slated to be on site where the laboratory environment is physically located; thus, hot washes will be held daily and more often if required, to ensure all appropriate data is collected consistently.**
8. Trial conditions variability: Are there uncontrolled changes in trial conditions for like trials?	**Medium**	**Green**	**The "as-is" is documented from interview and research. The "To Be" will be performed in a laboratory environment with only a series of vignettes vice trials; thus this issue is of minimum consequence.**
9. Low statistical power: Is the analysis sample sufficient?	**Medium**	**Yellow**	**Sample sizes for both the technical spirals and analytic wargame is expected to be relatively small. The controlling influence is cost associated with travel and man-hours, availability of participants, and real-world operations demands. It is unlikely that sample size will be larger than 15; thus, nonparametric statistical analysis will be used if required. Observations of experiment play will be closely monitored by analysts, observers, data collectors, subject matter experts, and solution developers to ensure all appropriate data is collected for further analysis and to attain a significant amount of viewpoints from different backgrounds, which will enhance the final analysis.**
Ability to Detect Results: Incorrectly detect an artificial effect			
10. Violation of statistical assumptions: Are correct analysis techniques used and	**Medium**	**Yellow**	**Once sample size is known, an appropriate application of techniques will be employed. Reliance on non-parametric analysis is expected.**

Table D-1 – Risk Evaluation Matrix			
Challenge	**Impact on this Event**	**Risk**	**Risk Mitigation Measures**
the error rate avoided?			
Ability to Isolate Reason for Results: Single Group			
11. Capability changes over time: Are there system (hardware or software) or process changes during the test?	**Medium**	**Green**	**There are only a series of vignettes, not multiple trials. If procedures are changed, it will be the result of hot-wash meetings and by design. If the experiment audience does not follow trained methods, an experiment 'time-out' can be called if the deviation will affect experiment validity.**
12. Player changes over time: Will the player unit change over time?	**Medium**	**Green**	**There are only a series of vignettes, not multiple trials which will take place over a consecutive two-day period. If some of the participants do arrive to complete the required training, then this could expose a team at a variety of levels of maturity to the processes and procedures. This is a very minimal concern as manning for the billets will be thoroughly vetted at the MPC and FPC with the customers who will be supplying the manning.**
13. Data collection changes over time: Are there changes in instrumentation or manual data collection during the experiment?	**Medium**	**Yellow**	**There are only a series of vignettes, not multiple trials; thus, this should be of minimal concern. The only stipulation to this would be if the PDE analysis does not yield enough baseline experimentation data to reveal adequate changes (or evidence of no change) in variables during the Analytic Wargame. This is not expected; however, if it does occur, every reasonable effort will be made to establish the missing data.**
14. Trial condition changes over time: Are there changes in trial conditions (such as weather, light, start conditions, and threat) during the experiment?	**Low**	**Green**	**No significant environmental condition changes are expected for the experiment. The most likely cause of a condition change will be service interruption with APAN, the internet, or experiment network. Efforts are underway to curb any disruption of APAN during the experiment. This may involve having a PACOM person on site for the experiment execution or someone on site with APAN administrative rights.**
Ability to Isolate Reason for Results: Multiple Groups			
15. Player differences: Are there differences between groups unrelated to the treatment?	**Medium**	**Green**	**There will only be one group operating during the Analytic Wargame; thus, there will not be differences between groups.**

Table D-1 – Risk Evaluation Matrix			
Challenge	**Impact on this Event**	**Risk**	**Risk Mitigation Measures**
16. Data collection differences: Are there potential data collection differences between treatment groups?	**High**	**Green**	**There will only be one group operating during the Analytic Wargame; thus, there will not be differences between groups.**
17. Trial condition differences: Are the trial conditions similar for each treatment group?	**Medium**	**Green**	**There will only be one group operating during the Analytic Wargame; thus, there will not be differences between groups.**
Ability to Relate Results to Operations			
18. Non-representative capability: Is the experimental surrogate functionally representative?	**High**	**Yellow**	**The customer will be intimately involved in the architecture of the laboratory environment; however, the laboratory will not be the actual environment that the audience normally operates. The experiment design and laboratory lay out is still under construction. Site surveys have been conducted and the design team is in communication with the customer concerning these matters. Also, the FPC will be conducted in the vicinity of where the Analytic Wargame will take place; thus, another site visit should occur prior to the experiment execution.**
19. Non-representative players: Is the player unit similar to the intended operational unit?	**High**	**Green**	**The experiment audience will be fielded by the customers' personnel who are experienced in the billets they will be playing in the Analytic Wargame. Control may not be filled by actual subject matter experts in all billets, but will have personnel familiar with the given role. Real-life operational requirements could force substitution of personnel to role play in the experiment audience, but will most likely be filled by personnel who are familiar with the billet.**
20. Non-representative measures: Do the performance measures reflect the desired operational outcome?	**High**	**Yellow**	**Measures are still being established. The decomposition of objectives is ongoing and will be fully vetted during the MPC and FPC, and in comparison with the final solutions determined and developed for experimentation.**
21. Non-representative scenario: Are the Blue, Green, and Red conditions	**High**	**Yellow**	**There has been a significant effort to recruit participation of personnel with functional expertise in military and non-military disciplines and areas. The cooperation of actual IOs/NGOs, IA, and foreign governments will help to bring consistency, fidelity and authenticity to vignettes and**

Table D-1 – Risk Evaluation Matrix			
Challenge	**Impact on this Event**	**Risk**	**Risk Mitigation Measures**
realistic?			**scenario. Participants that are real world responders to HA/DR scenarios and will provide expert knowledge to their representative group.**

6.0 Transition Planning

The Transition Plan is fully detailed in Annex L, the IMISAS Transition Plan, which lays out the basic actions to be executed in support of transitioning the products of the IMISAS Project to the joint warfighter. The goal is to improve information sharing between the U.S. DOD and non-military partners by mitigating the human factors, cultural, policy and procedural barriers to information sharing and collaboration, while leveraging other related initiatives at establishing sustained information sharing and collaborative relationships among organizations.

The primary transition pathway will be informal using change processes such as joint doctrine changes affected through the Joint Doctrine Development System (CJCSI 5120.02), changes or updates to tactics, techniques and procedures (TTPs), development of a pre-doctrinal handbook, adjustments to joint education curricula and training courses of instruction, and DOTMLPF changes that have portfolio impacts submitted to the Capabilities Portfolio Manager.

References

(n.d.). *Interagency Shared Situational Awareness Guide (IA SSA)*

(n.d.). *SHIFT Shared Information Framework and Technology Enabling focus area MNE5 High Level Overview Document*

(n.d.). *J86 Transisiton Case Officer Transition Handbook*

(2007, May 30). *Reference Architecture for MNE5 technical system*

(2008, September 30). *Information Exchange Architecture and Technology Concept in the MNE5 environment*

(2009, Feburary). *SHIFT Handbook Shared Information Framework and Technology*

(2009, January 20). *Shared Information Framework and Technology (SHIFT) Technical Solution for MNE 5*

(2010, June 25). *CJCSI 3010.02C*

(2010, June 25). *CJCSM 3010.02*

(2010). *Warfighter Challenge Submital*

All Partner Access Network (APAN) Specs. (n.d.)

Brundidge, G. L. (2010, June 4). *Unclassified/ Non-Classified Information Sharing*

CAPT J.G. Jerauld, U. (2010, Feburary 17). FY-11 Warfighter Challenge 1: Multi-National and Inter-Agency Information Sharing

CDR James H. Mills, U. (2008, April 8). Net-Centric Security Pilot Proposed Way Ahead.

Chairman of The Joint Chiefs Instruction CJCSI 6212.01E. (2008, December 15). *CJCSI 6212.01E*.

Charter for Command and Control Profolio Data and Services Steering Commitee. (2008, December 10). *V 3.1*

CIO, D. (2003, May 9). DOD Net Centric Data Strategy

Communities of Interest (COI). (2009)

Contract SOW N00189-09-D-Z046-0004. (n.d.)

Contract SOW N00189-10-Q-2499-0001. (n.d.)

Cooperative Implementation Planning, Management and Evaluation (CIP/CIME) Major Integrating Event. (2008, April)

Council, E. (2010, August 25). *Joint Concept Development and Experimentation (JCD&E)*

Data Strategy for Command and Control Capabilities Update. (2010, July 06). *JROCM 110-10*

Department of Defense (DOD) Enterprise Unclassified Information Sharing Service. (2010).

DOD Instruction NUMBER 2205.02. (2008, December 2). Under Secretary of Defense for Policy

DOD Instruction NUMBER 2205.3. (1995, January 27). *Implementing Procedures for the Humanitarian and Civic Assistance (HCA).*

DOD Instruction NUMBER 3000.05. (2009, September 16)

Donelly, T. G. (January 27, 1995). *DOD Instruction NUMBER 2205.3.* Principal Deputy.

Endosorment of All Partners Access Network. (2010, July 20)

Force, 1. M. (n.d.). 1MEF Case Study

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Planning Package Summary (2010)

J6. (2010, August 10). *Department of Defense (DOD) Enterprise Unclassified Information Sharing Service*

J82, U. (n.d.). DOD C2 Strategy Objective Capabilities Definition

J87. (2010, June 10). J87 Joint Data Service Division

Jumper, C. o. (2002). Cursor on Target . *CoT Narrative*

Kuusisto, R. (2009). *"SHIFT" THEORETICALLYPRACTICALLY Modivated Framework*

Leadership, J. S. (2008, October 27). *DOD Net-Centric Data Strategy (DS) and Community of Interest (COI) Training*

MNE-5 Major Integrating Event 2010. (n.d.)

NATO Network Enabled Capability Interaction Maturity. (n.d.)

OSD. (October 27, 2008). DOD Net-Centric Data Strategy (DS) and. *Power Point* , 65

Planning Package (P2) Summary for FY11 PoW. (2010, May 19)

RFQ N00189-10-Q-2499. (n.d.)

Ross, P. (2009, March 6). Joint C2 Data Strategy

SHIFT Shared Information Framework and Technology Concept Ver 9. (2009, Feburary)

Staff, V. C. (2010, July 6). Data Strategy for Command and Control Capabilites

USJFCOM Data Initiative Synchronization. (2009, March 09)

Winters, L. (2010, June 10). J87 Joint Data and Services Division

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions Project (IMISAS)

Annex E - BASELINE ASSESSMENT REPORT

Executive Summary

The Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) project advances unclassified information sharing through the venue of Joint Experimentation. The IMISAS project's intent is to improve information sharing between Department of Defense (DOD) and a wide variety of non-military mission partners, who may include civilian U.S. government agencies, other nations, inter-governmental organizations, and nongovernmental organizations. The project planning incorporates an appreciation for the value of joint experimentation and a thorough understanding of experiment design principles.

Consistent with Joint Concept Development and Experimentation (JCD&E) Enterprise design, the IMISAS project problem statement derives from a United States European Command (USEUCOM) and United States Africa Command (USAFRICOM) Fiscal Year 2011 (FY 11) Warfighter Challenge submission. That challenge identified Joint shortfalls in the current art and practice of unclassified information sharing (UIS) between a diverse community of potential mission partners as well as non-aligned organizations. This community includes enduring and familiar partners such as United States government agencies, coalition military and civilian partners, host nations, inter-governmental organizations, nongovernmental organizations and ad hoc organizations. The DOD frequently supports a lead agency, such as the Department of State (DOS) or other authorities, responsible for conducting the overall Humanitarian Assistance and Disaster Relief (HA/DR) mission.

The complexities of operating and sharing information with an evolving and often unfamiliar community of interest (COI) place a premium on DOD's ability to understand the nuances of potential partners' organizational cultures, needs, strengths and limitations. Therefore, the analysis of requirements, gaps and solutions associated with the IMISAS project pays particular attention to the enablers of cultural understanding and those implementing policies and procedures underpinning successful engagement and support to lead authorities, as well as the technical capabilities needed to share information. In essence, the baseline assessment is both a process and product. It examines the military problem; identifies, assesses and documents required capabilities and gaps; and proposes potential solutions to be tested through experimentation, explored through further research, or provided as supporting material to existing policy, procedural, or reference documents.

This Baseline Assessment Report (BAR) provides a snapshot of the current information sharing initiatives in DOD as of May 2011. It serves as a guide to current and future challenges for information sharing, for identifying and developing potential solutions,

and for crafting and executing an experimentation plan to evaluate solutions and deliver products for transition.

The outline of the document follows a logical intellectual path and order. Section 1 introduces the project and the issues associated with UIS and the reasons why that capability is important to the community of organizations associated with HA/DR missions as well as the DOD. Sections 2 and 3 focus on identifying the core objectives, tasks and outcomes of the IMISAS project and those assumptions, limitations and constraints shaping the boundaries and scope of what can be accomplished throughout the project lifecycle. Section 4 develops the research methodology and introduces the assessment tool employed to prioritize requirements, gaps and solutions. Section 5 describes the current baseline, identifies and assesses requirements and gaps, and documents potential solutions. Finally, section 6 summarizes and recommends possible courses of actions (COAs) and associated potential solutions for further consideration and refinement at subsequent planning conferences - the grist for eventual experimentation.

In executing the baseline assessment the IMISAS team, based upon research and direct input from the IMISAS project COI representatives, initially identified and ranked 23 stakeholder requirements and identified and ranked 28 capability gaps associated with these requirements. Thirty-nine potential solutions were identified to close these gaps. These solutions were ordered in a way that accounted for COI rankings of gaps and requirements, and the many-to-many relationships among requirements and gaps, and gaps and solutions. For the purposes of further solution distillation and as an organizing construct for metric development, these 39 nominations were grouped into 12 focus areas which span the Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Policy spectrum and address each identified gap with at least 2 potential solutions.

In December 2010, the gaps were presented, validated and prioritized and potential solutions were identified at the Stakeholder/Gap Validation Conference. The IMISAS team incorporated the results of the conference and completed a draft BAR in support of the problem statement: "COCOMs lack a coherent framework/capability to share information and collaborate across multiple domains with a broad range of mission partners (government/interagency, multi-national, multi-lateral & private sector) due primarily to restrictive policies, conflicting authorities, ad hoc/non-existent procedures, business rules and non-interoperable networks and systems." Subsequent to the publication of the draft BAR, the Warfighter Challenge sponsors analyzed the 28 gaps and developed a list of the 10 that were their highest priority.

In February 2011, a Solution Development Workshop (SDW)/Initial Planning Conference (IPC) was held at USEUCOM in Stuttgart, Germany. The purpose of the event was to further refine the capability gaps initially identified in the baseline

assessment, to evaluate potential solutions for experimentation value and further development and to shape planning for the project experiment. The IMISAS team successfully presented and validated specific gaps identified in the BAR and reviewed the initial cut on multiple potential solutions which would be viable for experimentation. The SDW/IPC sessions set the stage for the beginning of the planning process for the scheduled August 2011 Analytic Wargame (AWG).

The IMISAS team conducted a Process Documentation Event, 28-31 March 2011, at USAFRICOM and USEUCOM headquarters. The objective of the event was to define the "as-is" information sharing environment and processes. The results from this event provided validated documentation in support of continued event design and planning, and set the conditions for further refinement during the Mid-Planning Conference (MPC).

The IMISAS project MPC was conducted, 19-22 April 2011, at the MITRE office in Suffolk, Virginia (USA). The primary purpose of the MPC was to further define the shape and scope of the IMISAS AWG. MPC participants successfully accomplished all the pre-identified conference objectives including the validation of high-level potential solutions to be examined, discussion of the proposed foreign humanitarian assistance scenario that focused on multi-organizational unclassified information sharing, and refined planning of the key experiment design elements.

The IMISAS experiment event design refinement, as conducted during the MPC, was a creative cognitive process that envisaged possibilities and employed proven experiment design principles to provide coherent, integrated, and achievable demonstration and experimental events. The evolving experiment event design reflects the IMISAS partners and stakeholders' guidance with regard to allocation of resources, preparation of experimentation activities, management, and synchronized event execution. This experiment event design also identified critical event dependencies, long-lead items, and preparatory events required for key activities. The design is flexible enough to make adjustments to the event as available resources among the participants change (time, money, personnel, etc.), or as new opportunities arise.

Table of Contents

Executive Summary E-2
1.0 Introduction E-7
1.1 Background E-7
1.2 Statement of the Military Problem (The Genesis of the IMISAS Project) E-9
1.3 IMISAS Project Problem Outcomes: E-10
1.3.1 Original IMISAS Project Problem Outcomes E-10
1.3.2 Revised IMISAS Project Problem Outcomes E-10
1.4 Underpinning Issues and Necessity of Addressing the Problem E-10
1.4.1 Technical Issues E-11
1.4.2 Policy and Procedures E-13
1.4.3 Culture E-13
1.4.4 Knowledge Management E-15
2.0 Scope and Limitations E-17
2.1 Significant Project Influences E-17
2.2 Revised Objectives Overview: E-18
2.3 Revised Products: E-18
3.0 Problem Decomposition E-19
4.0 Research Methodology E-23
4.1 Research Schema E-23
4.2 Discovery E-25
4.3 Gap Analysis E-27
4.3.1 IMISAS Project Assessment Tool E-29
5.0 Assessment Summary E-30
5.1 Context, Constraints, Limitations, and Assumptions E-30
5.2 Current Baseline E-32
5.3 Other Relevant Work E-36
5.4 Required Capabilities E-39
5.5 Gaps Identified E-39
5.6 Potential Solutions E-40
5.7 Summary of Analytic Results E-40
6.0 Recommendations E-47
6.1 Experiment Objectives E-47
6.2 Project Products E-47
6.3 Experiment Design Courses of Action (COAs) E-48
6.3.1 COA #1 Description E-48
6.3.2 COA #2 ..... E-49
6.3.2.1 COA #2a Description E-49
6.3.2.2 COA #2b Description E-49
6.3.3 COA #3 Description E-49
6.3.4 COA #4 Description E-49
6.3.5 COA #5 (Selected) Descriptions E-49
6.3.6 COA Recommendations and Decision E-49

List of Appendices E-51

List of Figures

Figure E-1 – Problem Decomposition E-190
Figure E-2 – Community of Interest E-20
Figure E-3 – IMISAS Project Concept E-22
Figure E-4 – Analytic Framework E-24
Figure E-5 – IMISAS Project Process Model E-25
Figure E-6 – Source Review Spreadsheet Illustration E-28
Figure E-7 – Gap and Solution Development Process E-29
Figure E-8 – Baseline - Requirements vs. Validated Gaps E-36

List of Tables

Table E-1 – Solution breakout by Gaps and DOTMLPF-P Area E-46

1.0 Introduction

1.1 Background

The Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) project's intent is to improve information sharing between the United States (U.S.) Department of Defense (DOD) and a wide variety of non-military mission partners, who may include civilian U.S. government agencies, other nations, inter-governmental organizations (IOs), and nongovernmental organizations (NGOs). The project planning incorporates an appreciation for the value of joint experimentation and a thorough understanding of experiment design principles.

In the last decade, the U.S. DOD has worked toward improving civil-military coordination and cooperation, particularly during Humanitarian Assistance/Disaster Relief (HA/DR) operations, where the armed forces will usually be in a supporting role to highly specialized civilian organizations. The U.S. and the international community have witnessed and responded to human rights abuses, massive refugee movements and the endangerment and death of hundreds of thousands of civilians as a result of natural disasters, civil wars and major conflicts in countries like Somalia, the former Yugoslavia, Rwanda, Haiti, Iraq and Afghanistan.

Two quintessential events (the attacks on September 11, 2001 and Hurricane Katrina) within the borders of the U.S. reinforced and highlighted for the U.S. Government (USG) the need to embrace information sharing with an extended enterprise. Extending information sharing to include the broader international community poses even greater challenges.

> "No one agency can do it alone." **The 9 September 2001 Commission Report, p 418**
>
> "One would think we can share information by now. But Katrina again proved we cannot." **Congressional reports: H Rpt. 109-377.**

The NGO community consistently delivers vast amounts of emergency humanitarian assistance, medical supplies, water purification equipment and and shelters to people affected by disaster events. Although organizations such as these worked with militaries in the past, the increasingly harsh security environments now faced by humanitarian missions in often lawless areas have demonstrated the need for new working relationships with U.S. and other armed forces. One touch point which has gained some traction in easing the nominally tense relationship between them is the arena of information sharing.

Information sharing is not without difficulties. The challenges are formidable and involve dimensions of organizational culture, policy, procedure, and technology. Information sharing is impeded by sensitivities associated with the neutrality and independent policies of IOs and NGOs, lack of cultural and social situation awareness,

the political "will" of participants and organizations, differences in communication and authority structures across the span of HA/DR responders, and the need to build trust and a shared understanding of expectations. Further complicating information sharing are conflicts and shortfalls in policy, doctrine and tactics, techniques and procedures (TTPs). These include restrictions on information releasability, information management and assurance requirements, and organizational authority and resources for network and spectrum management. Technical challenges include the necessity of integrating ad hoc stove-piped capabilities, lack of a unifying architecture and concept of operations, large and complex problems in data management, the need to accommodate the disadvantaged user, and the need to address the problems of linguistic differences over a potentially vast set of languages and dialects.

The 2006 Quadrennial Defense Review (QDR) called upon the DOD to broadly improve "information sharing with other agencies and with international allies and partners" and develop a strategy that guides "operations with Federal, State, local and coalition partners". [1] Responding to the QDR, the DOD Chief Information Officer on May 4, 2007 signed the *Department of Defense Information Sharing Strategy*, and in April 2009 promulgated the *Department of Defense Information Sharing Implementation Plan*, which established a set of near term tasks to position DOD to progress toward implementation of the broader Strategy. On November 15, 2010 the Director Joint Staff J-3 released the *Unclassified Information Sharing Capability* (UISC) Concept of Operations (CONOPS), which "outlines the capability designed to assist joint and coalition military organizations in their efforts to collaborate, plan and coordinate operations, exchange information and build situational awareness with both traditional and non-traditional mission partners across various mission sets."[2]

It is within the context of utilizing joint experimentation to improve information sharing with non-DOD mission partners that the IMISAS project is chartered. Specifically, the IMISAS project seeks to identify Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) solutions to provide the Commander, U.S. Africa Command (USAFRICOM), the Commander, U.S. European Command (USEUCOM) and by extension other U.S. Combatant Commanders the ability to effectively share information with a range of mission partners in order to synchronize potential DOD contributions in a supported or supporting role across the full spectrum of potential operations. The expected recommended changes in DOTMLPF-P will lead to a further refinement and clarification of the concept of operations and capability to enable

[1] QDR 2006
[2] (J-3, 2010) UISC CONOPS, 15 November 2010

information sharing, collaboration and transactions between both real and virtual communities in order to reduce redundancies and inefficiencies of any potential DOD contribution. These communities include the DOD, USG agencies, interagency (IA) groups, coalition military and civilian partners, IOs, NGOs, ad hoc organizations and private partners.

The IMISAS project was approved as part of the FY 10/11 Joint Experimentation Program of Work by the Joint Experimentation Executive Council representing primary stakeholders from USEUCOM, USAFRICOM, and USJFCOM Joint Concept Development & Experimentation (JCD&E) Directorate (J9) in collaboration with the broader JCD&E Enterprise.

The appendices 1, 2, and 3, respectively, reference the acronyms, bibliography and glossary for this BAR.

1.2 Statement of the Military Problem (The Genesis of the IMISAS Project)

The IMISAS project problem statement was derived from the Warfighter Challenge submission and as framed in the Statement of Objectives (SOO) and Performance Based Work Statement (PBWS) delineates specific outcomes. Both objectives and outcomes have been analyzed in the Baseline Assessment (BA) and modified throughout the course of the project. Objectives and outcomes reached initial consensus following a 17-19 November 2010 USEUCOM and USAFRICOM site visit, and prior to the gap validation and solution process.

> **Warfighter Challenge: "**USEUCOM and USAFRICOM require the capability to share essential information with interagency partners, Coalition and Alliance partners, or emerging partner nations in bi-lateral or multinational efforts. The capability gap is the result of: restrictive network access and information sharing policies; restrictive and cumbersome accreditation procedures for coalition networks and systems; lack of a coherent/unified strategy for a whole-of-government (to include foreign government) approach to an information sharing/collaborative environment; and resourcing to support that environment and its associated network enterprise services."[3]
>
> **The IMISAS Project Problem Statement:** "COCOMs lack a coherent framework/capability to share information and collaborate across multiple

[3] (Warfighter Challenge Submital, 2010)

domains with a broad range of mission partners (government/interagency, multi-national, multi-lateral & private sector) due primarily to restrictive policies, conflicting authorities, ad hoc/non-existent procedures, business rules and non-interoperable networks and systems."

1.3 IMISAS Project Problem Outcomes:

1.3.1 Original IMISAS Project Problem Outcomes

Outcome 1: Operational prototype that provides information sharing capability and environment to allow real-time collaboration across domains with multiple mission partners.

Outcome 2: Improved processes, procedures and enabling policies to establish an information sharing collaborative networked environment that can work across organizational and security boundaries for mission partners.

1.3.2 Revised IMISAS Project Problem Outcomes

Outcome 1: Inform the development of the 'To Be' Unclassified Information Sharing Capability (UISC) employing an Analytic Wargame focused on using/integrating available portal and cross domain technologies.

Outcome 2: Improved processes, procedures and enabling policies to establish an information sharing collaborative networked environment that can work across organizational and security boundaries for mission partners.

1.4 Underpinning Issues and Necessity of Addressing the Problem

Impediments to information sharing as defined in the IMISAS project problem statement fall into three major categories: technical, policy and procedure, and organizational culture.

On the technical side these issues can be further categorized into Cross domain restrictions and other domain issues, functionalities, and administration and hosting associated with information sharing on a public, collaborative enterprise. These considerations apply to Secure Internet Protocol Router Network (SIPRNET), Non-Secure Internet Protocol Router Network (NIPRNET) and the Internet.

Underpinning the enabling technologies are doctrine, policies and procedures which move from strategic intent to actionable solutions. It is clear that DOD embraces and is moving toward a broad strategy of Unclassified Information Sharing (UIS) that encompasses coordination and collaboration with a diverse and expanding community of both traditional and nontraditional mission partners.[4] The goal is to strike the appropriate balance between the legitimate need to protect sensitive, proprietary or classified information while enabling efficient exchange of unclassified information. While technical, policy and procedural issues are formidable in themselves, it is the diversity of organizational cultures both within the DOD and across the whole of USG and community of potential mission partners that makes information sharing a most challenging proposition. It is not beyond the pale to presume in many cases that the role of DOD may be relegated to simply provisioning an UIS portal and pushing information to support other agencies with authority and charter for the mission at hand. In these cases, the UISC will be judged by its ability to accommodate others beyond the DOD ambit.

1.4.1 Technical Issues

Major challenges in the technical arena are in balancing requirements for information sharing, information security, and information assurance (authenticity, authentication, availability, non-repudiation, integrity, and confidentiality), implementing ergonomically simple user interfaces, and establishing "a least common denominator" architecture.

The effectiveness and timeliness of information transfer among networks having differing security classifications, access credentials, or other discriminating criteria heavily impacts the effectiveness of interaction between COCOMs and the broader HA/DR response base. The average internet experience is one of open or minimally conditioned access to e-mail, chat, multi-media applications, secure banking and commerce, and a vast array of other applications and information. Access to these networks usually only requires the user to outlay a requisite amount of personally identifiable information (PII) and to accept the provider's terms of use and applicable guarantees of privacy or security. In contrast, access to classified networks and many governmental networks protected by public key infrastructure (PKI) is inherently restricted to those with both need to know and appropriate credentials, which could include a successful background security investigation.

---

[4] (CJCS, Doctrine for Joint Urban Operations, 2009), (CJCS, Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations), (ASD-NII/CIO, 2009), (UISC CONOPS, 2010)

"Cross domain" transfers of information between these two types of networks, and between networks of different classification levels, involve verification checks on releasability of the information to the target domain. For transfers from a higher classification network to a lower classification network, for example, verification usually entails human-in-the-loop guard technology with several layers of adjudication. Automation of the process may accelerate the information flow, but risk of inadvertent disclosure may be increased, and the range of delivered information may have to be restricted. Notwithstanding these issues, USEUCOM and other COCOMs have warfighting responsibilities that place the majority of their workload on classified networks and create significant necessity for cross domain transfers during multi-phase operations.

The network connection itself may pose information security risks, as illustrated by the prospect of allowing social media feeds, with their multiplicity of security vulnerabilities, inside the boundaries of a protected network. Added to these difficulties are variations in the information assurance mechanisms employed by other HA/DR responders. The DOD certifies and accredits its information systems through a risk-assessed, department-wide configuration control and management process framed by a standards of information assurance controls.[5] Corporations and other U.S. government domains protect information within their respective organizations' rule sets. One organization's metric for authenticity of information gleaned from the open internet, for example, may simply be the number of "friends" a site hosts or the number of "hits" a particular feed receives, while others require the source itself to authenticate on their network. The issue of authentication requirements on government networks is troublesome for some HA/DR responders, who have concerns about the perception of being co-opted or otherwise having compromised their charter requirements for impartiality.

Many NGOs and Private Voluntary Organizations (PVOs) prefer to work on the open internet either because of internal resource limitations, or simply because the available applications are well developed, agile, and widely known. Private enterprise and open architecture standards combine to accelerate incorporation of user feedback and convergence to stable, popular application forms. A key technical challenge for the DOD is to provide a platform that delivers user-friendliness on the same order of popular social media sites, for example, while remaining within information security and information assurance risk boundaries.

From the perspective of infrastructure, the degree of maturity encountered from one HA/DR operation to another can be quite diverse. Haiti's telecommunications capability,

[5] (ASD-NII/CIO, DoD Instruction 8510.01, 2007)

for example, is heavily skewed toward cellular and satellite capability, with landline services nearly absent. A significant expanse of potential HA/DR response zones have almost no telecommunications infrastructure. Technical challenges include identifying the minimal connection capability and providing that level of service during the earliest phases of response. Even in relatively developed areas, the UISC technical infrastructure can be topologically frail if server or route redundancy is lacking.

1.4.2 Policy and Procedures

Policy may be composed of executive orders, regulations, instructions, and other forms of guidance that establish rules or standards to guide decisions and achieve rational outcomes. Review and modification of policy will be critical to employing new information sharing capability supporting planning and execution across the spectrum of operations.

Current information sharing and information assurance policies are not applied uniformly across DOD network domains among the various commands. Information assurance policy has evolved steadily to protect network domain enclaves during a long history of cyber attacks and unauthorized release of sensitive data. Although policy for information assurance is mature, its interpretation by network domain managers is not. This is due to accountability assigned to the Designated Approval Authority (DAA) at individual network domains. DAAs assume degrees of risk that vary from domain to domain. This contributes to variations in policy implementation, often based on personalities and specific operational requirements. DOD Services and Agencies often add layers of policy interpretation that further influence domain DAAs. Information sharing requirements with partners external to DOD are becoming increasingly essential. This evolution of external DOD information sharing is challenging domain DAAs to assume higher risks thereby creating more restrictive requirements to protect local domains.

Information sharing procedures vary widely from command to command. There are DOD commands that have current, detailed procedures offering guidance on information management and information sharing. Unfortunately, this is the exception and many commands rely on ad hoc procedures to govern information sharing. Some commands have information sharing procedures that only cover specific missions or situations and not the full range of missions and mission partners.

1.4.3 Culture

There is an increasing need for DOD to cooperate, support, and partner with organizations external to itself (e.g., U.S. departments and agencies, foreign governments and militaries, and non-military partners). The role of the U.S. military is trending from

exclusive mission leadership to routine support of various mission scenarios. To participate in a supporting role, an understanding of organizational culture by the DOD is necessary to achieve timely and relevant information sharing with new and diverse organizations.

Speaking at the 13-14 October 2010 Partnership Engagement Conference at the Office of the Director of National Intelligence, Dr. Andrew Natsios of Georgetown University enumerated five "clashes of development, defense, and democracy" and four key challenges affecting information sharing and coordination between the U.S. national security establishment and the greater body of organizations involved in HA/DR operations.

Illustrative examples of clashes are conflicts arising from mission and culture differences, disparate operational systems and implementation mechanisms, variability in the organization of linkages, and shortfalls in establishment interoperability. Part of the DOS's public diplomacy mission is to ensure the U.S.'s role in offering humanitarian assistance is clearly explained to the larger international audience. The charter of the United States Agency for International Development (USAID) is similar to that of the European Community Humanitarian Office (ECHO) and United Nations (UN) humanitarian relief "clusters". Along with its capabilities to provide immediate humanitarian assistance, USAID maintains a focus on long-term rebuilding and development programs and processes. This split focus can sometimes create the appearance of friction with NGOs, who generally maintain a much shorter-term relief perspective.

A long standing point of difficulty is the organizational structure mismatch among responding agencies. For illustration, a key military concern is to know who among the NGOs is in command of an operation or at least providing coordination for a group of NGOs. This is problematic, as a formal command hierarchy is typically absent in these organizations, which operate through lose federations of physical and social networks. It is a major point of contention with NGOs to have some kind of quasi-military command structure imposed upon them. In this case, the military could create significant political backlash by precipitating its command structure on civilian partners without careful deliberation and legitimate justification for the requirement.

The wide span of responding organizations, and their disparate sets of constraints and agendas, creates both excesses and deficits in information flow. Vast amounts of data are generated during an HA/DR operation, much of it unorganized by criticality or target audience; however, information is also hoarded by organizations who seek to garner individual visibility. Rigorous information management and leveraging of group dynamic skill sets are keenly needed to overcome the organizational barriers to information

sharing arising from resource and reward competition, NGO requirements for impartiality and non-alignment, differences in organizational communication structure, and sensitivities to military presence where the potential for reprisal against responders exists.

1.4.4 Knowledge Management

Knowledge Management (KM) is a unifying construct for information sharing, as it enfolds the technological, social, and cultural dimensions to information sharing. KM is frequently perceived in the limited context of technology solutions and information management, however, it more correctly addresses all impediments to the building and transfer of knowledge, for which technology is only a tool and information management a sub-process. One definition of KM is "the integration of people and processes, enabled by technology, to facilitate the exchange of operationally relevant information and expertise to increase organizational performance".[6] Importantly, this definition specifies the role of KM in bridging organizational boundaries to link tacit and explicit knowledge domains. Alternatively, the U.S. Army's KM program stresses the user-centricity of KM, pointing out that users rather than information technology providers own collaborative communities.[7] It cites the need to protect and secure the information flow among these communities, and also points out the necessity of standardization vehicles such as single sign-on capability. One of the Army's goals for KM is to adopt governance and cultural changes to become a knowledge-based organization. The cultural imperative is echoed in the U.S. Air Force's charter for its Air Force Knowledge Now initiative, which has had a better track record for knowledge sharing than many other technology-centric KM methodologies owing to its focus on social, behavioral and cultural elements[8]. The DOS stresses a holistic approach to KM as well, referring to its program as *Knowledge Leadership*, and again noting the importance of "self-forming, self-managing online communities for collaboration across geographic and organizational boundaries".[9] Moreover, as cited in a 2009 paper presented to North Atlantic Treaty Organization (NATO) Information Systems and Technology Panel Symposium, maintaining the operational relevance of KM solutions requires that organizations innovate and adapt their "organizational DNA" during natural, economical and security crises[10]. KM is a concern of NGOs as well; Save the Children is currently running a job announcement for

---

[6] (Department of the Navy Chief Information Officer, 2005)
[7] (Secretary of the Army, 2008)
[8] (Wikipedia contributors, 2010)
[9] (Department of State)
[10] (Ariely, 2009)

a Knowledge Manager, albeit with a focus seemingly limited to managing an affordable, industry standard IT solution aligned with its charter[11].

A critical challenge of KM in the context of information sharing is to overcome organizational culture impediments among a variety of organizational types. A long standing point of friction between the DOD and many NGOs, for example, is the latter's strict avoidance of interactions that create the perception that they are serving as instruments of the military. The most innocuous association with the DOD may be sufficient, in some situations, to cause NGOs to fear retaliation by hostile local actors. Clearly, a technological solution by itself will be ineffective in such situations; however, a combination of adroit executive engagement identifying the "win-win" space and mechanisms in the technological domain to ensure confidentiality or anonymity, may induce the flow of information in these channels. More generally, the technological solution should accommodate the range of legal, policy and operational restrictions among organizations through mechanisms that appropriately limit visibility and accessibility of information among users.

The organization of information is also a primary concern. The cascade of information flowing into the 22nd and 24th Marine Expeditionary Units during the recent Haiti earthquake relief efforts, for example, was vast and of widely varying reliability, nearly overwhelming the responders' ability to vet the sources and review the data. In that context, key KM enablers would have included: federated search capability; codified rules for staging, reviewing, archiving and verifying sources of information; ease of visibility and access of information; understandability of the information organization construct; and accommodation streams from a wide array of sources.

Finally, the innate transience of military manning places a premium on the capture of activity history and lessons learned. As military personnel are rotated into new positions and locations, their knowledge must be systematically and thoroughly captured and incorporated into training and lessons learned. This activity is a challenge with the military internally notwithstanding external organizations. If post-event capture of activity history or lessons is rushed or carelessly administered, the products may be poorly organized masses of information or simple enumerations of complaints with no suggestions for improvement – products of little use to subsequent responders. The challenges here are in codifying standard formats for capturing activity history and energizing the lessons learned process so that all lessons are firmly internalized.

[11] (IT/Knowledge Management Officer wanted at Save The Children)

2.0 Scope and Limitations

The original IMISAS project objectives were very broad in scope as initially envisioned under the IMISAS project problem statement. Continuing engagement between stakeholders and the broader community of interest has served to shape, focus, clarify and narrow objectives so that expected outcomes fall within a manageable scope in terms of project resources, schedule and acceptable risk. Objectives and outcomes have been socialized with stakeholders as well as the community of interest since September 2010 and vetted at the USEUCOM and USAFRICOM site visit, and the Stakeholders Conference. These decisions and agreements matured the collective understanding of the project's scope, objectives, and outcomes, and consequently informed and narrowed the breadth of this baseline assessment. Additional constraints, limitations and assumptions are further addressed in section 5.1.

2.1 Significant Project Influences

The most important events and decisions that broadly inform the IMISAS project are:

1. The release of the UISC CONOPS explicitly defining and scoping the boundaries of an envisioned 'To Be' DOD UISC.[12]

2. Joint Staff J6 endorsement of All Partner Access Network (APAN) as the initial capability for the Department of Defense's Unclassified Information-Sharing Service (UIS) for support to Stability Operations, Humanitarian Assistance/Disaster Relief, Theater Security Cooperation, and other civil-military missions.[13]

3. Replacing the IMISAS project objective of developing a prototype solution with an Analytic Wargame (AWG) focused on using available technologies to inform the development of the 'To Be' UISC.[14]

4. Agreement that the products associated with the IMISAS project are a handbook, technical enhancement recommendations, and policy/procedure recommendations.

5. Agreement that the AWG will focus on HA/DR operations and associated scenario(s) for experimentation and assessment.

---

[12] (UISC CONOPS, 2010)
[13] (Endosorment of All Partners Access Network, 2010)
[14] IPR November 8, 2010

Incorporating these assumptions into the IMISAS project design leads to a viable "way ahead" and a more specific and focused set of objectives and project products.

2.2 Revised Objectives Overview:

The revised objectives are:

1. Examine how the DOD can better work with and engage USG agencies internally and how to provide and share information with a range of global partners including IOs, NGOs and private organizations for HA/DR operations.

2. Examine policy and recommend changes to facilitate information sharing with a range of partners in an HA/DR environment.

3. Using UIS/APAN/Transnational Information Sharing Cooperation (TISC) capability as the technical proxy for the IMISAS project, conduct an AWG to examine APAN enhancement recommendations previously identified, focusing on those that will align with the capability gaps expressed in the USEUCOM/USAFRICOM warfighter challenge submission.

4. Examine potential security cross domain solutions for unclassified information during the period of the project.

2.3 Revised Products:

The revised products are:

1. Handbook for Unclassified Information Sharing

2. Experimentally validated recommendations for changes to facilitate information sharing with a range of partners (US interagency, coalition, NGO, IO):

- Doctrine
- Policy / Procedures
- Enhancements to UIS platform capabilities

3. Architecture mapping (OVs and SVs)

3.0 Problem Decomposition

This section examines and decomposes the IMISAS Project Problem Statement into the explicit and implicit objectives and outcomes of the evolved IMISAS project.

Figure E-1 is a top-level representation of the original problem statement and flow down of current objectives.

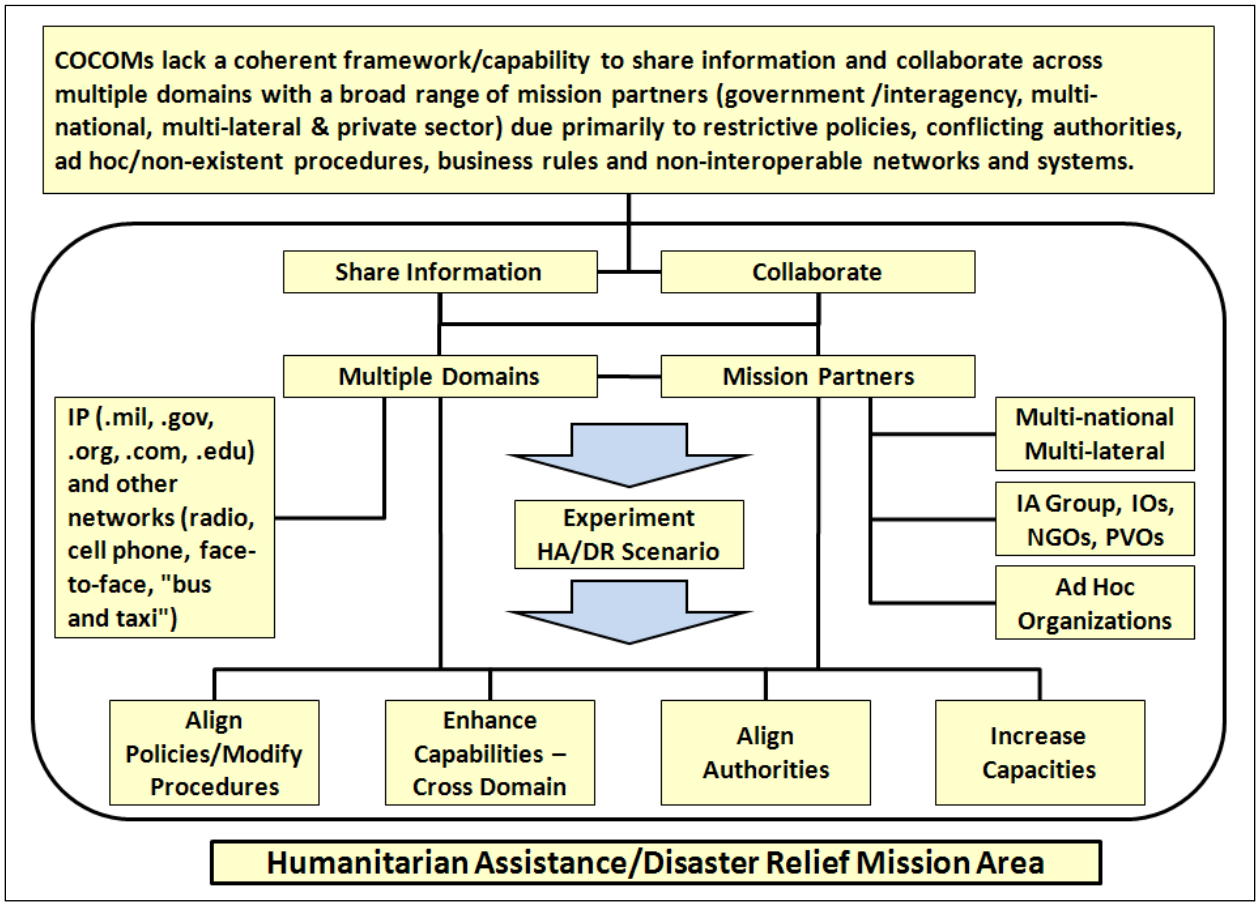


Figure E-1 – Problem Decomposition

The starting point for decomposing the problem is recognition of the primary stakeholders, specifically USEUCOM and USAFRICOM, who posed the initial Warfighter Challenge submission and represent sponsorship for the effort. Additional stakeholders include: Assistant Secretary of Defense Network Information and Integration (ASD NII), Defense Information Systems Agency (DISA), Joint Staff J6, USJFCOM and the USPACOM APAN team.

As the project has matured, US civilian interagency participants, such as the US Department of State and the US Agency for International Development, have indicated interest in participating in the project. In addition, the NATO Allied Command Transformation (ACT) and the German Bundeswehr Transformation Command are contributing to the effort. USAFRICOM and USEUCOM have stated their intent to approach several international organizations and non-governmental organizations to determine their interest in observing or participating in the experimental event as role players.

A third group, collectively referred to as the Community of Interest (COI) (Figure E-2) represents the broad domain of potential mission partners referred to in the problem statement. Continuing engagement between stakeholders, partners, the project team and the broader COI throughout the project planning, development and execution cycle remains a key enabler to project definition, refinement, outreach and eventual success.

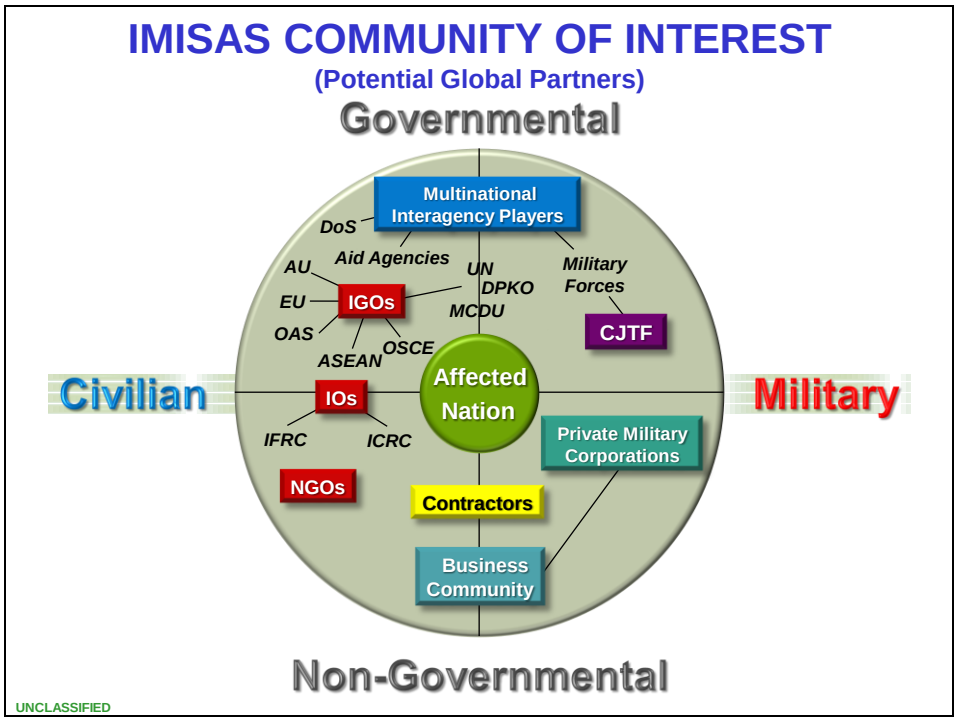


Figure E-2 – Community of Interest

Further inspection of the project statement identifies the top level requirement: DOD/Combatant Command (COCOM) capability to share information and collaborate across multiple domains with a potentially global set of both enduring and ad hoc mission partners. Also identified are shortfalls or gaps in authority, capability and/or capacity (restrictive policies, conflicting authority and jurisdiction, procedures and non-

interoperable networks and systems) that currently degrade the ability to share information and collaborate. The elaboration of both explicit and implicit capability requirements stemming from this broad capability requirement establishes a basis for further refinement of requirements and decomposition of existing capability gaps.

The process of discovery and engagement with stakeholders, partners and the COI continues to shape and scope this effort as discussed in section 3. The two expected outcomes and underpinning current objectives are outlined below.

Outcome 1:

Improved processes, procedures and enabling policies to establish an information sharing collaborative networked environment that can work across organizational and security boundaries for mission partners.

Objectives:

1.1: Develop an operating concept based on the UISC CONOPS to include processes, procedures, and an organizational construct reflecting required roles, responsibilities, authorities and policies.

1.2: Develop and verify operationally focused processes and procedures required to implement information sharing and collaboration for HA/DR operations.

1.3: Examine policy and recommend changes to facilitate information sharing with a range of partners in a HA/DR environment.

1.4: Define and design an experiment employing an HA/DR scenario to validate information sharing and collaboration capability enhancements and policy and procedure variables addressing capability gaps.

1.5: Develop a handbook and experimentally validated doctrine change recommendations addressing how the DOD can better engage other USG bodies and share information with IO/NGO/private partners in support of HA/DR.

Outcome 2:

Inform the development of the ‘To Be’ UISC employing a Analytic Wargame focused on using/integrating available portal and cross domain procedures.

Objectives:

2.1: Identify requirements and potential operational solutions and technical enhancements using UIS APAN as the technical backbone for experimentation.

2.2: Conduct user validation of the UIS/APAN TISC capability to inform development of the ‘To Be’ UISC.

The high level concept model of the information sharing environment which will shape the Analytic Wargame is provided in Figure E-3 below. The definition of the IMISAS project baseline in terms of the expanded list of required capabilities (requirements stemming from the problem statement) and gaps is described in section 5.2. The associated capability cross-walk is provided in Appendix 4.

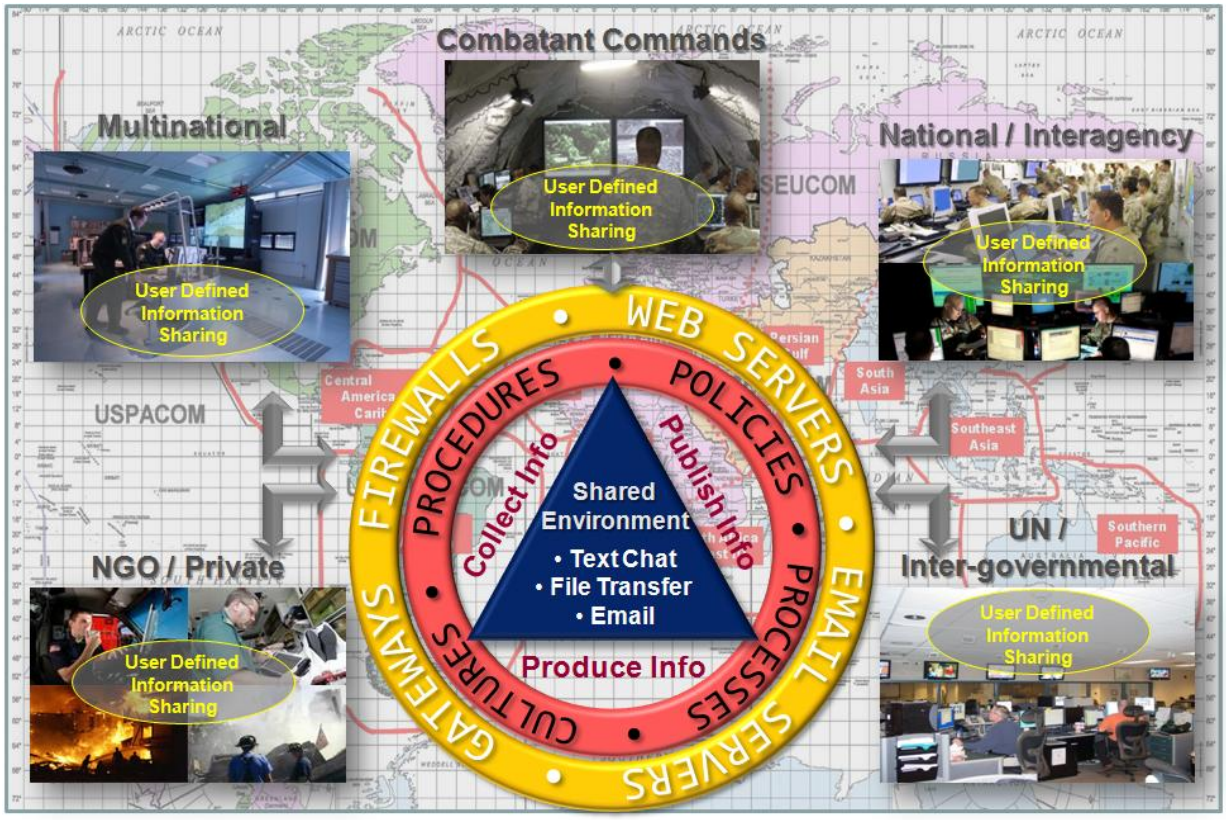


Figure E-3 – IMISAS Project Concept

4.0 Research Methodology

4.1 Research Schema

The schema for conducting the baseline assessment followed the approach outlined in USJFCOM BAR Guidelines.[15] Some latitude was taken with respect to the guidelines' sequence of activities in order to accommodate schedule constraints that necessitated parallel and spiral activities, particularly the brevity of the interlude between the USEUCOM/USAFRICOM site visit and the IMISAS Stakeholders/Gap Validation Conference where requirements and gaps were refined and validated and potential solutions identified. Coincident with the USEUCOM/USAFRICOM site visit, project focus underwent a major shift from the objective of delivering an operational prototype to focusing on UISC enhancements utilizing APAN as a proxy. Subsequently, a Process Documentation Event (PDE) (28-31 March 2011) was conducted as an additional USEUCOM/USAFRICOM site visit to further refine the 'As Is' information sharing processes. (The results of the PDE are detailed in Appendix 13.)

The general methodology and associated necessary activities leading to the baseline assessment consist of discovery (including requirement definition), assessment of discovery and validation (capability cross-walk), gap identification and alignment, assessment of gaps with respect to scope and viability of experimentation, gap prioritization, identification of potential solutions and associated risk assessment and recommendations.

Figure E-4 provides a temporal snapshot of the Analytic Framework (the nominal and expected level of activities, efforts and associated major analytical products relative to significant project events) just prior to the Stakeholders/Gap Validation Conference. Updated and detailed activities, milestones and deliverables are contained in the IMISAS Project Microsoft Project Work Breakdown Schedule available on USJFCOM J9 IMISAS Project Portal. An alternative visualization focusing on process rather than activity levels and schedule is depicted in Figure E-5.

[16] (Guidelines for Conducting A Baseline Assessment, 2010)

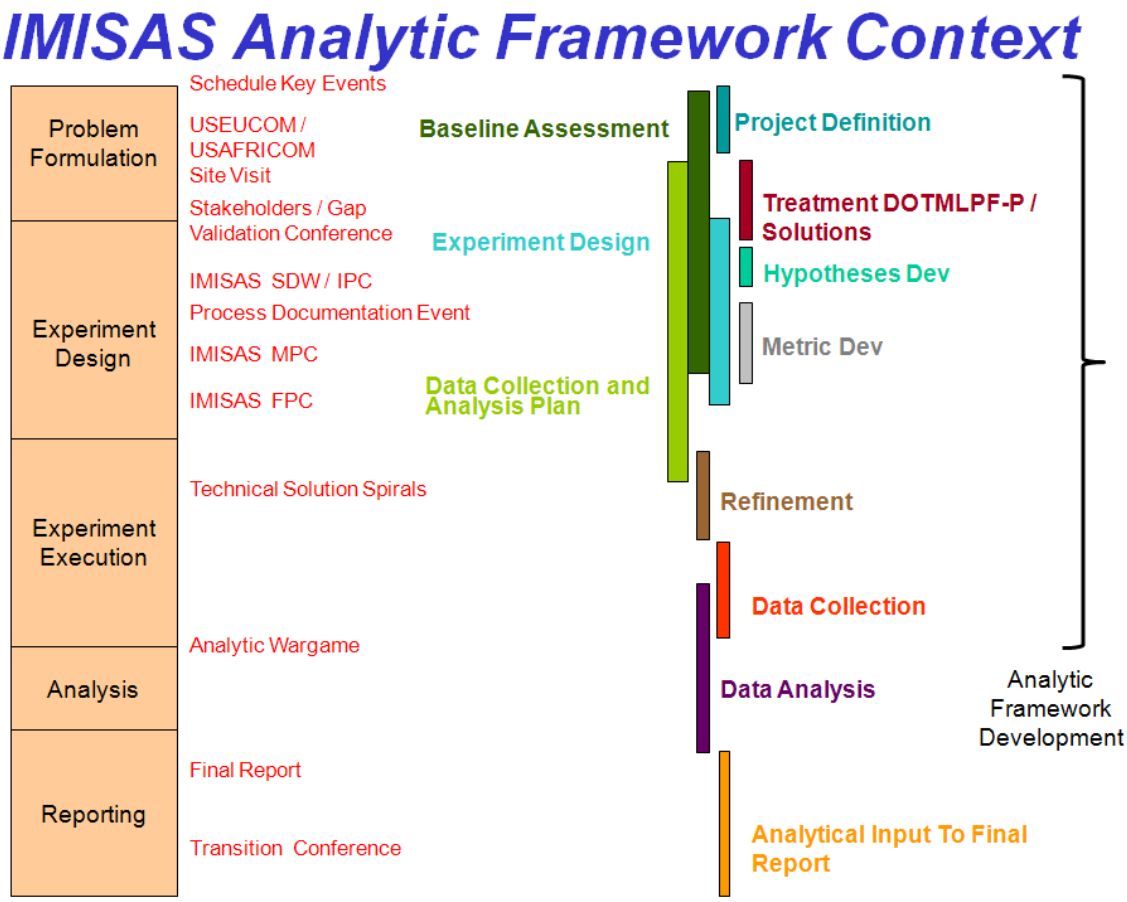


Figure E-4 – Analytic Framework

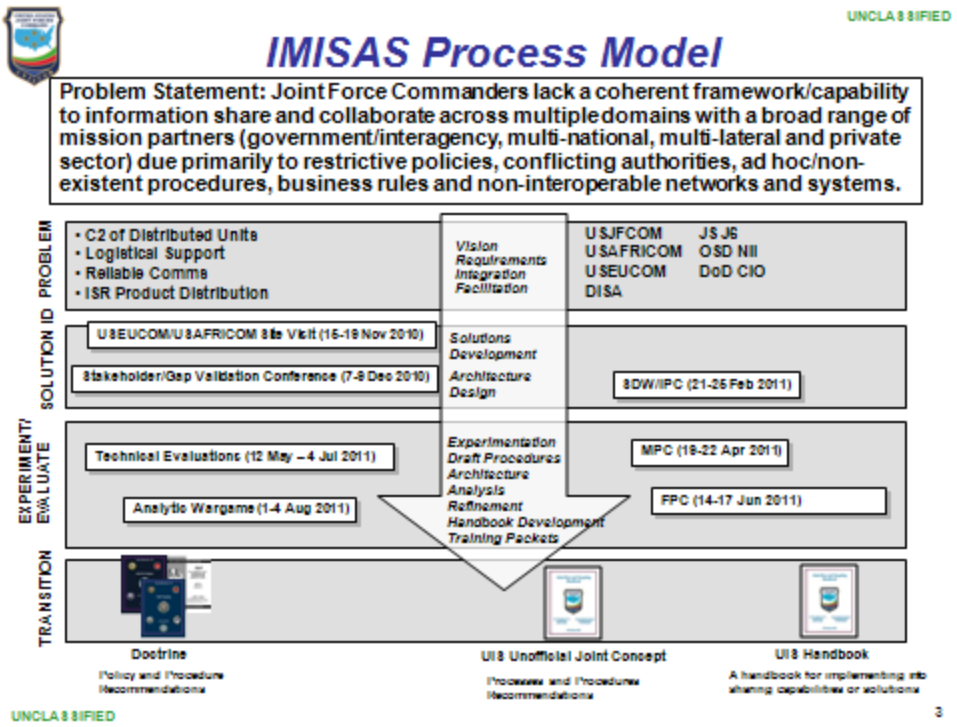


Figure E-5 – IMISAS Project Process Model

4.2 Discovery

The IMISAS project team conducted the initial discovery phase during the first wo months of the project. These activities included:

- an extensive literature review,
- meeting and conference attendance,
- Defense Connect Online sessions and telephone conferences with partners and the Community of Interest,
- telephone interviews with the Community of Interest (Appendix 5),
- the USEUCOM/USAFRICOM site visit, and
- the Stakeholders/Gap Validation Conference.

Discovery continued with a Process Documentation Event (PDE) which occurred after the Solution Development Workshop (SDW). The IMISAS team conducted a 4-day PDE with USAFRICOM and USEUCOM in Stuttgart, Germany. The IMISAS project will develop an operational construct that offers an enhanced information sharing capability across multiple domains and mission partners, by providing recommendations for improved processes, procedures and enabling policies in order to establish a collaborative environment that can promote unclassified information sharing across organizational

boundaries. The purpose of this event was to further document the 'As Is' information sharing architecture in sufficient detail to support the IMISAS AWG.

The team conducted a total of 28 interviews over the four-day period. At USEUCOM, the interviewees included Ambassador Katherine Canavan and Operations Planning Team representatives from ECJ35, ECJ32, ECJ5, ECJ6, ECJ4 JLOC, ECJ9, ECJ8, and Defense Information Systems Agency (DISA) Europe. At USAFRICOM, the interviewees included the Political Advisor, Dr. Raymond Brown, and interagency representatives from the Department of State, USAID and the Department of Commerce. The team also interviewed representatives from the USAFRICOM Foreign Disclosure Office (FDO), Special Security Office (SSO), the Knowledge Management office, J3, J4, J5, J9, and the Canadian Liaison Officer (LNO).

The team met all objectives of the visit. Support from USEUCOM and USAFRICOM was excellent; the AOs coordinated with participating directorates, codes, and LNOs to schedule interviews. Additionally, site visits and walk-through's for the anticipated venues to house the Final Planning Conference (FPC) and AWG locations were conducted. Team members were also able to gather key insights and lessons learned by observing exercise X24-Europe, a USEUCOM sponsored exercise integrating social media in an unclassified information sharing HA/DR environment.

The interviews that were conducted had captured current policies, processes and procedures for information sharing for the purpose of defining the 'As Is' information sharing architecture for the IMISAS project. The focus was on Unclassified Information Sharing (UIS) in a permissive HA/DR context, for which the COCOM (and Joint Task Force (JTF) when activated) is in a supporting role within the U.S. whole-of-government comprehensive approach. The temporal scope of consideration was from the Joint Planning Team/Operational Planning Team (JPT/OPT) establishment through the transition to JTF operations to achieve a steady state operations within a JTF. From a command perspective, the events of interest included all key COCOM (or JTF) interactions from the highest level down to the operational/tactical interface. Excluded were interactions from other organizations other than those made directly from the COCOM or JTF. Consideration was limited to major mission components only, focusing on current practices in UIS and on DOD capabilities routinely used during HA/DR operations, rather than on planning itself.

In the course of discovery approximately three hundred documents were reviewed. One hundred and forty-one documents were identified and tagged for further assessment and evaluation. A listing and assessment of those documents most pertinent to the baseline assessment and the project as a whole are consolidated in the Source Review Spreadsheet (Appendix 4). The Source Review Spreadsheet along with the aforementioned discovery

initiatives provide the basis for discovery and discovery assessment leading to identification and evaluation of requirements, gaps and potential solutions. Figure E-6 illustrates the Source Review Spreadsheet.

	JCA									Gap				DOTMLPF								
Document	Force Support	Battlespace Awareness	Force Application	Logistics	Command and Control	Net-Centric	Protection	Building Partnerships	Corporate Management and Support	Policy	Procedure	Technical	Cultural	Doctrine	Organization	Training	Materiel	Leadership	Personnel	Facilities	Priority (1 -5) (1 = highest)
15th International Command and Control Research and Technology Symposium (ICCRTS) Paper 001 ("On Facilitating Stability Operations: A Net-Centric, Federated Approach to Information Sharing")								X		X		X		X							5
2010 UIS CONOPS	X											X									4
A Snapshot of Emerging U.S. Government Civilian Capabilities to Support Foreign Reconstruction and Stabilizations Contingencies (Institute for Defense Analysis (IDA) May, 2006)					X										X				X		4
All Partners Access Network (APAN)/Transnational Information Sharing Cooperation (TISC) (Information Paper)												X									2
Always On - Preparing for the Next Engagement. Warren Suss, Government Computer News						X						X									2
Annex D to - Campaign Experiment Design Document: Cooperative Implementation Planning, Management and Evaluation (CIP/CIME) Major Integrating Event				X	X	X					X	X	X		X			X	X		3
APAN Capabilities						X						X					X				3
APAN TISC Information Slideshow												X									2
APAN User Manual Jun 09												X									2
ASD-NII Memorandum: Department of Defense (DoD) Enterprise Unclassified Information Sharing Service	X				X					X			X	X							2
ASD-NII Project Paper: Required Capabilities for HARMONIE												X									2

Figure E-6 – Source Review Spreadsheet Illustration

4.3 Gap Analysis

The gap analysis process employed by the IMISAS project follows the approach as outlined in USJFCOM BAR Guidelines. The general schema is depicted in Figure E-7. The process begins with enumeration of capabilities supporting stakeholder and partner requirements. That list is then evaluated against existing current joint capabilities to determine the existence of gaps. Gaps are decomposed by individual DOTMLPF-P areas and characterized as capability, capacity, or authority shortfalls. The requirements have been previously cross walked against the Universal Joint Task List and Joint Capabilities Areas.

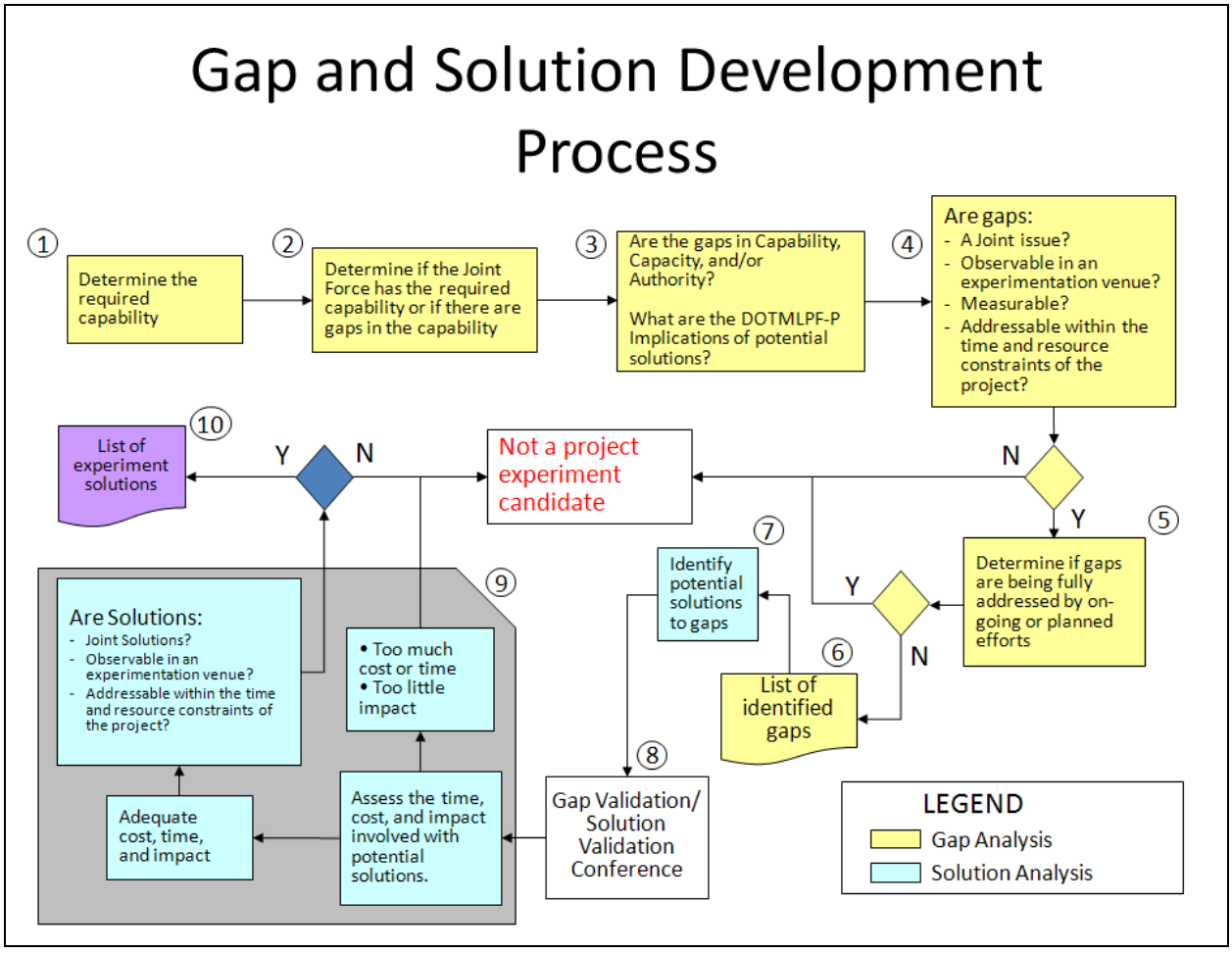


Figure E-7 – Gap and Solution Development Process

This process facilitates methodologies for grouping and prioritizing the gaps, removes ambiguities, and delineates the boundaries of the baseline assessment by ensuring key gaps are not overlooked, that nominated gaps have applicability to joint needs, and that the set of mitigation resources and authorities is defined.

Excluded from further consideration are those gaps already being addressed in ongoing or planned efforts by the services, industry, academia, or other government agencies, and gaps that are neither joint issues, experimentally observable, measurable or within project allocated resources (including time). Experimental partnerships should be considered for any gaps being addressed only partially.

Potential solutions are evaluated in terms of gap mitigating strategies by DOTMLPF-P area, projected sufficiency and effectiveness of incremental improvements, potential change agent(s)/organization(s), time to deliver the solution to the warfighter, cost of the complete solution, methods to determine value added, and potential sponsors for solution

implementation and risk. Those solutions whose projected value added (positive impact) are not justified in terms of cost, time, or other project resource constraints are excluded from further consideration, as are those solutions not having joint applicability or not observable in an experimentation venue (wargame, seminar, or AWG). The feasible set of solutions is then submitted to the Experiment Design Project Lead for development.

4.3.1 IMISAS Project Assessment Tool

Data (nominated solutions and rankings for requirements and gaps) from the Stakeholders/Gap Validation Conference were compiled and evaluated against correspondence tables specifying the many-to-many relationships among requirements and gaps, and gaps and solutions. These data and calculations are contained within a single spreadsheet, the IMISAS Project Assessment Tool, whose final product is an initial ranked set of potential solutions for further development and experimentation. A detailed discussion of the structure and calculations performed by the Assessment Tool is contained in Appendix 7.

5.0 Assessment Summary

5.1 Context, Constraints, Limitations, and Assumptions

Although the primary stakeholders are USAFRICOM and USEUCOM, the solutions examined in the IMISAS project will provide an UISC and a body of policy and procedure recommendations useful to the broader COI. The capability will be applicable to phase zero steady state operations as well as to contingency and crisis action planning and operations. Initial constraints identified are the following:

1. The project timeline is one year.
2. The solutions will conform to the following high level requirement documents:
   a. DOD Information Sharing Implementation Plan
   b. DOD Information Sharing Strategy
   c. National Institute of Standards and Technology. FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors.
   d. DOD Information Assurance and Certification Process (DIACAP) DOD 8510.01C
   e. National Security Presidential Directive – 1(NSPD-1)
   f. Homeland Security Presidential Directive. HSPD-12 Policy for Common Identification Standard for Federal Employees and Contractors. August 27, 2004.
   g. Under Secretary of Defense for Intelligence. Use of the "Not Releasable to Foreign Nationals" (NOFORN) Caveat on DOD Information May 17, 2005.
   h. Office of the Director of national Intelligence Community Policy Memorandum Number 2007-500-1. Unevaluated Domestic Threat Tearline Reports. November 19. 2007.
3. The solution is assumed to incorporate the UISC Concept of Operations (CONOPS) with the TISC Joint Capability Technology Demonstration (JCTD). This capability is proposed for implementation at DISAs) Defense Enterprise Computing Center Europe (DECC) facility as the core technical solution, although adjunct capabilities and processes will be considered in the analysis.
4. Software associated with the TISC JCTD will not be modified in support of this project.

5. Initial limitations identified are:
    a. Exploration of cultural interaction will be limited to organizational culture rather than social culture in the broader sense, although human factors as it influences information sharing will be considered in the analysis.
    b. Because the larger COI can be comprised of a variety of contributing organizations, the IMISAS project will work with select groups from the major categories (interagency, non-governmental, etc.) who may represent the issues and requirements of the larger COI.
6. Initial assumptions identified are:
    a. Doctrinal
        i. The doctrinal component of the solutions are limited to recommendations to DOD policy, within direct influence on interagency, non-governmental, and transnational policies
    b. Operational
        i. Solution is required to support collaboration during phase zero as well as contingency and crisis action planning and operations
            1. The solution needs to be applicable to alliances, coalitions, supported/supporting relationships, and ad-hoc partnerships
                a. DOD and interagency groups may be relegated to support roles
    c. Technical
        i. Solution must be DOD enterprise compliant
            1. The enterprise requirements have been vetted and approved
            2. Solution set must be DIACAP compliant
            3. The technical solution should have the look and feel of a .ORG rather than a .MIL product
            4. The solution content will contain only unclassified or non-classified information (However, the solution shall accommodate the transfer of unclassified information from a higher classification network)
            5. Cross domain information sharing of unclassified information from DOD to open internet is implied

5.2 Current Baseline

In examining the literature, previous studies, related experimentation having conducted a site visit and the Stakeholders/Gap Validation Conference several important observations are relevant to set the scene for the baseline.

First, a validated UIS Implementation Plan and a UISC CONOPS have been promulgated. These documents, among others, provide the necessary framework to support UIS across a spectrum of operations in terms of DOD Policy and a broad-based authority. They also acknowledge and embrace the importance and benefits of sharing information with both enduring mission partners and ad hoc potential participants. Similar guidance at the National Policy Level support information sharing within a "whole-of-government" context and approach. What these documents do not do is provide details, the "how to" for accomplishing UIS at the operational level.

Second, any consideration of an enterprise solution other than APAN appears moot. APAN was nominated as a Program of Record under Program Objective Memorandum 12 and there is neither penchant nor resources to fund multiple programs targeting similar objectives. While capabilities such as HARMONIEWeb will be migrated to the DISA DECC and continue to receive DOD resources in the near-term to preclude interruption of critical services for ongoing operations, the DOD long-term strategy looks toward integrating and federating capabilities within the APAN environment.

DiscussionsThere are ongoing discussions and deliberations (philosophical, political, programmatic and technical) are on going concerning the location to ultimately host APAN. Early momentum signals that APAN will be hosted by DISA. It is still to be determined how APAN would best be served, whether on the DISA DECC or a commercial location managed by DISA.

Third, concerns about the scalability of an UISC to meet the demands of potential subscribers needed to support both steady state and contingency operations should be mollified with the decision to accept APAN as a consideration for a DOD UISC solution. As the program matures with potentially hundreds of thousands of DOD subscribers alone, the flexibility of the program to shift and flex resources temporally to accommodate changing mission requirements appears executable and sustainable.

Fourth, the overarching DOD UIS architecture and how UISC aligns and is integrated with enclave systems supporting multiple levels of classification is currently at the Operational View (OV) -1 level of maturity. Precisely how UISC will be engineered and integrated into existing and future structures is less clearly articulated.

Stepping back from the broader DOD umbrella and focusing on the specific requirements and gaps for the COCOMs and JTFs specifically those of USEUCOM and

USAFRICOM, provides an UISC option for a more manageable domain to assess baseline capabilities. However, while similarities exist in capabilities and needs, the striking diversity in geography, infrastructure, cultures, ethnicities, languages and histories between Europe and Africa makes formalizing a single 'As Is' capability challenging.

To suggest that these commands do not have the authority, capability or capacity to operate within an UIS environment now is simply inaccurate; that significant shortfalls exist and if remedied would improve the effectiveness of operations seems uncontested.

On the UIS side of the technical communications equation, both COCOMs can connect to APAN specifically and the internet generally, thereby reaching a potentially vast domain of mission partners. Communication infrastructure is robust in Europe, however, there is a large variance of capability in Africa. The International Telecommunications Union has set the goal to connect African cities and villages by 2015. Many users have the Simple Messaging System (SMS) capability, but in general, they do not have internet connectivity. The active number of mobile subscriptions in Africa reached 506 million in September 2010, but only 12 million with broadband capability. In a large part of East Africa there is still a lack of connection of African cities to the internet backbone other than through satellite.

USEUCOM and USAFRICOM operations centers operate differently in their reliance on classified versus unclassified communications and information sharing systems. USEUCOM's Joint Operations Center (JOC) works on SIPRNET while USAFRICOM utilizes both SIPRNET and NIPRNET. USEUCOM's reliance on SIPRNET places a premium on provisioning a cross domain solution to the internet via NIPRNET. Guard technologies exist to accommodate high-low-high information flow, but no current automated capability exists at either command. Additionally, the complexity and ambiguities of release authority, the current classification marking systems and caveats, and over-classification of documents poses significant hurdles to efficiently implement automation across the spectrum of communication venues envisioned to enhance sharing and collaboration with potential partners connected through the internet.

APAN functionalities available currently to USEUCOM and USAFRICOM fall short in several critical technical areas: User Defined Operational Picture, geospatial situational awareness, identity management, source vetting and multilingual capabilities. To gain a sense of the scale of the problem, there are an estimated 2000 languages spoken in Africa in several linguistic families: Afro-asiatic, Nilo-Saharan, Niger-Congo, Khoe, Austronesian and Indo-European. About 100 of the languages of Africa are used for inter-ethnic communication: Berber, Arabic, Igbo, Swahili, Hausa, Amharic, and Yoruba.

If similar languages are counted together about 15 are spoken by 85% of the population, but Nigeria alone has over 250 languages.

During the PDE both USEUCOM and USAFRICOM staff indicated a major issue regarding the transfer of information between current DOD networks. The multinational staff indicated that there are problems in obtaining information due to the almost exclusive use of the SIPRNET and the "pull" culture of information for the current DOD organization. The U.S. staff indicated that the choke point for the information transfer for the requests of mission partners is the FDO. Interviews with the FDO indicated that the real reason that everything seems to go through his office was that the command members do not truly understand the responsibilities of the FDO. In addition, the practice of running everything through the FDO is exacerbated by the commands instruction ACI 5200.02 which dictates all personnel to "push" controlled unclassified information (CUI) through the FDO.

Although barriers to communication with multinational partners present a formidable challenge, both COCOMs have stressed that even communications with other U.S. government departments and agencies are far from optimum due to cultural tendencies, procedural methods, and technical means.These barriers remain prominent even though COCOMs have a significant number of U.S. Interagency liaisons embedded on their staffs.

While significant technical shortfalls remain, it is in the area of local policies, procedures and cultural engagement, education and training where current baseline capabilities are most strikingly lacking. Understanding the opportunities and barriers to working with both familiar and new partners, and our strengths and limitations relative to those activities, are our greatest challenges to information sharing. Within this arena are both near term and far term prospects to improve capabilities. Clearly DOD has demonstrated it has an operable framework from which to conduct complex operations particularly supporting HA/DR missions, but this study along with many similar efforts reinforce that while DOD is trained and effective in lead role operations, it is less precise and comfortable when it comes to relinquishing control and supporting the authorities of other USG agencies, host nations, IOs, NGOs and PVOs. While national level policy accommodates supporting roles and actively encourages strengthening those engagement opportunities, the associated tactics, techniques and procedures are less mature and deliberate planning less developed across echelons for these roles.

A recurrent theme encountered during the USEUCOM/USAFRICOM site visit,echoed during the Stakeholders/Gap Validation Conference, and the PDE was that effective utilization of LNOs and other interagency embedded staff, the conduit to interacting with enduring partner agencies, suffered from a fundamental lack of understanding of those

agencies' embedded staff roles, responsibilities, authorities, capabilities and limitations. By extension, familiarity and cohesion between USEUCOM and USAFRICOM and the broader set of potential mission partners not usually represented by LNOs or embedded staff pose even greater challenges to information sharing.

Finally, focusing on NGOs and the importance of these organizations within the context of supporting HA/DR missions, a bell weather issue recurs. Simply stated, "What's the incentive for NGOs to share information with DOD?" The issue of coordination with NGOs is rife with cultural and organizational mission friction. Most of these bodies have charter imperatives to maintain neutrality and impartiality, and their activities frequently carry them into direct engagement with U.S. military adversaries. Their political philosophies are often so incongruent with those of the DOD that there is great resistance to cooperation even under benign conditions. Many are suspicious of military motives and potential expectations of quid pro quo for assistance provided; indeed, some of these expectations are stated USG policy, such as requirements for "branding" supplied aid. In unstable political environments, any visibility of association with the U.S. Military may place NGO operations or even lives in jeopardy. How to engage these organizations, build trust and generate mutual benefit have been unanswerable questions.For the IMISAS project, focusing on USEUCOM and USAFRICOM, the most salient first step in addressing this issue is a clear definition as to "what can DOD do for you" to encourage information exchange, increase crisis response time, provided better support, and reduce cost. The foregoing exposition was intended to frame the more structured content of the baseline assessment, the "as is" condition reflected at USEUCOM and USAFRICOM. A set of requirements tailored to USEUCOM and USAFRICOM but derived from DOD source documents was prepared and analyzed to assure authority and consistency. Each required capability was cross-walked against Joint Capability Areas (JCAs) and Universal Joint task Lists (UJTLs) (Appendix 4) and prioritized at the Stakeholders/Gap Validation Conference. The delta between required capability (Appendix 7) and validated gaps (Appendix 8) provides the basis for the "as is" state. The baseline, the mapping of requirements to gaps, is illustrated in Figure E-8, with the complete table shown in Tables E-5 through E-16 of Appendix 8.

		Gap #	1	2	3	4
		Gap Description	Lack of a common suite of information sharing tools reduces the extent and timeliness of information sharing, impairing the effectiveness of HA/DR engagement by Combatant and Joint Force Commander staffs and other responders.	UIS web tool suites lack agility and dynamic scalability, limiting the range of operations that can be easily accommodated by Combatant and Joint Force Commander staffs and partner responders.	The UISC environment lacks a data sharing standard and system (or system of systems) for source vetting and identity management, impeding the validation of information supporting the goals of Combatant and Joint Task Force Commander staffs and partner responders.	Current language translation tools have insufficient fidelity and accuracy to render actionable translation across the range of geographic regions and associated languages and dialects in the span of activity of Combatant and Joint Task Force Commander staffs and their
Req't #	Requirement Description					
1	COCOMs require a validated UIS Operating Concept.		0	0	0	0
2	COCOMs require Tactics, Techniques, and Procedures (TTPs) to implement the UIS Operating Concept.		0	0	1	0
3	COCOMs require a uniform interpretation of policies.		0	0	0	0
4	COCOMs require policies which balance enclave security concerns with UIS policy intent.		0	0	1	0
5	COCOMs require standing UIS protocols and procedures for engagement with UIS enduring partners.		0	0	0	0
6	COCOMs require standing UIS protocol and procedure templates to support rapid integration with non-enduring and ad hoc mission partners.		0	0	1	0
7	COCOMs require a guidebook for cultural engagement with enduring UIS partners, particularly NGOs and IOs.		0	0	0	0
8	COCOMs require continuing enhancement of UIS information and collaboration tools while a unifying technical solution is implemented.		1	1	1	1
9	COCOMs require a web based Unclassified Information Sharing Capability (UISC) that accommodates multimedia information sharing and collaboration among the spectrum of potential mission partners to include both real and virtual members.		1	0	0	1
10	COCOMs require a collaborative portal which is available via the internet.		1	1	0	0
11	COCOMs require a UIS portal which is centrally funded and provisioned to ensure uninterrupted service across all DoD enclaves.		0	1	0	0
12	COCOMs require a UISC that supports both enduring and ad hoc communities.		0	0	1	1
13	COCOMs require a UISC unconstrained by geographical location.		0	1	0	0

Figure E-8 – Baseline - Requirements vs. Validated Gaps

5.3 Other Relevant Work

The IMISAS Team has reviewed a broad span of programs, events, and initiatives in the course of initial research and subsequent activities. Detailed descriptions of efforts related to the IMISAS project are contained in Appendix 6. These have both defined existing capability and informed potential improvements. The resulting body of information fundamentally informed requirement and gap definition, solution development, and experimental planning, and continues to do so as the project approaches the actual experimental venue.

Most recently, the March 2011 Process Documentation Event (PDE) highlighted policy/procedure and information management challenges within and between the two COCOMs, as well as with non-DOD mission partners. The PDE interviews also validated earlier observations of cultural schisms between military planniers and their civian interagency counterparts.

The management and evolution of the All Partners Access Network (APAN) presence in the aftermath of the devastating March 2011 tsunami illustrated a methodology for a partitioned hosting of both sensitive and non-sensitive unclassified information, as well as the benefits of a flexible structure for the presentation of information. The Interagency Shared Situational Awareness (IASSA) project demonstrated the efficiencies of composing information subscription and publishing feeds, and informs the IMISAS solutions relating to the methodologies for leveraging social media. Further illuminating

the challenges and advantages of embracing social media was the participation of USEUCOM in exercise X-24 Europe in March 2011, which heavily involved social media provided in the context of a user defined operational picture (UDOP). X-24 Europe illustrated both the value of compositing information streams from social media sources and the need for a metadata regime to mitigate information overload and ascribe levels of reliability to incoming reports. The IMISAS team's research into Ushahidi and Swift River further illuminated, respectively, the possibilities of integrating social media feeds within a geographical information system (GIS) framework and the state of the art in rating information coming from these sources. In a broader sense, the National Joint Operations and Intelligence Center (NJOIC) architecture has created a precedent for knowledge and information management in a web-enabled, multi-partner environment that must operate across broad ranges of urgency and mission type and amid information of varying levels of sensitivity. It will significantly inform the IMISAS projects' efforts to couple a KM methodology to the technical information sharing solution.

The IMISAS project conducted rearch into the Federal Aviation Administration's Next Generation air traffic management project (NextGen) due to its kindred necessity for information sharing across a vast range of capability and context. Although NextGen's developmental timeline largely post-dates IMISAS' experimental horizon, the project's focus on extending information sharing to a broad range of international partners resonates strongly with IMISAS goals, and the NextGen Implementation Plan may still inform the IMISAS solution set as both continue to mature.

Other experimentation venues such as Austere Challenge 2010 (AC10), IASSA, and the Multinational Experiment (MNE) series, illustrated continuing information sharing gaps in the following areas:

- Database and system interoperability
- Policy and authority alignment
- Language translation capabilities
- Collaborative tool federation
- Integration and standardization
- Training methodologies supporting collaborative tool use and acquisition
- A whole-of-government approach in building information sharing partnerships
- Knowledge management
- Reconciliation of information assurance requirements, constraints, and capabilities across the range of information sharing partners
- Provision of multiple information formats to support multiple partners

- Standardization of definitions, terms, taxonomies, and usable glossaries across COIs
- A balance of risk avoidance and risk acceptance with regard to information sharing integration of social media into the greater system of collaboration

The results of the USJFCOM multinational Experiment (MNE) series in particular validated the IMISAS project's initial view of the information sharing problem as mainly arising from policy, procedure, and cultural misalignment rather than technical shortfalls. Other related USJFCOM programs, such as the Cross Domain Collaborative Information Environment (CD-CIE), have demonstrated technical solutions and workarounds that can be implemented through the integration and composition of existing and emerging technical capabilities. The Coalition Warfare Interoperability Demonstration (CWID) is an ongoing program that illuminates the scope and integration possibilities of such emerging technologies. These include capabilities to accelerate communication linkages with civil authorities and NGOs, integrate commercial off the shelf technologies, rapidly create ground-independent communications infrastructure during natural disasters, expand the boundaries of language translation, better integrate geospatial products, extend the benefits of collaboration to low-bandwidth users, provide security for mobile device connections, and pre-screen sensitive information for release.

The Multinational and other Mission Partners (MNMP) and Global Theater Security Cooperation Management Information System (G-TCMIS) projects are ongoing DOD initiatives which will inform the IMISAS project. G-TSCMIS will provide a comprehensive picture of whole-of-government security cooperation activities. MNMP is a capability that enables the effective exchange of information among DOD components and their mission partners, including non-DoD agencies of U.S. Federal, State, local, and tribal governments, as well as, nongovernmental organizations (NGO), first responders, and the private sector within the United States as well as in a multinational environment, whether the United States is leading the operation or participating as a mission partner. Both initiatives stress integrative, technologically agile solutions. Developments and insights from these efforts will be leveraged as far as feasible and appropriate.

Finally, many references were consulted regarding the contextual environment for IMISAS. The most recent service documents are the DOD Support to Foreign Disaster Relief (FDR) - Handbook for JTF Commanders and Below, and the Foreign Humanitarian Assistance/Disaster Relief Handbook signature draft, are published by the Army Test and Evaluation Command and the Navy Warfare Development Command, respectively. Both handbooks provide useful perspectives for the IMISAS project as the

strategic, operational and tactical level procedures must be aligned. The guidance provided on communications and information sharing is consistent with the potential solutions being developed through the IMISAS project. The Navy handbook is particularly useful as it describes the considerations and limitations that uniquely apply to maritime forces.

5.4 Required Capabilities

The IMISAS Project Analysis Team distilled twenty three capability requirements (see Appendix 10) from review of documents cited in the Source Review spreadsheet, discussions and collaborative sessions with the IMISAS project COI, and discussions from the Office of the Director of National Intelligence Partner Engagement Conference of October 13-14, 2010. These requirements were ranked by COI participants at the Stakeholders/Gap Validation Conference. The ranking criterion was level of relevance to the Warfighter Challenge submission and the IMISAS project problem statement, specifically, level of contribution to UIS and collaboration in support of mission planning and operations in an HA/DR environment. A detailed breakout of requirement scorings and distribution of responses by the Stakeholders/Gap Validation Conference COI groups is provided in Table E-3 of Appendix 7.

5.5 Gaps Identified

Based on the same source material that generated the IMISAS project requirement list, the IMISAS Project Analysis Team initially discerned thirty three gaps relative to those requirements which were distilled down to 21. Each gap was assigned a primary thematic area from one of three categories: Technical, Cultural, or Policy/Procedure. Breakout groups at the Stakeholders/Gap Validation Conference were aligned according to these thematic areas. Each of the three breakout groups reviewed and ranked the list of gaps using criteria similar to those for requirement ranking, and giving particular attention to the gaps corresponding to their specific thematic areas. Recommendations were made by the COI participants to reword and combine some gaps. Following the conference, the IMISAS Project Analysis Team effected these revisions, in particular merging the data for gaps that were combined. The IMISAS Project Analysis Team assessed the many-to-many correspondences among these remaining gaps and the vetted requirements. This mapping, along with the gap rankings from the breakout group participants, was composited to generate a final ranked gap list for evaluation against potential solutions. A detailed breakout of gap scorings and distribution responses by the Stakeholders/Gap Validation Conference COI groups is presented in Table E-4 of

Appendix 9. Tables E-5 through E-16 of Appendix 9 provide the binary mappings of gaps to requirements.

At the SDW held in February 2011, the capability gaps initially identified in the baseline assessment were further refined. The IMISAS team successfully presented and validated specific gaps identified in the BAR focusing on the ten gaps identified by USEUCOM and USAFRICOM as having the highest priority.

5.6 Potential Solutions

Following the Stakeholders/Gap Validation Conference, Solution Development Workshop, and the PDE, potential solutions were distilled from both explicit nominations and implicit recommendations from recorded breakout session minutes. The IMISAS Project Analysis Team also assessed the many-to-many relationships among vetted gaps and solutions, and using the same compositing methodology, generated an initial ranked list of potential solutions for further vetting and distillation. A detailed breakout of solution rankings is presented in Table E-17 of Appendix 10. These will be subjected to further review and refinement, with a smaller set expected following removal of redundant solutions and those not meeting gate criteria specified in the USJFCOM J9 Baseline Assessment Guidelines (jointness, observability in an experimental venue, justification of cost and time in terms of impact, and feasibility of addressing within time and resource constraints of the project). This distillation of solutions is in progress and will proceed in consultation with the IMISAS project COI and in parallel with experimentation planning, with the intent of delivering a feasible spanning set of potential solutions for COI evaluation.

5.7 Summary of Analytic Results

The goal of analysis is to determine the viability of solutions through defensible insights that connect directly to project objectives through clearly focused lines of inquiry. The IMISAS Analytic Framework assures the coupling between solution development and the traceability chain from study issues to Essential Elements of Analysis (EEAs) to the measures necessary to address those EEAs. Both of these conceptual processes proceed ultimately from the common point of the IMISAS problem statement, and are brought to convergence through continuous iteration among the IMISAS analysis, solution development, and experiment design teams. Measures are the common endpoints for these two processes; they map directly to EEAs and define the variables to be stressed during experimentation. Metrics are currently under refinement as solution elements and experiment design come into focus. The specific balance of categorical and numerical data, methods for stressing the associated variables during experimentation, strategies for generating detectable change, and mechanisms for isolating causality to specific solution

elements remain key subjects of investigation. Intended methodologies for collecting and analyzing the associated data are contained in the IMISAS Data Collection and Analysis Plan, which will continue to be updated in concert with the End to End Experimentation Plan and Analysis Framework.

Appendices 8, 9, and 10 present requirements, gaps, and solutions, respectively, identified and ranked in connection with the Stakeholder/Gap Validation Conference. Appendix 7 describes the assessment tool used by the IMISAS team in generating requirement, gap, and solution rankings. The ranking process involved the following steps, applied in the order indicated:

- Capturing raw rankings of requirements, gaps, and solutions,
- Averaging and weighting rankings across seven COI categories represented
- Combining certain gaps based upon participant recommendations,
- Accounting for the strengths of the many-to-many relationships among requirements and gaps, and among gaps and solutions, and
- Weighting solutions in terms of cost and time, jointness, the ability to resource and observe them in an experimental venue, and the expected impacts of implementation versus cost and time.

The above process resulted in the identification and ranking of 23 requirements. A major theme from the top quarter of the requirement rankings was the need for a validated, overarching UISC. Implementing this capability necessitates requisite tactics, techniques, and procedures (TTPs), and a physical instantiation providing a cross domain capability, integrating or federating multi- mode services (including language translation, display fusion, social media, and collaboration capability), and embracing the needs of the disadvantaged user. However, the need was also recognized for simple, clear lines of authority for managing information sharing risk and adjudicating guidance for information release. The latter requirement was a crystallization point for a large number of directly and indirectly related culture and policy/procedure gaps in addition to those identified for technical implementation.

The methodology identified 28 gaps, the top ranking of which were those associated with the management of information and existence of impediments to information flow. These included shortfalls in understanding of other HA/DR responders' roles, responsibilities, limitations, authorities, potential contributions, and information exchange requirements; lack of organization and uniformity of information sharing processes and tools; restrictive policies (or restrictive interpretation of policies) that impede networking with and synchronizing efforts with external agencies, and ill-matched organizational communication models.

The upper quarter of the 39 identified solutions contained a complementary mix of recommendations that covered the major gaps. An effective means of identity establishment across the span of HA/DR responders and a best-of-breed approach toward web technologies allowing flexible evolution of user interfaces represented the top technical suggestions. These tied in with a cultural solution to establish COCOM presence in "safe spaces" such as internet cafés that by their nature provide a measure of anonymity and non-attribution with minimal outlay of personal information. Against the shortfall of familiarity with fellow HA/DR response agencies, the culture group offered the recommendation for frequent exercises designed from the ground up to build enduring rapport. A kindred suggestion addressed procedures for improved outreach and more effective engagement of liaison officers and other representatives of partner organizations. Tailored training was recommended for DOD personnel to engender a risk-managed rather than risk-averse approach to information release, as was brokering information visibility as an alternative to imposing strict releasability caveats. Covering information management shortfalls were recommendations to identify mappings between the planning activities among DOD and non-DOD responders, to develop pre-planned responses for information release, and to implement or emulate a standardized system of communication formats, procedures, lexicons, and application program interfaces serving the span of HA/DR responders.

Following the Stakeholder/Gap Validation Conference, significant additional solution refinement was effected in order to bring the number of solutions more realistically within resource bounds. The solutions were grouped into categories according to 12 major focus areas that ensured coverage of each gap by at least two of the 39 potential solutions, and the representation of all DOTMLPF-P areas among the solution groups (Table E-1). This methodology facilitated further vetting of the solution set, framed the initial exploration of potential metrics using the Command and Control Joint Operating Concept (C2 JIC) as a guide, and resulted in 11 solutions composited from the original 39. Concurrently, USEUCOM and USAFRICOM made recommendations for consolidating gaps, resulting in a smaller set of 10 gaps. The set of 11 solutions were reviewed again for experimentation and implementation feasibility and for completeness of mapping to the 10 gaps, and served as entering arguments for the SDW/IPC.

As detailed in section 2.1 of Appendix 12, both gaps and solutions were reworked further during the SDW/IPC. While the solution set in particular underwent significant reformulation in number, wording, and ranking, and reevaluation for feasibility of experimentation and implementation, the major themes identified during and subsequent to the Stakeholder/Gap Validation Conference remained largely intact. While the ranking and organization methodologies designed prior to that venue were not repeated during the SDW/IPC, the earlier efforts appear justified in terms of the enduring nature of the major

themes, the continued coverage of gaps by solutions, and the fact that the PDE interviews uncovered no additional gaps or solutions. The 10 gaps submitted for consideration at the SDW/IPC underwent only minor modifications at that venue, with the exception of one gap whose elements were subsumed into the remaining 9.

The primary outcome of the SDW/IPC was a set of 22 solutions and 6 experiment support activities grouped into the following categories:

- Tactics, techniques and procedures (TTP)
- Knowledge, skills and abilities (KSA)/Training
- Data standards
- APAN data compression
- APAN technical improvements
- APAN source reliability and rating
- APAN Social Media
- APAN graduated user accounts

Additionally, USAFRICOM provided the following "5 W's of information sharing" that have helped to further refine and focus solution development and assess potential solution impacts:

- With whom do we need to share information or collaborate:
    - In the interagency?
    - In the multinational community?
    - In the Intergovernmental Organization (IGO)/NGO community?
- What collaboration or information sharing do we need to accomplish:
    - With the interagency?
    - With the multinational community?
    - With the IGO/NGO community?
- Where geographically do we need to share information?
- When, with regard to the occurrence of HA/DR exigencies, do we need to share information?
- Why do we need to collaborate or share information:
    - With the interagency?
    - With the multinational community?

  - With the IGO/NGO community?

- How do we collaborate and share information relative to existing constraints on infrastructure, applications/tools, and policies/procedures?

A final outcome of the SDW/IPC was the USAFRICOM recommendation for a follow-on documentation venue (PDE) to more firmly define current COCOM information sharing processes in support of experimentation planning. The PDE was conducted at the end of March, 2011, and has provided valuable detail to the developing solutions, in addition to providing additional validation of identified requirements and gaps. Analysis for the PDE was not complete, however, in time for the IMISAS MPC.

During the MPC, conference participants discussed metric nomination for individual procedural solutions to be examined during the technical spirals and the AWG. The participants agreed on the need for continued work to flesh out details of solution decomposition; metrics identification by solution element; metrics stimuli and measurement; and related experimental manning, infrastructure, and scenario requirements relative to the solutions. Technical discussions included further detailing of the technical spiral plan, and APAN's potential contributions to automated data collection via its analysis tool package.

With the groupings and additional guidance resulting from the SDW/IPC, the "5 W's" guidance provided by USAFRICOM, the results of the PDE and MPC, and finally the decision to scope the experimentation venue to an analytic wargame (AWG) based upon real-world COCOM planning commitments for a military/political crisis in Libya, the following list of solutions emerged for evaluation during the AWG:

- Process and procedures for the expedited release of controlled unclassified information in a crisis response situation,
- Business rules governing the expedited transfer of unclassified information from classified networks to non-classified networks,
- Business rules governing the expedited transfer of unclassified information from classified networks to non-classified networks,
- Pre-defined templates and business rules for the establishment of UISC [portal] work sites in support of HA/DR operations,
- Processes and procedures to enable unclassified information sharing with mission partners via UISC,
- SOPs for combatant commands to use the UISC in support of HA/DR operations,
- Quick reference guides for the roles, responsibilities and general information requirements of potential mission partners for combatant commands in HA/DR operations, and

- Business Rules to define data types, standards, metadata requirements that facilitate posting, transfer and use of data.

The following solutions are to be evaluated via user surveys across a series of five technical spirals, the first of which has been completed as of the time of this writing. These solutions, pending successful evaluation during the technical spirals, will be used to support experimentation on the remaining solutions during the AWG:

- UISC capability to make automatic bandwidth recommendations in a restricted communications environment.
- Graduated user account permissions and procedures for anticipated and unanticipated users to facilitate allocating access to different levels of unclassified information based on trust.
- A rapid user registration system with the capability and capacity to support expansion of the UISC community of interest (COI) in crisis response.
- UIS capability to push or post aggregated data from dynamic sources to mission partners.
- UIS capability to capture, sort, categorize, filter information in the public domain.
- Business rules to maximize current automatic trust center capability including: rating, recommendations, and level of confidence.
- Source authenticity and information reliability capability for UISC use in filtering and verification of real-time data from channels such as Twitter, SMS, email and RSS feeds.
- UIS search capabilities (federated or integrated).

As described above, the IMISAS Analytic Framework was matured iteratively with the developing solutions. Measures are currently under refinement; these map to both EEAs and individual solution elements. Details of the decomposition chain from project outcomes to measures are contained in the IMISAS Analytic Framework. Methodologies for collecting and analyzing the associated data are contained in the IMISAS Data Collection and Analysis Plan. The specific balance of categorical and numerical data, and the methods for stressing the associated variables, remain key subjects of investigation as solution elements and experiment design come to fruition.

Recommendations based upon results of experimentation will be presented through the lens of the IMISAS conceptual model, which organizes information sharing needs from the perspective of hierarchical necessity. The conceptual model follows the construct of Abraham Maslow's hierarchy of needs, which provides a conceptual model of human motivation. In the context of IMISAS, the hierarchical model informs the allocation of

resources against the closure of identified gaps. The IMISAS conceptual model is further detailed in the Analytic Framework.

Solution Category	Number of Solutions	D	O	T	M	L	P	F	P	Number of Gaps Mitigated
Policy Review	4	X		X					X	6
Non-attribution	4				X		X		X	9
Outreach/COI Comprehension	8		X	X	X	X			X	10
Social Media Integration	2			X	X				X	3
UISC Training	2			X	X					4
Coordination Procedures	2	X	X	X						4
UISC tool suite	4				X					8
Information Management	4		X	X	X				X	15
Risk Management	5	X		X		X			X	5
Source Vetting/Reliability Assessment	1			X	X				X	3
Cross Domain	2			X	X			X	X	2
Identity Establishment	1				X		X			7

Table E-1 – Solution breakout by Gaps and DOTMLPF-P Area

6.0 Recommendations

The objective of the recommendations section is to capture the key ideas developed in the baseline assessment and propose choices and a way ahead for the project as a whole.

From the start of the project in September 2010, the IMISAS project team has iterated project objectives with the government to sharpen the focus of the effort and propose achievable outcomes within the constraints of available resources, manageable risk and schedule. That massaging of project scope in consultation with stakeholders and partners continued over the course of the baseline assessment and solidified during the USEUCOM/USAFRICOM site visit. The formalized objectives and outcomes were briefed at the Stakeholders/Gap Validation Conference. The delineation of the currently proposed objectives and outcomes is documented in section 3.0. The most salient features in terms of experiment objectives and project products are listed in the following sections.

Therefore, the first recommendation is to acknowledge and accept these experiment objectives and products as the agreed to foundation on which to proceed.

6.1 Experiment Objectives

1. Create an operational capability for UIS across domains which incorporates existing technologies.
2. Develop best process and procedure recommendations.
3. Examine, during technical spirals and an AWG, a set of proposed solutions designed to improve UIS between the U.S. DOD and a wide-variety of non-military mission partners, who may include civilian USG agencies, other nations, inter-governmental organizations, and NGOs.
4. Demonstrate and analyze processes and procedures to enable effective UIS across organizational, security, and to a limited extent, network domain boundaries.

6.2 Project Products

1. Experimentally validated recommendations for enhancements to UIS platform capabilities
2. Handbook and experimentally validated doctrine change recommendations addressing how the DOD can better engage other USG bodies and share information with IO/NGO/private partners in support of HA/DR.
3. Experimentally validated recommendations for changes in policy to facilitate information sharing with a range of partners in a HA/DR environment

6.3 Experiment Design Courses of Action (COAs)

Concurrently with the baseline assessment process (identification, validation and prioritization of requirements, gaps and solutions), the IMISAS team developed a set of broad Courses of Action (COAs) to assist in the experiment design

The IMISAS team reviewed the available information to better understand the purpose of the project and the problem statement, by identifing what the project must accomplish, when and where to best do it, and most importantly why it needs to be done. Based on this initial effort, the team developed several broad COAs to serve as the basis for a potential experiment design. The team developed and evaluated varying COAs for experiment design using the following screening criteria:

- Feasible – The COA can successfully complete the project within the established time, space, and resource limitations.
- Acceptable – The COA must balance cost and risk with the experiment analytic rigor gained.
- Suitable – The COA can accomplish the project within the Experiment Director's intent and planning guidance.
- Distinguishable – Each COA must differ significantly from the other efforts (such as experiment type or tasks to be performed).

This COA analysis enabled the IMISAS project team, in coordination with the project partners and stakeholders, to identify difficulties or coordination problems as well as probable consequences of planned actions for each COA being considered. After completing the analysis, the IMISAS team identified its preferred COA and made a recommendation to go forward. The IMISAS experiment director, in coordination with the project partners and stakeholders, selected the COA they thought would best accomplish the project goals.

The various COAs that were developed are outlined below.

6.3.1 COA #1 Description

Unclassified and Classified experiment networks with APAN instantiation on both. Focus on the synchronization of data between portals on different networks.

6.3.2 COA #2

6.3.2.1 COA #2a Description

Unclassified and Classified experiment networks with APAN instantiation only on the low side. Focus on the synchronization and movement of data between different networks.

6.3.2.2 COA #2b Description

Unclassified and classified experiment networks with APAN instantiation only on the low side. Include sharing with social/alternative networks. Focus on the synchronization and movement of data between different networks.

6.3.3 COA #3 Description

Unclassified experiment network with APAN instantiation only on the low side. Include sharing with social/alternative networks. Focus on the synchronization and movement of data inside and outside of the DOD.

6.3.4 COA #4 Description

Unclassified experiment network with a non-APAN portal (i.e., HARMONIEWeb) only on the low side. Include sharing with social/alternative networks. Focus on the synchronization and movement of data inside and outside of the DOD.

6.3.5 COA #5 (Selected) Descriptions

Unclassified series of five technical spirals to support continued development, demonstration, and evaluation of the technical solutions. Following the technical spirals, there will be an AWG to examine a set of proposed solutions designed to improve UIS between the U.S. DOD and a wide variety of non-military partners, who may include civilian USG agencies, other nations, inter- governmental organizations, and NGOs. The primary focus of the AWG is on staff policies, processes, and procedures to enable effective UIS across organizational, security, and to a limited extent, network domain boundaries.

6.3.6 COA Recommendations and Decision

Whereas COAs 1, 2a, 2b, and 3 are sufficiently robust and emulate the COCOM environment, the technical instantiation of the cross domain aspect of each entails a cost risk not supportable by the project.

COA 4 was rejected since it incorporates HARMONIEWeb (non-APAN portal) and therefore is inconsistent with the DOD decision to implement a UISC through spiral

development (integration and federation of new capabilities) utilizing the existing APAN as the proxy.

COA 5 was selected as the basis for the IMISAS experiment design. It was considered to be the most viable for successful completion of the project within the established time, space, and resource limitations. It also provided the best balance of cost and risk with the experiment analytic rigor gained while accomplishing the project within the Experiment Director's intent and planning guidance.

List of Appendices

Supporting appendices listed below are available on request.

Appendix 1 – Acronyms
Appendix 2 – Bibliography
Appendix 3 – Glossary of Terms
Appendix 4 – Source Review Spreadsheet and Capabilities Crosswalk
Appendix 5 – Organizations Interviewed
Appendix 6 – Other Relevant Work
Appendix 7 – Assessment Tool
Appendix 8 – Prioritized Requirements and Data Elements
Appendix 9 – Prioritized Gaps and Data Elements
Appendix 10 – Prioritized Potential Solutions
Appendix 11– Demographic Charts
Appendix 12 – Results of the Solution Development Workshop (SDW)
Appendix 13 – Process Documentation Event
Appendix 14 – Mid Planning Conference

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions Project (IMISAS)

Annex F – AFTER ACTION REPORTS

List of Appendices

Appendix 1 – Solutions Development Workshop/Initial Plannning Conference AAR

Appendix 2 – Process Documentation Event AAR

Appendix 3 – Mid-Planning Conference AAR

Appendix 4 – Final Planning Conference AAR

Appendix 5 – Analytic Seminar AAR

Appendix 6 – Transition Conference AAR

Appendix 1 - Annex F - After Action Reports

Solutions Development Workshop
and
Initial Planning Conference

Interagency And Multinational
Information Sharing
Architecture and Solutions
IMISAS

United States Joint Forces Command
Join Concept Development and Experimentation (JCD&E)

Interagency and Multinational Information Sharing Architecture and Solutions

Solutions Development Workshop
and
Initial Planning Conference
After Action Report

18 March 2011
Version 2.0

Purpose. This document summarizes the findings from the Interagency and Multinational Information Sharing, Architecture and Solutions (IMISAS) Solutions Development Workshop (SDW) and Initial Planning Conference (IPC), held at U.S. European Command (USEUCOM) Headquarters, Stuttgart, Germany from 22-25 February 2011. It documents the preparation, objectives, agenda, outcomes, and way ahead for the IMISAS project as executed during the workshop and the conference.

Background. The IMISAS SDW/IPC was an unclassified event that was held at the General Bernard P. Rogers Partnership Conference Center, at USEUCOM in Stuttgart, Germany. The IMISAS team with support from USEUCOM personnel managed conference registration, check-in and administrative support. USEUCOM coordinated facilities and logistics. The purpose of the SDW/IPC was to inform the IMISAS Community of Interest (COI) of capability gaps identified in the Baseline Assessment Report (BAR), to evaluate potential solutions for experimentation value and to initiate planning for the Limited Objective Experiment (LOE) scheduled for August, 2011.

Event Preparation. The IMISAS team developed and provided conference announcements and registration information to the IMISAS community of interest (COI). Conference registration was monitored by the planners, which allowed targeted invitations to be sent to organizations whose specific participation was desired. Conference read-aheads were cleared for public release through USJFCOM Public Affairs, and posted on both the IMISAS page of the All Partners Access Network (APAN) portal and the HARMONIEWeb web site. A rehearsal of concept (ROC) drill was conducted at the TASC facility in Suffolk, VA on 7 February. Rehearsals for each presentation were conducted at the TASC facility the week of 14 February and at the USEUCOM conference center site on 21 February. Key Personnel Associated with the SDW/IPC were:

Project Lead (Ms. Kathryn Smith)
- Hosted the event.
- Provided an overview briefing on the IMISAS project.
- Provided guidance throughout the event.

Contract Lead (Mr. John Sarcone)
- Facilitated the event.
- Adjusted the schedule and modified specific group processes to respond to emerging requirements.
- Ensured event objectives were met.
- Closed the event and outlined the way ahead.

Event Coordinators (Mr. Hawley Waterman & Mr. Dick McCrillis)
- Coordinated preparation and approval for the release of the presentations to the public.
- Ensured presentations and read-aheads were posted on the IMISAS portal.
- Coordinated technical requirements with USEUCOM.

- Sent registration announcements to COI.
- Monitored registration.
- Directed the activities of contractor personnel in preparation and execution of the workshops.
- Drafted Pre and Post-Event EXSUMs.

Group Presentations and Facilitators (Mr. Dick McCrillis; Mr. Stan Howard; Mr. Paul Danks; Mr. Steve Sullivan; Mr. Jim Welshans)

- Briefed experimentation outline, specific APAN issues and improvements, the Unclassified Information Sharing (UIS) Operating Concept, the UIS Policy and Procedures Handbook, and an extensive review of the analysis processes that yielded the current gap and solution pedigree.
- Facilitated interaction and data gathering with the workshop attendees.

IMISAS Recorders Team (Mr. Geoff Boals; Mr. Dave Moulton)

- Captured key points and issues discussed.
- Assisted in building briefings and reports.
- Provided technical support.

Mr. Mike Landino ensured IMISAS space, technical, and administrative requirements were fully identified, coordinated and supported. Mr. Dallas Jones was the USEUCOM Conference Planner lead and ensured that all of the requirements were met.

The official conference agenda is included as Appendix A to this report.

Objectives: The SDW provided a forum to develop and refine solutions that address the following military problem statement: "COCOMs lack a coherent capability to share information and collaborate across multiple domains with a broad range of mission partners (government / interagency, multi-national, multi-lateral & private sector) due primarily to restrictive policies, conflicting authorities, ad hoc/ineffective procedures, business rules and non-interoperable networks and systems." A critical element of the SDW is to obtain consensus from the project stakeholders, on the specific solutions on which the experiment should focus, and to begin to form those solutions into a viable experimentation plan.

SDW objectives included:

- Presenting the BAR gaps and solutions,
- Soliciting additional input from the IMISAS stakeholders for continued solution development and refinement,
- Identifying and prioritizing a comprehensive set of potential solutions for experimentation,
- Soliciting insight/input that helps to frame the UIS Informal Operating Concept, and:
- Soliciting insight/input that helps to frame the UIS Policy and Procedures Handbook.

The IPC provided a forum to discuss and further develop the solutions that originated at the SDW. This development included analysis of the solution set to determine the suitability and scoping for experimentation. It also provided the opportunity for further discussion of overall project goals, objectives and milestones.

IPC objectives focused on developing the initial requirements for the Experiment Plan to include:

- Potential training requirements,
- Initial manning requirements,
- Experimentation Data Collection & Analysis Plan (DCAP),
- Scenario and control plan requirements,
- Planning timelines and potential participants other than core stakeholders,
- Critical decision points and milestones for the experiment campaign, and:
- Critical event dependencies, long-lead items, and preparatory events required for key activities.

SDW Overview: The IMISAS Solutions Development Workshop began on Tuesday morning, 22 February. Keynote addresses by Mr. Michael Ritchie, USEUCOM J9 and Mr. Michael Ryan, Deputy USEUCOM J8 provided context for the conference, underscoring the importance of information sharing in theater engagement and crisis response. Ms. Kathryn Smith provided an IMISAS project overview briefing to the workshop plenary, consisting of representatives from USAFRICOM, USEUCOM, OSD NII, JS J7, DOD Executive Agent for Maritime Domain Awareness, DISA, DOS Humanitarian Information Unit, and the *Bundeswehr* Transformation Center. This was followed by Mr. Steve Sullivan, IMISAS Analysis Lead, who facilitated an in-depth review and validation of the capability gaps, encouraging thorough review and discussion of each one, including their applicability to an experimentation process. The end of the review produced a final list of nine defined gaps that were agreed to by the stakeholders present. The list is included as Appendix B.

The SDW remained in plenary to work development of specific solutions to the identified capability gaps. A wide range of potential solutions were identified and refined. The solutions were then evaluated with respect to project scope and applicability to experimentation. Solutions were then binned into general categories. The solution categories are: Tactics, Techniques and Procedures (TTP), data standards, knowledge, skills and abilities (KSA) training, and technical enhancement recommendations to APAN as an initial operational capability for UIS. This final list of solution candidates was validated and prioritized by the stakeholders for potential experimentation within the IMISAS project. The final list of 22 experimental candidate solutions is included as Appendix C.

Attendees were briefed on the draft UIS Operating Concept and the framework for the UIS Policy and Procedures Handbook and were provided an overview of the Transition Plan, which is designed to deliver improved capabilities to the warfighter. Stakeholder response was positive and it was agreed that both the UIS Operating Concept and the UIS

Policy and Procedures Handbook would be developed by the project team, distributed to the stakeholders and COI for comment, and be reported upon at the Mid-Planning Conference (MPC) and Final Planning Conference (FPC).

IPC Overview: After an introductory briefing that defined experimentation procedures and a campaign outline leading to the LOE itself, the COI received a presentation from the German *Bundeswehr* Transformation Center outlining their technical capabilities to support unclassified information sharing and experimentation. The major effort was spent to further refine the culled solution list into discrete pieces suitable for experimentation and analysis, including the types of tests that might be performed during the LOE. Method was similar to the solutions refinement process during the SDW, with participants articulating the kind of testing that was within the "art of the possible" given the resource and time parameters of the project. The Friday session shifted away from the scheduled events into a wider-ranging discussion on the scope and scale of the LOE and the nature of the products required by USAFRICOM and USEUCOM. As part of their input, USAFRICOM provided a series of "5W" questions to assist in framing the analysis problem (Appendix E). The AFRICOM input reinforced the need for well-documented, pre-experiment analysis and documentation of COCOM information sharing processes as currently performed. The COCOM representatives did not think that there was enough information available on current processes to establish a baseline for development of the experiment and final products. The group agreed that there should be a process documentation event with analysts from the IMISAS team visiting USAFRICOM and USEUCOM. After reviewing schedules, it was determined that 28-31 March would be the best time for this event.

Results and Way Ahead: Discussions from the SDW refined and validated the capability gaps previously identified in the IMISAS Baseline Assessment. These gaps were then used to develop a comprehensive list of potential solutions for further examination for use in the IMISAS limited objective experiment. The SDW sessions set the stage for the IPC the next day and the beginning of specific planning for IMISAS experiment. During the SDW, briefings and updates were provided on the status and way ahead for the UIS Operating Concept, the associated UIS Policy and Procedures Handbook, and a nominal transition plan for the post-experiment period. The handbook is structured to inform staff-level TTPs as they relate to information sharing between military and civilian partners.

The validated gaps and solutions developed at the SDW will be incorporated into the IMISAS Baseline Assessment as an annex. The experimental solutions will be further defined and refined by the IMISAS COI in preparation for the MPC and will form the basis for construction of the experiment. At the IPC, an outline for the experiment was developed including milestone events and the approach to experiment execution and analysis. The Process Documentation Event will be the next milestone followed closely by the MPC. The FPC will remain as originally planned. The Baseline Assessment Trials and Solution Assessment Trials will be combined with the LOE into a single two week event occurring 25 July to 05 August. Initial discussions from the IPC on experiment manning and resources will need to be mapped and refined before the MPC.

While much was accomplished at the SDW/IPC, there is much that needs to be done in order for the project to meet its objectives. The attendees agreed on the general approach to experimentation for the project, but this approach is only the framework and a lot of hard work will be required to develop the details of how to execute the experiment. There are many decisions that need to be made soon to define the experiment for the work required at the MPC. The COCOMs were emphatic on the need for IMISAS products, and their efforts along with the IMISAS Team and the rest of the COI will enable the completion of this work and successful execution of the experiment.

To focus these efforts, the SDW/IPC developed a set of specific action items, listed in Appendix E, which will help guide follow-on planning activities for all parties in the project. Appendix F is a list of everyone who attended either the SDW or the IPC.

Submitted: Kathryn Smith, 757-203-3164, DSN 668-3164

Appendices:

A- SDW / IPC Agenda
B- Validated Gaps Listing
C- Final Solution List
D- USAFRICOM “5W” Questions
E- SDW/IPC Action Items
F- SDW / IPC List of Attendees

Appendix A:

SDW Day 1, Tuesday 22 Feb 2011		
Time	**Event**	**Leader**
0800 – 0900	Registration	
0900 – 0915	Call to Order and Welcome	Mr. John Sarcone
0915 – 1000	Keynote Addresses	USEUCOM J9 and DJ8
1000 – 1015	Break	
1015 – 1030	IMISAS Project Overview	Ms. Kathryn Smith
1030 – 1045	Solutions Development Workshop Overview	Mr. Dick McCrillis
1045 – 1115	Gaps and Solutions Synopsis	Mr. John Sarcone
1115 – 1130	Gap Validation Review	Mr. Steve Sullivan
1130 – 1300	~~~~~~~~ LUNCH BREAK ~~~~~~~~	
1300 – 1315	IMISAS Proposed Solutions	Mr. Steve Sullivan
1315 – 1445	Potential Solutions Review/Refinement	Mr. Steve Sullivan
1445 – 1500	Break	
1500 – 1700	Potential Solutions Review/Refinement	Mr. Steve Sullivan
1700 – 1730	Opportunity for Organizational Meetings (Hot Wash)	Team Leads
1800 – 1930	No-Host Social	Manolito's (SSEC, Bldg 2505)

SDW Day 2, Wednesday 23 Feb 2011		
Time	**Event**	**Leader**
0800 – 0815	Day 1 Review Day 2 Agenda Overview	Mr. John Sarcone
0815 – 1000	Continuation of Potential Solutions Refinement/Backbrief	Mr. Steve Sullivan
1000 – 1015	Break	
1015 – 1130	Continuation of Potential Solutions Refinement/Backbrief	Mr. Steve Sullivan

SDW Day 2, Wednesday 23 Feb 2011		
Time	**Event**	**Leader**
1130 – 1300	~~~~~~~~ LUNCH BREAK ~~~~~~~~	
1300 – 1330	IMISAS Transition Plan	Mr. Paul Danks
1330 – 1430	UIS Operating Concept	Mr. James Welshans
1430 – 1500	Break	
1500 – 1600	UIS Handbook	Mr. Paul Danks
1600 – 1630	SDW Wrap-up / Outbrief / Way Ahead	Mr. John Sarcone
1630 – 1730	Opportunity for Organizational Meetings (Hot Wash)	

IPC Day 1, Thursday 24 Feb 2011		
Time	**Event**	**Leader**
0800 – 0815	IPC Kick-off / Admin	Mr. John Sarcone
0815 – 0830	IPC Review and Objectives	Mr. John Sarcone
0830 – 0900	Experiment Plan Outline	Mr. Dick McCrillis
0900 – 0915	DEU Experimentation Capabilities	CPT Seibert (DEU)
0915 – 0930	IMISAS APAN Site Recommendations	Mr. Stan Howard
0930 – 1000	LOE Environment & Procedures	Mr. Dick McCrillis
1000 – 1015	Break	
1015 – 1200	Breakout Groups: -Analysts -Design/Scenario/Planning	Leader: -Mr. Steve Sullivan -Mr. Dick McCrillis
1200-1300	~~~~~~~~ LUNCH BREAK ~~~~~~~~	
1300 – 1700	Breakout Groups: -Analysts -Design/Scenario/Planning	Leader: -Mr. Steve Sullivan -Mr. Dick McCrillis
1700 – 1730	Opportunity for Organizational Meetings (Hot Wash)	

IPC Day 2, Friday 25 Feb 2011		
Time	**Event**	**Leader**
0800 – 0815	Day 1 Review Day 2 Agenda Overview	Mr. John Sarcone
0815 – 0945	Breakout Groups: –Analysts –Design/Scenario/Planning	Leader: –Mr. Steve Sullivan –Mr. Dick McCrillis
0945 – 1000	Break	
1000 – 1045	Breakout Groups – Backbrief (Plenary)	Group Leaders
1045 – 1100	LOE Proposition	Mr. Steve Sullivan
1100 – 1130	Action Plan Review	Mr. John Sarcone
1130 – 1145	Updated Experiment Outline / Timeline / Way ahead	Mr. John Sarcone
1145 – 1200	Project Lead Comments / Closing	Ms. Kathryn Smith
1200	Dismissal / Out Processing	

Appendix B: Validated Gaps Listing:

1. Combatant and JTF Commander staffs lack sufficient knowledge, skills, and abilities to understand the roles, responsibilities, limitations, authorities, potential contributions, and information exchange requirements of interagency and other potential mission partners, resulting in ineffective information exchange.
2. Inconsistent information management schemes among existing DOD web portal implementations and standards impede information sharing among Combatant and Joint Task Force staffs and with mission partners, resulting in needless duplication of information, inefficient searches, lapses in event coordination, poor presentation of information to target audiences, and general information overload.
3. Combatant and JTF Commander staffs are impeded in rapid establishment of dynamic information sharing environments and/or sharing of information (e.g., government-provided imagery products) by inadequacy of procedures and restrictive interpretation and inflexibility of information sharing policies.
    a. Crisis Response
    b. Long Term Response
4. Information sharing between Combatant and Joint Force Commander staffs and USG Interagency and other mission partners is impeded by the incompatibility of the DOD's hierarchical information exchange methodologies/processes and USG Interagency and other mission partners with decentralized or ad-hoc processes.
5. Two-part
    a. Manual cross domain transfer mechanisms currently in place are cumbersome and inefficient, adversely affecting operations.
    b. Diverse cultural and operational habits among Combatant and Joint Force Commander staffs lead to work on multiple classified and unclassified government networks, as well as public domains.
6. Without a common strategy and standard procedures for effective integration, Combatant and JTF Commander staffs lack the ability to access and interpret valuable information in the public domain, such as social media.
7. Deleted
8. Combatant and JTF Commander staffs lack a DOD Unclassified Information Sharing Capability (UISC) that is flexible, accessible, user-friendly, and interoperable across the broadest pool of mission partners. This UIS capability should be standardized across DOD to minimize the need to train on a new tool when DOD personnel transition to a new AOR.
9. Two-part:

a. Combatant and JTF Commander staffs lack processes and procedures to include mission partners in existing DOD systems and networks for information sharing.
b. Combatant and JTF Commander staffs lack processes and procedures to access mission partners systems and networks for information sharing.

10. The ability for Combatant and Joint Force Commander staffs to collaborate is impaired by damaged, underdeveloped, or disparately developed network infrastructure in affected nations.

Appendix C - Final Solution Set for Experimentation

Gap #	Proposed Solution	Focus Area
10	Graceful degradation (Hi band to Low Band, automatic sensing and recommendation)	APAN Data Compression
6	IPhone/smartphone App or capability	APAN Data Compression
10	Disconnected Intermittent Low bandwidth (DIL) adaptability, in general	APAN Data Compression
3	Ability for SMS coding for '911 type' short codes. (E.g., text to report bridge out)	APAN Data Compression
10	Compression Utilities	APAN Data Compression
3	Graduated User Accounts permissions and methodology (from unknown to CAC enabled)	APAN Graduated User Accounts
3	Rapid User registration system including single log-on	APAN Graduated User Accounts
3	Provide Updates through dynamic sources (social media, Hotlines, news)	APAN Social Media
6	UIS connections to social media	APAN Social Media
6	Automatic Information Trust Center (rating, recommendations, validation, level of confidence)	APAN Source Reliability and Rating

2	Source reliability and rating system (Swift River for example)	APAN Source Reliability and Rating
2	Federated or Integrated search	APAN Technical
5	Identification of Data to be transferred (Standards)	Data Standards
1	Recommend JTF and combatant command staff skill set requirements	KSA/Training
1	Develop electronic searchable handbook like document, reference (Wiki?)	TTP
3	Dynamic level of information release based on operational scenario	TTP
1	TTP's for use of UISC	TTP
1	Quick references guides for different roles in an HA/DR response	TTP
5	Correctly mark data to the lowest classification appropriate	TTP
3	Templates for HA/DR	TTP
3	Business Practices	TTP
9	Streamline the process for HA/DR	TTP

Appendix D - SDW/IPC Action Items

Action	Organization	POC	Suspense
APAN in a degraded, intermittent or low bandwidth (DIL) environment. Identify current requirements for APAN.	USEUCOM	Amy Hamilton	3/7/11
APAN (Data Compression, User Accounts) Conduct liaison with APAN Team and determine availability of programmed spiral upgrades (DIL, I phone App, SMS coding, compression utilities, graduated permissions and user registration improvements) Nominate solutions for experimentation based on expected availability for experimentation.	USAFRICOM	Jordan Pritchard	3/21/11
APAN (Social Media) – Dynamic Sources, UIS Connections Identify current configuration and programmed upgrades available for experimentation and define 'As Is' and 'To Be' state.	USAFRICOM	Jordan Pritchard	3/21/11
APAN (Social Media) Touch Points – Define partner interactions as part of developing IERs.	USJFCOM	Paul Danks	4/4/11
APAN (Source Reliability and Rating) Trust Center – Write the TTP	USJFCOM	Paul Danks	6/13/11
APAN (Source Reliability and Rating) Trust Center – determine availability and usability for APN	USAFRICOM	Jordan Pritchard	3/21/11
APAN (Source Reliability and Rating) Source Authenticity-Swift River – investigate availability and usability.	USAFRICOM	Jordan Pritchard	3/21/11
APAN (Technical) – Integrated/Federated Search – Identify extant and near term search capabilities.	USAFRICOM	Jordan Pritchard	3/21/11
APAN (Technical) – UDOP – Research COTS/GOTS possible capabilities and indentify candidates for test.	USJFCOM	Stan Howard	4/4/11
APAN (Data Standards) – Meta Data – Investigate mediation as possible solution.	USAFRICOM	Jordan Pritchard	3/21/11
KSA/Training – Review existing Joint UIS training and provide courses of instruction.	USEUCOM	Amy Hamilton/ Dallas Jones	3/14/11
KSA/Training - Review existing Multinational/Interagency UIS training. MNE 4, 5 and ALN/MNE6.	USJFCOM	Paul Danks	3/14/11
TTPs – Write TTPs to include electronic handbook, quick reference guides and business rules and 5 Ws.	USJFCOM	Paul Danks	6/13/11
TTPs – Write TTP for procedure to release CUI and expedited FDO procedures.	USJFCOM	Paul Danks	6/13/11
Develop templates (written or electronic) to compliment UIS TTPs (specific to HA/DR).	USJFCOM	Paul Danks	7/1/11
TTPs – Write TTP to enable EUCOM/AFRICON to access key mission	USJFCOM	Paul Danks	6/13/11

portals.			
Define the "5Ws" for information sharing	USAFRICOM/ USEUCOM		3/7/11
Document the Processes (Baseline) • Event w/ vignettes • COCOM /Comp J3 • Partners	USJFCOM	Steve Sullivan, Paul Danks,	3/28-4/1/11
Identify SMEs for continual communication	USAFRICOM/ USEUCOM	Arthur Reyes/ LCDR Guy	3/14/11
Submit process survey questions	USJFCOM	Steve Sullivan	3/14/11
Respond to Process Survey Questions	USAFRICOM/ USEUCOM	Arthur Reyes/ LCDR Guy	3/28/11
Collect "What's" from Partners' Perspective	USJFCOM	Paul Danks	4/4/11
Collect "What's" from COCOM Perspective	USAFRICOM/ USEUCOM	Arthur Reyes/ LCDR Guy	3/14/11

Appendix E- AFRICOM "5W" Questions

Warfighter Challenge

WHO

With whom in the interagency (e.g., DoS, USAID) do we need to share information/collaborate?
With whom in the multi-national community (e.g., host country, NATO partner) do we need to share information/collaborate?
With whom in the IGO/NGO community do we need to share information/collaborate?

WHAT

What collaboration/information sharing do we need to do with the interagency?
What collaboration/information sharing do we need to do with the multi-national community?
What collaboration/information sharing do we need to do with the IGO/NGO community?

WHERE

On the African continent (e.g., Congo)

WHEN

In a HA/DR scenario (e.g., Volcanic Eruption)

WHY

Why do we need to collaborate/share information with the interagency?
Why do we need to collaborate/share information with the multi-national community?
Why do we need to collaborate/share information with the IGO/NGO community?

HOW

Do we have the necessary infrastructure, applications/tools, and policies/procedures to collaborate/share information?
H_0: We have the infrastructure to collaborate/share information with the interagency
H_0: We have the infrastructure to collaborate/share information with the multi-national community
H_0: We have the infrastructure to collaborate/share information with the IGO/NGO community

H_0: We have the applications/tools to collaborate/share information with the interagency
H_0: We have the applications/tools to collaborate/share information with the multi-national community
H_0: We have the applications/tools to collaborate/share information with the IGO/NGO community

H_0: We have the policies/procedures (e.g., data standards, classification policies) to collaborate/share information with the interagency
H_0: We have the policies/procedures to collaborate/share information with the multi-national community
H_0: We have the policies/procedures to collaborate/share information with the IGO/NGO community

Baseline: 27 June
Solution Assessment Trial: 18-29 July
Data Analysis:

Appendix F- List of Attendees

Last Name	First Name	Title	Nationality	Organization	Email
Acton	Thomas	Mr	USA	AFRICOM (JFD)	Thomas.Acton@africom.mil
Adam	Burhan	Mr	USA	DISA PEO C2C	burhan.adam@DISA.MIL
Ball	Shelby	Mr	USA	JS J7/JFDID	shelby.ball@js.pentagon.mil
Ballogh	Rebecca	Ms	USA	AFRICOM (Commerce LNO)	rebecca.balogh@africom.mil
Barlow	William	Mr	USA	OASD(NII)	william.barlow@osd.mil
Black	John	MAJ	USA	AFRICOM (SPP CWMD)	john.black@africom.mil
Boals	Geoffery	Mr	USA	JFCOM	Geoffrey.Boals@tbe.com
Briggs	Steven	Mr	USA	AFRICOM (Resources-CD&E)	steven.briggs@africom.mil
Brown	Lloyd	Mr	USA	JFCOM	lloyd.brown.ctr@jfcom.mil
Campbell	Joshua	Mr	USA	HIU	CampbellJS3@state.gov
Clark	Rashan	CPT	USA	AFRICOM (OTR-PD)	Rashan.Clark@africom.mil
Danks	Paul	Mr	USA	JFCOM	paul.danks@kcg-inc.net
Dare	James	Mr	USA	JFCOM	james.dare.ctr@jfcom.mil
Figueroa-Seary	Jose	MAJ	USA	EUCOM (ECJ9)	jose.figueroa-seary@eucom.mil
Gateau	Jamie	CDR	USA	EUCOM	james.gateau@eucom.mil
Guy	Blair	LCDR	USA	EUCOM	blair.guy@eucom.mil
Hamilton	James	Maj	USA	DISA Europe	James.Hamilton@disa.mil
Hamilton	Amy	Ms	USA	EUCOM	amy.hamilton@eucom.mil
Hamilton	Corey	Mr	USA	AFRICOM	corey.hamilton@africom.mil
Henry	Wayne	Mr	USA	AFRICOM (C4S-CA)	Harold.Henry@africom.mil
Howard	Stanley	Mr	USA	JFCOM	Stanley.Howard@tbe.com
Iulo	James	LtCol	USA	AFRICOM (OTR-PD)	James.Iulo@africom.mil
Jackson	Gregory	Mr	USA	JFCOM	gregory.jackson@jfcom.mil
Johnson	Ron	Mr	USA	EUCOM	ronald.johnson@eucom.mil
Jones	Dallas	Mr	USA	EUCOM	dallas.jones@eucom.mil
King	Dean	LtCol	USA	EUCOM	dean.king@eucom.mil
Krutar	Matt	Mr	USA	AFRICOM (OPL)	Matthew.Krutar@africom.mil
McCrillis	Richard	Mr	USA	JFCOM	richard.mccrillis@tasc.com
Miller	Kent	COL	USA	AFRICOM (OTR-PD)	Kent.Miller@africom.mil
Miller	Alyson	Ms	USA	JFCOM	alyson.miller.ctr@jfcom.mil
Moulton	David	Mr	USA	JFCOM	david.moulton@christmaslogistics.net
Paplos	Elaine	Ms	USA	AFRICOM	elaine.paplos@africom.mil
Pritchard	Jordan	Mr	USA	AFRICOM (C4S-KM)	Jordan.Pritchard@africom.mil
Rathbun	Jane	Ms	USA	AFRICOM (Resources)	jane.rathbun@africom.mil
Rathbun	Roy	Mr	USA	AFRICOM (representing NGA)	roy.rathbun@eucom.mil

Reyes	Arthur	Mr	USA	AFRICOM (OTR-PD)	Arthur.Reyes@africom.mil
Sarcone	John	Mr	USA	JFCOM	john.sarcone.ctr@jfcom.mil
Sasser	Dennis	Mr	USA	AFRICOM	dennis.sasser@africom.mil
Seibert	Thomas	CPT	DEU	Bundeswehr Transformation Ctr	thomasarminseibert@bundeswehr.org
Sisto	Frank	Mr	USA	DoD EA for MDA	frank.sisto@navy.mil
Smith	Heather	Ms	USA	AFRICOM (OTR-PD)	Heather.Smith@africom.mil
Smith	Kathryn	Ms	USA	JFCOM	kathryn.smith@jfcom.mil
Sullivan	Stephen	Mr	USA	JFCOM	stephen.sullivan@cc.capstonecorp.com
Van Dyne	Vernon	LTC	USA	JFCOM	vernon.vandyne@jfcom.mil
Vrtis	Robert	Mr	USA	OASD(NII)	Robert.Vrtis.ctr@osd.mil
Welshans	James	Mr	USA	JFCOM	james.welshans@tbe.com
Westenkirchner	Peter	LTC	DEU	Bundeswehr Transformation Ctr	peterwestenkirchner@bendeswehr.org
White	Mark	Mr	USA	AFRICOM	mark.a.white@africom.mil
Wilson	Tony	Mr	USA	AFRICOM	tony.wilson@africom.mil
Wooten	Preston	Mr	USA	JFCOM J7 Rep to EUCOM	wootenp@eucom.mil
Zanin	Bruce	Mr	USA	AFRICOM	bruce.zanin@africom.mil
Zwicker	Trina	Ms	USA	AFRICOM (OTR-PD)	Trina.Zwicker@africom.mil

Appendix 2 to IMISAS Final Report Annex F After Action Reports –

Process Documentation Event

United States Joint Forces Command
Joint Concept Development and Experimentation (JCD&E)

Interagency and Multinational Information Sharing Architecture and Solutions

Process Documentation Event
After Action Report

10 May 2011
Version 1.0

TABLE OF CONTENTS

1.0 Introduction **4**
1.1 Overview **4**
1.2 Event Preparation **5**
1.3 USJFCOM Participants **5**
2.0 Results **5**
2.1 Interview Findings **6**
2.2 Contributions to Development of Current Proposed Solution Set **16**
2.3 Mapping of Findings to Gaps **20**
3.0 Way Ahead **22**
Annex A: Process Documentation Event Questions **1**
Annex B: Interview Process Guide **1**

1.0 Introduction

This document summarizes the findings from the Interagency and Multinational Information Sharing, Architecture and Solutions (IMISAS) Process Documentation Event (PDE) interviews conducted at United States European Command (USEUCOM) and United States Africa Command (USAFRICOM) Headquarters in Stuttgart, Germany from 28-31 March 2011. It documents the preparation, objectives, agenda, outcomes, and way ahead for the IMISAS project as determined from the interviews.

1.1 Overview

The IMISAS team conducted a four-day PDE with USAFRICOM and USEUCOM in Stuttgart, Germany. The intent of the IMISAS project is to develop an operational construct offering enhanced information sharing capability across multiple domains and mission partners. This can be accomplished by providing recommendations for improved processes, procedures and enabling policies in order to establish a collaborative environment promoting unclassified information sharing across organizational boundaries. The purpose of this event was to document the current or 'as is' information sharing architecture with sufficient detail to support the IMISAS Analytic Wargame that will be conducted from 1-4 August 2011.

The team conducted a total of 28 interviews over the four-day period. At USEUCOM, the interviewees included Ambassador Katherine Canavan and representatives from ECJ35, ECJ32, ECJ5, ECJ6, ECJ4 JLOC, ECJ9, ECJ8, and Defense Information Systems Agency (DISA) Europe. At USAFRICOM, the interviewees included the Political Advisor (POLAD), Dr. Raymond Brown, and interagency representatives from the Department of State (DOS), United States Agency for International Development (USAID) and the Department of Commerce. The team also interviewed representatives from the USAFRICOM Foreign Disclosure Office (FDO), Special Security Office (SSO), the Knowledge Management (KM) office, OPS, LOG, SPP, Outreach, and the Canadian Liaison Officer (LNO).

The team met all objectives of the visit. Support from both Combatant Command (COCOM) staffs was excellent; the action officers coordinated with participating directorates, codes, and LNOs to schedule interviews. Additionally, a site visit and walk-through of the venue to conduct the Analytic Wargame was conducted. Team members were also able to gather key insights and lessons learned by observing exercise X24 Europe, a USEUCOM supported exercise integrating social media in an unclassified information sharing Humanitarian Assistance/Disaster Relief (HA/DR) environment.

The interviews captured current policies, processes and procedures for information sharing for the purpose of defining the 'as is' information sharing architecture for the IMISAS project. The focus was on unclassified information sharing (UIS) in a permissive HA/DR context, where the COCOMs, and the Joint Task Force (JTF), when activated, are in a supporting role within the U. S. whole-of-government comprehensive approach. The temporal scope of consideration is from the establishment of the Joint

Planning Team/Operational Planning Team (JPT/OPT) through the transition to JTF operations to achieve a steady state of JTF operations. From a command perspective, the events of interest included all key COCOM (or JTF) interactions from the highest level down to the operational/tactical interface. The interactions between organizations other than those made directly with the COCOM or JTF were excluded. Consideration was limited to major mission components only, focusing on current practices in UIS and on Department of Defense (DOD) capabilities routinely used during HA/DR operations, rather than on planning itself.

1.2 Event Preparation

The PDE was developed as a follow on activity to the Solutions Development Workshop and Initial Planning Conference held 21-25 February 2011. The findings of the PDE complement the research done for the Baseline Assessment Report by documenting actual 'as is' conditions on the COCOM staffs regarding their HA/DR information sharing policies, processes and procedures.

A questionnaire was developed and submitted to the COCOM staff's three weeks prior to the PDE allowing time for proper response and to garner information exchange requirements (IERs) and processes. The responses were documented and provided to USJFCOM three days before the event. The questionnaire is provided in Annex A.

In addition to the questionnaire, a formatted interview process was designed with thirty-one questions that helped to guide the responses relevant to the IMISAS project scope. The interview process guide was used as the method for recording the USAFRICOM responses. Due to security restrictions the USEUCOM team method used hand-written responses. The interview process guide is provided in Annex B.

1.3 USJFCOM Interview Team

Interviews were conducted by LTC Vernon Van Dyne and Mr. Stanley Howard using the interview guide to frame the interview questions for each of the participants from each COCOM staff. The recorders for each interview were Mr. Geoff Boals and Mr. Jimmie Pelton. They noted the responses to all of the interview questions and read back the key takeaways during each interview.

2.0 Results

Section 2.1 delineates the findings from the interviews conducted in terms of the discussions stimulated by the interview questions, and recommendations for improvement made either explicitly by the interviewees or clearly implicit in the context of the discussions. Because USEUCOM and USAFRICOM have significant differences in terms of information sharing maturity and practices, results specific to a particular COCOM are annotated in the detailed discussions of the findings. The mapping of individual observations and their associated findings to existing solutions and their

contributions to continued solution development is detailed in section 2.2. The mapping of findings to gaps is provided in Section 2.3.

2.1 Interview Findings

Recommendations and observations made by the COCOM staffs during the PDE interviews are summarized below. The list is partitioned into internal and external U.S. Government information sharing observations. Although there is not a definitive separation between the two, some challenges affect both internal and external information sharing. Following the summary list are detailed citations of the observations.

Internal U.S. Government Information Sharing Observations: These observations were evaluated by the PDE team as primarily affecting the ability of the military to share information with other government agencies.

A. Lack of knowledge of other government agency roles. (USAFRICOM)
B. The need for the linkage of a "new" UIS system to existing, internal and external unclassified systems and websites. (USAFRICOM, USEUCOM)
C. The need for comprehensive employment of interagency representatives in command planning. (USAFRICOM, USEUCOM)
D. There is a need for requirements and incentives for complete data entry into the UISC and other command information sharing systems and storage tools. (USAFRICOM)
E. The need for the codification of standard operating procedures for HA/DR operations. (USAFRICOM, USEUCOM)
F. The need for training and guidance documentation on document classification and originating authority as well as duties and responsibilities of the FDO. (USAFRICOM, USEUCOM)
G. The need for a selection and the mandated use of one UIS system. (USAFRICOM)
H. The need for the development of business practices for individuals working on multiple security domains. (USAFRICOM, USEUCOM)
I. Lack of understanding and awareness of knowledge management (KM) processes. (USAFRICOM, USEUCOM)
J. The need for a common understanding of information sharing requirements. (USAFRICOM)
K. The inability to accommodate and respond to a wide-range of communications capabilities. (USAFRICOM, USEUCOM)
L. Lack of a Non-Secure Internet Protocol Router Network (NIPRNet) portal. (USAFRICOM)
M. The need for a situation-dynamic HA/DR information release guidance chart. (USAFRICOM)
N. The need to be able to couple requirements information with resource information. (USEUCOM)
O. There is a need for a more agile and comprehensive Request for Information (RFI) management process. (USEUCOM)

External U.S. Government Information Sharing Observations: These observations were evaluated by the PDE team as primarily affecting the military sharing information outside of the government.

P. The need for the establishment of a common network for use by all multinational liaison officers. (USAFRICOM)
Q. The need to review policies and regulations that impede reach back by interagency representatives and the use of external organizations' web-based tools. (USAFRICOM, USEUCOM)
R. A need for any unclassified information sharing capability (UISC) to use business rules that allow the use of open source formats (i.e., Open Office) rather than requiring the use of proprietary formats (i.e., Microsoft). (USAFRICOM)
S. The need for a risk managed approach to information sharing. (USAFRICOM, USEUCOM)
T. The need for social media guidance and business rules. (USAFRICOM, USEUCOM)
U. The need to improve knowledge of, and interaction with, external partners. (USEUCOM)

Internal U.S. Government Observations In-depth:

A. Military staff has shown a lack of knowledge of other government agency roles. A USAFRICOM interviewee made a recommendation to implement an interagency orientation program as well as "listening training" as part of the continued learning program for their staff members.

- An observation was made by USAFRICOM interagency interviewees stating "that military staffs of the COCOM seemed to pay little attention to any briefs but their own during meetings." The interviewees thought that this seeming lack of attention may be based on lack of understanding of roles of the other interagency organizations and might be mitigated through interagency orientation training, to include a course in listening skills.

B. A need to connect the "new" UIS system to the existing databases and tools was voiced by most USAFRICOM interviewees. USAFRICOM recommended that providing access to these tools through a single portal will assist in collaboration and information sharing for the COCOMs - a well-designed interface to these resources could alleviate this problem.

- A set of observations from USAFRICOM reflected the need to include an interface to internal databases and tools (e.g., Overseas Humanitarian Assistance Shared Information System (OHASIS), Civil Affairs databases, Defense Connect Online, etc.) and external information sharing systems such as NGO websites. Interviews conducted at USEUCOM also

indicated the need for the creation of a single, user-friendly interface to simplify access to multiple sources and encourage external participation. Comments were made that portals are too numerous, frequently require a CAC or password authentication for access, and often have interfaces that detract from the discoverability of information. In particular, from one COCOM directorate's perspective, it is difficult to get non-military partners to use APAN because it is simply much easier to access other tools and portals like Facebook and ReliefWeb. Observation of the exercise X24 Europe (taking place during the Process Documentation Event) also provided a valuable opportunity to explore the value of integrated portal technologies. It can be assumed that this single interface would enable better monitoring of HA/DR websites which appear to lack a comprehensive approach, with coverage of individual sites falling within individual directorates - in some cases devolving upon a single person within a directorate. Observation also noted that international sites, particularly those associated with the African Union (AU), are often not monitored.

C. Members of the USAFRICOM staff indicated that interagency interactions within the COCOM are often misinterpreted or misunderstood and they recommended that the COCOM proactively engage with interagency representatives within the command's problem solving process to better realize their potential to contribute to HA/DR operations. The interviewees specifically recommended to launch the initiative by having interagency representatives deliver a brief once a week, and endorse their role as active participants with valuable insight into HA/DR operations and to be included on distribution lists and meeting invitations.

- Observations at USAFRICOM and USEUCOM indicate that there is a tendency for the core directorates to focus on their own lines of activity, leading to shortfalls in integration of interagency representatives. Reciprocally, there are indications that interagency liaisons could better understand and accommodate the military environment and culture into their organizational structures. This "schism" continues to often marginalize the inputs of the interagency liaisons, many of whom if brought into the planning process earlier, could provide agency-unique perspectives that would improve planning for a coordinated Government response. An interviewee stated that without full integration of the interagency representatives, "the OPT won't know what it doesn't know" in terms of the other agencies' responsibilities and perspectives. It was noted by another interviewee at AFRICOM that the situation is improving through the avid engagement of a few individuals in the Future Plans and Outreach directorates and a few key interagency LNO's; including the USAID representative.

D. Members of the USAFRICOM staff interviewed noted the need for a risk managed approach to information sharing which would require and incentivize

data entry into the UISC and other command information systems and storage tools. Their recommendation was that incentives could include an award for the best way to share unclassified information or the most helpful contributors to unclassified information sharing.

- A major challenge identified with unclassified information sharing at USAFRICOM was the lack of unclassified information being entered into the data repository tools maintained by the COCOM.

E. Members of the USAFRICOM staff interviewed recommended that lessons learned and other documents from USCENTCOM and USSOUTHCOM be referenced to inform a HA/DR standard operating procedure (SOP), and that applicable templates from those COCOMs should serve as the standards for USAFRICOM.

- USAFRICOM, as a four year old command, had not yet supported or participated in a HA/DR operation at the time of the interviews, although planning and support of the current Libyan crisis had begun, and guidance had been issued to the Combined Joint Task Force, Horn of Africa (CJTF HOA) to prepare for HA/DR operations in response to the recent Sudan referendum. In response to planning requests it was noted that there was a lack of documented processes and procedures for supporting HA/DR operations. The command was able to develop ad hoc procedures but it was suggested that permanent procedures be developed and implemented. The current ad hoc procedures worked and could be used as the baseline for any newly documented procedures. Specific mention was made for the requirement of the USSOUTHCOM Execution Order (EXORD) as a template that would be of high interest for use in HA/DR responses. Currently, USAFRICOM is developing guidance that includes a Civil-Military Cooperation (CIMIC) Liaison and Coordination Architecture draft appendix to the Deployable Joint Force Headquarters JTF SOP. USEUCOM has a HA/DR SOP under draft review, and has guidance for its HA/DR Working Group (HAWG) based upon a USJFCOM template. USEUCOM's Command Instruction 3111.01 (JTF Headquarters Operations) has been submitted for signature.

F. The need was identified by the COCOM staff for the development of additional training and guidance documentation for USAFRICOM on document classification and originating authority, as well as the duties and responsibilities of the FDO.

- Every interview conducted at USAFRICOM indicated shortfalls in the understanding of the roles and responsibilities of the FDO. The FDO was identified as a key choke point, but discussions with the FDO indicated that this interpretation resulted from a misperception of the FDO's roles and responsibilities. FDOs at USEUCOM were likewise generally

perceived as bottlenecks to information sharing, requiring lead times of up to 2 hours for review of leadership briefs. The OPT's product cycle is further stressed by the sheer magnitude of information that requires vetting during HA/DR operations, which exceeds the existing FDO's capabilities as stated by the Office of Secretary of Defense review of the USAFRICOM FDO office.

G. Members of the USAFRICOM staff interviewed recommended the identification of and mandated use of a single command-standard UIS system. Such a mandate might encourage the collaboration of staff for day-to-day interaction and training through experience, and ensure the availability of a centralized experience base in support of HA/DR operations.

H. Members of USAFRICOM staff interviewed recommended that the command make a decision to mandate the use of NIPRNet as their primary means for sharing information, with the Secret Internet Protocol Router Network (SIPRNet) only used as necessary. The staff observed that a paradigm shift is needed to move both production and briefing activities onto the unclassified domain.

- Prevalent throughout the interviews was the mention of cross security domain challenges where there is a requirement to have the capability to move documents between SIPRNet and NIPRNet (in both directions) for common operations. The amount of time it takes for information to transit this interface greatly extends the amount of time to perform simple, required tasks. USAFRICOM interviews indicated that a majority of staffing was done on the SIPRNet. Some interviewees indicated that they did most of their daily work on NIPRNet; however, where their products were required as part of a larger staffing package, the information was frequently required to be transferred to SIPRNet in order for the staffing action to be checked off as complete. There were reported instances of unclassified Notices to Mariners (NOTAMS) being generated on the SIPRNet and distributed via the SIPRNet Automated *Message* Handling System (AMHS), when the entire NOTAMS subscription base resides on the unclassified domain. A lack of standard business practices for working with multi-security domain information systems was cited, and specific recommendations were made by both COCOMs for a command directive to be developed specifying NIPRNet as a network of first resort, with SIPRNet to be used only as necessary. USEUCOM interviews also indicated a significant demand to migrate HA/DR activity from SIPRNet to NIPRNet, and echoed the necessity of moving unclassified documents from NIPRNet to SIPRNet to have a larger operational impact. Once placed on the SIPRNet, unclassified information must be sanitized and verified as unclassified in order to be transferred back down to the unclassified networks. The process is time-intensive and unevenly employed across directorates within the COCOMs, placing high stress on the OPT product cycle and posing a risk for unintended disclosure.

Nonetheless, information such as logistics stocks is in great demand by agencies who work exclusively on unclassified networks. Particularly challenging is the release of imagery files to unclassified networks. Although sources of unclassified imagery (e.g., Scan Eagle video feeds) are available, they tend to be far inferior to those from classified sources.

I. Interviews from both USAFRICOM and USEUCOM indicated the need for a consistent implementation of, and training on, KM policies, processes, and initiatives.

- USAFRICOM interviewees noted that many documents resident on the current portals are missing data fields necessary to differentiate them from other posted files. Such challenges, while of minor impact in other settings, are particularly impacting to HA/DR-focused operational planning teams (OPTs), which must process very large amounts of information under constantly accelerating operational tempos. The stress of dealing with quick information flows is only expected to increase for some directorates due to manning reductions associated with Secretary of Defense's efficiency initiatives. USEUCOM interviews indicated a significant need for:

  - The standardization of user interfaces;
  - Formatting information (version control, metadata to facilitate searches, etc.);
  - Methodologies for connecting existing resources to needs;
  - Implementing publish/subscribe information streams;
  - Prioritizing and summarizing information;
  - Integrating geographical context into information streams; and
  - Increasing the timeliness of certain reports and the frequency with which planning snapshots are provided to the greater partner community.

  It was noted by USEUCOM interviewees that specific attention should be given to the intuitiveness and the ease of the use of interfaces with tools. A slow web interface may make it untenable to track requests for information (RFIs) in a high-tempo decision cycle, for example, and an awkward interface for attaching metadata may likewise be abandoned under those circumstances. While it is important to implement new tools where the need is clear, decisions regarding their adoption should recognize the users' need for a certain amount of constancy. The search for new tools should not drive the improvement of information sharing but rather should be framed by the evolution of policies, processes and procedures. Finally, a need was indicated by USEUCOM interviewees for comprehensive training on their information management policies and tools. Operation ODYSSEY DAWN triggered the improvement of collaboration and the proliferation of the best information sharing

practices between USEUCOM and USAFRICOM, and this may serve as a springboard for a continued comprehensive familiarization with existing policies. Of note, the KM policy is codified for both COCOMs in European Command Instruction 6001.01 (European Command Knowledge Management), Africa Command Instruction 5600.01 (USAFRICOM Knowledge Management Plan), and Africa Command Memorandum 5600.01 (USAFRICOM Knowledge Management SOP).

J. From discussions at USAFRICOM, there was a cited need to develop a formal set of IERs.

- Some USAFRICOM staff interviewees indicated that there were "tons" of information to share but were unable to indicate specific categories or examples. The interviewees' responses and subsequent review and discussion indicated a lack of common understanding of information sharing requirements.

K. Many of those interviewed on the USAFRICOM staff made the recommendation to review existing communication capabilities and procedures under varying environments, in particular the consideration of augmenting USAFRICOM's telephone capabilities, which might better posture the COCOM to respond to a range of contingencies.

- Critical to HA/DR support is the ability to respond to a wide-range of communications for connectivity in the field. During interviews, the lack of a USAFRICOM voicemail system was cited as a major problem particularly exacerbated given the relative scarcity of internet access on the African continent and consequent prevalence for the use of the telephone system as a major information sharing tool under normal conditions. It was also pointed out by USAFRICOM's Foreign Policy directorate, that communications are typically among the first casualties of an HA/DR contingency, and situational awareness is often initially established via lower technology means. Radio often provides this means, but in situations involving conflict even radio communication can be prevented by jamming, and information transmission may become relegated to foot, car or horse. Knowledge about the status of infrastructure, scope of current response, or existence of political conflict can be greatly facilitated by establishing temporary networking, telephone, or television points of presence in the field. Those locations and connection modes should be communicated as rapidly as possible to responding partners. The reciprocal is also true, particularly in noncombatant evacuation operations (NEO), where the establishment of the evacuation control center is keyed to the availability of key telecommunication nodes. Based upon the use of dedicated commercial digital subscriber line (DSL) connections provided for unclassified internet connectivity during the recent exercise X24 Europe, one

USEUCOM directorate representative interviewed cautioned against the headquarters' becoming dependent upon high-level applications possibly not supportable at JTF level, and almost certainly not at unit level, where field information originates.

L. USAFRICOM interviewees expressed the desire for a decision to develop and mandate the use of a NIPRNet portal as a primary venue for sharing unclassified information.

- Every interviewee from the USAFRICOM staff indicated the lack of a USAFRICOM NIPRNet portal as a major impediment to information sharing. This leads to overuse of the SIPRNet for unclassified activity, and in particular the use of the SIPRNet portal as the only source for the storage of unclassified documentation.

M. Following a discussion of a possible scenario to develop an understanding of KM requirements, the creation of a HA/DR information release guidance chart that will address different phases of a crisis was identified by some USEUCOM staff members as an opportunity to improve responsiveness.

- The chart would be updated by the security management representatives to facilitate instant response to HA/DR operational needs, and would reference the guidance documents defining the requisites for information release, and the processes required to release the data. This lack of guidance was indicated by several interviewees to be a significant problem.

N. The USEUCOM staff interviewed suggested that the data fields be better organized within the OHASIS system to match resources to requirements and allow better tracking within the commands.

- There was acknowledgement of a general need for greater timeliness, visibility, aggregation and de-confliction of information concerning requirements consumed by USEUCOM directorates. Coordination with external partners, and ultimately efficiency of resource use, would also benefit from a closer coupling of information on requirements and identified resources. Web technologies offer the possibility of concentrating information feeds of both types, and composing and displaying the information in ways that facilitate matching them.

O. A recommendation to improve the scope and utility of the RFI management processes was suggested by USEUCOM staff members interviewed.

- RFIs supporting the USEUCOM OPT process are managed using the TMT. However, the system does not footprint all RFI activity. Some RFIs occurring during low tempo operations are handled in an ad hoc

manner, while during recent high tempo operations (specifically, one directorate's planning in support of the current contingency in Libya), the TMT interface was not agile enough to keep up with the volume of requests, necessitating an offline tracking solution. A USEUCOM ECJ2 representative pointed out the possibility of opening up the RFI process to incorporate information from external sources.

External U.S. Government Observations In-depth:

P. Recommendations from the multinationals supporting USAFRICOM included the creation of a network on which all the LNOs can work.

- The absence of a NIPRNet portal and the current policy restrictions allowing only certain trusted partners to operate on the SIPRNet present a challenge for those LNOs not granted SIPRNet access.

Q. Interviewees at USAFRICOM indicated the need to review policies and regulations that impede reach back by interagency representatives and the use of external organizations' web-based tools.

- Interviewees at USAFRICOM indicated an inability to access certain information posted on the web sites of NGOs and other external organizations due to ActiveX components being blocked by the DOD system. This suggests a need to review interface regulations that prevent the use of nongovernmental organizations' web portals and tools. USEUCOM's ECJ9 Interagency representatives face a similar problem, being impeded in communication with their stateside offices by the inability of the latter to access the USEUCOM unclassified web portal or send emails through USEUCOM's .mil exchange server. The result is an end of day "bread line" for use of webmail services over ECJ9's few DSL terminals. This was a challenge that impacted USEUCOM's exercise X24 Europe requiring additional external DSL lines. In general, there is a problem across the unclassified internet, for example, where emails sent between disparate domains (e.g., from TRANSCOM.mil to EUCOM.mil) are stripped of attachments or undelivered due to mismatches in file size or type restrictions between servers.

R. USAFRICOM interviewees stated the need for any unclassified information sharing capability (UISC) to use business rules that allow for the use of open source formats (i.e., Open Office) rather than requiring the use of proprietary formats (i.e., Microsoft).

- The USAFRICOM staff indicated that African nations would not have access to some of the proprietary software formats and tools used by the COCOM. The use of open formats would allow the African countries to interact effectively.

S. The COCOM interviewees indicated that a dynamic risk-managed approach, one that ensured the prompt release of information necessary to save lives, should be the goal for HA/DR.

- USAFRICOM interviewees mentioned that the staff currently exercises a risk averse approach to information sharing, one that is ineffective in HA/DR responses. USEUCOM interviewees also echoed a tendency for excessive internal vetting of products. One directorate suggested, as an alternative, the use of a BLOG format to develop OPT products with full participation by interagency representatives from the outset, in order to mitigate groupthink, reduce the risk of proceeding with untenable plans, and facilitate convergence upon good ideas faster than would otherwise be possible.

T. Staff at both COCOMs made the recommendation to develop processes and procedures for social media integration.

- During the Process Documentation Event interviews, exercise X24 Europe was taking place. This event was a springboard for creating operational guidance and business rules for the use of social media, including mechanisms like Crowdsourcing, a capability whose use at both USEUCOM and USAFRICOM is currently both irregular and infrequent. Although no codified process is evident for integrating social media into operations, its potential to improve mission effectiveness was largely acknowledged, particularly by the USEUCOM ECJ5, ECJ35, and Public Affairs directorates. Several directorates representatives agreed that for USEUCOM to work more effectively with its external partners, its transactions in unclassified information should shift outward toward the social media hubs and tools those organizations frequent. One directorate cited the use of chat rooms by merchant vessels to exchange information about pirates operating in the Gulf of Aden. This and other ad hoc networks set up by nongovernmental agencies are largely preferred over dedicated portals, and because their formation is agile and intimately keyed to the desires of their community of interest. From the control perspective, one USEUCOM directorate representative cautioned that the use of social media could be dangerous without mechanisms to validate the information and define acceptable levels of credibility. Another voiced the need to define responsibilities for monitoring social media outlets throughout the various stages of operations.

U. Both COCOMs identified the need for processes and procedures to be developed to allow inclusion of external (to DOD) partners that are not traditionally included on an ‘on demand’ basis.

- Interviews with USAFRICOM staff indicated a desire to engage the private sector in HA/DR operations; however, such engagement is hindered by the lack of guidance on processes to include them. Additionally, the ability to include experts or academics into the planning and operations for HA/DR is not well developed, resulting in the loss of potential opportunities. Interviewees stated that USEUCOM continues to have relationship challenges with external partners, particularly in discerning the identities and activities of organizations in the field. Reportedly, USEUCOM's external partners want to collaborate as much as possible, and there is fertile ground for better, faster information sharing with these actors. Specific challenges include physical separation, which makes it hard to develop camaraderie; disparate vocabularies, which lead to conflicts in coordination; innate lack of knowledge of which organizations will respond to a given contingency; and information security concerns, which pose barriers to continuity of information sharing (as with a recent "Baltic Round Table", to which USEUCOM ECJ9 invited country representatives, but was unable to tell them why they were being asked to participate). The Strategic Environmental Assessment Program is an effort that seeks to overcome these barriers through cultural analysis, sharing of contacts and situational awareness, and organizing venues to bring the outside community and "J-codes" together to share information.

2.2 Contributions to Development of Current Proposed Solution Set

The findings of the PDE generated no additional proposed solutions. However, they significantly contributed to the body of investigation for developing solution elements and their associated physical products. In some cases, the PDE findings led to a restatement of the solution statement itself. Additionally, the PDE findings are expected to inform the development of the Policy and Procedures Handbook. With the exception of some specific technical solutions there is little "orphaning" of either the solution set or the PDE findings in their comparison. This in a sense validates the previous work performed by USAFRICOM, USEUCOM, and the IMISAS team at the initial site survey and subsequent conferences where gaps and solutions were identified and refined. Discussed below by individual solution are the expected contributions of the PDE findings to the solutions continued development.

Solution 1-1: *Policy and procedures for the expedited release of controlled unclassified information in a crisis response situation.* The PDE's recommendations for a situation-dynamic HA/DR information release guidance chart and a risk-managed approach to information sharing were combined into a single deliverable (graduated criteria for unclassified information release based on Operational Risk Management). USAFRICOM's recommendation for a collaborative unclassified information sharing space was included as a solution element and associated deliverable (business rules for unclassified data storage on UISC). Three solution deliverables are under development

(procedures for For Official Use Only, procedures for foreign disclosure of controlled unclassified information, and procedures for public release of unclassified information). These will include elements of PDE recommendations to incentivize complete data entry into the UISC, develop policies and procedures to include non-traditional partners, and provide training and guidance on the classification origination authority and duties and responsibilities of the Foreign Disclosure office.

Solution 1-2: *Business rules governing the expedited transfer of unclassified information from classified networks to non-classified networks.* The PDE's recommendation for business practices for working on multiple security domains informs the development of the two deliverables (manual procedures for cross-domain transfer, and business rules for unclassified data storage on UISC) for this solution. Additionally, development of these deliverables is informed by the PDE's recommendations for training and guidance documentation on classification origination authority, better implementation of and training on KM processes, and documentation of information sharing requirements.

Solution 1-3: *Pre-defined templates and business rules for the establishment of UISC [portal] work sites in support of HA/DR operations.* The two deliverables for this solution (APAN worksite, and business rules for portal establishment) directly address the PDE recommendations for selection and mandated use of one UIS system, development of an unclassified information sharing portal, and establishment of a common network for use by all multinational liaison officers. Development of these deliverables is informed by the following PDE recommendations:

- Better implementation of and training on KM processes;
- Coupling of requirements information with resource information;
- Review of interface regulations that impede reach back by Interagency representatives and use of external organizations' web tools;
- Guidance and business rules on social media; and
- Linkage of "new" UIS system to existing internal and external unclassified systems and websites.

Solution 1-4 was combined with Solution 1-3.

Solution 1-5: *Processes and procedures to enable unclassified information sharing with mission partners via UISC.* The deliverables for this solution are approaches and SOPs for coordination with academia, interagency, host nation, intergovernmental organizations, and non-governmental organizations. These deliverables are directly supported by the PDE's recommendations to engage private sector in HA/DR operations, and to improve knowledge of, and interaction with, external partners. The deliverables are implicitly supported by the recommendations for training for better understanding and integration of products provided by Interagency LNOs, and comprehensive employment of interagency representatives in command planning. The following PDE recommendations inform development of these deliverables:

- Incentivize data entry into the UIS;

- Develop policies and procedures to include non-traditional partners;
- Situation-dynamic HA/DR information release guidance chart; and
- Risk-managed approach to information sharing.

Solution 1-6 was combined with Solution 1-7.

Solution 1-7: *SOPs for combatant commands to utilize the UISC in support of HA / DR operations.* The deliverables for this solution include SOPs for unclassified information management; information sharing, collaboration, coordination and cooperation via UISC; use of LNOs to facilitate integration and access, and an electronically searchable handbook available to watch standers/UISC users. The following PDE recommendations directly inform further development of these deliverables:

- Better implementation of and training on KM processes;
- Coupling of requirements information with resource information;
- Review of interface regulations that impede reachback by interagency representatives and use of external organizations' web tools;
- Guidance and business rules on social media; and
- Linkage of "new" UIS system to existing internal and external unclassified systems and websites.

Solution 1-8: *Quick reference guides for the roles, responsibilities and general information requirements of potential mission partners for combatant commands in HA/DR operations.* The PDE recommendations supporting the deliverables for this solution are:

- Develop policies and procedures to include non-traditional partners;
- Improve knowledge of, and interaction with, external partners;
- Develop documentation of information sharing requirements.

Solution 3-1: *Business Rules to define data types, standards, metadata requirements that facilitate posting, transfer and use of data.* The PDE recommendation for better implementation of and training on KM processes addresses this solution fully, and the underlying discussion points supporting the recommendation are expected to inform the development of the solution elements. Additionally, the following PDE recommendations inform the deliverables for this solution:

- Linkage of the "new" UIS system to existing internal and external unclassified systems and websites;
- Requirements and incentives for data entry into the UIS and other command information systems and storage tools;
- Business practices for working on multiple security domains;
- Develop documentation of information sharing requirements;
- Accommodating and responding to a wide range of communications capability;

- Coupling requirements information with resource information;
- Improving the scope and utility of the RFI management processes
- Use of open source (i.e., Open Office) formats vice proprietary formats (i.e., Microsoft).

Solution 4-6: *Graduated user account permissions and procedures for anticipated and unanticipated users to facilitate allocating access to different levels of unclassified information based on trust.* The PDE recommendations associated with this solution center on the dynamic balance between releasable unclassified information and controlled unclassified information. Implicit in that division are the differences in the external partner organizations the COCOM is expected to engage. Development of the deliverables associated with this solution (business rules and granular permission structure within the UIS portal) will thus be informed by the following PDE recommendations:

- Situation-dynamic HA/DR information release guidance chart,
- Improving the scope and utility of the RFI management processes,
- Establishment of a common network for use by all multinational liaison officers,
- Engage private sector in HA/DR operations,
- Risk managed approach to information sharing, and
- Improve knowledge of, and interaction with, external partners

Solutions 4-8: *UIS capability to push or post aggregated data from dynamic sources to mission partners.* The PDE discussion germane to this solution was the need to leverage the benefits of social media while ensuring mechanisms to manage the information and ascribe levels of reliability to that information. The directly applicable PDE recommendations are therefore processes and procedures for social media integration, and better implementation of and training on KM processes. The following recommendations relate to the need to dynamically define the level of metadata required for information to be considered reliable:

- Situation-dynamic HA/DR information release guidance chart; and
- Risk-managed approach to information sharing.

Solution 4-11: *Source authenticity and information reliability capability for UISC use in filtering and verification of real-time data from channels such as Twitter, SMS, email and RSS feeds.* The business rules and technical capability associated with this solution are directly supported by the PDE recommendations for a situation-dynamic HA/DR information release guidance chart and risk-managed approach to information sharing.

Solution 4-12: *UIS search capabilities (federated or integrated).* Most directly supporting the development of the filters, metadata tags, and business rules associated with this solution are the PDE recommendations for better implementation of and training on KM processes and documentation of IERs. The COCOMs' KM plans and other

applicable HA/DR related documentation will also serve as a guide for defining search categories.

2.3 Mapping of Findings to Gaps

No additional gaps associated with unclassified information sharing were identified, although one finding did not map to existing gaps. This finding (the need to codify standard operating procedures for HA/DR operations) is a challenge related to the operational context of information sharing, but is not germane to information sharing itself. For reference, the list of the eight gaps agreed upon during the Solutions Development Workshop/Initial Planning Conference is provided below, followed by Table 1, which provides the mapping of those gaps against the PDE findings summarized in section 2.1.

Identified capability gaps:

1. Combatant and Joint Force Commander staffs lack sufficient knowledge, skills, and abilities to understand the roles, responsibilities, limitations, authorities, potential contributions, and information exchange requirements of interagency and other potential mission partners, resulting in ineffective information exchange.
2. Inconsistent information management schemes among existing DoD web portal implementations and standards impede information sharing among Combatant and Joint Task Force staffs and with partner responders, resulting in needless duplication of information, inefficient searches, lapses in event coordination, poor presentation of information to target audiences, and general information overload.
3. Combatant and Joint Force Commander staffs are impeded in rapid establishment of dynamic information sharing environments and sharing of information (e.g., government-provided imagery products) by inadequacy of procedures and restrictive interpretation and inflexibility of information sharing policies.
4. Information sharing between Combatant and Joint Force Commander staffs and USG Interagency and other mission partners is impeded by the incompatibility of the DOD's hierarchical information exchange methodologies/processes and USG Interagency and other mission partners with decentralized or ad-hoc processes.
5. Manual cross domain transfer mechanisms currently in place are cumbersome and inefficient, adversely affecting operations. Diverse military cultural and operational constraints among Combatant and Joint Force Commander staffs necessitate work on multiple classified and unclassified government networks, as well as non-classified domains accessed via civilian internet service providers.
6. Without a common strategy and standard procedures for effective integration, Combatant and JTF Commander staffs lack the ability to access and interpret valuable information in the public domain, such as social media.
7. Deleted

8. Combatant and Joint Force Commander staffs lack a DOD UISC that is flexible, accessible, user-friendly, and interoperable across the broadest pool of mission partners. This UIS should be standard across DOD to minimize the need to train on a new tool when DOD personnel transition to a new AOR.
9. Combatant and Joint Force Commander staffs lack processes and procedures to include mission partners in existing DOD systems and networks for information sharing and access mission partners systems and networks for information sharing.

Finding Number	External/Internal	PDE Finding	Associated Gaps
A	Internal	Lack of knowledge of other government agency roles. (USAFRICOM)	1
B	Internal	The need for the linkage of a "new" UIS system to existing, internal and external unclassified systems and websites. (USAFRICOM, USEUCOM)	2, 8
C	Internal	The need for comprehensive employment of interagency representatives in command planning. (USAFRICOM, USEUCOM)	1
D	Internal	There is a need for requirements and incentives for complete data entry into the UISC and other command information sharing systems and storage tools. (USAFRICOM)	3, 5
E	Internal	The need for the codification of standard operating procedures for HA/DR operations. (USAFRICOM, USEUCOM)	None
F	Internal	The need for training and guidance documentation on document classification and originating authority as well as duties and responsibilities of the FDO. (USAFRICOM, USEUCOM)	3, 5
G	Internal	The need for a selection and the mandated use of one UIS system. (USAFRICOM)	2, 8, 9
H	Internal	The need for the development of business practices for individuals working on multiple security domains. (USAFRICOM, USEUCOM)	5
I	Internal	Lack of understanding and awareness of knowledge management (KM) processes. (USAFRICOM, USEUCOM)	1, 2
J	Internal	The need for a common understanding of information sharing requirements. (USAFRICOM)	1, 2
K	Internal	The inability to accommodate and respond to a wide-range of communications capabilities. (USAFRICOM, USEUCOM)	8
L	Internal	Lack of a Non-Secure Internet Protocol Router Network (NIPRNet) portal. (USAFRICOM)	8, 9
M	Internal	The need for a situation-dynamic HA/DR information release guidance chart. (USAFRICOM)	3
N	Internal	The need to be able to couple requirements information with resource information. (USEUCOM)	2, 3, 4, 5, 6, 9
O	Internal	There is a need for a more agile and comprehensive Request for Information (RFI) management process. (USEUCOM)	2, 6, 9
P	External	The need for the establishment of a common network for use by all multinational liaison officers	8, 9
Q	External	The need to review policies and regulations that impede reach back by interagency representatives and the use of external organizations' web-based tools. (USAFRICOM, USEUCOM)	8

Finding Number	External/Internal	PDE Finding	Associated Gaps
R	External	There is a need to use open source (i.e., Open Office) formats vice proprietary formats (i.e., Microsoft). (USAFRICOM)	1, 3, 4, 8, 9
S	External	The need for a risk managed approach to information sharing. (USAFRICOM, USEUCOM)	2, 4, 6
T	External	The need for social media guidance and business rules. (USAFRICOM, USEUCOM)	1, 3, 4, 9
U	External	The need to improve knowledge of, and interaction with, external partners. (USEUCOM)	9

Table 1: Mapping of PDE findings to IMISAS Capability Gaps

3.0 Way Ahead

During the 19 – 22 April 2011 IMISAS Mid-Planning Conference, the IMISAS Community of Interest and IMISAS Project Team examined each potential solution in depth from perspectives of specific solution elements, metrics to demonstrate solution effectiveness, scenarios and vignettes to assist with experiment context, actions necessary to stimulate the associated variables, manning and infrastructure requirements to support experimentation, and the control plan for execution of the analytic wargame. Metrics and data gathering methodology in support of the technical spirals were also discussed, both in plenary and during breakout sessions. Insights and recommendations gleaned from PDE discussions have already been incorporated into the ongoing solution refinement process, and their specific contributions will continue to be leveraged to the maximum extent possible during regularly convening solution refinement working groups. The PDE insights and recommendations will be used to refine solution statements as necessary, clarify and make more explicit individual solution elements and associated physical artifacts, establish differences between the ‘as-is’ and ‘to-be’ cases for experimentation, and inform the means of stimulating experiment play as required to examine the potential solutions.

Annex A: Process Documentation Event Questions

I. **Overview and Scope.** The following questions are intended to capture current processes and procedures for information sharing for the purpose of defining the "as is" information sharing architecture for the IMISAS project. The focus is on Unclassified Information Sharing (UIS) in a permissive Humanitarian Assistance/Disaster Relief (HA/DR) context, for which the COCOM (and JTF when activated) is in a supporting role within the US whole of government response. The temporal scope of consideration is from Joint Planning Team/Operational Planning Team (JPT/OPT) establishment through transition to JTF operations to achievement of steady state JTF operations. From a level of command perspective the events of interest include all key COCOM (or JTF) interactions from highest level down to the operational/tactical interface. Excluded are interactions of other organizations other than those made directly with the COCOM or JTF. Consideration should be limited to major mission components only, focusing on current practices in UIS and on DOD capabilities routinely used during HA/DR operations, rather than on planning itself.

II. These questions serve as a point of departure for a data collection event scheduled with USAFRICOM and/or USEUCOM staff members from 28 March – 31 March 2011. The expectation is that these preliminary questions will be completed by respective staff codes prior to the arrival of the data collection team. Responses to this questionnaire will serve as a starting point for detailed interviews during the visit. The interviews will more fully document the information sharing activities associated with the command's HA/DR mission, the attributes of information exchanges supporting those activities, and the systems supporting those information exchanges.

III. The target audience for this questionnaire as well as the collection event includes those COCOM and or JTF staff codes and LNOs routinely involved with HA/DR events from JPT/OPT to steady state operations. Although the collection team defers to the operators for final determination of the interviewees, the following staff codes are recommended for initial consideration: USAFRICOM - IKD, OPL, SPP, C4S, JFD, Outreach and USEUCOM - J35, J2, J4, J5, and J6 Desk Officers as appropriate.

IV. **Scenario Synopsis** – "Disaster in Goma", 16 July 2020

This scenario is provided to set the scene and context for pre event and interview questions. It represents a snapshot of the scenario anticipated for the IMISAS experiment. However, respondents are also encouraged to draw on their most recent experiences with the Libyan crisis when considering responses.

SITUATION: Mt. Nyiragongo volcano erupted this morning 16 miles north of the city of Goma, Democratic Republic of the Congo. Initial reports indicate 25 people were killed, and it appears several hundred thousand persons will be displaced. In addition, the US will support a UN HCR

response from the UN location in Entebbe, Uganda. The Ambassador, in coordination with the Assistant Secretary for African Affairs, has established a team in the Operations Center and a location on the State INTELINK. USAFRICOM has been tasked to establish a JTF and to deploy 2500 troops from the US Army Africa location in Italy to support humanitarian relief locations outside the city. The mission of the JTF is to support feeding, medical care, and the distribution of clean potable water due to potential contamination caused by the ash plume. Lava has cut the city's main airport runway, making it unusable for at least a month.

V. Process Documentation Event Plan

a. Interview Process:

The interviews will be following the Diamond interview structure model. This model starts with closed questions and works to open questions then focuses answers with closed questions at the end of the interview. The time period for a one hour interview will be 15 minutes of closed questions, 30 minutes of open questions, and a closing 15 minutes of closed focused questions. For interviews that occur over several time blocks the interviewer will follow the diamond structure but will skip the warming up questions that have already been answered.

The interviewers will be walking into the interviews with a set of introductory questions answers, and research into the techniques, tactics, and procedures as well as standard operating procedures for the COCOMs. These answers guide the topics of discussion through the interview but the data collection items will remain constant for all interviewees. The gathering of data required to develop a DODAF level diagrams is the end goal of the interview and the closed questions will be reflected in those requirements.

b. Exercise 24 Europe (X24 Europe):

It would be advantageous to have the interview team observe some of the X24 Europe event and gather any "Lessons Learned" and data. This could be a passive data collection event, however if any of the staff are available for a brief period of time during the event, it would be valuable to conduct brief interviews after observing the event. Alternatively scheduling follow up interviews through Adobe Connect Online would valuable. USEUCOM provides the Rules for Engagement for observation of the exercise.

c. Liaison Officers (LNO):

All the liaison personnel are touch point nodes and should be interviewed. The interviewers will need a listing of all LNO's.

VI. <u>Pre Event Questions</u> (to be interpreted in the context of a permissive HA / DR contingency).

Name:
Organization/Code:
Role:
Phone:
Email:

A. With regard to planning prior to establishment of a JTF and/or Civil/Military Operations Cell (CMOC):
1. Which codes or directorates are typically involved in the planning?
2. What authority typically triggers the COCOM's JPT/OPT?
3. What LNOs are typically involved in the JPT/OPT process?

B. What organizations do you work with external to your command during a permissive HA/DR operation? Examples are:
1. Other DoD activities (e.g., higher headquarters, subordinates, peers)
2. Civilian interagency (e.g., Department of State, US Agency for International Development (USAID))
3. Intergovernmental organizations (e.g., European Union (EU), Organization for Security and Cooperation in Europe (OSCE), African Union (AU), North Atlantic Treaty Organization (NATO))
4. International Organizations (e.g., International Committee of the Red Cross (ICRC), United Nations (UN))
5. Nongovernmental Organizations (e.g., InterAction, Doctors without Borders, World Food Program)
6. Host Nation
7. U.S. Embassy

C. Are there any Standard Operating Procedures (SOPs) or directives that govern your command's HA / DR internal response or outreach to external organizations? Examples include:
1. ECI 3111.01
2. CONPLAN 4269
3. Multinational Planning Augmentation Team (MPAT) SOP v2.5

D. What major recurring activities do you perform in support of HA / DR operations?

E. For each of the above activities, what are the Information Exchange Requirements (IERs) both within your organization and with outside organizations?
1. What is the content of the information you share?
2. What are the classifications and classification caveats associated with the information?

3. Which organization and office code do you exchange this information with?
4. Who is the person/role that usually shares this information?
5. What are the format types (e.g., database, document, spreadsheet, conversation) of the information you share?
6. Where is the information stored?
7. What is the transmission security level?
8. How is this data transmitted and received? (e.g., telephone, email, portal post, letter, word of mouth, social networking sites)

F. Are there barriers (networks, polices, procedures) to your information exchanges? If so, what are they?

G. What do you do if you don't get the information you request/what alternative information exchange vehicles are available?

H. What do you do if you cannot exchange the information requested of you/what alternative routes/networks, portals (APAN, InRelief, HarmonieWeb, etc.) might be used?

Annex B: Interview Process Guide

A. (Interview Time: 0-10) Information Sharing SOP, TTP (Time for Question Block: 10 minutes) 0900

1. What information is required to be shared?
    i. Where do you get your information?
2. Do guidelines or SOP's exist governing the handling, transfer and dissemination of the information?
    i. (If Yes) Can you please send us a copy after this interview?
3. How is the handling, transfer and dissemination of information initiated?
4. How is data / information summarized for review?

B. (Interview Time: 10-12) UIS Tools (Time for Question Block: 2 minutes)

5. Have you used Social Media in support of HA/DR operations?
    i. (If Yes) Which Social Media Tools?
    ii. (If Yes) Which operations do those tools support?
    iii. (If Yes) How are Social Media Tools used?
6. What Portals do you use to share information on?
    i. (If APAN listed) Have you used APAN operationally?
    ii. (If APAN listed) What is your command's KM strategy for APAN?

C. (Interview Time: 12-28) Department Goals, Objectives, Procedures (Time for Question Block: 16 minutes)

7. What are the critical objectives of your department?
8. Who is responsible for the coordination and prioritization of information sharing requirements?
    i. Who has information sharing release authority?
9. What are your business rules/relationships regarding information sharing with other organizations?
    i. (If known) Can you provide to us the business rules after the interview?
10. How do you employ Liaison Officers (LNO's) with respect to information sharing in your organization?
11. What information do you see your organization as being able to share that is useful to others in a civil-military partnership or endeavor?
12. Are there other partners you would like to share information with?
    i. (If yes) Can you name them?

13. What required information are you not receiving?
    i. (If known) Who should provide this information?
    ii. (If known) How should it be provided?
14. What required information are you receiving?
    i. What mission activity or activities directly require the information element?
    ii. Who is providing it?
    iii. How is it provided?
15. How is shared information used by the chain of command as far as decision making goes? Example: Support CCIRS, intelligence brief.
16. How often do you share information across security domains?

D. (Interview Time: 28-38) Partners Information Handling (IO, IA, NGO, Host country, Inter office) (Time for Question Block: 10 minutes)

17. Is the information altered (sanitized: ClassUnClass/Message Control) before it reaches its destination?
    i. (If yes) How is information altered?
18. Describe the monitoring process for data updates on the HA/DR website.
19. How does an organization coordinate a request for information?
20. How much of the information is actually used by the external organizations with whom you collaborate (e.g., NGOs, other agencies)?

E. (Interview Time: 38-42) Partners conflict (Time for Question Block: 4 minutes)

21. What existing governmental, intergovernmental and nongovernmental written authorities are in conflict; negatively impacting information sharing and collaboration?
22. What existing procedures have proven ineffective and detract from information sharing and collaboration?

F. (Interview Time: 42-52) What can be changed to improve what is wrong? (Time for Question Block: 10 minutes)

23. List your top two priorities for improving information sharing at your command.
24. What is your biggest frustration with information sharing?
    i. (If known) How can this be resolved?
25. What kinds of data errors are commonly made in your information exchanges?
26. What interoperability shortfalls inhibit information sharing and collaboration?
27. In your opinion, what is the effectiveness of information sharing in your command?
    i. What information is effectively shared?

ii. What information is ineffectively shared?

28. What procedural changes would be required to enable/improve information sharing and collaboration?
29. Is there anything not covered or discussed that we should know to improve the commands information sharing?
30. Is there anything from a prior organization/command that could be integrated to improve your current command's information sharing?

Mid-Planning Conference

United States Joint Forces Command
Joint Concept Development and Experimentation (JCD&E)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS)

Mid-Planning Conference After-Action Report

5 May 2011

Purpose: This document summarizes the results from the Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Mid-Planning Conference (MPC), 19-22 April 2011, held at the MITRE office in the Bridgeway Technology Center, Suffolk, Virginia (USA). The primary purpose of the MPC was to further define the shape and scope of the IMISAS Analytic Wargame (AWG) scheduled for 1 – 4 August 2011.

Background: The IMISAS project's intent is to improve information sharing between the U.S. Department of Defense (DOD) and a wide variety of non-military mission partners, who may include civilian U.S. government agencies, other nations, inter-governmental organizations, and nongovernmental organizations. The project planning incorporates an appreciation for the value of joint experimentation and a thorough understanding of experiment design principles.

In December 2010, the gaps and potential solutions were presented, validated and prioritized at the Stakeholder/Gap Validation Conference. The IMISAS team incorporated the results of the conference and completed a Baseline Assessment Report (BAR) in support of the problem statement: "COCOMs lack a coherent framework/capability to share information and collaborate across multiple domains with a broad range of mission partners (government/interagency, multi-national, multi-lateral & private sector) due primarily to restrictive policies, conflicting authorities, ad hoc/non-existent procedures, business rules and non-interoperable networks and systems."

In February 2011, a Solution Development Workshop (SDW)/Initial Planning Conference (IPC) was held at United States European Command (USEUCOM) in Stuttgart, Germany. The purpose of the event was to further refine the capability gaps initially identified in the baseline assessment, to evaluate potential solutions for experimentation value and further development and to shape planning for the project experiment. The IMISAS team presented and validated specific gaps identified in the BAR and reviewed the initial cut on multiple potential solutions which would be viable for experimentation. The SDW sessions set the stage for the beginning of the planning process for the scheduled August 2011 AWG.

The IMISAS team conducted a Process Documentation Event, 28-31 March 2011, at United States Africa Command (USAFRICOM) and USEUCOM headquarters. The objective of the event was to define the "as-is" information sharing environment and processes. The results from this event provided validated documentation in support of continued event design and planning, and set the conditions for further refinement during the MPC.

MPC Objectives: During the MPC, the conference participants addressed and accomplished the primary MPC objectives listed below:

- Agreed on solutions for examination in the AWG;
- Identified technical spiral requirements and schedule;

- Obtained all inputs required to complete a draft Event Directive (ED);
- Agreed on a draft Experiment Manning Document (EMD);
- Developed scenario vignettes' requirements;
- Continued refinement of the Data Collection and Analysis Plan (DCAP); and
- Agreed on the Final Planning Conference (FPC) objectives.

MPC Execution:

The IMISAS sponsors and primary partners, USAFRICOM, USEUCOM as well as the Office of the Secretary of Defense, Networks and Information Integration/Chief Information Officer (OSD NII/CIO), fully participated and provided subject matter expertise. Additional representatives from the following organizations attended: United States Pacific Command (USPACOM) (Pacific Warfighting Center/All Partners' Access Network (APAN)), Department of State - Humanitarian Information Unit, Defense Information Services Agency (DISA), J9 German Foreign Liaison Officer, Bundeswehr Transformation Center, NATO Civil Military Fusion Center (CFC) and USJFCOM Joint Public Affairs Support Element (JPASE), J6 and J8. A complete list of conference participants can be found in Annex A.

The MPC participants agreed on the shape and scope of the IMISAS AWG to be conducted, 1-4 August 2011 at Patch Barracks, USEUCOM, Stuttgart, Germany. MPC participants successfully accomplished all the pre-identified conference objectives including the validation of high-level potential solutions to be examined, discussion of the proposed foreign humanitarian assistance scenario focused on multi-organizational unclassified information sharing, and refined planning of the key experiment design elements. The MPC agenda is included as Annex B of this report.

The IMISAS experiment event design refinement, as conducted during the MPC, was a creative cognitive process that envisaged possibilities and employed proven experiment design principles to provide coherent, integrated, and achievable demonstration and experimental events. The evolving experiment event design reflects the IMISAS partners and stakeholders' guidance with regard to allocation of resources, preparation of experimentation activities, management, and synchronized event execution. This experiment event design also identified critical event dependencies, long-lead items, and preparatory events required for key activities. The design is flexible enough to make adjustments to the event as available resources among the participants change (time, money, personnel, etc.), or as new opportunities arise.

During the MPC, the conference participants validated the high-level potential solutions to be evaluated during the technical spirals and the AWG. This validation included identifying the linkages between gaps – solutions – key elements of the solutions – transition – experimental event considerations. Experimental event considerations included analysis, metrics and measures, and scenario event stimulus requirements. A complete list of the potential solutions to include linkages and event considerations is included in Annex C of this report.

The MPC participants reached agreement on the basic elements of experiment design to include: timing and locations; concept of operations; plus identification of mission-essential tasks and responsibilities. During the MPC, the participants agreed to conduct an AWG at the Rodgers Center at Patch Barracks (Stuttgart, Germany), 1–4 August 2011. Day 1 of the event will be devoted to pre-experiment orientation and collective training for all participants. The AWG execution will be a two-day event (Tuesday and Wednesday, 2-3 August 2011). On Day 4 (Thursday, 4 August 2011), there will be a fifth experiment period for reattack on any solution followed by a half-day after-action review and survey for all experiment participants, both the experiment audience plus the role players and response cells.

The AWG is focused on the sharing of unclassified information with non-DOD mission partners in a notional USAFRICOM operation in support of a multinational, civilian-led humanitarian assistance and disaster relief operation in Central Africa. The AWG will be an unclassified event consisting of an introductory scene-setter and two separate scenario vignettes linked to the USAFRICOM CONPLAN 7200-09. The vignettes provide the specific context for examining solutions dealing with unclassified information sharing among mission partners. The vignettes will shape the experiment environment to examine the effectiveness of the proposed solutions in addressing information-sharing challenges.

The AWG participants (experiment audience) will consist of military and civilian interagency planners who would emulate a crisis action planning team working at the Combatant Command level. The experiment audience will consist of 15-to-25 seminar participants drawn primarily from the USEUCOM and USAFRICOM staffs. In addition, role players and response cells will interact with the experiment audience to generate actions and responses within the scenario vignettes.

The role players or response cells will have intermittent interaction with staff planners (the experiment audience) in a series of faster-than-real-time scenario vignette changes managed by experiment control. As an experiment in information sharing, the AWG is not meant to test or exercise military crisis-action planning, or to solve the particular scenario or vignette problem. Any crisis action planning by the AWG participants would be used to generate and examine unclassified information sharing activity in order to carefully analyze the validity of the proposed solutions.

The MPC participants agreed on a draft EMD to include the types, number, skill sets, and sourcing organization. This draft EMD will be finalized during the FPC to include the actual names of participants.

The MPC participants agreed on the general scenario and supporting vignette requirements. The supporting Master Scenario Event List (MSEL) development will be an iterative process among the IMISAS partners.

During the MPC technical solution and spiral discussions, USEUCOM, USAFRICOM, and USPACOM/APAN representatives expressed their interest in the continued

development, demonstration, and evaluation of the technical solutions by means of five technical spirals. Technical break-out groups met to prioritize the COCOM's needs and align the spirals with APAN's scheduled future spiral of upgrades. The group also reviewed the IMISAS experimental APAN site (to be used as the unclassified information sharing capability proxy for the AWG) and the proposed use of APAN's current capabilities, Telligent's analytic tools, and some future APAN upgrades.

USEUCOM and USAFRICOM representatives expressed particular interest in spirals three and four supporting social media interfaces and the use of a User Defined Operating Picture (UDOP) (solutions: 3-1, 4-8, 4-9, and 4-11). The USPACOM/APAN representative supported the objectives of all five scheduled spirals, and stated that APAN would benefit from the results of both the IMISAS technical spirals and AWG.

During the MPC, the Analysis team provided a brief overview of the analytical approach to experimentation, stressing the traceability of metrics and measures, essential elements of analysis, and study issues to study objectives. The conference participants discussed metric nomination for individual procedural solutions to be examined during the technical spirals and the AWG. The participants agreed on the need for continued work to flesh out details of solution decomposition; metrics identification by solution element; metrics stimuli and measurement; and related experimental manning, infrastructure, and scenario requirements relative to the solutions.

The MPC was a major milestone in the experiment campaign planning process that addressed many of the vital requirements and outstanding issues that are necessary to plan and conduct the AWG. The MPC was conducted as a true working session where participants provided immediate feedback because they were empowered to make decisions on behalf of their organization. A list of post-MPC action items is found in Annex D of this report.

Way Ahead: During the MPC, USAFRICOM proposed moving the June FPC from Stuttgart to the Suffolk MITRE facilities. USEUCOM and USJFCOM concurred with the proposal. In addition, the parties concerned agreed to move the FPC up a week earlier than previously scheduled. The FPC will be held at the MITRE Office in Suffolk, 14 – 17 June 2011.

While much was accomplished at the MPC, there is still more that needs to be done in order to prepare for the AWG. Much of the preparation will be an iterative planning process among the IMISAS stakeholders and community of interest prior to the FPC. The primary FPC goal is to finalize and approve plans for the AWG, 1 – 4 August 2011. To focus these efforts, the MPC participants agreed to the following Objectives to be addressed during the FPC.

- Final agreement on solution elements for the AWG;
- Review the results of the technical spirals;
- Approve the ED to include the supporting DCAP for the AWG;

- Agree on EMD; and
- Agree on scenario vignettes and supporting MSEL development.

Submitted: Kathryn Smith, 757-203-3164, DSN 668-3164

Annexes: (Note: Appendicies available upon request)

G- MPC list of Participants
H- MPC Agenda (as executed)
I- IMISAS Solution Slides (updated to reflect MPC discussions)
J- MPC Agreed Action Plan

Appendix 4 to IMISAS Final Report Annex F After Action Reports –

Final Planning Conference

United States Joint Forces Command
Joint Concept Development and Experimentation
(JCD&E)

Interagency and Multinational Information Sharing Architecture and Solutions
(IMISAS)

Final Planning Conference
After-Action Report

13 July2011

Purpose: This document summarizes the results from the Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project Final Planning Conference (FPC) held 14-16 June 2011 at the MITRE office in the Bridgeway Technology Center, Suffolk, Virginia (USA). The primary purpose of the FPC was to finalize the shape and scope of the IMISAS Project Analytic Wargame (AWG) scheduled for 1–4 August 2011.

Background: The IMISAS project objective is to improve information sharing between the U.S. Department of Defense (DOD) and a wide variety of non-military mission partners, who may include civilian U.S. Government agencies, other nations, inter-governmental organizations, and non-governmental organizations.

In December 2010, gaps and potential solutions were validated and prioritized at the Stakeholder/Gap Validation Conference. The IMISAS project team incorporated the results of the conference and completed a Baseline Assessment Report (BAR).

In February 2011, a Solution Development Workshop (SDW)/Initial Planning Conference (IPC) was held at United States European Command (USEUCOM) in Stuttgart, Germany to further refine the capability gaps initially identified in the baseline assessment, to evaluate potential solutions for experimentation value and further development and to shape planning for the project experiment. The IMISAS project team successfully presented and validated specific gaps identified in the BAR and reviewed the initial cut on multiple potential solutions which would be viable for experimentation. The SDW sessions set the stage for the beginning of specific planning for the IMISAS project experimentation, which began immediately following the SDW. The SDW/IPC marked a shift toward concentrated planning for the scheduled August 2011 AWG.

The IMISAS project team conducted a Process Documentation Event, 28-31 March 2011, at United States Africa Command (USAFRICOM) and USEUCOM. The objective of the event was to better define the 'As Is' information sharing environment and processes to validate documentation in support of continued event design and planning, and set the conditions for further refinement during the Mid-Planning Conference (MPC).

The MPC, 19-22 April 2011, validated the high-level potential solutions for examination, agreed on a foreign humanitarian assistance scenario focused on multi-organizational unclassified information sharing, and further refined planning of the key experiment design elements.

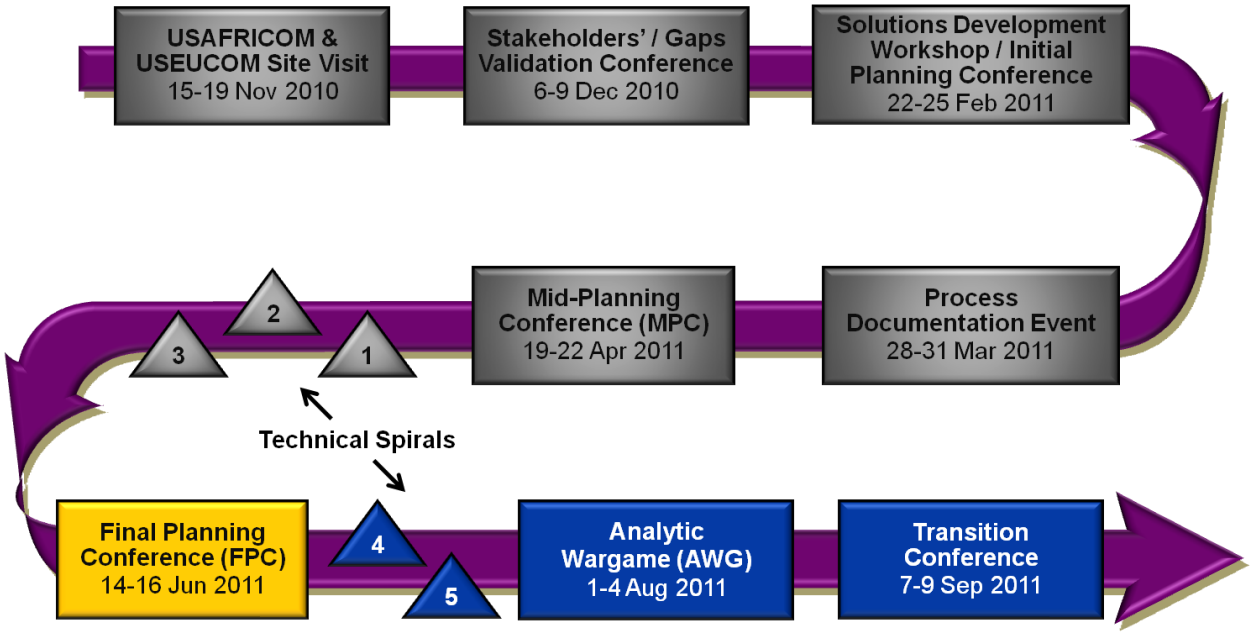
FPC Objectives: During the FPC, the conference participants addressed and accomplished the FPC objectives listed below:

- Agreed on the solution elements to be examined during the AWG;
- Review the results of technical spirals 1, 2 and 3;
- Agreed on the major elements that will be included in the AWG Event Directive (ED) to include the supporting AWG Data Collection and Analysis Plan (DCAP);

- Obtained consensus on the Experiment Manning Document (EMD); and
- Obtained consensus on the scenario vignettes and supporting Master Scenario Events List (MSEL) development.

FPC Execution: The IMISAS project sponsors and primary partners, USAFRICOM, USEUCOM as well as the Office of the Assistant Secretary of Defense, Networks and Information Integration/Chief Information Officer (OSD NII/DOD CIO), fully participated and provided subject-matter expertise. Additional representatives from the following organizations attended: Defense Information Services Agency (DISA); USJFCOM J9 German Foreign Liaison Officer; Bundeswehr Transformation Center and Joint Staff J8. A complete list of conference participants is in Annex A.

The graphic below depicts where the FPC fell within the project schedule.



The FPC provided the primary forum to finalize the requirements for the AWG. The conference addressed outstanding concerns and finalized the experiment event requirements in the areas of potential solutions, manning, processes, organizations, roles and responsibilities, technology, analysis, scenario, experiment control, and training for the experiment participants. The FPC was a working session where participants were encouraged to provide immediate feedback and were empowered to make decisions on behalf of their organization. Read-aheads were sent out to all the registered attendees to assist individuals in preparing for these discussions prior to the start of the conference.

During the first day of the FPC, the participants used the plenary sessions to review the project status that set the stage for Days 2 and 3. On Day 2, the participants conducted three concurrent breakout sessions focused on potential solutions, technical support, and experiment design. The breakout sessions used facilitated discussion to establish a common situational awareness and forge consensus among the participants. On Day 3, during the plenary sessions, participants synchronized the results of the previous day's

breakout sessions dealing with potential solutions, measures, information technology (IT) infrastructure, experiment design, and preparations for the AWG. The FPC participants confirmed their intent to conduct the IMISAS Project AWG, –4 August 2011, at Patch Barracks, USEUCOM. The resulting experiment event design reflects the IMISAS project partners and stakeholders' guidance with regard to allocation of resources, preparation of experimentation activities, management, and synchronized event execution. The FPC participants also discussed the format and participants for the Transition Conference. The FPC agenda is included as Annex B of this report.

During the FPC, the conference participants reached a consensus and achieved greater clarity on the IMISAS project solution elements. The participants concurred with how the solutions were contained in the Handbook for Unclassified Information Sharing (UIS) and provided substantive input on further handbook refinement. The participants examined the linkage between gaps, solutions, key solution elements, measures, and experimental event considerations (i.e., MSEL injects). As part of this process, analytic measures were aligned to desired solution impacts. The agreed schedule for promulgating, staffing, examining, and refining the Handbook for UIS is found in Annex C, the FPC Agreed Action Plan.

The lead analyst will modify the AWG DCAP based on the solutions and measures refinement method mentioned in the preceding paragraph. The AWG analytic results will include discovery findings, summary statistics and, where possible, comparative statistics. During the FPC, the participants reviewed the analytical approach to experimentation, stressing the traceability of metrics and measures, essential elements of analysis, and comparing study issues to study objectives. For the AWG getting a credible and comprehensive analytic depiction is more important than the number of repetitions for the procedure-based solutions. Selected technical enhancements will also be demonstrated and evaluated during the AWG. The analysis work plan developed during the FPC also addressed the associated training requirements such as the VOVICI survey tool and the J9 Observation Tool (JOT) for data collectors and analysts.

During the conference, participants finalized the agreement on all key elements of experiment design to include: timing; locations; concept of operations; and preparation to include identification of mission-essential tasks and responsibilities. The participants agreed on the contents of the EMD to include billet descriptions, sponsoring organizations, and specific names. To ensure agreement on the AWG scenario and MSEL outline, selected personnel stayed for a half-day post-FPC meeting on Friday, 17 June. This post-FPC meeting was successful in finalizing agreement on the AWG scenario and MSEL outline. The continuation of MSEL development will be an iterative process among the IMISAS project partners. Of particular note, a new preparatory event was scheduled to occur the week of 18-22 July 2011 in Stuttgart, Germany to serve as an experiment audience (the augmented operational planning team) forming event. The complete list of AWG preparatory activities and milestones are found in Annex D, AWG Planning Calendar.

FPC participants reached agreement on the Information Technology and service requirements to support the AWG. During the FPC discussions, USEUCOM and USAFRICOM representatives also reviewed the three completed technical spirals and the two remaining planned technical spirals as a means to develop, demonstrate, and evaluate technical solutions. Specific technical issues addressed include incorporating imagery overlays in a user-defined operational picture (UDOP), and the utility of using the Telligent user ranking system during the AWG. The FPC participants agreed on the IMISAS project experimental All Partners Access Network (APAN) site (to be used as the unclassified information sharing capability proxy for the AWG) and the proposed use of APAN's current capabilities with some future APAN upgrades.

AWG Overview: The AWG is focused on the sharing of unclassified information with non-DOD mission partners in a notional USAFRICOM operation in support of a multinational, civilian-led humanitarian assistance and disaster relief operation in Central Africa. The AWG will be an unclassified event consisting of scenario vignettes linked to the USAFRICOM CONPLAN 7200-09. The vignettes provide the specific context for examining potential solutions dealing with unclassified information sharing among mission partners. The vignettes will shape the experiment environment to examine the effectiveness of the potential solutions in addressing information sharing challenges.

The AWG participants (experiment audience) will consist of military and civilian interagency planners who would emulate a crisis action planning team working at the combatant command level. The experiment audience will consist of approximately 25 participants drawn primarily from the USEUCOM and USAFRICOM staffs. In addition, role players and response cells will interact with the experiment audience to generate actions and responses within the scenario vignettes.

The role players or response cells will have intermittent interaction with staff planners (the experiment audience) in a series of scenario vignettes managed by the experiment controller. As an experiment in information sharing, the AWG is not meant to test or exercise military crisis-action planning, or to solve the particular scenario or vignette problem. Any crisis action planning by the AWG participants would be used to generate and examine unclassified information sharing activity in order to carefully analyze the validity of the potential solutions.

The AWG will be conducted at the Rodgers Center at Patch Barracks (Stuttgart, Germany), 1–4 August 2011. Day 1 of the event will be devoted to pre-experiment orientation and collective training for all participants. The AWG execution will be a two-day event (Tuesday and Wednesday, 2–3 August 2011). On Day 4 (Thursday, 4 August 2011), there will be a fifth experiment period available for re-addressing any solution followed by a half-day after-action review and survey for all experiment participants.

Summary and Way Ahead: The FPC was the final milestone in the experiment campaign planning process addressing the vital requirements and outstanding issues for the final preparation and conduct of the AWG. Due to the overarching conference objectives to finalize AWG planning, the FPC was a true working session where

participants provided immediate feedback and guidance on behalf of their organization. The conference participants addressed all the outstanding concerns and finalized experiment event requirements in the areas of potential solutions, manning, processes, organizations, roles and responsibilities, technology, analysis, scenario, experiment control, and training for the experiment participants.

Still critical to successful AWG execution, are the post-FPC final preparations to include final scenario and MSEL development, handbook refinement, participant orientation, training and rehearsal.

.

Submitted: Kathryn Smith, 757-203-3164, DSN 668-3164

Annexes: (Note: Appendicies available upon request)

K- FPC list of Participants
L- FPC Agenda (as executed)
M- FPC Agreed Action Plan
N- AWG Preparation Planning Calendar

Appendix 5 to IMISAS Final Report Annex F After Action Reports –

Analytic Seminar

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS)

Analytic Seminar
After-Action Report

26 August 2011

Distribution:
Not Approved for Public Release
Administrative/Operational Use – 26 August 2011
Other requests for this document shall be referred to:
Joint Development
Joint Staff/Joint and Coalition Warfighting
115 Lakeview Parkway
Suffolk, VA 23435-2697
Attn: Ms Kathryn Smith, Phone: 757- 203-3164

Purpose: This report summarizes the Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project Analytic Seminar (AS) activity, execution and preliminary results. The AS was conducted 1-4 August 2011 at United States European Command (USEUCOM), Stuttgart, Germany. The AS examined in an experimentation structure, six proposed solutions designed to improve unclassified information sharing (UIS) among Department of Defense (DOD) and a wide variety of non-military mission partners.

Background: The objective of the IMISAS project is to improve information sharing between the DOD and a wide variety of non-military mission partners, who may include civilian United States (U.S.) government agencies, other nations, inter-governmental organizations (IGOs), and nongovernmental organizations (NGOs).

In December 2010, gaps and potential solutions were validated and prioritized at the Stakeholder/Gap Validation Conference. The IMISAS project team incorporated the results of the conference and completed a Baseline Assessment Report (BAR).

In February 2011, a Solution Development Workshop (SDW)/Initial Planning Conference (IPC) was held 22-25 February at USEUCOM in Stuttgart, Germany to further refine the capability gaps initially identified in the baseline assessment, to evaluate potential solutions for experimentation value and further development and to shape planning for the project experiment. The IMISAS project team successfully presented and validated specific gaps identified in the BAR and reviewed the initial cut on multiple potential solutions which would be viable for experimentation. The IPC sessions, which began immediately following the SDW, set the stage for the specific planning for the IMISAS project experimentation. The SDW/IPC marked a shift toward concentrated planning for the scheduled August 2011 AS.

The IMISAS project team conducted a Process Documentation Event, 28-31 March 2011, at United States Africa Command (USAFRICOM) and USEUCOM. The objective of the event was to better define the 'As Is' information sharing environment and processes to validate documentation in support of continued event design and planning, and set the conditions for further refinement during the Mid-Planning Conference (MPC).

The MPC was held 19-22 April 2011 in Suffolk, VA. At the MPC, participants validated the high-level potential solutions for examination, agreed on a foreign humanitarian assistance scenario focused on multi-organizational unclassified information sharing, and further refined planning of the key experiment design elements.

The IMISAS project team conducted the Final Planning Conference (FPC), 14-16 June 2011, in Suffolk, VA, to finalize planning for the AS. At the conference, participants agreed on the event requirements to include: manning; processes; organizations; roles and responsibilities; technology; analysis; scenario; and experiment control.

The AS focused on planning and coordinating USAFRICOM support to a notional multinational, civilian-led humanitarian assistance and disaster relief operation in Central Africa with a mixed Operations Planning Team (OPT). The OPT, as the experiment

audience, was led through four vignettes that were developed in concert with OPT experienced SMEs to provide context for examining IMISAS solutions dealing with unclassified information sharing among mission partners. The vignettes directed the seminar participants to address a specific information-sharing challenge using the proposed solutions. The event was primarily a concept refinement experiment to examine the extent to which proposed solutions solve information-sharing problems.

Experiment Design: Jointly sponsored by the USEUCOM, USAFRICOM, and Joint Staff (JS) J7, Joint and Coalition Warfighting (JCW) partners, the AS examined a set of proposed solutions designed to improve UIS between the U.S. DOD and a wide variety of non-military partners, who may include civilian, U.S. government agencies, other nations, IGOs, and NGOs. Although the AS used the All Partners Access Network (APAN) as a proxy for the UISC, it is important to note that the experiment was not an APAN-specific test.

The design of the experiment event for the AS employed proven experiment design principles to provide coherent, integrated, and achievable demonstration and experimental events. The design of the experiment event reflected the IMISAS project partners' and stakeholders' guidance with regard to allocation of resources, preparation of experimentation activities, management, and synchronized event execution. This experiment event design also identified critical event dependencies, long-lead items, and preparatory events required for key activities. The design was flexible enough to make adjustments to the event as available resources among the participants changed (time, funding, personnel, etc.), or as new opportunities arose. The experiment design allowed for some elements of concept discovery or discovery learning to identify potential new problems and solutions informing future information sharing efforts

The experiment design provided a realistic environment in which to examine how the participants used procedures and technology to share unclassified information and developed knowledge in a cooperative manner with non-DOD mission partners.

The primary emphasis of the AS was on staff procedures to enable effective UIS across organizational and security boundaries. The AS information sharing activities were focused on planning and coordinating USAFRICOM support to a notional, multinational, civilian-led, HA/DR operation in Central Africa. The AS was an unclassified event consisting of an introductory, overarching, scene-setter with separate follow-on vignettes. The scenario vignettes provided context for examining the IMISAS project solutions dealing with the sharing of unclassified information with mission partners. The four vignettes were developed to guide the seminar participants to address information sharing challenges which leveraged one or more proposed solutions linked to the USAFRICOM CONPLAN 7200-09.

The experiment was run by an experiment control staff that monitored the execution and tempo of the experiment. The control staff included a Senior Controller, Deputy Controllers, cell leads, data collectors, role players, and analysts. The control staff ensured that the experiment objectives were met and that the experiment audience was performing the required information sharing activities.

The potential solutions for evaluation in the AS were developed and refined to address specific gaps identified and validated by USAFRICOM and USEUCOM. The potential

solutions focus was to provide recommended processes, procedures, and business rules. In addition to providing a pre-doctrinal reference point for use during the development of military staff standard operating procedures, the potential solutions highlighted below mitigated related gaps identified in the areas of staff knowledge, skills and abilities, and the effective employment of UIS capabilities, including the application of data standards to improve information sharing.

Solution		Element	
1-1	Process and procedures for the expedited release of controlled unclassified information (CUI) in a crisis response situation	**1-1a**	Pre-planned release matrix --Linked to Commander's release guidance --Release matrix applies risk management --Additional release authorities
		1-1b	Unclassified information storage – UISC --Business rules for storage of unclassified information on the UISC
1-2	Business rules governing the expedited transfer of unclassified information from classified networks to non-classified networks.	**1-2a**	Business rules for manual cross-domain transfer
1-3	Pre-defined template and business rules for the establishment of UISC work sites	**1-3a**	UISC work site template --UISC collaboration tools (e.g., wikis, blogs and widgets)
		1-3b	Business rules to support UISC work site --Portal establishment --Work site management
1-5	Guides to enable UIS with mission partners via a UISC	**1-5a**	Processes and procedures to effectively engage mission partners for information sharing --US Interagency, Host Nation (HN), multinational/coalition partners, IGOs and NGOs --Use of staff embeds/LNOs --Address all UIS capabilities (portal, email, phone, etc.)
1-7	Guides for staff use of UISC in support of operations	**1-7a**	Best practices to maximize use of UISC --IM/KM business rules
1-8	Quick reference guides for the roles, responsibilities and general information requirements of potential non-DOD mission partners	**1-8a**	Reference guide for mission partners --US Interagency, HN, IGOs and NGOs --Roles, responsibilities and general information requirements --Electronically searchable

The solutions and their elements listed above were contained in a draft *Handbook for Unclassified Information Sharing (UIS).* The Handbook was given to experiment participants in order to provide guidance, planning considerations, techniques and procedures for ensuring an effective information sharing environment during military operations in support of a wide variety of civilian and other non-DOD partners, regardless of the particular mission. The vignettes were designed to lead the experiment

participants to address a specific information-sharing challenge using the proposed solutions in the Handbook.

Experiment Schedule: A Rehearsal of Concept (ROC) Drill or key-person rehearsal was conducted on 29 July 2011. The purpose of the ROC Drill was to synchronize event controllers, analysts, observers, scenario, master scenario events list (MSEL), and role players. The intent was to practice and refine control and analyst procedures over the actual experiment network and tools. A secondary purpose was to conduct limited training, e.g., analysis and data collection procedures, prior to the start of the main event.

Day 1 of the event, 1 August, was devoted to pre-experiment orientation and collective training for all participants. Execution of the AS experiment was conducted over two-days (Tuesday and Wednesday, 2-3 August). On Day 4 (Thursday, 4 August), there was an hour long seminar discussion with the experiment audience followed by the after-action review (AAR) and survey for all experiment participants.

MON	TUE	WED	THU
Experiment Period 0 Set-up Preparation Early Registration	**Experiment Period 2** (CONPLAN Phase 1) Mission Analysis **Op Day 1**	**Experiment Period 4** (CONPLAN Phase 1) Branch Planning **Op Day 3**	Seminar Surveys Interviews AAR Audience Dismissal
Meal Break	*Meal Break* *Time Jump*	*Meal Break* *Time Jump*	*Meal Break*
Experiment Period 1 Orientation Training (CONPLAN Phase 0) Pre-Crisis / Road to Crisis	**Experiment Period 3** (CONPLAN Phase 1) COA Development **Op Day 2**	**Experiment Period 5** (CONPLAN Phase 1) Branch Planning **Op Day 6**	Control Team Closeout
End of Day *Time Jump*	*End of Day* *Time Jump*		

Experiment Execution: The Experiment Audience consisted of military and civilian interagency planners who replicated an augmented operational planning team (OPT) working at the COCOM level. The 19 seminar participants were drawn from the USEUCOM and USAFRICOM staffs. In addition, Role Players and Response Cells interacted with the Experiment Audience to generate actions and responses within the scenario vignettes.

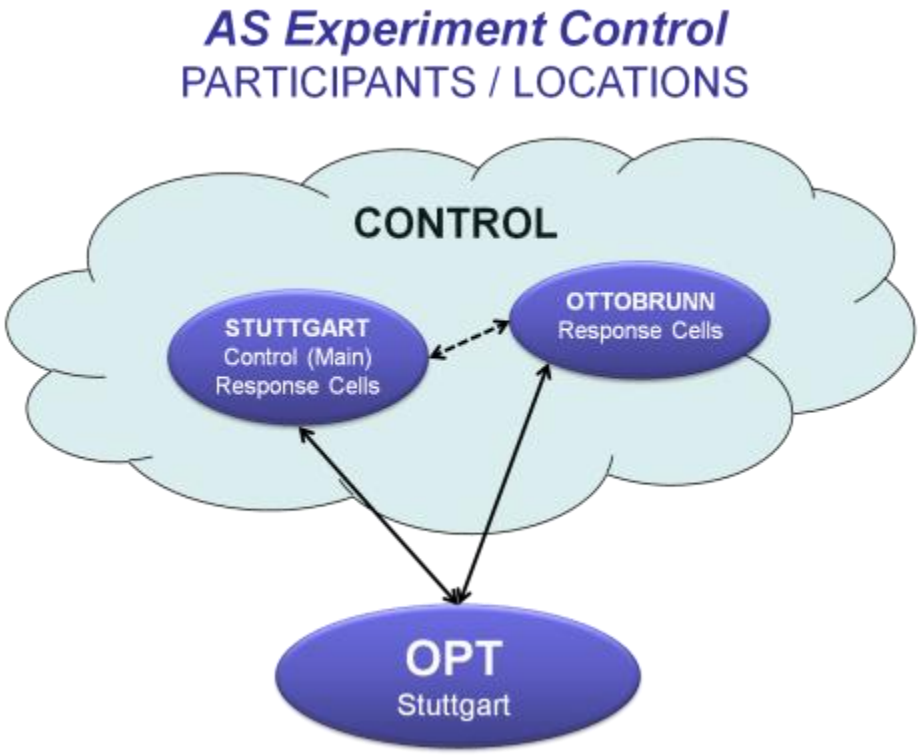
Role Players and Response Cells, co-located in Stuttgart and at a distributed site in Ottobrunn, Germany, served as the "character actors" that helped establish the environment for the experiment by representing other entities involved in the scenario. For the AS, there were credible Role Players that replicated the skill sets and organizations necessary to properly interact with and stimulate the Experiment Audience.

As an experiment in information sharing, the AS was not intended to test or exercise military crisis-action planning or to solve the particular scenario or vignette problem. The planning by the AS participants served only to generate UIS activity in order to analyze the validity of the proposed solutions. Each experiment day (2-3 August) had a minimum of six hours of experiment play per day.

USEUCOM provided IT equipment and network access to services during the AS. The NIPRNet network was used during the event with Windows-based clients. Logons derived from the Experiment Manning Document were created by USEUCOM. Access to the various web-based services was provided during the AS, including portal, wiki, chat, collaboration and survey tools, as well as geographic and data verification and filtering services. Far beyond the IT infrastructure and services, USEUCOM provided excellent experiment facilities and support which contributed significantly to the event's success.

The Chief Controller was responsible for ensuring that the event was conducted in accordance with the experiment design and in a fashion that attained the event objectives and study issues. There were three Deputy Controllers who assisted at the primary location, and one Deputy Controller in Ottobrunn.

AS - Participants and Locations



The Chief Controller and the Deputy Controllers worked closely with the Lead Analyst and the solution developers to ensure the environment in which the solutions were examined was as realistic as possible and that it met experimental needs. Experiment Control "set the environment" in which the Experiment Audience and Support groups operated.

Experiment Control and Analysis were closely linked. The key elements of this linkage were listed below:

- Analysis representatives were present full-time in Experiment Control to monitor experiment progress;
- Lead Analyst and Senior Controller were a close team;
- Data Collectors were assigned to each of the sites and with separate groups within each sire;
- All Analysts and Data Collectors were informed of injects which drove Experiment Play (enabled observations);
- Analysts provided feedback to Experiment Control on progress towards achieving experiment objectives; and
- Analysts made recommendations to Control on proposed changes to experiment stimulation and execution.

Data collection was accomplished through a combination of open-format survey questions, closed form survey questions, quantitative measures as appropriate, observations, and interviews. The primary sources for data were the surveys. Answers for the were solicited as both open responses (inviting discovery learning), and closed Likert scale responses constraining the respondent to rate, on a scale of 1 to 5, his or her level of agreement with a given statement. Where it was meaningful to solicit a comparison between the respondent's satisfaction with and without a given solution, the Likert scale questions were posed to capture such comparison. In other cases, the Likert scale questions were posed to solicit responses of an absolute rather than relative character. VOVICI was the survey tool used during the AS.

Experiment control injected scenario information throughout each experiment time period to stimulate thought and action for the Experiment Audience. These injects were provided by APAN, email, telephone or by-hand injection. The MSEL itself was both time and event driven in that some MSELs were pre-scripted to be injected at specific times while others were provided based on participants' actions or inactions to other stimuli. The MSEL Manager exercised positive control of all MSELs and did not release them until authorized by the Senior Controller. The Deputy Controller in Ottobrunn ensured that the scenario updates and MSEL injects were understood and, if necessary, prompted the on-site participants to take action.

To manage the control challenges, the Senior Controller conducted daily control meetings to review each experiment period's activity against the control tracking and MSEL matrices to ensure that all potential solutions were examined. This review was conducted in conjunction with Role Players, Analysts and the OPT chief as a "trusted agent." Based on the discussion during the meeting, the Senior Controller provided direction and guidance for the next experiment period.

On Day 4 (4 August), the Senior Controller conducted a joint AAR for the Experiment Audience and Experiment Control Groups. The purpose of the AAR was to:

- Provide immediate feedback to both the Experiment Audience and Experiment Support Groups on why their efforts were important;
- Provide the Experiment Audience and Experiment Support Groups initial insights of in-stride analysis;
- Stimulate discussion and elicit feedback on reasons for some unexpected results;
- Discuss, document, and attempt to evaluate any discovery material relevant to IMISAS; and
- Provide input to the follow-on outbriefs for senior leaders on 5 August 2011.

Hypotheses: The high-level, experimental hypotheses examined during the AS are outlined below:

Hypothesis 1: If the unclassified information sharing capability (UISC) combines knowledge management methodologies with a minimum-demand user interface and

carefully designed software composition including social media interfaces, then accessibility, completeness, responsiveness, and timeliness of information will increase, with attendant increases in relevance to the activity of responders and their situational understanding.

Hypothesis 2: If Combatant Commands (COCOMs) foster coordination with outreach to, and holistic comprehension of the span of humanitarian assistance and disaster relief (HA/DR) responders, then the coherence, agility, responsiveness, robustness, and speed of combined HA/DR responses will increase.

Hypothesis 3: If a risk-managed approach to information sharing is adopted, to include information release policy, mechanisms for identity establishment and source vetting, and methods for assuring confidentiality and anonymity, then within acceptable limits of information accuracy and security, improvements will be garnered in information accessibility and the agility, flexibility, responsiveness, speed, and timeliness of an HA/DR response.

Preliminary Analysis: The analysis herein is preliminary and is provided in a format that ties it to solutions. Additional analysis is ongoing. The solution set is a construct that was used throughout the project and is used for consistency in the discussion.

Due to previously agreed scheduling of the AS session, resulting in time constraints limiting the time the Experimental Audience was available, as well as Controller decisions to reapply a stimulus to test another solutions, physical application of several of solution elements were not able to be explored during the sessions. As a result, those survey questions directed at those particular solutions were answered with "open" format fields indicating the respondent could provide no meaningful opinion. Participants answered many survey questions with positive or negative responses, based evidently upon the interactions and discussion of the solution expositions in the Handbook which generated valuable critiques by the Experiment Audience and Role Players. Discussions among the Experiment Audience included differences in planning styles, the need to accommodate the collaborative methods of others, the necessity and impact of vetting unclassified information prior to release, the appropriate balance of local terminology relative to a more general use lexicon, and suggestions regarding the Request for Information (RFI)/Request for Action (RFA) interface with external partners.

While the cross domain procedure (Handbook solution 1-2) and the risk managed approach to information release evaluation (Handbook solution 1-1a) were not physically exercised, pre-experiment surveys indicated considerable variance in staff expectations for the time required to execute existing procedures. Regarding the timeliness and security of the Handbooks cross domain solution, relative to their current method, 6 of 14 respondents gave positive marks at the end of period 4, as opposed to noncommittal responses at the end of period 2. However, no significant valuation was evident in an end of experiment survey regarding the same attributes of the risk-managed approach to information release evaluation which leads to no clear finding on the data from the AS.

Open format comments on the pre-planned release matrix supporting solution 1-1a included suggestions for making risk categories more flexible and clarifying the instructions for updating those categories. Other comments dismissed the value of the matrix entirely, one noting that decisions regarding the release of unclassified information would ultimately be made by the Foreign Disclosure Officer, a function that also figured heavily in the pre-experiment survey questions addressing currently employed processes. Discussions during the experiment indicated uncertainty as to how to implement the function of the Designated Release Authority, along with a general discomfort with the term itself. The discussion ensued on the same concerns addressed during the genesis of the Handbook's risk-management-based solution, including questions regarding storage for uncontrolled but still sensitive unclassified information, and when to post information to publicly accessible forums given the need for maturity of documentation. One participant noted that early, robust collaboration mitigates information sharing shortfalls occurring due to posting restrictions, and there was general consensus that information already in the public domain or passed to the OPT via open source means could be posted to the UISC without further approval.

Solution 1-3 addressed the template and business rules for the provided UISC web portal. Satisfaction with the ease of use of provided capabilities and their applicability to HA/DR operations in general was positive, although both survey results and comments reflect frustration with the functionality of some of the interfaces. In particular, interactions with MapView and CrowdMap were minimal due to long lag times; however, the majority of non-neutral responses indicated that the capability would be useful in a crisis response situation. Many comments were provided regarding improvements to the user interface, including the need for more intuitive, robust, and mission-tailored content layout; easier navigation and file movement; better visibility of chat windows; elimination of a redundant capability as a means to increase bandwidth efficiency; better visibility of log-on requirements, notification and adaptability of automatic logout; implementation of a user address list; a more formal and informative folder scheme; and a voice to text capability for limited bandwidth situations. Business rules for the RFI/RFA capability were favorably evaluated in terms of their ease of use and the expected responsiveness and relevance of posts. The expected impact on partner situational awareness through the use of the Situational Report (SITREP) tool also evaluated positively. The high number of observed RFI/RFAs was unexpected, and evidently prompted a participant comment on the need for a management process for this vehicle. Likewise, a set of business rules was suggested for the posting of messages, along with the need for a version control system for released documents. Regarding the collaboration tool suite within the UISC, one respondent mentioned that intra-DOD collaboration needs could be satisfied by a searchable folder hierarchy for draft documents and a simple instant messaging tool. Another pointed out that whatever the collaborative tool set used, each component application had its own limitations.

The effectiveness of solution 1-5 (guide to non-DOD mission partners) in informing the how, why, what, and with whom information should be shared, received positive evaluations during surveys, with negative reviews only associated with two respondents. Suggestions for improvement included basing the template upon the *DOD Support to Foreign Disaster Relief (FDR) Handbook for Joint Task Force Commanders and Below*, clarifying the fact that the span of partners is mission-set dependent, and including a

section on DOD regulations restricting information sharing with external entities. Related discussion cited differences between military and governmental planning styles, procedures, and engagement approaches. These included: initial group focus (internal for an OPT, but external for NGO's); source of subject matter expertise (codified references for the OPT, but networking via Skype, instant messaging, and chat for NGOs); and mission focus (rationale and goals for the OPT, but for civilian responders there were specific, requirement details such as the number of trucks to be provided). The general wariness of some NGOs was cited multiple times during discussions, with a concern by an NGO role player that an Adobe Connect Online session was being recorded.

Solution 1-7 involved information management best practices, with a focus on awareness and accommodation of the preferred collaboration venues of external partners. The helpfulness of the content was evaluated positively, with particularly strong support for inviting external partners (via the RFI/RFA tools) to suggest venues and tools for collaboration. Throughout discussions during experiment play, the need for information management "outreach" was a common theme. The experiment audience and role players agreed that the civilian, military, and government speak different languages, with acronyms and phrases such as "RFI" and "Phase 1" mean nothing to many external partners. However, it was also commented that using the "local dialect" is best for efficiency of internal processes. There was significant practice among the role players in using their own collaborative tool sets, with one role player stating a preference for collaborating over telephone. Pre-experiment surveys indicated about twice as many respondents had familiarity with their partners' collaboration tools and venues as otherwise; however, the majority also noted their organizations' current reference materials for identifying mission partner roles, responsibilities, capabilities, and limitations were not adequate.

Solution 1-8 involved a Quick Reference Guide for the roles, responsibilities and general information requirements of potential non-DOD mission partners, along with a suggested format for an Information Exchange Requirement (IER) matrix that could be used to dynamically track means and content of collaboration. Survey responses were neutral or positive with regard to the accuracy, level of detail, and comprehensiveness of the Quick Reference Guide's descriptions of partner roles and responsibilities. Feedback to the guide included suggestions to add the World Health Organization's regional organization and the United Nations Operational Satellite Applications Programme (UNOSAT) of the United Nations Institute for Training and Research (UNITAR), and an observation that other agencies mentioned during the population of RFIs were not in the Handbook. One respondent cautioned against relying on a static list of roles and responsibilities, however, as in an emergency additional roles are assumed as matters of situational necessity. The IER matrix itself was not implemented during the exercise, however, period 5 survey questions indicated that using such a limited agreement tool would be an improvement over the respondents' current means of deciding the best means to collaborate, and that specifying the contingency means of collaboration would be useful. Open format feedback suggested that the tool would have been better understood and employed had it been better explained in the Handbook; an additional suggestion was that the IER matrix be synchronized with FDO matrices.

Metadata Standards was the subject of Solution 3-1. Data tagging was not fully explored during the AS. Discussions during the experiment included a general agreement that tags are important and necessary for sorting and finding information for a wide-range of problems; however, one respondent pointed out that that the tagging schema can be organization-specific.

Solutions 4-8 and 4-9 regarded social media publishing and subscription, respectively. Use of the former capability was not indicated during the experiment. Additionally, for MapView and CrowdMap, the subscription mechanisms provided on the UISC portal, did not work on the network instantiation. However, survey responses addressing the general utility of CrowdMapping to HA/DR operations were mostly positive, with the citation to rapidly build awareness of needs and priorities through real-time, visual composition for a broad range of key indicators. Open format comments also included a caution about the potential for unverified crowd map reports to distract or even misdirect planning efforts.

Key Observations and Way Ahead: The AS was designed to examine solutions to address and mitigate the problem that U.S. commanders do not have a coherent framework and capability to share essential information across military domains with a range of non DOD mission partners. The AS was successful in meeting the purposes and objectives of the event. The professionalism and keen interest of the military and non-military representatives ensured that all of the discussions were relevant to the solutions being examined. The participants were conscientious about completing the survey which enabled the team to collect sufficient data for analysis. In addition to the findings regarding specific solutions, there were some larger themes and findings:

Throughout the AS, the OPT continued to express hesitation and uncertainty regarding information release and sharing responsibilities and procedures despite frequent reminders by Experiment Control to reference the solutions outlined in the *Handbook for Unclassified Information Sharing (UIS).* This observation underscores the information sharing prerequisite for a willingness to adapt to new procedures, tools, and mission partners. It also highlights the associated requirement for education and training, both individual and collective, on information sharing procedures. Much of the release problem stems from the "need to know" mentality found in DOD and aversion to the risk associated with sharing information.

The AS highlighted the recognition that unclassified information sharing is not just a technical problem. Technology solutions exist to allow increased information sharing capabilities. But in order to use that technology, the development of realistic, dynamic information sharing policies, updated processes and procedures to uniformly utilize that technology are critical. As the UIS capability continues to develop, arriving at an effective solution will require involvement of military planners, operational experts, logisticians, civil affairs and the intelligence community in defining what role and functions the UIS has in their respective missions. These subject matter experts will have the best awareness of the information sharing requirements and their involvement will help shape future policy, process and procedures to further enable the greatest interaction with other partners.

A comprehensive solution to the unclassified information sharing problem must also accommodate non-DOD mission partner requirements and organizational cultures. As an AS participant noted, "posting a document is not sharing." To accommodate the non-DOD mission partners, the COCOM needs a better understanding of how the partners operate and what their requirements are. This understanding cannot wait until the crisis happens but has to be built over time during steady state operations.

DOD information sharing with non-DOD mission partners is different depending on the partner. Some mission partners already have an established and trusted information sharing relationship, while others may not. Building these trusted relationships may simply require time, familiarity, understanding and possibly agreements with one another. Therefore, an effective UISC requires the ability to provide various degrees of user access (e.g., additional access to established U.S. agency counterparts or coalition partners). An option for "private" information sharing with key partners via point-to-point distribution vice broadcasting on a public portal is desirable when some form of control is required.

AS results also indicate that the solutions contained in the Handbook are flexible enough to be adapted to differing situational and organizational requirements. The OPT responses suggest that the Handbook solutions did not need to be limited to USAFRICOM or USEUCOM, nor did they need to be limited to only HA/DR operations. These responses validate the notion that the Handbook can be introduced to a wider audience conducting various operations. In addition to real world operations, the Handbook could be introduced into COCOM exercises and/or current training programs.

Experimental analysis for the AS continues and further detailed findings, with subsequent recommendations, will be produced in the IMISAS Final Report. IMISAS project partner inputs will be consolidated into the report and its supporting appendices.

The AS was the final experimentation event for the IMISAS project. The IMISAS project transition strategy is based on the acceptance and advocacy, by the IMISAS project partners, of the recommendations resulting from the project for implementation, further study or future development.

Submitted: Kathryn Smith, 757-203-3164, DSN 668-3164

Annexes: (Note: Appendicies available upon request)

Annex A. Event Directive

Annex B. Handbook for UIS

Annex C. Experiment Manning Document

Annex D. Master Scenario Event List Spreadsheet

Annex E. List of Survey Questions

Annex F. Master Scenario Event List Booklet

Annex G. Event After-Action Review Slides

Annex H. Out-briefs to USAFRICOM and USEUCOM

Appendix 6 to IMISAS Final Report Annex F After Action Reports –

Transition Conference

UNCLASSIFIED

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS)

Transition Conference After-Action Report

23 September 2011

Distribution:
Not Approved for Public Release
Administrative/Operational Use – 23 September 2011
other requests for this document shall be referred to:
Joint Development
Joint Staff/Joint and Coalition Warfighting
115 Lakeview Parkway
Suffolk, VA 23435-2697
Attn: Ms. Kathryn Smith, Phone: 757- 203-3164

Preface: This report summarizes the results from the Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project Transition Conference

(TC) conducted 7-8 September 2011 at the Ronald Reagan Building and International Trade Center in Washington, D.C. The TC achieved the goal of bringing together working-level (O5/O6, GS-14/15) partner and community of interest (COI) representatives to review findings from the IMISAS project experiment, recommendations for doctrine, training, materiel (technical enhancements), leadership, and education, policy. The participants also discussed the implementation of the IMISAS project products and recommendations. Conference participants reviewed the IMISAS project product status and presented the planned transition of these products. Change agents were identified and their representatives acknowledged responsibility. Participants at the conference included representatives from U.S. Africa Command (USAFRICOM), U.S. European Command (USEUCOM), Department of Defense Chief Information Officer (DOD CIO), Defense Information Systems Agency (DISA), Joint Staff J8 Combat Capability Developer Division (CCDD), U.S. Pacific Command (USPACOM), Department of State Humanitarian Information Unit, Department of Commerce, Bundeswehr Transformation Center and National Defense University. Annex A of this report contains a detailed conference attendance list.

Background: The objective of the IMISAS project is to improve information sharing between the U.S. DOD and a wide variety of non-military mission partners, who may include U.S. government (USG) agencies, other nations, international organizations and nongovernmental organizations (NGOs).

In December 2010, the IMISAS COI met at the Stakeholders and Gap Validation Conference. They identified gaps and potential solutions which were then validated and prioritized.

In February 2011, a Solution Development Workshop/Initial Planning Conference was held at USEUCOM in Stuttgart, Germany to further refine the capability gaps identified in the draft baseline assessment, to evaluate potential solutions for experimentation value and further development, and to shape planning for the project experiment.

The IMISAS project team conducted a Process Documentation Event, 28-31 March 2011, at USAFRICOM and USEUCOM. The objective of the event was to define the current information sharing environment and processes and provide additional information to the baseline assessment report in support of continued experimental event planning and design. The IMISAS project team used the results of the conference in completing a Baseline Assessment Report.

The Mid-Planning Conference (MPC) was conducted19-22 April 2011 and served as a forum for validating the high-level potential solutions for examination, allowed for consensus on a foreign humanitarian assistance scenario focused on multi-organizational unclassified information sharing, and further refined additional planning considerations for experiment design.

During the period from 12 May - 7 July 2011, the IMISAS project team conducted a series of five Technical Spirals. These events brought together participants from the IMISAS project COI to evaluate existing capabilities and potential technical solutions using the All Partners Access Network (APAN) as a proxy for the unclassified information sharing capability (UISC).

At the Final Planning Conference (FPC), 14-16 June 2011, participants reviewed the results of technical spirals conducted to date and agreed to the non-technical solution elements to be examined during the Analytic Seminar (AS). The FPC provided the primary forum to finalize all planning and execution requirements for the AS.

The AS was conducted 01-04 August 2011 at USEUCOM Headquarters, Stuttgart, Germany and focused on staff procedures to enable effective unclassified information sharing across organizational and security boundaries. The AS examined six proposed non-technical solution elements designed to improve unclassified information sharing between DOD, and non-DOD mission partners, including USG agencies, international organizations, other nations and NGOs. The AS also served to demonstrate the technical solutions developed during the technical spirals.

Objectives and Outcomes:

TC objectives were to:

- Review the IMISAS project products for transition;
- Review and refine the IMISAS project preliminary findings;
- Review, refine and reach consensus on the IMISAS project recommendations; and
- Inform the way ahead for DOD unclassified information sharing.

TC desired outcomes included:

- Consensus on the IMISAS project recommendations; and
- Agreement on transition pathways.

Execution: The TC was the final conference of the one year IMISAS project. Conference participants reviewed the findings and recommendations from the AS and refined the latest version of IMISAS project products (described in the next section). The TC provided a map of the pathways for experimentation results to feed into the appropriate doctrine, training, materiel (technical enhancements), leadership and education, policy and implementation processes. The TC was conducted as a working session, and where participants were able to accept responsibility on behalf of their organization for championing project products.

Annex B of this report provides the detailed TC agenda. During Day 1 of the conference, the IMISAS project team outlined the status of the IMISAS project products, and presented the findings and recommendations from the project. On Day 2, the team conducted group discussions of the transition of IMISAS project products and the implementation of recommendations in conjunction with the proposed change agents, During the afternoon session of Day 2, the IMISAS project partners and sponsors, USAFRICOM, USEUCOM, DOD CIO, and DISA discussed their organization's plan for implementation of the IMISAS project products and recommendations. Annex C of this report contains the TC Event Directive providing further details about the event planning, preparation, and execution. Annex D contains the consolidated event briefing slides presented at the TC.

IMISAS Project Products: A general description of the four major products presented to the TC is provided below. Details of proposed recommendations, proposed change agents, and product descriptions are found in Annex D.

- *Commander's Handbook for Unclassified Information Sharing (UIS).* The handbook provides a pre-doctrinal reference point for use during development of military staff standard operating procedures, and a basis for continuing research and development regarding the issue of unclassified information sharing with USG civilian agencies, coalition, and other potential non-DOD mission partners. It addresses information sharing guidelines and consideration for use during military planning and execution processes on existing DOD networks, and "pushes the envelope" by emphasizing the "need to share" with non-DOD partners using non-military networks. Procedures included in the handbook address the current DOD unclassified information sharing technology and how feeds from other non-classified domains and applications, such as Facebook or Twitter, can be imported using Really Simple Syndication (RSS) and safely utilized under existing DOD policy. Use of these non-DOD systems will enhance information flow between DOD and non-DOD partners including other USG agencies, multinational/coalition partners, international organizations, NGOs and private organizations.
- Recommendations for changes/additions to doctrine, training, materiel (technical enhancements), leadership, and education and policy.
    - Training recommendations address inclusion of UIS in the training for deploying units such as mission-rehearsal exercises, as well as staff evaluation during any exercise involving non-DOD partners (e.g., USAFRICOM's Exercise JUDICIOUS RESPONSE 12).
    - Leadership and education curricula recommendations will address the range and diversity of partners in all joint operations with the focus being on recognizing and mitigating differences in organizational cultures in order to achieve successful communications and collaboration with non-DOD mission partners.
    - Doctrine recommendations will address the implications of UIS in all military operations.
    - Policy recommendations will address the UIS challenges that may be caused by the lack of standardization in COCOM and Service implementation of existing DOD policies.
    - Technical recommendations for UISC software enhancements and system capabilities, based on experimental findings and observations, will inform DOD's implementation of the initial UISC in fiscal year (FY) 12, and planning for future enterprise implementation and enhancements.
- UIS architectures: Describes, in architectural views and a supporting narrative for the organizations, activities and information exchange requirements at the strategic, theater-level in a foreign humanitarian assistance/disaster relief context. This effort will contribute to the development of a DOD architectural framework

(DoDAF) describing a broader UIS Enterprise solution across the spectrum of operations.

- UIS Unofficial Joint Operating Concept (JOC): A "think piece" describing the near-term (three-to-five years) UIS operating environment in which DOD will be expected to operate.

The products outlined above were developed with transition in mind. During the TC, the products were discussed in detail for group consensus and the assignment of an office of primary responsibility for implementation.

Key Observations: The TC provided an effective forum for the IMISAS project partners to reach a consensus on the "what" and the "how" for transition and implementation of the IMISAS project recommendations and products. The conference met its objectives and allowed the discussion resulting in a consensus with the partner organizations on the IMISAS project recommendations. The conference served a secondary purpose of providing a platform for the key partners, (USAFRICOM, USEUCOM, DOD CIO, and DISA) to discuss UIS writ large. The discussions were purposeful and focused directly on the need for advocacy and championing by both the Joint Staff J7 Joint and Coalition Warfighting (JCW) lead and the project partner organizations. Project partners want the IMISAS project products to immediately improve staff operations and also to inform the unclassified information sharing way ahead.

The TC participants reached agreement on the project recommendations on the first day, while Day 2 discussions focused on the "how", "when" and "with whom" of transition. The transition discussion was enabled by the senior representatives present from DOD CIO and DISA. Their active participation in the transition discussions was important because both of these organizations have direct Joint Requirements Oversight Council Memorandum (JROCM) tasking to use the findings from the IMISAS project to inform the DOD UIS Enterprise capability and the FY 14 POM. The JS J8 CCDD representative reviewed the role of JS J8 with both DISA and DOD CIO in the requirements process.

Both USAFRICOM and USEUCOM representatives indicated that they plan to integrate UIS guidelines and considerations in their FY 12 training and exercise plan using the products from the IMISAS project. Additionally, the representative from the Pacific Warfighting Center expressed a need for the *Commander's Handbook for UIS* for use by the exercise planners at USPACOM. All three combatant commanders stated their desire to have the handbook available for their use as soon as possible; they did not see a need to wait for a formal, doctrinal product.

A USAFRICOM representative expressed questions about how training on the handbook would be provided for the JUDICIOUS RESPONSE 12 exercise which starts its cycle in October 2011. The entire group acknowledged that implementation into training and exercises is an issue that will need to be addressed in the near-term, but there was no resolution of this issue at the TC.

All conference participants rated the event as highly successful. The Ronald Reagan Building and International Trade Center, by virtue of its location in downtown Washington D.C., proved to be a convenient venue, for attracting USG interagency

representatives and senior DOD officials. The individual visits by BG Steven Salazar, (Assistant, Deputy Director for Joint Development, Joint Coalition Warfighting) and Mr. Greg Knapp (Vice Assistant Deputy Director for Joint Development), etc. on Day 1 were valuable opportunities for the JCW senior leadership to meet with representatives of the COCOM project partners.

.

Submitted: Kathryn Smith, 757-203-3164, DSN 668-3164

Annexes: (Note: Appendicies available upon request)

Annex A – TC Attendance List

Annex B – TC Agenda

Annex C – TC Event Directive

Annex D – TC Consolidated Briefing Slides

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS)

Annex G - Analytic Framework

Table of Contents

1. PURPOSE G-2
2. PROJECT ANALYSIS LOGIC G-5
2.1. Conceptual Model G-5
2.2. Traceability G-6
3. ANALYSIS PLAN G-22
3.1. Experimental Hypotheses G-22
3.2. Data Collection and Analysis Plans (DCAPs) G-22
4. EXPERIMENT DESIGN AND EXECUTION G-24
4.1. Technical Spirals (May – July) G-24
4.2. Analytic Wargame (01 Aug – 04 Aug) G-25
4.3. Data Collection G-25
5. EXPERIMENTATION OUTPUTS AND OTHER SIGNIFICANT PROJECT EVENTS .. G-26
5.1. Data Analysis G-26
5.2. Reporting Phase G-27
5.3. Analytical Input to Final Report G-27
5.4. Way Ahead G-27
Annex A - ACRONYMS G-a-1

List of Figures

Figure G-1 - IMISAS Analytic Framework Context G-3
Figure G-2 – Analytic Framework Development G-4
Figure G-3 – IMISAS Conceptual Model G-6
Figure G-4 – Traceability of Data Elements to the Problem Statement G-8
Figure G-5 – Analytic Wargame Framework G-25

1. PURPOSE

The purpose of the Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Analytic Framework is to specify the connections among IMISAS analysis and experimentation design and execution activities and their mapping to project objectives. The framework seeks to ensure a coherent campaign of activities and a structured approach to gaining knowledge and understanding of the problems associated with unclassified information sharing. This framework provides the foundation for the project analysis logic, establishes the analytical plan, lays the foundation for experimental design and execution, defines intended outputs of experiments and other significant project events, and ensures the design, execution, analysis and reporting will produce defensible results that support that output. The Analytic Framework serves as a planning document and is included as an annex to the Experiment Plan. It will be revised and updated as necessary to reflect the latest coordinated experiment activity plans.

Figure G-1 illustrates the context of the analytic framework within five of the six principal phases of the project (Problem Formulation, Experiment Design, Experiment Execution, Analysis, and Reporting), showing the serial and parallel relationships among activities, tasks, and analysis products. These phases are defined as distinct serial sets of activity; however, analysis planning, data collection and analysis, assessment, and reporting continue as minor spirals throughout the entire project to support deviations and adjustments to experiment design and execution.

Figure G-2 depicts the Analytic Framework development process implemented in the evaluation of gaps and solutions. This process, envisioned within the overall Joint Concept Development and Experimentation Life Cycle Management Framework, informs and shapes the domain space of experiment design and supporting data collection and analysis leading to assessment of experimental outcomes. The framework development process appropriately approaches the task from two perspectives. While focusing on the steps leading to potential solutions that address the problem, it also identifies and aligns concurrent considerations so that outcomes and products are positioned for transition. This reverse engineered review process ensures that the experimental outcome and the supporting scenario, vignettes, data collection and analysis leads ultimately to solutions which can be translated and transitioned into a real capability for the Warfighter.

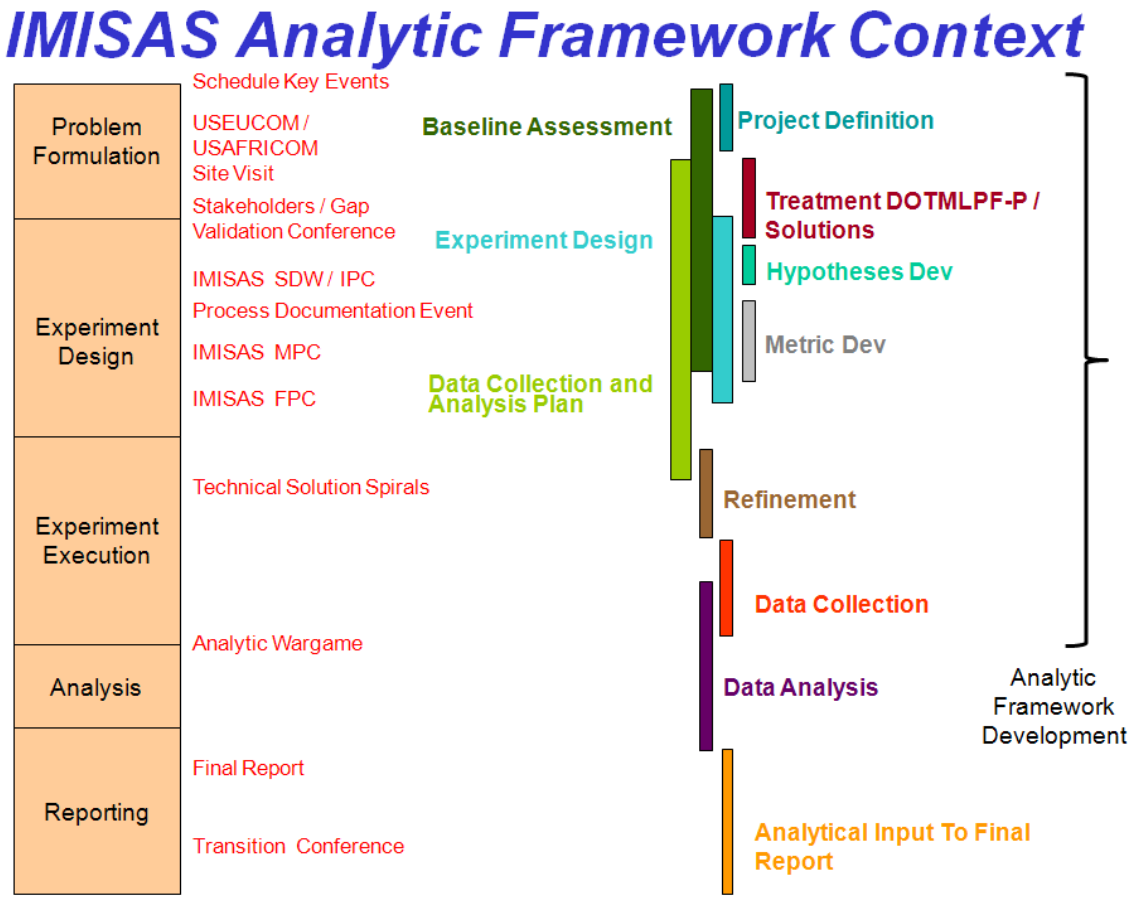


Figure G-1 - IMISAS Analytic Framework Context

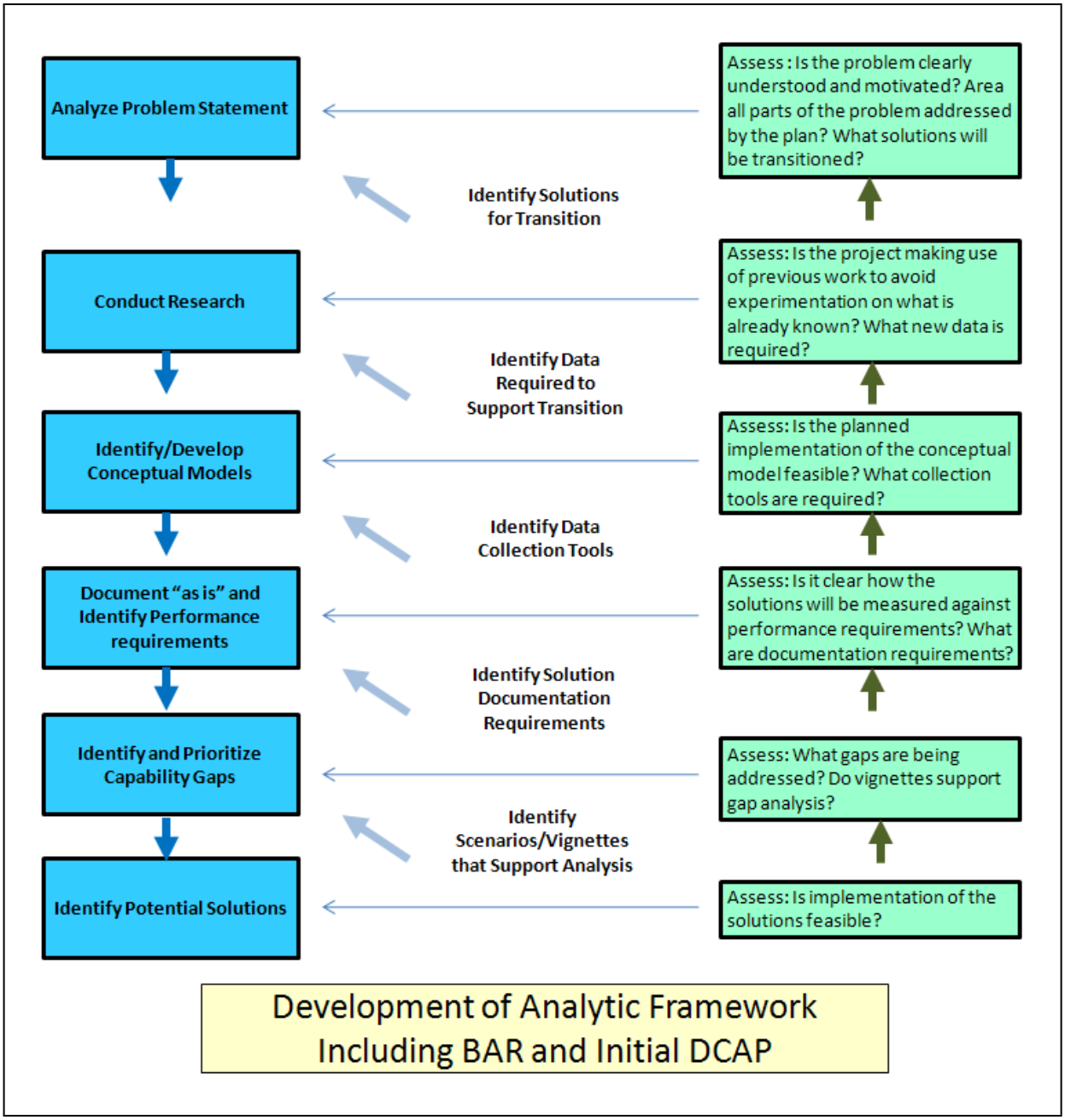


Figure G-2 – Analytic Framework Development

2. PROJECT ANALYSIS LOGIC

2.1. Conceptual Model

The IMISAS conceptual model follows the premise of hierarchically nested requirements, much in the same way that the Open Systems Interconnection (OSI) model divides communication systems into successively supported layers, or in the way Abraham Maslow's hierarchy of needs addresses human motivation in terms of increasing levels of deprivation. From the standpoint of a prospective exchange of information between two persons, hereafter referred to as "A" and "B", there are a multitude of effects that can potentially prevent such exchange. Those effects can be categorized in order of dependency, so that as with the OSI model or Maslow's hierarchy, the effectiveness of an information exchange with regard to a given "layer" presumes the success of the supporting "layers". Referring to Figure G-3, we can define five increasingly dependent layers of information sharing requirements: awareness, physical means, permission, sanction, and user comfort. The most basic requirement for A and B is to communicate awareness on the part of A or B (or both) as to the presence of the other. In the context of Humanitarian Assistance/Disaster Relief (HA/DR) operations, the participation of nongovernmental organizations (NGOs) is unpredictable in time and scope, for example, and it is not uncommon for the Combatant Command to be unaware of the presence of certain NGOs working in its area of responsibility. If the basic requirement of awareness is not satisfied, then the physical means by which A and B might communicate is moot, as is the relevance of permission, sanction, and user comfort. Given that at least one of A and B has become aware of the presence of the other, information exchange now presumes the physical means (e.g., network, infrastructure, sufficient data rate) for their connection, which can be either synchronous or asynchronous, or even over dissimilar paths (e.g., email from A to B, responding chat from B to A). Permission for A to communicate with B (through tangible mechanisms such as account access or electronic credentials, or through business rules such as liaison authorization) in turn presumes the physical requirements are satisfied. Given permission is assured, there may be organizational cultural inhibitors to the exchange of information between A and B, for example, unwillingness on the part of an NGO to sanction exchange of information with the Combatant Commands (COCOM) due to the sensitivity of the perception that the former has aligned itself with the military. Finally, even if no external constraints are levied, A might decide not to exchange information with B even if there is a need. Such a situation might occur if the only means available has an interface that is awkward, or with which A is unfamiliar; it might also stem from an unhealthy personal dynamic between A and B.

For any layer where the requirements have been satisfied, it may be presumed that the requirements of all preceding layers have been satisfied. On the other hand, any case for which the requirements of a given layer are not met terminates the possibility of information exchange

between A and B. In this case, if the causes of the failure in that layer are corrected, then information exchange occurs provided all successive layers meet all requirements. The hierarchical nesting of requirements provides a way to segregate the issues that might hinder information exchange, but more importantly, it suggests a corresponding hierarchy of resource allocation against such issues. It may be questionable to apply current resources to a problem of cultural impasse, for example, when infrastructure shortfalls prevent communication by all but the most primitive means.

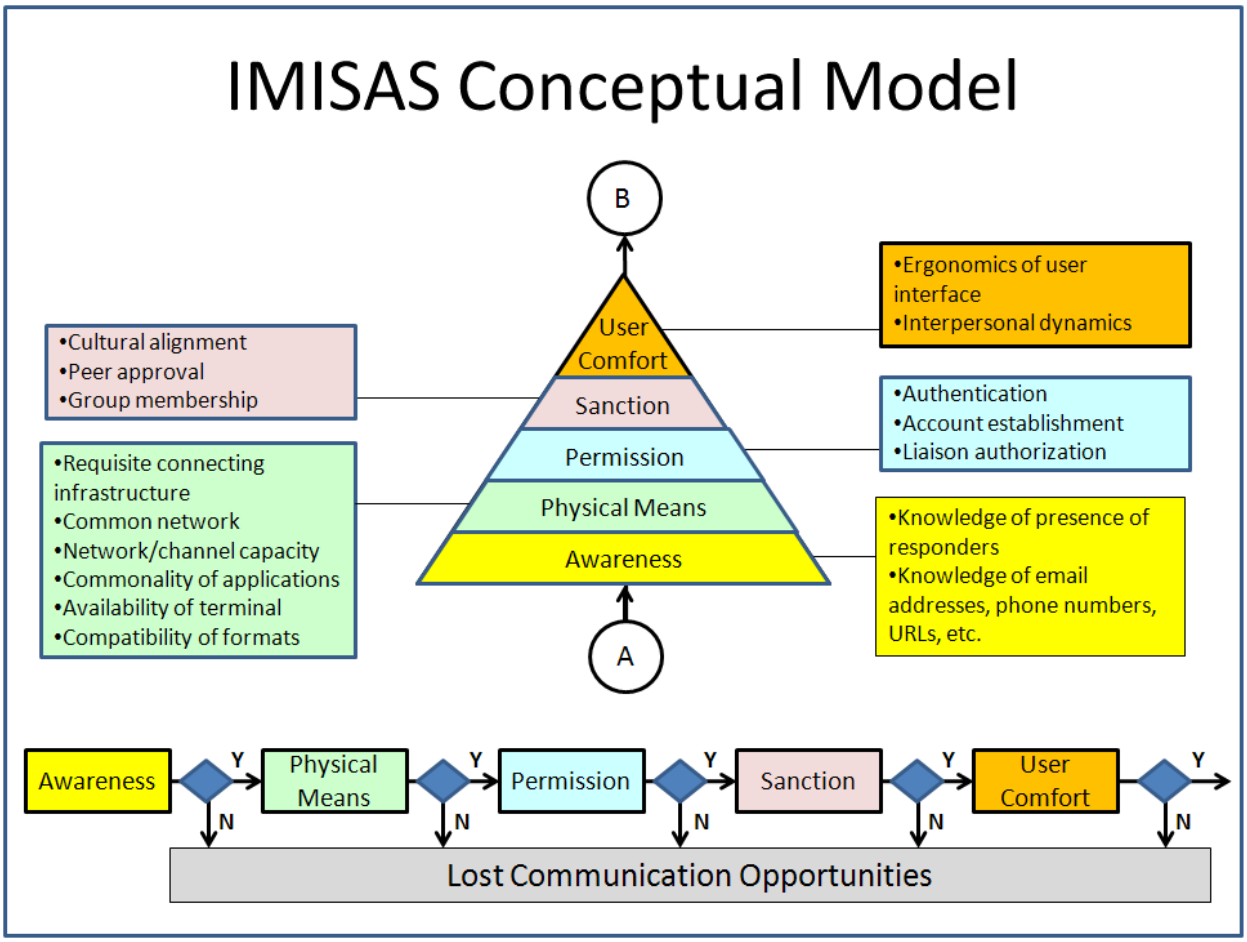


Figure G-3 – IMISAS Conceptual Model

2.2. Traceability

Experimental rigor demands backward traceability from the data elements used to discriminate relative value of existing and alternative capabilities, to the metrics from which those data elements derive, to the Essential Elements of Analysis (EEAs) that frame the metrics, to the study issues that provide analytic focus to experimental objectives, back to those objectives, the

outcomes and ultimately the problem statement. These components of traceability are defined more fully below and their relationship to other activity supporting experimentation shown in Figure G-4.

- Problem Statement: Provided or developed from Study Sponsor guidance – Clearly articulates the problem or challenge and provides focus for the campaign.
- Outcomes: Describes the changes in behavior, capacity, or capability that can be measured to solve the problem.
- Objectives: Describe the scope and detail of work that must be accomplished for the project to meet the outcomes.
- Study Issues: Relevant, appropriate questions decomposed from experiment objectives that provide analytic focus. When answered, the issues should satisfy the experiment objectives.
- EEAs: Focused questions, developed for each issue that are essential in the investigation of experimental objectives and appropriate for the experiment level, type, and venue.
- Metrics, or measures of merit (MOM): any measure of interest with application to a specific experiment. Typical measures include:
    - Measures of Effectiveness (the degree to which an innovation performs a task or meets an objective)
    - Measures of Performance (technical performance of a system or process, e.g., time to acquire a given target)
- Data Elements: Definable, specific and measurable quantities and activities that support calculation of Measures of Merit. Data elements are related to one or more measures.

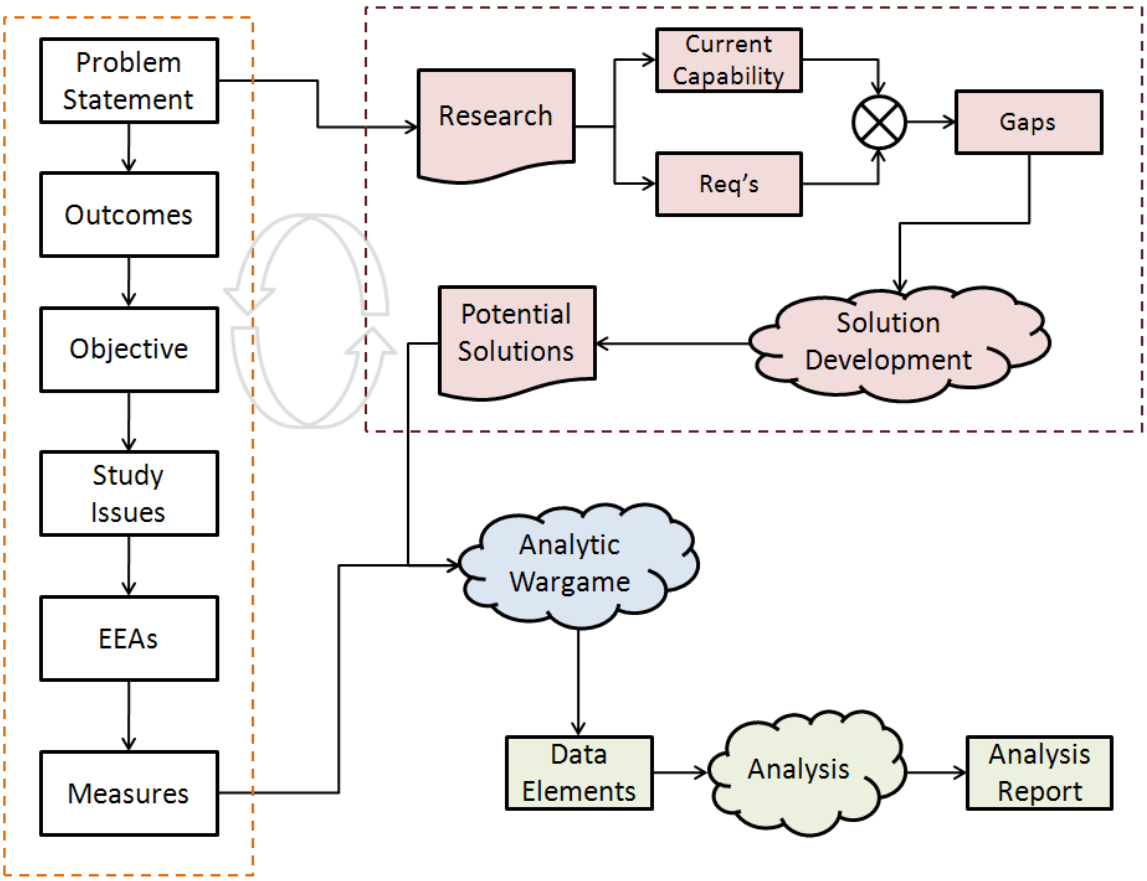


Figure G-4 – Traceability of Data Elements to the Problem Statement

The definition of this project began with the United States (U.S.) European Command (USEUCOM) and U.S. Africa Command (USAFRICOM) Warfighter Challenge (WFC) and the preliminary IMISAS Problem Statement:

Warfighter Challenge: United States European Command (USEUCOM) and United States Africa Command (USAFRICOM) require the capability to share essential information with interagency partners, Coalition and Alliance partners, or emerging partner nations in bi-lateral or multinational efforts. The capability gap is the result of: restrictive network access and information sharing policies; restrictive and cumbersome accreditation procedures for coalition networks and systems; lack of a coherent/unified strategy for a whole of government (to include foreign government) approach to an information sharing/collaborative environment; and resourcing to support that environment and its associated network enterprise services.

IMISAS Problem Statement: COCOMs (Combatant Commands) lack a coherent framework/capability to share information and collaborate across multiple domains with a broad range of mission partners (government/interagency, multi-national, multi-lateral & private sector) due primarily to restrictive policies, conflicting authorities, ad hoc/non-existent procedures, business rules and non-interoperable networks and systems.

Experimental outcomes and objectives proceeded from a Statement of the Problem/Outcome/Objective/Product/Activity decomposition of the WFC statement. One of the original outcomes (operational prototype) was subsequently determined to be infeasible, yielding the following outcomes and objectives:

- Outcome 1: Inform the development of the 'To Be' Unclassified Information Sharing Capability (UISC) employing Technical Spirals and an Analytic Wargame focused on using/integrating available portal and cross domain technologies.

- Objectives:
  - 1.1: Identify requirements and potential operational solutions and technical enhancements using All Partners Access Network (APAN) as the technical backbone for experimentation.
  - 1.2: Pursue, as feasible, required authority and/or certifications required to test or demonstrate a cross domain capability to USEUCOM/USAFRICOM. (NOTE: This objective will not be part of the experiment activities. If anything of value is gleaned from the experiment activity, that is deemed useful, it can be noted in the Analysis Report.)
  - 1.3: Define and design an experiment employing a HA/DR scenario to validate information sharing and collaboration capability enhancements and policy and procedure variables addressing capability gaps.

- Outcome 2: Improved processes, procedures and enabling policies to establish information sharing collaborative networked environment that can work across organizational and security boundaries for mission partners.

- Objectives
  - 2.1: Develop an unofficial joint operating concept (white paper) based on the UISC Concept of Operations to include processes, procedures, and an organizational construct reflecting required roles, responsibilities, authorities and policies.
  - Objective 2.2: Develop and verify operationally focused processes and procedures required to implement information sharing and collaboration for HA/DR operations.

- Objective 2.3: Examine policies, processes, and procedures, and recommend changes to facilitate information sharing with a range of partners in a HA/DR environment.
- 2.4: Conduct user validation of potential UISC to provide enhancement recommendations for current UISC.
- 2.5: Develop a handbook and experimentally validated doctrine change recommendations addressing how the Department of Defense (DOD) can better engage other U.S. Government bodies and share information with International Organizations (IO)/NGOs/private partners in support of HA/DR.

With the problem framed sufficiently and outcomes and objectives determined to fall broadly within scope, quality, schedule, and budget and risk, the rigorous and formal process of the baseline assessment leading to identification of detailed gaps and potential solutions began with the following activity:

- Further defining, decomposing and articulating the problem to clarify the underlying components of the issue.
- Analyzing the problem to ensure that it conformed broadly to accepted Joint required capabilities and/or tasks (Joint Capability Areas (JCAs) and Universal Joint Task Lists (UJTLs)).
- Determining in general whether the problem could be addressed through experimentation and results measured.
- Acknowledging constraints, assumptions and limitations that determined the feasibility of initial project objectives.

As described previously in this section, the decomposition of Outcomes and Objectives into Study Issues, EEAs, and Measures is below. These will be refined as needed as peer review, brainstorming, and continuous learning progresses through the project timeline.

- **Outcome 1:** Inform the development of the 'To Be' UISC employing an Analytic Wargame focused on using/integrating available portal and cross domain technologies.
- **Objective 1.1:** Identify requirements and potential operational solutions and technical enhancements using Unclassified Information Sharing (UIS) APAN as the technical backbone for experimentation.
- **Study Issue – 1.1.1** – What existing information exchange systems could be used operationally by DOD during an HA/DR event?
  - **Proposition/Hypothesis:** Existing information exchange systems could be used by DOD.

- **EEA 1.1.1.A:** Are certain operational federations of existing information exchange hubs significantly more effective than others across the span of responders to an HA/DR event? (solution 1-3)
  - Measures:
    - Information that could be passed
    - Information that could not be passed
    - Length of time to pass information
    - Length of time to receive information
    - Degree of user satisfaction?
    - Ease of use
      - By DOD
      - By outside organizations

- **EEA 1.1.1.B:** What body of information is most effectively and appropriately hosted within the DOD UISC?
  - Measures:
    - Types of information hosted
    - Ease of use on the UISC
    - Types of information that could not be hosted
    - Accessibility of information hosted
      - By DOD
      - By outside organizations
        - Degree of user satisfaction

- **EEA 1.1.1.C:** What capabilities hosted on information exchange hubs could serve as a basis for work site templates in support of an HA/DR event? (solutions 1-3, 3-1)
  - Measures:
    - Time required to establish the work site
    - Ease of using the collaborative working site
    - Accessibility of the work site
    - Diversity of the tool sets

- **Study Issue – 1.1.2** – Are there standards or guidelines for storage and search capability of documents and other data that could prove useful to practical data storage, searchability, and utility?
  - **Proposition/Hypothesis:** Standard usage of tags, metadata, and types of data will make data storage more useful.

- **EEA 1.1.2A:** What tags would be useful to information searching on a UISC? (solution 3-1)
  - Measures:
    - Ease of use
    - Ease of understanding
    - Searchability
    - Tags make sense
    - Tags that were misleading

- **EEA 1.1.2B:** What metadata would be useful to information searching on a UISC? (solution 3-1)
  - Measures:
    - Ease of use
    - Ease of understanding
    - Searchability
    - Metadata makes sense
    - Metadata that was misleading

- **Study Issue – 1.1.3** – How can those involved in information sharing be confident that the information being received is accurate and authentic?
  - **Proposition/Hypothesis:** Rating criteria will assist the information user in determining validity of information.

  - **EEA 1.1.3A:** What information rating criteria will be useful to attaining a reasonable level of confidence in the information's authenticity and accuracy? (solution 4-10)
    - Measures:
      - Criteria used
      - User comfort level for each criteria

- **Objective 1.2:** Testing or demonstration of a cross-domain capability as part of this project was not deemed feasible.

- **Objective 1.3:** Define and design an experiment employing an HA/DR scenario to validate information sharing and collaboration capability enhancements and policy, process and procedure variables addressing capability gaps.

  NOTE: This is primarily a project objective; thus, it does not have separate EEAs and measures associated with it.

- **Outcome 2:** Improved processes, procedures and enabling policies to establish information sharing collaborative networked environment that can work across organizational and security boundaries for mission partners.
- **Objectives 2.1:** Develop an operating concept based on the UISC Concept of Operations (CONOPS) to include processes, procedures, and an organizational construct reflecting required roles, responsibilities, authorities and policies.

  NOTE: This is primarily a project objective; thus, it does not have separate EEAs and measures associated with it. The findings from the experimentable objectives will contribute to the creation of the UIS Unofficial Joint Concept.

- **Outcome 2.2:** Develop and verify operationally focused processes and procedures required to implement information sharing and collaboration for HA/DR operations.

- **Study Issue – 2.2.1** – What is the degree of policy misalignment among represented organizations, and to what degree are those differences reconcilable?

  - **Proposition/Hypothesis:** Reconciling information sharing policies amongst organizations will allow an improved level of information flow.

  - **EEA 2.2.1.A:** What is the quality of service and adaptability of the COCOM's framework supporting unclassified information sharing with mission partners via UISC? (solution 1-5)
    - Measures:
      - Time to deliver
      - Time to receive
      - Time to approve release
      - Time to validate
      - Comparison to previous
      - Amount of time operational/not operational
      - Amount of time communication method operational/not operational
      - Incidence rate of successful information communication without regard to method
      - Robustness of collaboration

  - **EEA 2.2.1.B:** To what degree does a well-structured and comprehensive framework for establishing communication across a broad range of organizations accelerate a combined response to HA/DR exigencies? (solutions 1-3, 1-5)

        - Measures:
            - Communications available on a timeline
            - Organizations in communications
            - Organizations not in communication

- **Study Issue – 2.2.2** – Is the risk inherent in sharing of information acceptable? What is the true necessity of operating on restricted access when engaged in operations in an HA/DR environment?
    - **Proposition/Hypothesis:** The gains from moving unclassified information from controlled environments to lesser controlled environments for the purpose of increased information sharing outweigh the risks.

    - **EEA 2.2.2.A:** Does the exercise of recommended business rules indicate an unacceptable level of unintended disclosure risk relative to the volume, urgency, and potential impact of the information?
        - Measures:
            - Controlled information that was inadvertently passed
            - Length of time to extract unclassified information
            - Degree of user satisfaction
            - Degree of receiver satisfaction
            - Usefulness of received information

    - **EEA 2.2.2.B:** Assuming sufficient training is provided is the level of use of the business rules sufficient to justify their necessity?
        - Measures:
            - Length of time to complete tasks
            - Degree of user satisfaction

    - **EEA 2.2.2.C:** What challenges, limitations, and risks exist in effecting information sharing from controlled environments to lesser controlled domain of the UISC? (solution 1-2)
        - Measures:
            - Accreditation time
            - Average latency time for transfer across network boundaries
            - File types allowed for transfer across network boundaries
            - Percentage of automated steps to total steps for transfer across network boundaries

- Likelihood/impact matrix of spills (including assessed likelihood of intentional breach of procedure)

- **EEA 2.2.2.D:** What challenges, limitations, and risks exist in effecting information sharing from controlled environments to lesser controlled domains (social media sites)? (solution 4-8)
  - Measures:
    - Average latency time for transfer across network boundaries
    - File types allowed for transfer across domain boundaries
    - Number of user steps to transfer information
    - Likelihood/impact matrix of spills (including assessed likelihood of intentional breach of procedure)
    - User comfort level with sharing information from controlled environments to lesser controlled environments

- **EEA 2.2.2.E:** What challenges, limitations, and risks exist in effecting information sharing from lesser controlled domains (social media sites) to controlled environments? (solution 4-9)
  - Measures:
    - Average latency time for transfer across network boundaries
    - File types allowed for transfer across domain boundaries
    - Number of steps to retrieve information
    - Likelihood of malicious elements entering the controlled domain
    - User comfort level of receiving of information from lesser controlled environments into controlled environments

- **Study Issue – 2.2.3** – To what degree could a quick reference guide detailing the capabilities of non-DOD organizations, descriptions of roles and responsibilities in an HA/DR environment, and general information requirements be beneficial to information sharing in an HA/DR environment?

  - **Proposition/Hypothesis:** A quick reference guides will expedite and improve the information capabilities of a DOD organization.

  - **EEA 2.2.3.A:** What are the primary roles and responsibilities during an HA/DR operation? (solution 1-8)
    - Measures:
      - Roles and responsibilities descriptions that are accurate

- Roles and responsibilities descriptions that were not accurate
- Number of connections to reach correct partner of interest
- User satisfaction with roles and responsibility descriptions

- **EEA 2.2.3.B:** What mission partner capabilities and limitations that are valuable to know during an HA/DR operation? (solution 1-8)
  - Measures:
    - Partner capabilities and limitations descriptions that were accurate
    - Partner capabilities and limitations descriptions that are not accurate
    - User satisfaction with capabilities and limitations descriptions

- **EEA 2.2.3.C:** To what degree does organization description of information exchange requirements (IERs) impact unclassified information sharing? (solution 1-8)
  - Measures:
    - Service completion of IERs
    - Requester satisfaction of IERs

- **Objective 2.3:** Examine policies, processes, and procedures, and recommend changes to facilitate information sharing with a range of partners in a HA/DR environment.

- **Study Issue – 2.3.1** – What current policies, processes and procedures are hindering information sharing and how can they be discarded, changed, or improved to facilitate information sharing?

  - **Proposition/Hypothesis:** The gains from sharing unclassified information with partners outweighs the risks.

  - **EEA 2.3.1.A:** Does the exercise of a risk managed approach handling and release positively impact unclassified information sharing? (solutions 1-1, 1-2)
    - Measures:
      - Controlled information that was inadvertently passed
      - Length of time to transfer unclassified information
      - Information types that were transferred
      - Business rules that were not value added
      - Business rules that appear to be missing
      - Degree of user satisfaction
      - Degree of receiver satisfaction

- Usefulness of received information

- **EEA 2.3.1.B:** Does having a pre-planned information release process expedite usable unclassified information sharing within acceptable risk? (solution 1-1)
  - Measures:
    - Controlled information that was inadvertently passed
    - Length of time to transfer unclassified information
    - Information types that were transferred
    - Parts of the process that worked well
    - Parts of the process that did not work well
    - Degree of user satisfaction
    - Degree of receiver satisfaction
    - Usefulness of received information

- **EEA 2.3.1.C:** What challenges, limitations, and risks exist in effecting information sharing from controlled environments to lesser controlled domains? (solutions 1-1, 1-2)
  - Measures:
    - Controlled information that was inadvertently passed
    - Length of time to transfer unclassified information
    - Information types that were transferred
    - Degree of completeness of information transfer
    - Degree of latitude in determining release policy
    - Degree of user satisfaction
    - Degree of receiver satisfaction
    - Usefulness of received information

- **Study Issue – 2.3.2** – What policies, processes, and procedures can be implemented in order to facilitate expeditious and accurate information sharing with mission partners via the use of a UISC?
  - **Proposition/Hypothesis:** User friendly and partner accommodating practices can facilitate information sharing with partners.
  - **EEA 2.3.2.A:** Does a set of business rules to standardize labeling of data types, metadata, and tagging facilitate the ability to share pertinent information? (solution 3-1)
    - Measures:
      - Amount of information found via search

- Amount of information omitted from search
- Degree of user satisfaction
- Degree of receiver satisfaction
- Usefulness of received information

- **EEA 2.3.2.B:** Does a set of business rules for allowing mission partners to utilize a UISC facilitate expeditious, useful, and accurate information sharing? (solutions 1-5, 3-1)
  - Measures:
    - Controlled information that was inadvertently passed
    - Length of time to transfer unclassified information
    - Length of time to allow access to UISC
    - Length of time to establish contact with mission partners
    - Degree of user satisfaction
    - Degree of receiver satisfaction
    - Usefulness of received information
    - Accuracy of received information

- **EEA 2.3.2.C:** Do graduated user account permissions facilitate UIS? (solution 4-6)
  - Measures:
    - Length of time to approve access to UISC compartment
    - Ease of user request process
    - User comfort level with the requested Personally Identifiable Information (PII)

- **EEA 2.3.2.D:** Does rapid user registration to a UISC facilitate COI response utilizing the UISC? (solution 4-7)
  - Measures:
    - Length of time to approve access to the UISC
    - Number of users seeking approval
    - Number of users approved
    - Number of unique organizations seeking approval
    - Number of unique organizations approved
    - Ease of user request process
    - User comfort level with the requested PII

- **EEA 2.3.2.E:** Do improvements in internal COCOM information management policies and procedures improve quality of service of unclassified information flow to mission partners? (solution 1-7)
  - Measures:
    - Timeliness of unclassified information relative to latest time information is of value (LTIOV)
    - Degree of mission partner satisfaction
    - Usefulness of received information
    - Accuracy of received information

- **Objective 2.4:** Conduct user validation of potential UISC to provide enhancement recommendations for current UISC.

- **Study Issue – 2.4.1** – Can a technological solution overcome barriers to information sharing arising from organizational differences in structure, culture, or restrictions on handling or association with information?

  - **Proposition/Hypothesis:** Upgrades to existing UISC allow for improved information sharing between the Joint Task Force and NGOs/IOs/etc.
  - **EEA 2.4.1.A:** When potential information sharing partners have reservations about providing PII due to concerns about creating a perception of affiliation with the military, to what degree can technical enhancements to identity management mechanisms facilitate the exchange?
    - Measures: TBD

  - **EEA 2.4.1.B:** To what degree can improvements to the comprehensiveness, accessibility, and discoverability of portal-based information overcome shortfalls in inter-organizational communication?
    - Measures: TBD

  - **EEA 2.4.1.C:** Does a flexible, risk-managed set of authentication requirements accelerate the flow of information having release sensitivities?
    - Measures:
      - Speed of authentication
      - Accuracy of authentication
      - Degree of user comfort level
      - Degree of ease of use

- **EEA 2.4.1.D:** Is the UISC technical solution sufficient from the perspective of: latency, connecting the disadvantaged user, user friendliness, training overhead, accessibility, and interface to social media networks outside the .org domain?
  - Measures:
    - Time for uploading document
    - Time for establishing synchronous collaborative session
    - Incidence rate of bandwidth precluded connection attempts
    - Proportions of connections by application
    - Operational availability of connection modes
    - User feedback on ergonomics of technical solution
    - User feedback on amount of training required to effectively use the solution
    - Percentage of information artifacts originating in social media networks

- **EEA 2.4.1.E:** Does ensuring confidentiality and anonymity increase the interchange of meaningful information?
  - Measures:
    - Information exchange rate between organizations of interest with mechanisms in place
    - Information exchange rate between organizations of interest without mechanisms in place
    - Comparison of with vs. without
    - User feedback on level of visibility of these mechanisms

- **EEA 2.4.1.F:** What percentage of information entering the boundaries of the UISC is actively provided (pushed) and how much is pulled from the public domain?
  - Measures:
    - Network traffic analysis
    - User feedback

- **EEA 2.4.1.G:** What percentage of information exiting the boundaries of the UISC is actively sent to a subscriber (pushed) and how much is pulled by the subscriber from the solution's public interface?
  - Measures:
    - Network traffic analysis

- **EEA 2.4.1.H:** What are the best categorization and presentation schemes for the UISC's public interface?

        - Measures:
            - Link visitation rates by information category and information hierarchy level
            - User feedback on discoverability of information

- **Study Issue – 2.4.2** – What processes and procedures are required in order to effect efficient UISC registration and access and provide user permissions that allow for adequate information sharing?

    - **Proposition/Hypothesis:** Expediting user registration and privileges increases positive information sharing.

    - **EEA 2.4.2.A:** What are the processes and procedures to granting user account permissions? (solution 4-6)
        - Measures:
            - What procedures worked well?
            - What procedures did not work well?
            - What appeared to be the pitfalls to the procedures?
            - Ease of use for custodian
            - Ease of use for user

    - **EEA 2.4.2.B:** What are the processes and procedures to granting rapid user registration? (solution 4-7)
        - Measures:
            - What procedures worked well?
            - What procedures did not work well?
            - What appeared to be the pitfalls to the procedures?
            - Ease of use for custodian
            - Ease of use for user

- **Objective 2.5:** Develop a handbook and validated doctrine change recommendations addressing how DOD can better engage other U.S. Government bodies and share information with IO/NGO/private partners in support of HA/DR operations.

  NOTE: This is primarily a project objective; thus, it does not have separate EEAs and measures associated with it. The findings from the experimentable objectives will contribute to the creation of the UIS Handbook.

3. ANALYSIS PLAN

3.1. Experimental Hypotheses

According to the DOD Command and Control Research Program Code of Best Practice for Experimentation, unless a simple "if...then...condition" hypothesis can be developed, experiment results will not be clear. A good hypothesis differentiates between two or more treatments and includes independent and dependent variables. The high level experimental hypotheses to be tested during the IMISAS Analytic Wargame are:

Hypothesis 1: If the UISC combines knowledge management methodologies with a minimum-demand user interface and carefully designed software composition including social media interfaces, then accessibility, completeness, responsiveness, and timeliness of information will increase, with attendant increases in relevance to the activity of responders and their situational understanding.

Hypothesis 2: If COCOMs foster coordination with, outreach to, and holistic comprehension of the span of HA /DR responders, then the coherence, agility, responsiveness, robustness, and speed of combined HA/DR response will increase.

Hypothesis 3: If a risk-managed approach to information sharing is adopted, to include information release policy, mechanisms for identity establishment and source vetting, and methods for assuring confidentiality and anonymity, then within acceptable limits of information accuracy and security, improvements will be garnered in information accessibility and the agility, flexibility, responsiveness, speed, and timeliness of HA/DR response.

3.2. Data Collection and Analysis Plans (DCAPs)

The IMISAS Data Collection Plans and DCAPs will be stand-alone documents, each one detailing how data will be collected and analyzed for particular events in the experimentation campaign. Data Collection Plans will be created to collect data during workshops and conferences while DCAPs will cover a range of purposes and data formats depending on the venue. The Analytic Wargame DCAP will address information relative to both processes, including the information and analysis for the statistical testing of experimental hypotheses. For some events not part of the experimentation proper, data collection instruments employing some subset of DCAP tools and methodologies will be used. These events include the Solution Development Workshop (SDW), Initial Planning Conference (IPC), Process Development Event (PDE), Mid-Planning Conference (MPC), Final Planning Conference (FPC) and other venues supporting the evaluation, refinement, and ranking of solutions for experimental development and to initiate planning for the Technical Spirals and Analytic Wargame. Data collection instruments will be submitted for the following venues, with full DCAPs annotated where applicable:

- SDW
- IPC
- PDE
- MPC
- FPC
- Transition Conference
- Experimentation Phases
    - Technical Spirals
    - Analytic Wargame / Seminar

The DCAP as appropriate to the venue or experiment phase will include:

- Background
- Experiment design description
- Collection plan
- Analysis plan
- Document mapping decomposed gaps and decomposed solutions to the hypothesis,
- Research questions and measures
- Data archiving plan

The IMISAS DCAP format will be in accordance with the United States Joint Forces Command (USJFCOM) J9 Analysis, Standards, and Tools Division template as appropriate to the project and will contain the sections below:

- Section One – Introduction. Section One will address the basis for the experiment.
- Section Two – Problem Statement and End State. Section Two will explain the Warfighter Challenge problem statement and the derivation to the IMISAS project problem statement. Additionally, the projected end state and goals of the project and experiment will be addressed.
- Section Three – Hypothesis. Section Three will list the overarching project hypothesis for the campaign.
- Section Four – Outcomes and Objectives. Section Four explains the beginning of decomposing the problem statement into Outcomes and the Objectives that must be accomplished in order to satisfy the Outcomes.
- Section Five – Study Issues, EEAs, and Measures. Section Five is the significant decomposition of the traceability chain into measures. This is the heart and soul of the analysis.
- Section Six – Proposed Activity. Section Six gives a basic background of the proposed experiment activity and how the important functions integrate with the analysis team.

- Section Seven – Analysis and Data Collection. Section Seven explains the primary data collection methods for the experiment activity, security and privacy issues, training, daily battle rhythm, and data archiving.
- Section Eight – Reporting. Section Eight explains the reports that are expected to be generated from the experiment activity and what future events the report will support.
- Section Nine – Experiment Risk Assessment. Section Nine will detail the 21 threats to an experiment coupled with a mitigation plan.

4. EXPERIMENT DESIGN AND EXECUTION

The experimentation campaign will validate, though scenario-based experimentation, the solutions recommended for identified information sharing gaps. Additionally, the campaign will validate a UIS Policy and Procedures Handbook addressing how the COCOM can best engage and work with the U.S. Government internally and provide and share information with other partners (multi-national, coalition, Intergovernmental Organization, NGO, private sector) in HA/DR operations. Finally, the campaign will produce recommendations for changes to doctrine, policies, procedures, UISC platform capabilities, and documentation of DOD Architectural Framework operational and system views.

During the IPC, the original alignment of events was altered due to USAFRICOM availability issues and the experiment activities were reduced from several events to Technical Spirals and an Analytic Wargame.

4.1. Technical Spirals (May – July)

The Technical Spirals will be conducted in order to examine potential technical solutions to UIS. Five separate events, held at two week intervals, will be conducted in a distributed environment utilizing APAN as the work site. The potential solutions examined and the exact EEAs investigated will be further explained in a separate DCAP.

Planning/Preparation	AWG Execution	Outputs
• Refined Solutions	• Solution validation for	• Analysis Report
• Experiment Design	- Policy	• UISC Recommendations
• User Guide for participants	- Processes	• UIS Handbook
• SOP for participants	- Procedures	• UIS Unofficial Operating Concept
• DCAP	• Data Capture & Analysis	• Input for Transition Conference

Figure G-5 – Analytic Wargame Framework

4.2. Analytic Wargame (01 Aug – 04 Aug)

The Analytic Wargame is the experiment activity in which experimental hypotheses will be tested. The Analytic Wargame will follow the Experiment Plan, which aligns scenario vignettes, control and test group subjects, and solution variables in such a way that effects can be unambiguously ascribed to causes. A PDE was held in order to gain information from operators as to the present day information sharing processes and procedures. The findings of the PDE are being combined with all other research including the baseline assessment, which will be referenced as part of the Analytic Wargame baseline for analysis. Also, additional insights will be gathered for the UIS Policy and Procedures Handbook and recommendations across the Doctrine, Organization, Training, Material, Leadership, Policy, Facilities, and Policy spectrum. Figure G-5 displays the Analytic Wargame Framework.

4.3. Data Collection

The purpose of the experiment is to produce data for the analysis phase. The analysis phase seeks to support or refute the solution hypotheses, and answer questions or illuminate continuing issues salient to the development of the handbook and change recommendations for doctrine, policies, processes, or procedures. Although the majority of data will be captured during experiment execution, data collection will occur throughout the remaining life of the project. Regardless of the point of capture of data, process integrity is crucial to ensure a valid, credible, reliable product. The Lead Analyst will ensure procedures are in place to supervise the collection and storage of all data, and that collection agents are competent, unbiased, and consistent in their activities. Data collected in support of analysis during this phase will be in

raw form (e.g., observations, participant demographics) and will support either hypothesis testing or experiment improvement. Hypothesis testing data will be directly applicable to event objectives, research questions, and/or hypotheses; i.e., data collected in support of EEAs and Measures to enable comparison of the value of different alternatives. Experiment improvement data will consist of suggestions or lessons learned on improving the conduct of the experiment itself (e.g., more computers, larger rooms). The below list provides a span of potential methods for capturing data.

- Observations and analyst notes capturing interactions, behavior, key discussions
- Surveys (manual or via SurveyMonkey or equivalent survey tool as available)
- Interviews (personal, telephone, email),
- APAN system logs, and log data from other experimentation communications systems or applications
- Audio, video, or Adobe Connect Online recordings as appropriate
- Screen captures
- After action reports and hot washes

Depending upon availability and ease of use at the Analytic Wargame's network, USJFCOM's J9 Observation Tool, commonly called JOT, may be used to record and organize observations. Additionally, if available, use of USJFCOM J9's licenses to Vovici could be used for survey collection and analysis.

5. EXPERIMENTATION OUTPUTS AND OTHER SIGNIFICANT PROJECT EVENTS

5.1. Data Analysis

Data collected during the experiment and its associated events (i.e., IPC, MPC, FPC) will be recorded in the form of observations, surveys, logs, electronic, automated, and others; as appropriate for a given event. Analysis of this data will, in turn, produce insights, findings, and recommendations via a synthesis process. The following are descriptions of observations, insights, findings, and recommendations.

- Observation: A behavior, statement, or action seen (observed) during an experiment. Unlike a finding or insight, an observation is a statement of fact or occurrence and requires no inference from collected data. See also, Finding and Insight.
- Insight: The synthesis of a set of observations that reveal a capability, an enabler of a capability, or an impact. New thoughts or patterns that emerge as the project analyst looks at the observations and reviews them in light of the larger body of knowledge.
- Finding: A conclusion reached after examination or investigation, normally based on the corroboration of an insight from multiple venues. A finding is usually supported by a

combination of quantitative and statistical comparisons of various cases or treatments examined, supplemented and amplified by qualitative observations and assessments. See also, Insight and Observation.

- Recommendation: A relevant, proposed action determined to be appropriate and advisable based on analysis of data.

5.2. Reporting Phase

This phase produces the IMISAS Final Report with findings and recommendations based on the analysis of experiment results. The compilation of all data collected and synthesized during the project will be found in Annex J Analysis.

5.3. Analytical Input to Final Report

The Lead Analyst will be responsible for including the analytical input as a separate annex (Annex J of the Final Report). The following categories will be addressed:

- Objectives, issues, applicable UJTLs, JCAs, and research questions as appropriate
- Mapping of objectives to variables, metrics, and data
- Observations, insights, findings, and recommendations
- Areas for future experimentation and/or research

5.4. Way Ahead

This analytic framework is a living document. As experiment design and solution refinement continues, it will be updated to capture salient developments. Information from planning conferences with partners and stakeholders will be used to refine the measures and data elements for use in the analysis of Technical Spirals and Analytic Wargame and in order to support the evaluation and validation solutions. This information, along with discussions from other working sessions covering metrics, scenario/vignette design, and experimental resource identification, will be used to further refine and align experimental hypotheses and EEAs. Based upon these inputs, and in concert with the experiment design plan, the analytic framework will gain the detail necessary to guide the development of the experimental data collection and analysis plan(s).

ACRONYMS

APAN	All Partners Access Network
COCOM	combatant command
DCAP	Data Collection and Analysis Plan
DOD	DOD
EEA	essential element of analysis
FPC	Final Planning Conference
HA/DR	humanitarian assistance/disaster relief
IER	information exchange requirement
IMISAS	Interagency and Multinational Information Sharing Architecture and Solutions
IO	international organization
IPC	Initial Planning Conference
JCA	joint capability area
JOT	J9 observation tool
MOM	measure of merit
MPC	Mid-Planning Conference
NGO	non-governmental organization
PII	personally identifiable information
SDW	Solutions Development Workshop
UIS	unclassified information haring
UISC	unclassified information sharing capability
UJTL	Universal Joint Task List
USAFRICOM	United States Africa Command
USEUCOM	United States European Command
USJFCOM	United States Joint Forces Command
WFC	Warfighter Challenge

United States Joint Staff

Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions Project

(IMISAS)

Annex H - Data Collection and Analysis Plan (DCAP) - Technical Spirals

TABLE OF CONTENTS

1. INTRODUCTION H-1
2. PROBLEM STATEMENT AND END STATE H-1
3. PROPOSITIONS/HYPOTHESES H-1
4. OUTCOMES AND OBJECTIVES H-1
5. STUDY ISSUES, ESSENTIAL ELEMENTS OF ANALYSIS, AND MEASURES H-2
6. PROPOSED ACTIVITY H-8
7. ANALYSIS AND DATA COLLECTION H-8
7.1. Collection Methods H-9
7.1.1. Automated/Instrumented H-9
7.1.2. Observations H-9
7.1.3. Interviews H-9
7.1.4. Surveys H-9
7.2. Analysis Methods H-10
7.3. Privacy and Protection of Human Subjects in Research H-10
7.4. Classification H-10
7.5. Analysis Team Training H-10
7.6. Hot-Washes H-11
7.7. Data Archive H-11
7.7.1. Data Storage and Archiving Locations H-11
8. REPORTING H-11
8.1. Analysis Report H-12
9. EXPERIMENT RISK/THREAT ASSESSMENT H-12
APPENDIX A: ACRONYMS H-17
APPENDIX B: DATA COLLECTION MATRIX H-18
APPENDIX C: Technical Spiral One, Data Collection Plan H-19
APPENDIX D: Technical Spiral Two, Data Collection Plan H-21
APPENDIX E: Technical Spiral Three, Data Collection Plan H-24
APPENDIX F: Technical Spiral Four, Data Collection Plan H-26

SUB-APPENDIX G: Technical Spiral Five, Data Collection Plan H-28

1. INTRODUCTION

The Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Technical Spirals Data Collection and Analysis Plan (DCAP) provides the specific details for the data collection and analysis activities for the Technical Spirals. It addresses specific data collection areas, methodology for data generation, collection, analysis, and archiving in support of the Technical Spirals. Additionally, the DCAP provides specification of data fields for collection instruments and their relationships demonstrating traceability from data elements back to the problem statement (see the IMISAS End-to-End Experiment Plan, Analytic Framework Annex). Appendix A contains a full list of acronyms used in this document.

2. PROBLEM STATEMENT AND END STATE

See the IMISAS End-to-End Experiment Plan, Analytic Framework Annex.

3. PROPOSITIONS/HYPOTHESES

See the IMISAS End-to-End Experiment Plan, Analytic Framework Annex.

4. OUTCOMES AND OBJECTIVES

Only those Outcomes and Objectives that will be investigated during the Technical Spirals will be listed below. For a full view of all experiment Objectives, see the IMISAS End-to-End Experiment Plan, Analytic Framework Annex.

- Outcome 1: Inform the development of the 'To Be' Unclassified Information Sharing Capability (UISC) employing an Analytic Wargame focused on using/integrating available portal and cross domain technologies.
    - Objective 1.1: Identify requirements and potential operational solutions and technical enhancements using All Partners Access Network (APAN) as the technical backbone for experimentation.
- Outcome 2: Improved processes, procedures and enabling policies to establish information sharing collaborative networked environment that can work across organizational and security boundaries for mission partners.

- Objective 2.3: Examine policies, processes, and procedures, and recommend changes to facilitate information sharing with a range of partners in a humanitarian assistance (HA)/disaster relief (DR) environment.

- Objective 2.4: Conduct user validation of potential UISC to provide enhancement recommendations for current UISC.

5. STUDY ISSUES, ESSENTIAL ELEMENTS OF ANALYSIS, AND MEASURES

The following is the decomposition from Outcomes → Objectives → Study Issues → Essential Elements of Analysis (EEAs) → Measures. The Data collection matrix in Appendix B also includes the collection methodology and the data elements that will be used to obtain the data necessary to meet the Measures. Only those relevant elements will be listed in this DCAP. For a full view of the experiment decomposition, see the IMISAS End-to-End Experiment Plan, Analytic Framework Annex.

NOTE: As the Technical Spirals progress, due to learning, findings, analysis, and refinement, some of the Objectives, Study Issues, EEAs, and Measures may change or be updated.

Outcome 1: Inform the development of the 'To Be' UISC employing Technical Spirals and an Analytic Wargame focused on using/integrating available portal and cross domain technologies.

Objective 1.1: Identify requirements and potential operational solutions and technical enhancements using Unclassified Information Sharing (UIS) APAN as the technical backbone for experimentation.

- Study Issue – 1.1.1 – What existing information exchange systems could be used operationally by Department of Defense (DOD) during an HA/DR event?

  - Proposition/Hypothesis: Existing information exchange systems could be used by DOD.

  - EEA 1.1.1.C: What capabilities hosted on information exchange hubs could serve as a basis for work site templates in support of an HA/DR event? (solution, 3-1)

    - Measures:
      - Ease of using the collaborative working site
      - Accessibility of the work site
      - Diversity of tool sets

- Study Issue – 1.1.2 – Are there standards or guidelines for storage and search capability of documents and other data that could prove useful to practical data storage, searchability, and utility?

  - Proposition/Hypothesis: Standard usage of tags, metadata, and types of data will make data storage more useful.

  - EEA 1.1.2A: What tags would be useful to information searching on a UISC? (solutions 3-1, 4-12)

    - Measures:
      - Ease of use
      - Ease of understanding
      - Searchability
      - Tags make sense
      - Tags that were misleading

  - EEA 1.1.2B: What metadata would be useful to information searching on a UISC? (solution 3-1)

    - Measures:
      - Ease of use
      - Ease of understanding
      - Searchability
      - Metadata makes sense
      - Metadata that was misleading

  - EEA 1.1.2.C: What are the best practices when sharing information with low bandwidth devices and only low bandwidth availability? (solution 4-1)

    - Measures:
      - Ability to access information
      - Ability to post information
      - Adequacy of information accessed
      - Low bandwidth device used
      - Functionality of low bandwidth device used
      - Comfort level with lack of verification criteria
      -

- Study Issue – 1.1.3 – How can those involved in information sharing be confident that the information being received is accurate and authentic?

    - Proposition/Hypothesis: Rating verification tools and criteria will assist the information user in determining validity of information.

    - EEA 1.1.3.A: What information rating criteria will be useful to attaining a reasonable level of confidence in the information's authenticity and accuracy? (solution 4-10)

        - Measures:
            - Criteria used
            - User comfort level for each criteria

    - EEA 1.1.3.B: What information verification tools will be useful to attaining a reasonable level of confidence in the information's authenticity and accuracy? (solution 4-11)

        - Measures:
            - Verification tool used
            - User comfort level with tool

- Study Issue – 1.1.4 – How can the use of a User Defined Operational Picture (UDOP) assist with information sharing amongst mission partners? (solution 3-1)

    - Proposition/Hypothesis: A UDOP will assist DOD with information sharing amongst mission partners.

    - EEA 1.1.4.A: How can a UDOP assist with sharing of information amongst mission partners? (solution 3-1)

        - Measures:
            - Types of information that can be shared via a UDOP
            - Usefulness of the information shared from or via a UDOP
            - Limitations of the UDOP

Outcome 2: Improved processes, procedures and enabling policies to establish an information sharing collaborative networked environment that can work across organizational and security boundaries for mission partners.

Objective 2.2: Develop and verify operationally focused processes and procedures required to implement information sharing and collaboration for HA/DR operations.

- Study Issue – 2.2.2 – Is the risk inherent in sharing of information acceptable? What is the true necessity of operating on restricted access when engaged in operations in an HA/DR environment?

    - Proposition/Hypothesis: The gains from moving unclassified information from controlled environments to lesser controlled environments for the purpose of increased information sharing outweigh the risks.

    - EEA 2.2.2.D: What challenges, limitations, and risks exist in effecting information sharing from controlled environments to lesser controlled domains (social media sites)? (solution 4-8)

        - Measures:
            - Average latency time for transfer across network boundaries
            - File types allowed for transfer across domain boundaries
            - Number of user steps to transfer information
            - Likelihood/impact matrix of spills (including assessed likelihood of intentional breach of procedure)
            - User comfort level with sharing information from controlled environments to lesser controlled environments

    - EEA 2.2.2.E: What challenges, limitations, and risks exist in effecting information sharing from lesser controlled domains (social media sites) to controlled environments? (solution 4-9)

        - Measures:
            - Average latency time for transfer across network boundaries
            - File types allowed for transfer across domain boundaries
            - Number of steps to retrieve information
            - Likelihood of malicious elements entering the controlled domain
            - User comfort level of receiving of information from lesser controlled environments into controlled environments
            -

Objective 2.3: Examine policies, processes, and procedures, and recommend changes to facilitate information sharing with a range of partners in a HA/DR environment.

- Study Issue – 2.3.2 – What policies, processes, and procedures can be implemented in order to facilitate expeditious and accurate information sharing with mission partners via the use of a UISC?

  - Proposition/Hypothesis: User friendly and partner accommodating practices can facilitate information sharing with partners.

  - EEA 2.3.2.A: Does a set of business rules to standardize labeling of data types, metadata, and tagging facilitate the ability to share pertinent information? (solutions 3-1, 4-12)

    - Measures:
      - Amount of information found via search
      - Amount of information omitted from search
      - Degree of user satisfaction
      - Degree of receiver satisfaction
      - Usefulness of received information

  - EEA 2.3.2.B: Does a set of business rules for allowing mission partners to utilize a UISC facilitate expeditious, useful, and accurate information sharing? (solution 3-1)

    - Measures:
      - Controlled information that was inadvertently passed
      - Length of time to transfer unclassified information
      - Length of time to allow access to UISC
      - Degree of user satisfaction
      - Degree of receiver satisfaction
      - Usefulness of received information

  - EEA 2.3.2.C: Do graduated user account permissions facilitate UIS? (solution 4-6)

    - Measures:
      - Length of time to approve access to UISC compartment
      - Ease of user request process
      - User comfort level with the requested Personally Identifiable Information (PII)

  - EEA 2.3.2.D: Does rapid user registration to a UISC facilitate Community of Interest (COI) response utilizing the UISC? (solution 4-7)

- Measures:
  - Length of time to approve access to the UISC
  - Number of users seeking approval
  - Number of users approved
  - Number of unique organizations seeking approval
  - Number of unique organizations approved
  - Ease of user request process
  - User comfort level with the requested PII

- EEA 2.3.2.F: What processes and business rules are appropriate when using an information verification tool for information sharing with mission partners? (solution 4-11)

  - Measures:
    - Processes and business rules that assist in valid verification
    - Processes and business rules that did not assist in valid verification
    - Processes and business rules that did could improve in valid verification

- EEA 2.3.2.G: What processes and business rules are appropriate when using a UDOP for information sharing with mission partners? (solution 3-1)

  - Measures:
    - Processes and business rules that assist in relaying information via UDOP
    - Processes and business rules that did not assist in relaying information via UDOP
    - Processes and business rules that could improve in relaying information via UDOP

Objective 2.4: Conduct user validation of potential UISC to provide enhancement recommendations for current UISC.

- Study Issue – 2.4.2 – What processes and procedures are required in order to effect efficient UISC registration and access and provide user permissions that allow for adequate information sharing?

  - Proposition/Hypothesis: Expediting user registration and privileges increases positive information sharing.

- EEA 2.4.2.A: What are the processes and procedures to granting user account permissions? (solution 4-6)
  - Measures:
    - What procedures worked well?
    - What procedures did not work well?
    - What appeared to be the pitfalls to the procedures?
    - Ease of use for custodian
    - Ease of use for user
- EEA 2.4.2.B: What are the processes and procedures to granting rapid user registration? (solution 4-7)
  - Measures:
    - What procedures worked well?
    - What procedures did not work well?
    - What appeared to be the pitfalls to the procedures?
    - Ease of use for custodian
    - Ease of use for user

6. PROPOSED ACTIVITY

The IMISAS Technical Spirals will demonstrate and evaluate current capabilities in order to provide recommendations and potential solutions for a UISC. The spirals will be held at two week intervals beginning May 12, 2011 and concluding July 09, 2011 for a total of five distributed events. Use cases will be written and tested prior to the actual event and will demonstrate processes and procedures on a UISC, APAN as a proxy, to determine potential improvements for a new UISC. The significant details for each spiral will be published in separate documents, one for each use case/spiral.

The analysis team will participate in the dry runs for the use cases. In conjunction with the UISC specialists, the analysis team will provide peer review for refinement of future spirals, create surveys in conjunction with the UISC specialists, determine data collection methodologies, and analysis planning.

7. ANALYSIS AND DATA COLLECTION

Selecting specific data elements to support measures, metrics, and indicators for these Technical Spirals will be directly related to the hierarchy in Section 5. Appendix B – Data Collection

Matrix will address all elements specifically for analysis in the Technical Spiral to include collection methodology.

7.1. Collection Methods

The Analysis Team will employ a variety of collection methods depending upon the spiral and the objectives of the given spiral. More than one measure or type of measure may be utilized to support a given essential element of analysis. This will enhance insights into the realities of the experiment activities.

7.1.1. Automated/Instrumented

Time stamps will be made when possible and appropriate so that timing can be accurately measured. Significant time stamps may not be possible in this type of experimentation event; however, every effort will be made to collect this type of data when it can be captured accurately.

7.1.2. Observations

Analysts and Subject Matter Experts (SMEs) will be listening and observing the spiral from distributed locations. Notes will be taken with regard to the actions of the experiment audience in relation to the spiral's objectives and solutions being examined. All analysts and SMEs will be given a copy of the use case and objectives for the spiral being examined prior to the date of the event in order to prepare. Discovery is always a potential outcome of any experiment activity.

7.1.3. Interviews

The Analysis Team will conduct interviews when appropriate. If conducted, it will most likely be via the telephone and conducted in order to clarify responses or actions taken during the spiral.

7.1.4. Surveys

Surveys are foreseen as very prominent for the spirals. Likert scale questions coupled with essay questions will be the most frequent question type for the spirals.

7.2. Analysis Methods

It is foreseen that data will consist of observation, subject matter expert opinion, interview data, and survey data. Most of this data will be qualitative. Some of the qualitative survey responses will be based upon a Likert scale and represented in a quantitative manner. Likert scale results will be compared with open-ended survey question in order to derive any trends or characteristics of the current capability and its potential use in a UISC.

As with any experiment, there may be discovery elements that surface during the spirals. These will be included for analysis and reporting.

7.3. Privacy and Protection of Human Subjects in Research

As a U.S. led event, the IMISAS Technical Spirals will comply with all applicable provisions of U.S. regulations and directives regarding the protection of human subjects in research experimentation and the safeguarding of experiment data. If individual partner nation rules and directives require additional provisions for their own events, participants or sites, they will be implemented on a case by case basis only for those instances. Presently this may include Germany.

7.4. Classification

The experiment will use unclassified information only (no simulated classified information will be utilized), some of which may reside on simulated classified networks. Care must be taken to ensure that information is given the appropriate protection and marking, to include Controlled Unclassified Information and 'For Official Use Only' or FOUO. This information must be protected by dissemination restrictions, and all persons receiving this information must protect it in accordance with those restrictions.

7.5. Analysis Team Training

The analysis team will consist of observers, analysts, and SMEs. All will be given specific duties and focus areas of observation and analysis. At a minimum, all members must understand the basic flow of the designed processes and procedures the experiment audience will be conducting in accordance with the appropriate policies. Data collection sheets will be provided, as required, as well as an explanation of what data should be collected and how to categorize the observations.

APAN will serve as the proxy UISC for all the Technical Spirals. All observers, analysts and SMEs must obtain a user account and gain familiarization with the proxy UISC prior to the first

spiral. Additionally, observers, analysts, and SMEs must gain familiarity with SharePoint, Face Book, Twitter, GeoCommons, and SwiftRiver.

Should interviews be required of the experiment audience, those required to collect data from these interviews will be given instruction on how to ask the questions and for key elements to facilitate asking more probing questions depending upon the response of the interviewee.

7.6. Hot-Washes

Upon completion of each spiral, the principals of the USJFCOM portion of the IMISAS team will conduct a meeting for initial viewing of the data collected in order to ascertain if enough data was collected, what data could not be collected, and what the team must do in subsequent spirals. Additionally, lessons discovered will be part of the discussion to facilitate readjustment of subsequent spirals.

These hot-washes are not sufficient alone as refinement will continue to take place between spirals.

7.7. Data Archive

During the experiment, data that is collected will require safe keeping ensuring that the data is not lost or misplaced and the PII is not compromised. Secure locations and back-up locations will be required.

7.7.1. Data Storage and Archiving Locations

- Participant survey data and interview data will be stored in Microsoft Office (MS) Office files and statistical analysis files (as appropriate) and posted to the IMISAS portal.
- Observer data will be stored in MS Office files and posted on the IMISAS portal.
- Comments and Recommendations from all sources will be stored in MS Office files and posted on the IMISAS portal.
- Automated data collection from APAN will be transferred to MS Office files.
- Data will be copied to Compact Discs to ensure an additional, non-web-based back-up exists.

8. REPORTING

Reports for each spiral will provide an audit trail of the Technical Spiral activities and execution results. By explaining activities that occurred before, during, and after the spirals, and by codifying the outcomes, findings, and recommendations from the project as a whole, they form

the foundation for understanding the results and serve as a baseline for future experiments or follow-on analyses.

8.1. Analysis Report

The Lead Analyst will lead the efforts of collating and analyzing the data in order to create an analysis report in accordance with the Analytic Framework. This report will provide input to the Analytic Wargame, Transition Conference and the IMISAS Final Report.

Each Technical Spiral will have its own unique set of survey(s) and data collection that will be included in Appendices C – G.

9. EXPERIMENT RISK/THREAT ASSESSMENT

Evaluation of the 21 threats to experimentation detailed in the Guide for Understanding and Implementing Defense Experimentation, commonly referenced as the GUIDEx, is covered as part of the End-to-End Experimentation Plan. The identified threats to experimentation, their assessed levels of risk and mitigation implementations will be reviewed and refined for each spiral. The current assessment is below:

Table 1 – Risk Evaluation Matrix

Challenge	Impact on this Event	Risk	Risk Mitigation Measures
Ability to use capability			
1. Capability not workable: Does the hardware and software work?	High	Green	APAN software is already a fielded capability and the Analytic Seminar involves no physical modifications to the hardware or software. The experiment may introduce new mature applications not previously integrated on the APAN network. The newly introduced applications will be tested individually and as a system before use in the experiment. USPACOM will provide 24 hour APAN administrative support during and off APAN help desk hours during the Analytic Seminar.
2. Player non-use:	High	Green	During the Technical Spirals, recommendations will be

Table 1 – Risk Evaluation Matrix			
Challenge	**Impact on this Event**	**Risk**	**Risk Mitigation Measures**
Do the players have the training and TTP to use the capability?			gathered for streamlining the procedures and approval process for APAN site instantiation. For the experiment audience, training will be conducted for the processes, procedures, and APAN enhancements they will utilize during the experiment. Additionally, support personnel will be trained on the processes, procedures, and APAN enhancements to fully enable them to support the experiment.
3. No potential effect in output: Is the output sensitive to capability use?	High	Yellow	"As Is" and "To Be" capabilities were captured in separate events. The Process Documentation Event documented the existing capabilities, processes, and procedures as well as barriers. Technical Spirals verify APAN (UIS) processes to be utilized during the Analytic Seminar.
4. Capability not exercised: Does the scenario and Master Scenario Event List (MSEL) call for capability use?	High	Yellow	MSEL construction is ongoing but is expected to be fully developed and robust for the Analytic Seminar. Challenges are expected in scripting vignettes stressing non-technical (particularly cultural) solutions as their effects are inherently more difficult to quantify and stimuli more difficult to craft. Controllers, solution developers, and analysts will be involved in developing the MSEL to ensure the appropriate objectives and data collection from the experiment can be collected. Technical Spirals will not have a fully developed MSEL, but will utilize scripted use cases to be developed.
Ability to Detect Results: Correctly detect a true effect			
5. Capability variability: Is systems (hardware and software) and use in like trials the same?	Low	Green	The "As Is" is documented from interview and research. The "To Be" will be performed in a laboratory environment with only a series of vignettes vice trials; thus this issue is of minimum consequence. Technical Spirals will be checking that APAN enhancements operate properly. APAN will be managed from its home server with someone who has been given administrative credentials.
6. Player variability: Do individual operators/units in like trials have similar	Medium	Green	The "As Is" is documented from interview and research. The "To Be" will be performed in a laboratory environment with only a series of vignettes vice trials; thus this issue is of minimum consequence. Training will be conducted on the experiment audience in the

Table 1 – Risk Evaluation Matrix			
Challenge	**Impact on this Event**	**Risk**	**Risk Mitigation Measures**
characteristics?			days immediately prior to experiment execution; thus, the individual operators will be the same.
7. Data collection variability: Is there large error variability in the data collection process?	High	Green	A large proportion of data is expected to be captured through observations, surveys and interviews and collated in a central location. The use of a standard survey tool, Survey Monkey is being used. All data collectors, observers, and analysts are involved in dry runs and hot washes.
8. Trial conditions variability: Are there uncontrolled changes in trial conditions for like trials?	Medium	Green	The "As Is" is documented from interview and research. The "To Be" will be performed in a laboratory environment with only a series of vignettes vice trials; thus this issue is of minimum consequence.
9. Low statistical power: Is the analysis sample sufficient?	Medium	Yellow	Sample sizes for both the Technical Spirals and Analytic Seminar is expected to be relatively small. The controlling influence is cost associated with travel and man-hours, availability of participants, and real-world operations demands. It is unlikely that sample size will be larger than 15; thus, nonparametric statistical analysis will be used if required. Observations of experiment play will be closely monitored by analysts, observers, data collectors, subject matter experts, and solution developers to ensure all appropriate data is collected for further analysis and to attain a significant amount of viewpoints from different backgrounds, which will enhance the final analysis.
Ability to Detect Results: Incorrectly detect an artificial effect			
10. Violation of statistical assumptions: Are correct analysis techniques used and the error rate avoided?	Medium	Yellow	Once sample size is known, an appropriate application of techniques will be employed. Reliance on non-parametric analysis will be done as applicable.; however, descriptive statistics are most likely.
Ability to Isolate Reason for Results: Single Group			
11. Capability changes over time: Are there system	Medium	Green	There are only a series of vignettes, not multiple trials. If procedures are changed, it will be the result of hot-wash meetings and by design. If the experiment audience does not

Table 1 – Risk Evaluation Matrix			
Challenge	**Impact on this Event**	**Risk**	**Risk Mitigation Measures**
(hardware or software) or process changes during the test?			follow trained methods, an experiment 'time-out' can be called if the deviation will affect experiment validity.
12. Player changes over time: Will the player unit change over time?	Medium	Green	There are only a series of vignettes, not multiple trials which will take place over a consecutive two-day period. If some of the participants do arrive to complete the required training, then this could expose a team at a variety of levels of maturity to the processes and procedures.
13. Data collection changes over time: Are there changes in instrumentation or manual data collection during the experiment?	Medium	Green	There are only a series of vignettes, not multiple trials; thus, this should be of minimal concern. The Technical Spirals are primarily demonstration thus this is not a major concern.
14. Trial condition changes over time: Are there changes in trial conditions (such as weather, light, start conditions, and threat) during the experiment?	Low	Green	No significant environmental condition changes are expected for the experiment. The most likely cause of a condition change will be service interruption with APAN, the internet, or experiment network.
Ability to Isolate Reason for Results: Multiple Groups			
15. Player differences: Are there differences between groups unrelated to the treatment?	Medium	Green	There will only be one group operating during the Technical Spirals and the Analytic Seminar; thus, there will not be differences between groups.
16. Data collection differences: Are there potential data collection differences between treatment	High	Green	There will only be one group operating during the Technical Spirals and the Analytic Seminar; thus, there will not be differences between groups.

Table 1 – Risk Evaluation Matrix			
Challenge	**Impact on this Event**	**Risk**	**Risk Mitigation Measures**
groups?			
17. Trial condition differences: Are the trial conditions similar for each treatment group?	Medium	Green	There will only be one group operating during the Technical Spirals and the Analytic Seminar; thus, there will not be differences between groups.
Ability to Relate Results to Operations			
18. Non-representative capability: Is the experimental surrogate functionally representative?	High	Yellow	The customer will be intimately involved in the architecture of the laboratory environment; however, the laboratory will not be the actual environment that the audience normally operates.
19. Non-representative players: Is the player unit similar to the intended operational unit?	High	Green	The experiment audience will be fielded by the customers' personnel who are experienced in the billets they will be playing in the Analytic Wargame. Control may not be filled by actual subject matter experts in all billets, but will have personnel familiar with the given role. Real-life operational requirements could force substitution of personnel to role play in the experiment audience, but will most likely be filled by personnel who are familiar with the billet.
20. Non-representative measures: Do the performance measures reflect the desired operational outcome?	High	Yellow	Measures are in their final states of solidification. They have been vetted with peer review and customer input.
21. Non-representative scenario: Are the Blue, Green, and Red conditions realistic?	High	Yellow	There has been a significant effort to recruit participation of personnel with functional expertise in military and non-military disciplines and areas. The cooperation of actual IOs/NGOs, IA, and foreign governments will help to bring consistency, fidelity and authenticity to vignettes and scenario. Participants that are real world responders to HA/DR scenarios and will provide expert knowledge to their representative group.

APPENDIX A: ACRONYMS

APAN	All Partners Access Network
COI	community of interest
DCAP	Data Collection and Analysis Plan
DOD	Department of Defense
EEA	essential element of analysis
FOUO	For Official Use Only
HA/DR	humanitarian assistance / disaster relief
IMISAS	Interagency Multinational Information Sharing Architecture and Solutions
IA	inter-government organization
IO	international organization
JCD&E	Joint Concept Development and Experimentation
MS®	Microsoft®
MSEL	Master Scenario Event List
NGO	non-government organization
PII	personally identifiable information
SME	subject matter expert
UDOP	user defined operational picture
UIS	unclassified information sharing
UISC	unclassified information sharing capability
USJFCOM	United States Joint Forces Command
USPACOM	United States Pacific Command

APPENDIX B: DATA COLLECTION MATRIX

NOTE: The Data Collection Matrix is a living document in a separate Excel spread sheet.

APPENDIX C: Technical Spiral One, Data Collection Plan

Technical Spiral One focuses on UISC Registration, UISC Graduated user permissions, and UISC Data Standards. The latter focus area is not developed in sufficient detail to inform metrics; however, it will be developed to greater detail in subsequent technical spirals. The use case for Technical Spiral One guides the user through the processes of creating an APAN account, joining APAN groups, and employing the portal's colleague feature, chat capability, and document posting utility.

The following EEAs are addressed either in full or in part in Technical Spiral One.

- EEA 2.3.2.A: Does a set of business rules to standardize labeling of data types, metadata, and tagging facilitate the ability to share pertinent information? (solution 3-1)
- EEA 2.3.2.B: Does a set of business rules for allowing mission partners to utilize a UISC facilitate expeditious, useful, and accurate information sharing? (solution 3-1)
- EEA 2.3.2.C: Do graduated user account permission facilitate UIS? (solution 4-6)
- EEA 2.3.2.D: Does rapid user registration to a UISC facilitate COI response utilizing the UISC? (solution 4-7)
- EEA 2.4.2.A: What are the processes and procedures to granting user account permissions? (solution 4-6)
- EEA 2.4.2.B: What are the processes and procedures to granting rapid user registration? (solution 4-7)

The following survey questions, evaluated on the 1-5 Likert Scale, will directly inform the EEAs listed above.

- The user account registration process you used today asked appropriate questions. (EEA 2.4.2.B)
- The user account registration process you used today required too much detail. (EEA 2.4.2.B)
- It was easy join the IMISAS Experimental Site I was looking for. (EEA 2.3.2.A)
- It was easy to post the document to APAN. (EEA 2.3.2.B)
- It was easy to chat with other APAN users. (EEA 2.3.2.B)
- The APAN chat features were intuitive. (EEA 2.3.2.B)

The following open-format survey questions are expected to provide additional details mapping to the metrics for the above EEAs:

- What is your general impression of APAN? (all EEAs)
- Based upon your experience today, what APAN features did you like? (all EEAs)
- Based upon your experience today, please describe any recommended changes you would make to the APAN user interface. (all EEAs)

The following demographic survey questions will be used as necessary to weight or exclude responses based on skew.

- Participant's name, organization, job title, and location
- Participants stated interest in information sharing
- Participants years of experience in HA/DR
- Participant's background in HA/DR
- Participant's experience using APAN

A more detailed mapping of survey questions to elements of Section 5 of this DCAP, STUDY ISSUES, ESSENTIAL ELEMENTS OF ANALYSIS, AND MEASURES, is contained in a separate Excel spread sheet.

APPENDIX D: Technical Spiral Two, Data Collection Plan

Technical Spiral Two focuses on UISC Source Reliability and Rating and UISC Data Standards. The use case for Technical Spiral Two guides the user through the processes of navigating blogs, commenting upon blogs, submitting and contributing to RFIs, and rating the reliability of the previous elements listed. Additionally the use of tagging of documents will be accomplished.

The following EEAs are addressed either in full or in part in Technical Spiral Two.

- EEA 1.1.3A: What information rating criteria will be useful to attaining a reasonable level of confidence in the information's authenticity and accuracy? (solution 4-10)
- EEA 2.3.2.A: Does a set of business rules to standardize labeling of data types, metadata, and tagging facilitate the ability to share pertinent information? (solution 3-1)

The following survey questions, evaluated on the 1-5 Likert Scale, will directly inform the EEAs listed above.

- I found it easy to submit a RFI (Request for Information). (EEA 1.1.3A)
- I found it easy to post responses to RFIs. (EEA 1.1.3A)
- I found the 'star' rating easy to use. (EEA 1.1.3A)
- How trusting are you of star ratings? (EEA 1.1.3A)
- The verification of an answer to a RFI/Question is a useful capability in unclassified information sharing. (EEA 1.1.3A)
- The following information would be useful in assisting me to determine the level of reliability of information. (EEA 1.1.3A)
    - Star rating provided by other APAN site member users
    - Knowing that all posters of information have been approved by the site owner. (No anonymous posts)
    - Poster's background
    - Poster's Colleagues
    - Sites to which the poster belongs
    - Poster's Favorites
    - Poster's organization
    - Poster's email
    - Poster's activities
    - Green bar rating indicating relative number of posts

- It was easy to add a comment to the Situation Report blog. (EEA 1.1.3A)
- It was easy to tag a post. (EEA 2.3.2.A)
- The list of tags was complete and adequate for an HA/DR operation. (EEA 2.3.2.A)
-

The following open-format survey questions are expected to provide additional details mapping to the metrics for the above EEAs:

- What other generic tags would be useful to help locate data easier? (EEA 2.3.2.A)
- What confidence ranking criteria that was not listed in question 11 would you personally find useful to gaining an appropriate confidence level in a posting (information/document)? (EEA 1.1.3A)
- Based upon your experience today, what APAN features would you find most useful in future information sharing activities with non-DOD partners (U.S. Government Agencies, foreign government agencies – both civilian and military, IOs, NGOs, host nation, etc.)? Please include the organization or type of organization and how the feature would be useful. (all EEAs)
- Based upon your experience today, please describe any recommended changes you would make to the APAN user interface. (If no recommendations, please type "none" in the comment box.) (all EEAs)
- Please provide any other comments you wish to make concerning your experience in this technical spiral. (If you have no additional comments, please put "none" in the comment box.) (all EEAs)
-

The following demographic survey questions will be used as necessary to weight responses as needed.

- Participant's name, organization, and location,
- Participants stated interest in information sharing,
- Participants years of experience in HA/DR,
- Participant's experience using APAN.

A more detailed mapping of survey questions to elements of Section 5 of this DCAP, STUDY ISSUES, ESSENTIAL ELEMENTS OF ANALYSIS, AND MEASURES, is contained in a separate Excel spread sheet.

APPENDIX E: Technical Spiral Three, Data Collection Plan

Technical Spiral Three focuses on utilization of the group chat function, document collaboration, and use of RSS feeds from within APAN and via external link. The use case for Technical Spiral Three guides the user through the processes of collaborative work, group chat, and observing incoming RSS feeds as well as pushing information via RSS feeds.

The following EEAs are addressed either in full or in part in Technical Spiral Three.

- EEA 1.1.1.C: What capabilities hosted on information exchange hubs could serve as a basis for work site templates in support of an HA/DR event? (solution 3-1)

- EEA 2.2.2.D: What challenges, limitations, and risks exist in effecting information sharing from controlled environments to lesser controlled domains (social media sites)? (solution 4-8)

- EEA 2.2.2.E: What challenges, limitations, and risks exist in effecting information sharing from lesser controlled domains (social media sites) to controlled environments? (solution 4-8)

The following survey questions, evaluated on the 1-5 Likert Scale, will directly inform the EEAs listed above.

- Group Chat was easy to use. (EEA 1.1.1.C)
- Group Chat would be useful in a crisis response operation. (EEA 1.1.1.C)
- Access to the information received via the RSS from a social media source such as "Facebook" would be useful when working in a crisis response operation. (EEA 2.2.2.E)
- The document collaboration capability was easy to use. (EEA 1.1.1.C)
- The document collaboration capability that I used today would be useful in a crisis response operation. (EEA 1.1.1.C)
- Transferring information from the APAN portal; via a situation report blog post, to the social media site "Facebook" was easy. (EEA 2.2.2.D)
- Tagging collaboration document was easy. (EEA 1.1.1.C)

The following open-format survey questions are expected to provide additional details mapping to the metrics for the above EEAs:

- Based upon your experience today, what would you change about the group chat feature? (If nothing, please put 'nothing' in the comment box.) (EEA 1.1.1.C)
- Based upon your experience today, how would you suggest changing the process by which you transferred information from APAN to social media sites ("Facebook")? (If nothing, please put 'nothing' in the comment box.) (EEA 2.2.2.D)
- What types of information/files would you envision posting to social media sites when working in a crisis response operation? (If nothing, please put 'nothing' in the comment box.) (EEA 2.2.2.D)
- What types of information/files would you find useful to receive from social media sites when working in a crisis response operation? (If nothing, please put 'nothing' in the comment box.) (EEA 2.2.2.E)
- What other social media or dynamic internet site would be useful to link to UISC in a crisis response operation. Please explain Why? (If nothing, please put 'nothing' in the comment box.) (EEA 2.2.2.E)
- Based upon your experience today, how would you improve or change the business rules for collaboration on a document/product? (If nothing, please put 'nothing' in the comment box.) (EEA 1.1.1.C)
- What is your general impression of APAN? (If you participated in the Technical Spirals, please indicate if you have experienced a change in your impression from the previous survey.) (If nothing, please put 'nothing' in the comment box.) (EEA 1.1.1.C)
- Please provide any other comments you wish to make concerning your experience in this technical spiral. (If you have no additional comments, please put "none" in the comment box.) (all EEAs)

The following demographic survey questions will be used as necessary to weight responses as needed. Only those who have not previously participated in technical spiral surveys will be asked to complete these demographic survey questions.

- Participant's name, organization, and location,
- Participants stated interest in information sharing,
- Participants years of experience in HA/DR,
- Participant's experience using APAN.

A more detailed mapping of survey questions to elements of Section 5 of this DCAP, STUDY ISSUES, ESSENTIAL ELEMENTS OF ANALYSIS, AND MEASURES, is contained in a separate Excel spread sheet.

APPENDIX F: Technical Spiral Four, Data Collection Plan

Technical Spiral Four focuses on usage of a User Defined Operational Picture (UDOP) and verification of internet based data channels. The use case for Technical Spiral Four guides the user through the processes of using a UDOP and the verification tool, SwiftRiver.

The following EEAs are addressed either in full or in part in Technical Spiral Four.

- EEA 1.1.3.B: What information verification tools will be useful to attaining a reasonable level of confidence in the information's authenticity and accuracy? (solution 4-11)
- EEA 1.1.4.A: How can a UDOP assist with sharing of information amongst mission partners? (solution 3-1)
- EEA 2.3.2.F: What processes and business rules are appropriate when using an information verification tool for information sharing with mission partners? (solution 4-11)
- EEA 2.3.2.G: What processes and business rules are appropriate when using a UDOP for information sharing with mission partners? (solution 3-1)

The following survey questions, evaluated on the 1-5 Likert Scale, will directly inform the EEAs listed above.

- Map View in APAN was easy to use. (EEAs 1.1.4.A and 2.3.2.G)
- Map View in APAN provided a capability that would be useful in crisis response operations. (EEA 1.1.4.A)
- Crowdmapping provides a capability to view data that would be useful in a crisis response operation. (EEA 1.1.3.B)
- It was easy to report information in Crowdmap. (EEAs 1.1.3.B and 2.3.2.F)
- Creating a map in GeoCommons was easy. (EEAs 1.1.4.A and 2.3.2.G)
- Uploading a layer of information to the GeoCommons map was easy. (EEA 2.3.2.G)
- GeoCommons provided a capability to upload information that would be useful in crisis response operations. (EEA 1.1.4.A)

The following open-format survey questions are expected to provide additional details mapping to the metrics for the above EEAs:

- What layers (overlays in the Map View in APAN) used in this spiral would be most useful in a crisis response operation? (If none, please put 'NONE' in the text box.) (EEA 1.1.4.A)
- What other layers would you need to support a crisis response operation? (EEA 1.1.4.A)

- What layers (overlays in the Map View in APAN) used in this spiral would be least useful in a crisis response operation? (If none, please put 'NONE' in the text box.) (EEA 1.1.4.A)
- What were the most useful features of the Map View in APAN? How would you use them? (If none, please put 'NONE' in the text box.) (EEA 1.1.4.A)
- What were the most difficult and non-useful features of the Map View in APAN? (EEAs 1.1.4.A and 2.3.2.G)
- What is your impression of Crowdmap and how would it be useful in a crisis response operation? (EEAs 1.1.3.B and 2.3.2.F)
- Based upon your usage of Crowdmap today are there any aspects that could be counterproductive in a crisis response operation? (EEAs 1.1.3.B and 2.3.2.F)
- What is your general impression of GeoCommons? (EEAs 1.1.4.A and 2.3.2.G)
- What is your general impression of APAN? (If you participated in previous Technical Spirals, please indicate if you have experienced a change in your impression from the previous surveys.) (all EEAs)
- Please provide any other comments you wish to make concerning your experience in this technical spiral. (If you have no additional comments, please put "none" in the comment box.) (all EEAs)

The following demographic survey questions will be used as necessary to weight responses as needed. Only those who have not previously participated in technical spiral surveys will be asked to complete these demographic survey questions.

- Participant's name, organization, and location,
- Participants stated interest in information sharing,
- Participants years of experience in HA/DR,
- Participant's experience using APAN.

A more detailed mapping of survey questions to elements of Section 5 of this DCAP, STUDY ISSUES, ESSENTIAL ELEMENTS OF ANALYSIS, AND MEASURES, is contained in a separate Excel spread sheet.

APPENDIX G: Technical Spiral Five, Data Collection Plan

Technical Spiral Five focuses on usage of search functions within and external to a UISC for stored information that has a tagging storage conventions and storage sites that do not use tagging (searching for key words and phrases within a document) . The use case for Technical Spiral Five guides the user through the processes of searching information using tagging conventions and key words or phrases.

The following EEAs are addressed either in full or in part in Technical Spiral Five.

- EEA 1.1.2.A: What tags would be useful to information searching on a UISC? (solutions 3-1 and 4-12)
- EEA 1.1.2.C: What are the best practices when sharing information with low bandwidth devices and only low bandwidth availability? (solution 4-1)
- EEA 2.3.2.A: Does a set of business rules to standardize labeling of data types, metadata, and tagging facilitate the ability to share pertinent information? (solution 3-1)

The following survey questions, evaluated on the 1-5 Likert Scale, one one-choice question, and one multiple-choice question will directly inform the EEAs listed above.

- What device did you use for today's spiral? (EEA 1.1.2.C)
- It was easy to access the information from RFI using APAN Lite. (EEA 1.1.2.C)
- It was easy to post the image to APAN Lite. (EEA 1.1.2.C)
- The response time with the APAN Lite site was adequate. (EEA 1.1.2.C)
- The APAN Lite site I used today has adequate functionality for use in crisis response operations. (EEA 1.1.2.C)
- I would be comfortable using this information from the APAN Lite capability in a crisis response operation. (EEA 1.1.2.C)
- The search capability in APAN was easy to use. (EEA 1.1.2.C)
- What tags on documents and other information would you find most useful in crisis response operations? (EEA 1.1.2.A)

The following open-format survey questions are expected to provide additional details mapping to the metrics for the above EEAs:

- What functionality would you add or delete from the APAN Lite current capability? (EEA 1.1.2.C)
- Please describe what would add to your comfort level in using this information from the APAN Lite capability in a crisis response operation. (EEA 1.1.2.C)

- What types of information would you feel comfortable sharing using a low bandwidth device? (EEA 1.1.2.C)
- What types of information would you NOT feel comfortable sharing using a low bandwidth device? (EEA 1.1.2.C)
- List any other tags on documents and other information that were not listed above and you feel would be useful in crisis response operations? (EEA 1.1.2.A)
- What is your general impression of APAN? (If you participated in previous Technical Spirals, please indicate if you have experienced a change in your impression from the previous surveys.) (all EEAs)
- Please provide any other comments you wish to make concerning your experience in this technical spiral. (If you have no additional comments, please put "none" in the comment box.) (all EEAs)

The following demographic survey questions will be used as necessary to weight responses as needed. Only those who have not previously participated in technical spiral surveys will be asked to complete these demographic survey questions.

- Participant's name, organization, and location,
- Participants stated interest in information sharing,
- Participants years of experience in HA/DR,
- Participant's experience using APAN.

A more detailed mapping of survey questions to elements of Section 5 of this DCAP, STUDY ISSUES, ESSENTIAL ELEMENTS OF ANALYSIS, AND MEASURES, is contained in a separate Excel spread sheet.

United States Joint Staff
Joint and Coalition Warfighting (JCW)

United States Joint Staff

Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions Project

(IMISAS)

Annex I - Data Collection and Analysis Plan (DCAP) – Analytic Seminar (AS)

TABLE OF CONTENTS

1. INTRODUCTION I-1
2. PROBLEM STATEMENT AND END STATE I-1
3. PROPOSITIONS/HYPOTHESES I-1
4. OUTCOMES AND OBJECTIVES I-1
5. STUDY ISSUES, ESSENTIAL ELEMENTS OF ANALYSIS, AND MEASURES I-2
6. PROPOSED ACTIVITY I-10
6.1. Analytic Wargame/Seminar I-10
6.2. Scenario and Experiment Design I-10
6.3. Control I-11
7. ANALYSIS AND DATA COLLECTION I-12
7.1. Collection Methods I-14
7.1.1. Automated/Instrumented Collection I-14
7.1.2. Observations I-15
7.1.3. Interviews I-15
7.1.4. Surveys I-15
7.2. Privacy and Protection of Human Subjects in Research I-16
7.3. Classification I-16
7.4. Analysis Team Training I-16
7.5. Analysis Hot-Washes I-17
7.6. Data Archive I-17
7.6.1. Data Storage and Archiving Locations I-18
8. REPORTING I-18
8.1. Analysis Report I-18
9. EXPERIMENT RISK/THREAT ASSESSMENT I-18
APPENDIX 1: ACRONYMS I-24
APPENDIX 2: DATA COLLECTION MATRIX I-1

1. INTRODUCTION

The Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Analytic Seminar (AS) Data Collection and Analysis Plan (DCAP) provides the specific details for data collection and analysis activities for the AS. It addresses specific data collection areas, methodology for data generation, collection, analysis, and archiving in support of the AS. Additionally it demonstrates analytic traceability from measures through Essential Elements of Analysis (EEAs), experimental hypothesis, and study questions back to the high level project objectives. Appendix 1 contains a full list of acronyms used in this document.

2. PROBLEM STATEMENT AND END STATE

See the IMISAS End-to-End Experiment Plan, Analytic Framework Annex.

3. PROPOSITIONS/HYPOTHESES

See the IMISAS End-to-End Experiment Plan, Analytic Framework Annex.

4. OUTCOMES AND OBJECTIVES

Note: Only those outcomes and objectives being investigated during the AWG are listed below. For a full view of all experiment Objectives, see the IMISAS End-to-End Experiment Plan, Analytic Framework Annex.

- **Outcome 1**: Inform the development of the 'To Be' unclassified information sharing capability (UISC) employing technical spirals and an AS focused on using/integrating available portal and cross domain technologies.
    - **Objective 1.1**: Identify requirements and potential operational solutions and technical enhancements using All Partners Access Network (APAN) as the technical backbone for experimentation.
- **Outcome 2:** Improved processes, procedures and enabling policies to establish an information sharing collaborative networked environment that can work across organizational and security boundaries for mission partners.
    - **Objective 2.2:** Develop and verify operationally focused processes and procedures required to implement information sharing and collaboration for humanitarian assistance/disaster relief HA/DR operations.

- **Objective 2.3:** Examine policy and recommend changes to facilitate information sharing with a range of partners in an HA/DR environment.

5. STUDY ISSUES, ESSENTIAL ELEMENTS OF ANALYSIS, AND MEASURES

The following is the decomposition from outcomes to objectives to study issues to essential element of analysis (EEAs) to measures. The Data Collection Matrix in Appendix 2 also includes the collection methodology and the data elements that will be used to attain the data necessary to meet the measures.

> **Note:** Some of the Objectives, Study Issues, EEAs, and Measures have been refined, combined, augmented, or removed as solutions have matured; in these cases, the respective elements may not match those in the Analytic Framework, which was intended to provide the structure and initial template for analytic traceability.

Outcome 1: Inform the development of the 'To Be' UISC employing an AS focused on using/integrating available portal and cross domain technologies.

Objectives 1.1: Identify requirements and potential operational solutions and technical enhancements using unclassified information sharing (UIS) network APAN as the technical backbone for experimentation.

- **Study Issue – 1.1.1** – What existing information exchange systems could be used operationally by the Department of Defence (DOD) during an HA/DR event?
  - **Proposition/Hypothesis:** Existing information exchange systems could be used by DOD.
  - **EEA 1.1.1.A:** Are certain operational federations of existing information exchange hubs significantly more effective than others across the span of responders to an HA/DR event? (solution 1-7)
    - Measures:
      - Degree of understanding of partners' preferred collaboration methods and tools
      - Flexibility of response to changes in collaboration tools and modes
      - Degree of accommodation of partners' preferred collaboration capabilities

- **EEA 1.1.1.B:** Deleted. This material was subsumed into EEA 1.1.1. C.

- **EEA 1.1.1.C:** What capabilities and business rules implemented on information exchange hubs could serve as a basis for work site templates in support of an HA/DR event? (solution 1-1b, 1-3a, 1-3b, 4-12)

  - Measures:
    - Ease of use of collaborative work site capabilities (1-3a)
    - Degree of accessibility of the collaborative work site (1-3a)
    - Degree of utility of collaboration tool sets to HA/DR operations (1-3a)
    - Comprehensiveness of collaboration tool sets in support of HA/DR operations (1-3a)
    - Degree of intuitiveness of user interface (1-3a)
    - Speed of information retrieval (4-12)
    - Speed of information staging (1-1b)
    - Effectiveness of content management rules (1-3b)
    - Sufficiency of storage capacity provided by UISC (1-1b)
    - Sufficiency of file types accommodated by UISC (1-1b)
    - Degree of protection of private data afforded by UISC (1-1b)

- **Study Issue – 1.1.2 –** Are there standards or guidelines for storage and search capability of documents and other data that could prove useful to practical data storage, searchability, and utility?

  - **Proposition/Hypothesis:** Standard usage of tags, metadata, and types of data will make data storage more useful.

  - **EEA 1.1.2A:** What tags would be useful to information searching on a UISC? (solution 3-1)

    - Measures:
      - Degree of utility of tags to crisis response operations
      - Degree of comprehensiveness of tags as they relate to HA/DR crisis response

  - **EEA 1.1.2B:** Deleted. The intent of this EEA was met by other EEAs dealing with data tagging.

- **EEA 1.1.2.C:** What are the best practices when sharing information with low bandwidth devices and only low bandwidth availability? (solution 4-1)

  - Measures:
    - Degree of ease of access to information
    - Degree of ease in posting information
    - Response Time
    - Low bandwidth device used
    - Degree of functionality of capability
    - Comfort level with lack of verification criteria

- **Study Issue – 1.1.3 –** How can those involved in information sharing be confident that the information being received is accurate and authentic?

  - **Proposition/Hypothesis:** Rating verification tools and criteria will assist the information user in determining validity of information.

  - **EEA 1.1.3.A:** What information rating criteria will be useful to attaining a reasonable level of confidence in the information's authenticity and accuracy? (solution 4-10)

    - Measures:
      - Completeness of criteria
      - Effectiveness of criteria

  - **EEA 1.1.3.B:** (Deleted. This EEA addressed the question of what information verification tools would be useful in attaining a reasonable level of confidence in information's authenticity and accuracy. There will be no attempt to explore the span of such tools during the AS. The focus will rather be on functional aspects of the particular tools in APAN that provide this capability).

- **Study Issue – 1.1.4 –** How can the use of a User Defined Operational Picture (UDOP) assist with information sharing amongst mission partners?

  - **Proposition/Hypothesis:** A UDOP will assist DOD with information sharing amongst mission partners.

- **EEA 1.1.4.A:** How can a UDOP assist with sharing of information amongst mission partners? (solution 1-3a)

  - Measures:
    - Enumeration of types of information that can be shared via a UDOP
    - Degree of usefulness of the information shared from or via a UDOP
    - Limitations of the UDOP
    - Degree of ease with the UDOP interface is manipulated

Outcome 2: Improved processes, procedures and enabling policies to establish an information sharing, collaborative, networked environment across organizational and security boundaries for mission partners.

Objective 2.2: Develop and verify operationally focused processes and procedures required to implement information sharing and collaboration for HA/DR operations.

- **Study Issue – 2.2.1 –** What is the degree of policy misalignment among represented organizations, and to what degree are those differences reconcilable?

  - **Proposition/Hypothesis:** Reconciling information sharing policies among organizations allows an improved level of information flow.

  - **EEA 2.2.1.A:** What is the quality of service and adaptability of the combatant command's (COCOM's) framework supporting unclassified information sharing with mission partners via UISC? (solution 1-5)

    - Measures:
      - Level of knowledge of what unclassified information we need to share.
      - Level of knowledge of why we need to share unclassified information.
      - Level of knowledge of how best to share unclassified information.
      - Level of knowledge of whom we need to share information with.

  - **EEA 2.2.1.B:** Deleted. This material was duplicative of EEA 1.1.1.A.

- **Study Issue – 2.2.2 –** Is the risk inherent in sharing of information acceptable? What is the true necessity of operating on restricted access networks when engaged in operations in an HA/DR environment?

- **Proposition/Hypothesis:** The gains from moving unclassified information from controlled environments to lesser controlled environments for the purpose of increased information sharing outweigh the risks.

- **EEA 2.2.2.A:** Deleted. Subsumed into EEA 2.2.2.D and EEA 2.2.2.E.

- **EEA 2.2.2.B:** Deleted. Subsumed into EEA 2.2.2.D and EEA 2.2.2.E.

- **EEA 2.2.2.C:** Deleted. Subsumed into EEA 2.2.2.D and EEA 2.2.2.E.

- **EEA 2.2.2.D:** What challenges, limitations, and risks exist in effecting information sharing from selected access unclassified information environments to social media environments? (solution 4-8)

  - Measures:
    - Acceptability of risk relative to benefit
    - Acceptability of cost relative to benefit
    - Identification of potential adverse consequences
    - Degree of effectiveness of demonstrated process for pushing information to social media channels

- **EEA 2.2.2.E:** What challenges, limitations, and risks exist in effecting information sharing from social media sites to selected access unclassified information environments? (solution 4-9)

  - Measures:
    - Acceptability of risk relative to benefit
    - Degree of potential for information overload
    - Identification of other potential adverse consequences
    - Degree of effectiveness of demonstrated process for composing information from social media channels

- **Study Issue – 2.2.3 –** To what degree could a quick reference guide detailing the capabilities of non-DOD organizations, descriptions of roles and responsibilities in an HA/DR environment, and general information requirements be beneficial to information sharing in an HA/DR environment?

- **Proposition/Hypothesis:** A quick reference guide expedites and improves the information capabilities of a DOD organization.

- **EEA 2.2.3.A:** What are the primary roles and responsibilities during an HA/DR operation? (solution 1-8)

  - Measures:
    - Accuracy of role and responsibility descriptions
    - Sufficiency of detail in role and responsibility descriptions
    - Completeness of coverage in role and responsibility descriptions
    - Recommended changes to role and responsibility descriptions

- **EEA 2.2.3.B:** What mission partner capabilities and limitations that are valuable to know during an HA/DR operation? (solution 1-8)

  - Measures:
    - Accuracy of mission partner capability descriptions
    - Sufficiency of detail in partner capability descriptions
    - Completeness of coverage in partner capability descriptions
    - Accuracy of mission partner limitations, including charter restrictions
    - Sufficiency of mission partner limitations, including charter restrictions
    - Completeness of coverage in mission partner limitations, including charter restrictions
    - Recommended changes to mission partner capability and limitation descriptions

- **EEA 2.2.3.C:** To what degree does maintenance of an Information Exchange Matrix (IER) facilitate unclassified information sharing? (solution 1-8)

  - Measures:
    - Extent to which IER matrix is referenced in establishing collaboration venues
    - Frequency with which IER matrix is updated in response to dynamic changes in collaboration capabilities across partner base
    - Frequency with which IER matrix is updated in response to partner preferences for collaboration venues

Objective 2.3: Examine policies, processes, and procedures, and recommend changes to facilitate information sharing with a range of partners in a HA/DR environment.

- **Study Issue – 2.3.1 –** What current policies, processes and procedures are hindering information sharing and how can they be eliminated, changed, or improved to facilitate information sharing?

    - **Proposition/Hypothesis:** The gains from sharing unclassified information with partners outweighs the risks.

    - **EEA 2.3.1.A:** Does the exercise of a risk managed approach to the handling and release of potentially sensitive unclassified information positively impact information sharing? (solution 1-1a)

        - Measures:
            - Likelihood and impact of unintended or premature release of unclassified information to an unrestricted access space
            - Degree of incidence of unintended or premature release of unclassified information to an unrestricted access space
            - Degree of completeness of information transfer
            - Degree of delegation in determining releasability to unrestricted access space
            - Timeliness of information provision to unrestricted access space
            - Clarity and simplicity of the procedure
            - Suggested changes to the procedure

    - **EEA 2.3.1.B**: Deleted. This material was subsumed into EEA 2.3.1.A.

    - **EEA 2.3.1.C**: What challenges, limitations, and risks exist in transferring unclassified information from classified to unclassified networks? (solution 1-2)

        - Measures:
            - Degree of work required relative to that required for decentralized transfers
            - Degree to which process accelerates information flow to unrestricted unclassified access spaces
            - User confidence in the transfer process
            - Suggested changes to the procedure

- **Study Issue – 2.3.2 –** What policies, processes, and procedures can be implemented in order to facilitate expeditious and accurate information sharing with mission partners via the use of a UISC?

  - **Proposition/Hypothesis:** User friendly and partner accommodating practices can facilitate information sharing with partners.

  - **EEA 2.3.2.A:** Does a set of capabilities and business rules to standardize labeling of data types, metadata, and tagging facilitate the ability to share pertinent information? (solutions 1-3a, 3-1, 4-12)

    - Measures:
      - Degree of usefulness of search results (3-1)
      - Degree of difficulty in implementing business rules for tagging (3-1)
      - Ease of use of search utility (4-12)
      - Ease of use of data tagging utility (1-3a)

  - **EEA 2.3.2.B:** Deleted. The intent of this EEA is captured among EEAs 1.1.1.C, 2.2.3.B, and 2.2.3.C.

  - **EEA 2.3.2.C:** Deleted. This capability (Graduated user account permissions, solution 4-6) will not be demonstrated during the Analytic Seminar.

  - **EEA 2.3.2.D:** Deleted. This capability (Rapid user registration, solution 4-7) will not be demonstrated during the Analytic Seminar.

  - **EEA 2.3.2.E:** Deleted. The intent of this EEA is captured by EEA 1.1.1.A.

  - **EEA 2.3.2.F:** Deleted. This capability (information verification tool, solution 4-11) will not be demonstrated during the Analytic Seminar.

  - **EEA 2.3.2.G:** What processes and business rules are appropriate when using a UDOP for information sharing with mission partners? (solution 1-3b)
    - Measures:
      - Effectiveness of processes facilitating information transfer via UDOP
      - Effectiveness of business rules facilitating information transfer via UDOP

Objective 2.4: Conduct user validation of potential UISC to provide enhancement recommendations for current UISC. The capabilities associated with this objective (rapid user registration [solution 4-7] and user account permissions [4-6]) will not be demonstrated during the Analytic Seminar.

6. PROPOSED ACTIVITY

6.1. Analytic Wargame

The IMISAS project AS event is slated for 01-04 August. This timeframe will be preceded by preparatory activities to include network set-up and test, ROC drills, experiment rehearsal, analyst and observer training, and experiment audience training. The significant details for this event will be published in a separate document, the IMISAS Analytic Wargame (AS) Event Directive.

6.2. Scenario and Experiment Design

The scenario for the AS provides a backdrop to assist the experiment audience in simulated environment reacting to a potential real-world situation. While the scenario encompasses military planning in response to a HA/DR contingency, the focus of experimental stimulation and data collection is the collection of issues affecting unclassified information sharing; specifically those foot-printed by the IMISAS handbook solutions. The scenario provides temporal and situational context to the collected data, and a framework from which to stress the solution set sufficiently and in a manner that avoids confounding of variables. The scenario for the AS is fictional and all documentation or references to the AS scenario will be labeled as 'For Experiment Use Only.'

Figure 1 shows the planned sequencing of the solutions relative to the experiment scenario, and the periods identified for administering surveys associated with the given solutions. This information is also contained in the Data Collection Matrix (DCM), an Excel spreadsheet maintained as Appendix 2 to this annex. Exercise of solutions is separated temporally according to their best placement in terms of supporting scenario activity. Some solutions subject to this overriding concern are also distributed so as to avoid overburdening the experiment audience with surveys for a given exercise period, with one 30-minute survey period following each of the four 3.5 hour survey periods. The exercise of multiple solutions concurrently was unavoidable due to the multiplicity of solutions and the limited time for experimentation, however, the individual solution elements are sufficiently discrete to support survey questions that will avoid confounding. Solutions 1-1a through 1-8 are considered procedural solutions, and their mapping to the scenario has temporal significance. The non-technical solutions (4-1, 4-6, 4-8, 4-9, 4-10, and 4-12) are expected to be stimulated equally throughout all periods of the experiment, and

surveys for those solutions will be conducted during the final survey period. Detailed mapping of solutions to specific Master Sequence Event List (MSEL) injects is contained in the MSEL Matrix.

		Tuesday, 02 Aug		Wednesday, 03 Aug	
Solution	Solution Description	Mission Analysis	COA Development	Branch Planning Lake Kivu	Branch Planning PIID
1-1a	Process and procedures for the expedited release of controlled unclassified information in a crisis response situation: Pre-planned release matrix.				X
1-1b	Process and procedures for the expedited release of controlled unclassified information in a crisis response situation: Storage and business rules for storage of information on UISC.	X			
1-2	Business rules governing the expedited transfer of unclassified information from classified networks to non-classified networks: Business rules for manual cross domain transfer.	X			
1-3a	Pre-defined template and business rules for the establishment of UISC work sites: UISC work site template.			X	
1-3b	Pre-defined template and business rules for the establishment of UISC work sites: Business rules to support UISC work site.			X	
1-5	Guide to enable unclassified information sharing with mission partners via UISC.		X		
1-7	Guides for staff use of UISC in support of operations: Best practices to maximize use of UISC.			X	X
1-8	Quick reference guides for the roles, responsibilities and general information requirements of potential non-DOD mission partners:		X		
3-1	Business Rules to define data types, standards, metadata requirements that facilitate posting, transfer and use of data .			X	
4-1	UISC to make automatic bandwidth recommendations in a restricted communications environment (Demonstrated by APAN Lite).				X
4-8	UIS capability to push or post aggregated data from dynamic sources to mission partners.				X
4-9	UIS capability to capture, sort categorize, filter information in the public domain.				X
4-10	Business rules to maximize current automatic trust center capability including: rating, recommendations, and level of confidence (Demonstrated by APAN Star Rating System).				X
4-12	UIS search capabilities (Federated or integrated).				X

= Solution in play

X = Survey administered at end of period

Figure 1. Sequencing of solution elements with respect to exercise scenario.

6.3. Control

The Chief Controller is responsible for ensuring the event is conducted in accordance with the experiment design and in a fashion attaining event objectives and study issues. The Chief Controller works closely with the Director of Experiment Design, with the Lead Analyst, and with the Solution Development Leads to ensure an environment where the concepts are examined is as realistic as possible and meets the experiment requirements.

Specific details concerning the Control Plan will be developed by the Director of Experiment Design and documented in separately. Additionally, the Chief Controller is responsible for creation of the Experiment Manning Document. The Lead Analyst supports these efforts to ensure proper analyst, observer, and data collector billets are adequate.

7. ANALYSIS AND DATA COLLECTION

Selecting specific data elements to support measures, metrics, and indicators for the AS is directly related to the hierarchy in Section 5. If a data element is not required for analysis or cannot be directly mapped via the hierarchy of Section 5 to an objective, then it will not be collected. Appendix 2 – Data Collection Matrix (DCM) contains the analytic chain from project outcomes to measures, and also includes collection methodology, survey questions where applicable and mappings of measures to solutions and measures to experiment periods.

Because experimental artificialities and time constraints do not support meaningful direct quantitative measures for the majority of solutions, survey questions will account for the majority of data collection during the AS. These will include a mix of open, discovery type questions, and closed form questions. These limitations, as well as significant differences between information sharing practices and equities at USEUCOM and USAFRICOM, render direct comparisons between "As Is" and "To Be" information sharing equally infeasible. Finally, time limitations forbid the execution of a repeated trials approach. To mitigate the lack of a baseline run and provide context to the results of surveys conducted during the experiment, a baseline survey will be administered prior to initiation of game play. Additionally, with respect to certain measures, it is possible to indirectly compare perceptions of information sharing effectiveness in the presence and absence of the recommended solutions. Such cases can be addressed using appropriately crafted Likert scale questions, and the significance of responses evaluated statistically by treating them as individual binomial experiments. Measures that can be evaluated in such a way are those for which it is meaningful to solicit a response to, "The solution provided is superior [in some respect] to the method I currently use to [conduct some activity]". For a collection of responses to such a survey question, a 40% success rate can be equated to the absence of either a positive or negative effect, because 40% would be the proportion of "successes" resulting from random selection of scores. Given a specific number of successes obtained, a binomial experiment based on a 0.4 success probability will discriminate a successful solution from one having no effect with a certain level of confidence. This confidence level, or equivalently the probability of falsely concluding that the solution has value (referred to as Type I error, or alpha) is based upon the cumulative distribution function of the specific binomial distribution. As the number of successes in a given sample size increases, the probability of committing a Type I error decreases. Conversely, a specified level of alpha determines the critical number of successes. Figure 2 provides a graphical example of the

interplay between sample size, number of successes, and alpha level, while Figure 3 provides a table of alpha values for given sample sizes and number of successes. For large sample sizes, the binomial distribution approaches the normal distribution; however, the validity of the binomial test does not depend upon normality or sample size. It is thus a flexible discriminating method for a wide range of expected sample sizes. This is the expected case for surveys administered during the AS, as the multiplicity of solution elements is of varying impact across the experiment audience.

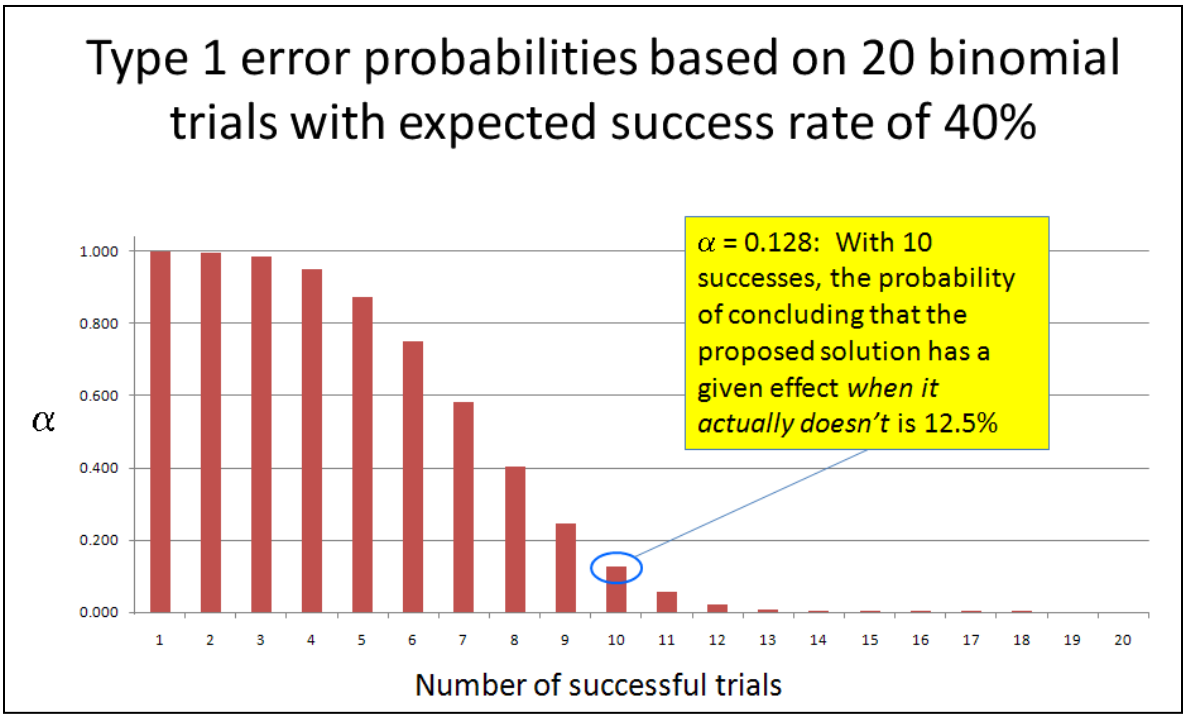


Figure 2. Type I error (α) related to number of binomial trials and number of successes.

Where comparative statistics are not appropriate, survey questions will be posed in absolute rather than relative terms. While such results do not demonstrate the merits of the solution relative to its absence, they nonetheless add to the holistic body of evidence and have value in supporting judgments regarding further development of the associated capabilities.

A few of the measures to be evaluated during the AS are quantitative metrics; these are treated in absolute terms as additional supporting evidence to survey questions.

Number of Successes (4 or 5 on Likert Scale)	Number of Surveys																		
	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	0.160	0.352	0.525	0.663	0.767	0.841	0.894	0.929	0.954	0.970	0.980	0.987	0.992	0.995	0.997	0.998	0.999	0.999	0.999
2	0.000	0.064	0.179	0.317	0.456	0.580	0.685	0.768	0.833	0.881	0.917	0.942	0.960	0.973	0.982	0.988	0.992	0.995	0.996
3		0.000	0.026	0.087	0.179	0.290	0.406	0.517	0.618	0.704	0.775	0.831	0.876	0.909	0.935	0.954	0.967	0.977	0.984
4			0.000	0.010	0.041	0.096	0.174	0.267	0.367	0.467	0.562	0.647	0.721	0.783	0.833	0.874	0.906	0.930	0.949
5				0.000	0.004	0.019	0.050	0.099	0.166	0.247	0.335	0.426	0.514	0.597	0.671	0.736	0.791	0.837	0.874
6					0.000	0.002	0.009	0.025	0.055	0.099	0.158	0.229	0.308	0.390	0.473	0.552	0.626	0.692	0.750
7						0.000	0.001	0.004	0.012	0.029	0.057	0.098	0.150	0.213	0.284	0.359	0.437	0.512	0.584
8							0.000	0.000	0.002	0.006	0.015	0.032	0.058	0.095	0.142	0.199	0.263	0.333	0.404
9								0.000	0.000	0.001	0.003	0.008	0.018	0.034	0.058	0.092	0.135	0.186	0.245
10									0.000	0.000	0.000	0.001	0.004	0.009	0.019	0.035	0.058	0.088	0.128
11										0.000	0.000	0.000	0.001	0.002	0.005	0.011	0.020	0.035	0.057
12											0.000	0.000	0.000	0.000	0.001	0.003	0.006	0.012	0.021
13												0.000	0.000	0.000	0.000	0.000	0.001	0.003	0.006
14													0.000	0.000	0.000	0.000	0.000	0.001	0.002
15														0.000	0.000	0.000	0.000	0.000	0.000
16															0.000	0.000	0.000	0.000	0.000
17																0.000	0.000	0.000	0.000
18																	0.000	0.000	0.000
19																		0.000	0.000
20																			0.000
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Number of successful trials

Figure 3. Type I error (α) for specified number of binomial trials and successes.

7.1. Collection Methods

Collection will be achieved through a combination of open-format survey questions, closed form survey questions, quantitative measures as appropriate and feasible, observations, and interviews as appropriate.

7.1.1. Automated/Instrumented Collection

Automatic stamps are created in APAN when any participant posts a document or comment to a posted document within a content area. Measures for the cross domain and risk management solutions require special posting an annotation procedures. The requirements for posting applicable documents will be briefed to the experimental audience during the introductory training period, and reinforced by observer interaction where necessary to ensure collection requirements for certain solution measures. APAN time stamps are in Hawaiian time, and conversion will be made as necessary to local time in Stuttgart. As well, the "experiment clock" is expected to be discontinuous with real time. These effects will not be impacting, however, as it is the traceability aspect of the time stamps and not numerical operations based upon those time stamps that are germane to the measures.

7.1.2. Observations

A set of study questions and measures, their relationships to the solutions, and their mapping to experiment periods, will be staged in the J9 Observation Tool (JOT) database for use by analysts and observers in collecting data. These questions and measures will assist the observer in focusing the important details of the experiment play. Additionally, analysts and observers will be fully versed with the Data Collection Matrix to gain an overview of the entire project, not just this specific activity. Analysts/observers will have the direction to note any action or occurrence appearing to have significance to the project regardless of the focus of the AS. Discovery is a potential and highly desired outcome of the anticipated experiment activity.

7.1.3. Interviews

An interview is defined as a person-to-person(s) discussion where notes are taken as to responses to questions and amplifying questions can be asked. This is desired over surveys that do not allow for further amplification in certain areas. Where the capture of insights, discovery, or more detailed information on the rationale for actions taken during a specific experimental period justifies the necessary interruption of experiment rhythm, the Study Director will assign particular personnel among the analyst/observer base to administer an interview to specific experiment audience personnel. Interviewers will be selected in terms of their familiarity with the issues of interest, and will be assigned specific questions. Interviews will be conducted in room 403 during end of session survey periods, and will be kept as short as possible, recognizing that the interviewees may also be among the survey participants for that period. If Room 403 is unavailable for a particular interview, the interview will be held on the OPT floor, in a manner that minimizes disruption of experiment play.

7.1.4. Surveys

Surveys are a method of data collection where numerous individuals are asked the same questions. Answers for the AS surveys will be solicited as both open responses (inviting discovery learning), and closed Likert scale responses constraining the respondent to rate, on a scale of 1 to 5, his or her level of agreement with a given statement. Where it is meaningful to solicit a comparison between the respondent's satisfaction with and without a given solution, the Likert scale questions will be posed to capture such comparison. In other cases, the Likert scale questions will be posed to solicit responses of an absolute rather than relative character. Surveys may be directed at the OPT, Response Cell or subsets of the union thereof depending on the variables of interest. Vovici will be the survey tool used during the AS, with Survey Monkey available as a standby capability, and paper surveys as a final fallback solution.

7.2. Privacy and Protection of Human Subjects in Research

As a U.S. led event, the IMISAS project AS will comply with all applicable provisions of U.S. Government regulations and directives regarding the protection of human subjects in research experimentation and the safeguarding of experiment data. If individual partner nation rules and directives require additional provisions for their own events, participants or sites they will be implemented on a case-by-case basis only for those instances. Presently this may include Germany.

7.3. Classification

All information handled during the experiment will be unclassified and contain no controlled unclassified information (CUI) or CUI caveats. However, CUI will be represented notionally, with appropriate markings, during the AS. Storage space will be available on the NIPRNet to notionally represent a CUI holding space. It is currently under consideration to use actual SIPRNet storage in the exercise of solution 1-2 (centralized cross domain solution); however, any documents that transit between SIPRNet and unclassified storage will be unclassified documents. Finally, in addition to any notional markings, all documents handled during the course of experimentation will be marked "Unclassified – For Experimentation Purposes Only".

7.4. Analysis Team Training

The analysis team consists of observers, analysts, and Subject Matter Experts (SMEs). These are assigned specific duties and focus areas for observation and analysis. At a minimum all members must understand the basic flow of the designed processes and procedures the experiment audience will be conducting in accordance with enabling policies. Data collection sheets will be provided as well as an explanation of what data should be collected and how to categorize the observations. Training will additionally include the following:

- Familiarization with JOT, both the mechanics of data entry and an overview of the data contained in the specific fields of the IMISAS JOT database.
- Familiarization with VOVICI as the primary survey collection tool.
- Familiarization with Survey Monkey as the contingency survey collection tool.
- Should an experiment network be established, all members of the analysis team must gain familiarization with the working aspects and where to post and collect data.
- Should interviews be required of the experiment audience, those required to collect data from these interviews will be given instruction on how to ask the questions and for key elements to facilitate asking more probing questions depending upon the response of the interviewee.

7.5. Analysis Hot-Washes

The analysis team will meet daily at the conclusion of each day's events. The purpose of these meetings is to gauge the progress of the Analytic Framework. The key items for review will be the discussion of expected and unexpected observations, the status of data collection, threats associated with the experiment, and mitigation factors and decisions. The results of these hot washes will be conveyed to the design and control team. If correction is required, the team leads will converse and come to a resolution. "In stride" analysis will occur on a continuous basis, with the aim of refocusing collection priorities or stimulation, gathering additional data where developing results appear anomalous, or concentrating observations where more detail is needed. Key observations, discovery items, and trends will be compiled as the experiment proceeds. These will be provided, along with raw summary statistics and preliminary evaluation of solution effectiveness, for the experiment After Action Report.

7.6. Data Archive

During the experiment, collected data requires safe keeping. This ensures it is not lost or misplaced and personally identifiable information (PII) is not compromised. Secure locations and back-up locations are required.

7.6.1. Data Storage and Archiving Locations

- Participant survey data and interview data will be stored in Microsoft Office (MS) files and statistical analysis files (as appropriate) and posted to the IMISAS project portal.
- Observer data will be stored in MS® Office™ files and posted on the IMISAS project portal.
- Comments and recommendations from all sources will be stored in MS Office files and posted on the IMISAS project portal.
- Automated data collection from network services and applications usage logs and network monitoring tool logs will be transferred to MS® Office™ files.
- Data will be copied to compact discs to ensure an additional, non-web-based back-up exists.

8. REPORTING

Experiment reports will provide an audit trail of experiment planning activities and experiment execution results. By explaining activities occurring before, during, and after the experiment, and by codifying the outcomes, findings, and recommendations from the experiment, they form the foundation for understanding the results and serve as a baseline for future experiments or follow-on analyses.

8.1. Analysis Report

The Lead Analyst leads the efforts of collating and analyzing the data in order to create an analysis report in accordance with the Analytic Framework. This report will provide input to the Transition Conference and the IMISAS project Final Report.

9. EXPERIMENT RISK/THREAT ASSESSMENT

Evaluation of the 21 threats to experimentation detailed in the Guide for Understanding and Implementing Defense Experimentation, commonly referenced as the GUIDEx, is covered as part of the End-to-End Experimentation Plan. The identified threats to experimentation, their assessed levels of risk and mitigation implementations will be refined as the experimentation plan matures.

Table 1 – Risk Evaluation Matrix			
Challenge	**Impact on this Event**	**Risk**	**Risk Mitigation Measures**
Ability to use capability			
1. Capability not workable: Does the hardware and software work?	High	Yellow	APAN software is a fielded capability and the AS involves no physical modifications to the hardware or software, and all APAN capabilities intended for use during the AS have been tested during a series of 5 technical evaluations with all reported technical issues resolved. Previously reported technical support issues have also been resolved, with 2 system administrators in Hawaii assigned to experiment support. Of the non-technical solutions, all but two are simple rule-based tools such as an IER matrix, quick reference guide to mission partner engagement, information management best practices, and a risk management methodology, all with an explicit aim, in part, to solicit feedback on their helpfulness. The two remaining non-technical solutions involve significant interaction with workstations. One involves APAN portal template and business rules; however, these matured along with other APAN capabilities during the technical evaluations. The other is the cross domain solution, whose manual air gap procedure requires CD-ROM burning capability (hardware and software). We are still awaiting confirmation that this capability will be present at the experiment site. However, the value of the solution can still be demonstrated even if this step is done notionally via a reasonable time delay.
2. Player non-use: Do the players have the training and TTP to use the capability?	High	Low	During the technical spirals, recommendations were gathered for streamlining the procedures, policies and approval process for APAN site instantiation. For the experiment audience, training will be conducted for the processes, procedures, policies and technical APAN enhancements they will use during the experiment, as well as the procedures for the non-technical solutions. Additionally, support personnel will be trained on the processes, procedures, policies and technical APAN enhancements to fully enable them to support the experiment.
3. No potential	High	Yellow	Time constraints prevent the execution of control runs or an

Table 1 – Risk Evaluation Matrix			
Challenge	**Impact on this Event**	**Risk**	**Risk Mitigation Measures**
effect in output: Is the output sensitive to capability use?			explicit "As is" vs. To Be comparison. The experiment will rely heavily on survey data, soliciting where possible comparisons with the subjects' status quo. While it is thus not meaningful to evaluate expected sensitivity, discourse with the two COCOMs during the project and the Process Documentation Event (PDE) suggest there will be strong feedback on the solutions.
4. Capability not exercised: Does the scenario and Master Scenario Event List (MSEL) call for capability use?	High	Green	The MSEL is nearly mature and represents all solutions intended for exercise at the AS. A robust collection of MSEL injects is already scripted, and these are being mapped to ensure coverage all solutions with sufficient multiplicity. The limited amount of time for the experiment (4 periods of 3.5 hours each) has necessitated parallel play of most solutions. While complicating separation of effects, this does ensure adequate exercise of all solutions.
Ability to Detect Results: Correctly detect a true effect			
5. Capability variability: Is systems (hardware and software) and use in like trials the same?	Low	Green	Due to time constraints, a repeated trials scheme will not be used for the AS; however, the capabilities provided by the UISC will remain static throughout the exercise.
6. Player variability: Do individual operators/units in like trials have similar characteristics?	Medium	Green	Training will be conducted on the experiment audience in the days immediately prior to experiment execution; thus, the individual operators will be the same. As discussed above, the experiment will not involve repeated trials.
7. Data collection variability: Is there large error variability in the data collection process?	High	Green	A large proportion of data is expected to be captured through observations, surveys and interviews and collated in a central location. The use of a standard survey tool, such as Vovici, will be used if available. Training for data collectors, observers, and analysts will be held prior to the experiment. All data collectors, observers, and analysts are slated to be on site where the laboratory environment is physically located; thus, hot washes will be held daily and more often if required, to ensure all appropriate data is collected consistently and

Table 1 – Risk Evaluation Matrix			
Challenge	**Impact on this Event**	**Risk**	**Risk Mitigation Measures**
			accurately.
8. Trial conditions variability: Are there uncontrolled changes in trial conditions for like trials?	Medium	Green	The experiment will not involve repeated trials; however, uncontrolled changes in capabilities or experiment conditions are not expected to occur.
9. Low statistical power: Is the analysis sample sufficient?	Medium	Yellow	Because the experiment will not involve repeated trials, sample sizes will be based upon the number of survey respondents for which Likert Scale questions are posed. The sample sizes are expected to be relatively small due to the size of the participant audience and the fact that not all surveys will be germane to the entire audience. Where it is possible to make a statistical comparison as described in section 7, a binomial trials test will be used to discriminate significance. Observations of experiment play will be closely monitored by analysts, observers, data collectors, subject matter experts, and solution developers to ensure all appropriate data is collected for further analysis and to attain a significant amount of viewpoints from different backgrounds, which will enhance the final analysis. Additionally, some survey questions posed during the technical evaluations will be augmented by the same survey questions provided to members of the experiment audience who will actively interface with the UISC portal.
Ability to Detect Results: Incorrectly detect an artificial effect			
10. Violation of statistical assumptions: Are correct analysis techniques used and the error rate avoided?	Medium	Yellow	Survey questions that accommodate statistical comparison with the responder's "status quo" will be treated as binomial trials and a binomial test administered to determine significance. Because sample size cannot be controlled a priori, the alpha level will vary for each test.
Ability to Isolate Reason for Results: Single Group			
11. Capability changes over time: Are there system (hardware or software) or process	Medium	Green	There are only a series of vignettes, not multiple trials. If procedures are changed, it will be the result of hot-wash meetings and by design. If the experiment audience does not follow trained methods, an experiment 'time-out' can be called

Table 1 – Risk Evaluation Matrix			
Challenge	**Impact on this Event**	**Risk**	**Risk Mitigation Measures**
changes during the test?			if the deviation affects experiment validity.
12. Player changes over time: Will the player unit change over time?	Medium	Green	There are only a series of vignettes, not multiple trials that will take place over a consecutive two-day period. If some of the participants do not arrive to complete the required training, then this could expose a team at a variety of levels of maturity to the processes, policies and procedures. This is a very minimal concern as manning for the billets will be thoroughly vetted at the MPC and FPC with the customers who will be supplying the manning.
13. Data collection changes over time: Are there changes in instrumentation or manual data collection during the experiment?	Medium	Green	There are only a series of vignettes, not multiple trials; thus, this should be of minimal concern.
14. Trial condition changes over time: Are there changes in trial conditions (such as weather, light, start conditions, and threat) during the experiment?	Low	Green	No significant environmental condition changes are expected for the experiment. The most likely cause of a condition change is a service interruption with APAN, the internet, or experiment network. The contingency plan for an APAN outage is to continue the experiment using phones. Primary survey capability (Vovici) will be backed up by Survey Monkey, with paper surveys as a final fallback. Paper observations can be taken in case of a failure of JOT.
Ability to Isolate Reason for Results: Multiple Groups			
15. Player differences: Are there differences between groups unrelated to the treatment?	Medium	Green	There will only be one group operating during the AS; thus, there will not be differences between groups.
16. Data collection differences: Are there potential data collection differences	High	Green	There will only be one group operating during the AS; thus, there will not be differences between groups.

Table 1 – Risk Evaluation Matrix			
Challenge	**Impact on this Event**	**Risk**	**Risk Mitigation Measures**
between treatment groups?			
17. Trial condition differences: Are the trial conditions similar for each treatment group?	Medium	Green	There will only be one group operating during the AS; thus, there will not be differences between groups.
Ability to Relate Results to Operations			
18. Non-representative capability: Is the experimental surrogate functionally representative?	High	Yellow	The capabilities hosted on APAN are representative of those hosted on other U.S. military portals. Of the non-technical solutions, the cross domain solution is the most notional if "SIPRNET" is emulated as a part of NIPRNet. This artificiality is not expected to influence the results significantly provided observers ensure that the manual air gap procedure is not by-passed.
19. Non-representative players: Is the player unit similar to the intended operational unit?	High	Green	The experiment audience will be fielded by the customers' personnel who are experienced in the billets they will be playing in the AS. Control may not be filled by actual subject matter experts in all billets, but will have personnel familiar with the given role. Real-life operational requirements could force substitution of personnel to role play in the experiment audience, but will most likely be filled by personnel who are familiar with the billet.
20. Non-representative measures: Do the performance measures reflect the desired operational outcome?	High	Green	Measures have been vetted at the MPC and FPC, and stakeholder input has been incorporated in this version of the DCAP. Where it was necessary to ensure analytical traceability, measures were added to those discussed at the FPC; however, none were deleted.
21. Non-representative scenario: Are the Blue, Green, and Red conditions realistic?	High	Green	There has been a significant effort to recruit participation of personnel with functional expertise in military and non-military disciplines and areas. The cooperation of actual IOs/NGOs, IA, and German government representatives are help to bring consistency, fidelity and authenticity to vignettes and scenario. Participants that are real world responders to HA/DR scenarios and will provide expert knowledge to their representative group.

APPENDIX 1: ACRONYMS

APAN	All Partners Access Network
AS	analytic seminar
COCOM	combatant command (command authority)
DCAP	Data Collection and Analysis Plan
DOD	DOD
EEA	essential element of analysis
FPC	final Planning Conference
HA/DR	humanitarian assistance / disaster relief
IMISAS	Interagency and Multinational Information Sharing Architecture and Solutions
IO	international organization
IER	information exchange requirement
JOT	J9 Observation Tool
JTF	joint task force
LTIOV	latest time information is of value
MPC	Mid-Planning Conference
MS®	Microsoft®
MSEL	master scenario event list
NGO	non-governmental organization
PDE	Process Documentation Event
PII	personally identifiable information
SME	subject matter expert
UIS	unclassified information sharing
UISC	unclassified information sharing capability

USAFRICOM	United States Africa Command
USEUCOM	United States European Command
USAID	United States Agency for International Development

APPENDIX 2: DATA COLLECTION MATRIX

NOTE: The Data Collection Matrix is maintained in an Excel spread sheet and available on request.

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project

Annex J - ANALYSIS

TABLE OF CONTENTS

1. Purpose J-1
2. Background J-1
3. Annex J Organization J-1
4. Demographics J-1
5. Data Collection J-2
6. Non-materiel Solutions J-3
6.1. Pre-planned UIS Release Matrix (Solution 1-1a) J-4
6.2. Unclassified Information Storage (Solution 1-1b) J-9
6.3. Business Rules for Cross-domain Transfer (Solution 1-2) J-11
6.4. Guide to Enable UIS with Mission Partners via a UISC (Solution 1-5) J-13
6.5. Information Management and Knowledge Management Business Rules for Unclassified Information Sharing (Solution 1-7) J-17
6.6. Quick-reference Guide to Potential non-DOD Mission Partners (Solution 1-8) J-19
6.6.1. Information Exchange Requirements (IER) Matrix J-22
7. Materiel Solutions J-24
7.1. Work Site Template (Solution 1-3a) J-25
7.1.1. Overall Usability J-26
7.1.2. File Management J-30
7.1.3. Document Collaboration J-31
7.1.4. Chat J-32
7.1.5. Mapping J-33
7.1.6. Email J-36
7.1.7. Training J-36
7.1.8. Network J-37
7.2. Business Rules for the UISC Work Site (Solution 1-3b) J-37
7.3. Business Rules for Data and Metadata Standards (Solution 3-1) J-41
7.4. Accommodating Disadvantaged Users (Solution 4-1) J-44
7.5. Graduated User Accounts (Solution 4-6) J-46

7.6. Rapid User Account Registration (Solution 4-7) J-46
7.7. Pushing and Posting Data from Dynamic Sources (Solution 4-8) J-48
7.8. Capturing, Sorting, and Categorizing Information (Solution 4-9) J-51
7.9. Business Rules for Automatic Trust Center Capability (Solution 4-10) J-54
7.10. Source Authenticity and Reliability Rating (Solution 4-11) J-55
7.11. UISC Search Capabilities (Solution 4-12) J-56
SUB-Appendix A – Binomial Significance Test J-A-1

1. Purpose

The purpose of this annex is to provide the analytically derived findings and recommendations from the Process Documentation Event, the Technical Spirals, planning conferences, and the Analytic Seminar. Data collected during these experimental events were captured in the form of observations, surveys, logs, and electronic records. Analysis of this data produced insights, findings, and recommendations.

2. Background

Development of IMISAS project solutions-based findings and recommendations began with gap analysis and validation at the Stakeholder/Gap Validation Conference in November 2010 generating a wide-ranging collection of 138 potential solutions for consideration.

By the end of the Solutions Development Workshop in February 2011, the IMISAS project team developed and refined 22 discrete proposed solutions for improving the current state of unclassified information sharing (UIS) and collaboration. Upon further examination and coordination with community of interest (COI) members over the next few months, the team deferred five solutions for further exploration, because they were not experimentally verifiable within the scope of the IMISAS project. Two solutions were combined with others on the list, leaving a total of 5 non-technical and 10 technical solutions for analysis. Annex J outlines both the non-materiel and materiel solution findings and recommendations in detail.

3. Annex J Organization

This annex is organized by solution and includes observations, findings, and recommendations for each solution. Observations are data collected from events to include observations, survey results, interview notes, and electronic data. Findings are a summary of what one or more observations implies regarding the solution. Recommendations are actions that are suggested to implement or improve the solution.

4. Demographics

Based upon the Demographic Survey results (including only those who completed the survey), the OPT survey group was comprised of personnel who were assigned to military commands, either as a contractor, active-duty military, or government civilian. Commands represented were USAFRICOM – nine, USEUCOM – seven, and USTRANSCOM – one. This group served as a credible representative of an augmented OPTS at the combatant command level.

The Response Cell, based upon the Demographic survey data, consisted of 17 personnel who were role players. Only four were active-duty military (all members of the German armed forces) while the balance consisted of contractors, nongovernmental organization (NGO) representatives and international organization (IO) representatives.

There were varying levels of participation ranging from 6 to 14 participants during the five technical spirals. Nearly all the participants were military centric including active duty military, civil servants assigned to military commands, and retired-military contractors.

5. Data Collection

Data collection for the project was conducted during two site visits, three planning conferences, five technical spirals, and in the culminating Analytic Seminar.

Data was collected in the form of interviews and observations, as well as research and survey questions. Survey data was collected in the form of qualitative Likert Scale[1] questions and open-ended essay questions. The Likert Scale questions generally offered the following five-point scale: strongly disagree; disagree; neither agree nor disagree; agree; strongly agree. Some of the Likert Scale questions included an option for the respondents to indicate that they did not have enough information to answer the question.

For survey questions administered during the Analytic Seminar, participants were grouped as follows:

- Augmented Operational Planning Team (OPT) members (designated as survey group "OPT")
- Members of the Response Cell (designated "Response Cell")
- All Partners Access Network (APAN) Users group was a combined group of the OPT and Response Cell

The APAN Users survey was specifically directed towards answering questions concerning the functionality of APAN (the proxy used for the unclassified information sharing capability (UISC) during the technical spirals and Analytic Seminar).

In the survey data tables included with each solution discussion in the following sections, the survey name, period administered, and question number are cited in the heading of the table along with the text of the survey question.

The survey abbreviations and survey groups are:

[1] When responding to a Likert questionnaire item, respondents specify their level of agreement or disagreement on a symmetric "agree-disagree scale for a series of statements. The scale range captures the intensity of their feelings for a given item.

- OPT Pre- Pre-Experiment Survey to the OPT members
- OPT Post- Post-Experiment Survey to the OPT members
- OPT Period 2/4 Period 2/4 survey to the OPT members
- OPT Period 3/5 Period 3/5 survey to the OPT members
- HF OPT 2 Human Factors Survey Period 2 to the OPT members
- HF OPT 3 Human Factors Survey Period 3 to the OPT members
- HF OPT 4 Human Factors Survey Period 4 to the OPT members
- HF OPT 5 Human Factors Survey Period 5 to the OPT members
- HF OPT Final Human Factors Survey Final to the OPT members
- RC Period 4 Response Cell Survey Period 4 to the Response Cell members
- RC Period 5 Response Cell Survey Period 5 to the Response Cell members
- TS1, 2, 3, 5 Technical Spiral Survey One, Two, Three, or Five

For the Likert Scale questions, the categorical survey responses include levels of confidence for agreement and disagreement, based upon the binomial test for significance detailed in Appendix A of this annex.

Example:

In the example below, the survey question was given to participants of the OPT at the conclusion of the experiment week. The confidence level indicates there is an 85% chance that agreement to the question is not random and shows a significant trend to the positive.

HF Final-Q3: I would feel comfortable providing all available unclassified Information requested by my mission partners on a site similar to the IMISAS Experimentation site.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	0	1	1	4	8	0	14	0.8%	85.0%

6. Non-materiel Solutions

Focused primarily on policy, process and procedures outlined in the *Handbook for Unclassified Information Sharing (UIS)*,[2] the IMISAS project team evaluated five solutions (Table J-1), with the majority of findings generated from the August 2011 Analytic Seminar event.

[2] *Handbook for Unclassified Information Sharing (UIS)*, included in the IMISAS Final Report, Annex M.

Table J-1 – IMISAS Project Non-materiel Solutions			
Solution		**Element**	
1-1	Process and procedures for the expedited release of controlled unclassified information (CUI) in a crisis response situation	**1-1a**	Pre-planned release matrix • Linked to Commander's release guidance • Release matrix applies risk management • Additional release authorities
		1-1b	Unclassified information storage – UISC • Business rules for storage of unclassified information on the UISC
1-2	Business rules governing the expedited transfer of unclassified information from classified networks to non-classified networks.	**1-2a**	Business rules for manual cross-domain transfer
1-5	Guides to enable UIS with mission partners via a UISC	**1-5a**	Processes and procedures to effectively engage mission partners for information sharing • U.S. Interagency, Host Nation (HN), multinational/coalition partners, IGOs and NGOs • Use of staff embeds/LNOs • Address all UIS capabilities (portal, email, phone, etc.)
1-7	Guides for staff use of UISC in support of operations	**1-7a**	Best practices to maximize use of UISC • Information Management/Knowledge Management (IM/KM) business rules
1-8	Quick reference guides for the roles, responsibilities and general information requirements of potential non-DOD mission partners	**1-8a**	Reference guide for mission partners • U.S. Interagency, HN, IGOs and NGOs • Roles, responsibilities and general information requirements • Electronically searchable

6.1. Pre-planned UIS Release Matrix (Solution 1-1a)

This solution involved processes and procedures for the expedited release of controlled unclassified information in a crisis response situation. This element of the solution entailed a pre-planned release matrix linked to Commander's release guidance and applied risk management in the context of additional release authorities.

The *Handbook for Unclassified Information Sharing (UIS)* included a pre-planned UIS release approval matrix designed to assist information release and decision making at the staff and action officer level.

Observation: Survey responses and observations regarding this solution ranged widely, reflecting the complexity of the issue and differing Analytic Seminar participant perspectives. Open-ended comments and suggested changes to the matrix, solicited via a survey, explain this observation. Representative of the responses are:

- The matrix added little value
- The matrix did not apply to the Public Affairs Office (PAO) function
- The solution would not be implemented because the Foreign Disclosure Officer (FDO) would always fulfill the functions stated in the release matrix
- Recommended mechanisms for accommodating changing risk situations and information categories (NOTE: These features were contained in the pre-planned release matrix and its associated instructions.)
- Confusion existed as to how the release matrix was referenced within the *Commander's Handbook for Unclassified Information Sharing (UIS)*. The reference was different during experiment play

Observation: An issue of concern is the OPT members' confusion over who the release authority is and the process for gaining release approval. During subject discussions at the Analytic Seminar, with many participants looking to the FDO for resolution, the FDO representative repeatedly asserted that an FDO's authority only extends to the release of classified information. One respondent suggested release was the prerogative of the holder, but if the information had a high level of sensitivity, that person would seek an answer from the legal office, "which took forever." Another cited DOD policy requiring all information slated for public release to undergo a security and policy review.

Observation: There was wide disparity amongst the OPT members as to how long an information element might take to process. This disparity was illustrated by the variance in responses to the question of expected approval times for the release of sensitive unclassified information. Amplifying statements included the following:

- Varies – 3 responses
- Hours to days – 6 responses
- One to two weeks – 1 response
- Unsure – 6 responses

Observation: While the pre-planned risk matrix was not fully employed as envisioned during the experiment, participant comments and discussions indicate the concept was reviewed by the OPT members during the Analytic Seminar event. Most survey responses related to the pre-planned release matrix were neutral, with some slight variation toward acceptance.

Observation: Although no OPT members felt the pre-planned release matrix posed an unacceptable risk, the result was predominantly neutral.

Post-Q1: The pre-planned release matrix poses an unacceptable risk of unintended disclosure of controlled unclassified information.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	0	0	3	9	0	0	12	8.3%	0.0%

Observation: The OPT members' responses were generally neutral on the issue of whether the preplanned release matrix and associated procedures delivered timelier availability of information to mission partners.

Post-Q2: Mission partners will receive timelier unclassified information using the pre-planned release matrix and its associated procedures as compared to my current organization's information sharing processes and procedures.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	0	0	1	9	2	0	12	0.2%	2.0%

Observation: The OPT members showed moderate agreement for sharing information with mission partners, despite significant concerns raised by some members about protection, or at least temporary sequestering of unclassified information as per observations of OPT discussions.

HF Final-Q3: I would feel comfortable providing all available unclassified Information requested by my mission partners on a site similar to the IMISAS Experimentation site.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	0	1	1	4	8	0	14	0.8%	85.0%

HF Final-Q5: I will provide all available unclassified Information requested by my mission partners regardless of the information sharing mechanism.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	0	0	2	2	9	1	14	0.8%	98.2%

Observation: In the Pre-Experiment survey, a significant proportion of OPT members (12 vs. 5) indicated they have never been prevented from sharing unclassified information with mission partners. However, in a follow-up open-ended survey question, OPT members generally indicated they withheld information as a "matter of habit." Information withheld beyond legally restricted information, was mainly related to planning (e.g., situation reports, briefings, information regarding real-world operations in Afghanistan), a result consistent with internal OPT member discussions about the unconditional release of planning artifacts.

Observation: In open-ended survey question responses in the Pre-Experiment survey, OPT members also voiced they are less likely to share information regarding force dispositions, For Official Use Only (FOUO) or Sensitive but Unclassified (SBU) information, partially complete products, and information mission partners asked to be kept private, regardless of the information sharing mechanism. It was noted during the event that some external agencies (i.e., non-DOD) also have restrictions on sharing information outside their respective agencies. This shared characteristic provided common ground in understanding information review requirements and decision making expectations prior to information release by the OPT.

Observation: Other OPT member comments regarding reasons for not releasing of information covered a wide-range of policy, process and procedural issues to include:

- Unclear designation of "who is part of what coalition"
- The requirement for release approval by senior leadership (FDO or other government release authority)
- Working exclusively on a classified network
- Political sensitivities
- The need to gain approval from the originating author
- Fears of mistakenly sharing sensitive information
- Procedural misunderstandings

Other discussions began defining the set of information requiring review, such as isolated pre-decisional or draft information. To remedy this potential issue, the OPT Chief directed the KM to establish a "fenced off" information storage location within the UISC proxy system.

Observation: The pre-planned release matrix was intended as a point of departure for further development of a standard process for reviewing the release of unclassified information. Participant responses regarding the utility of the release matrix were essentially noncommittal. This result may have proceeded in part from the limited time afforded the experiment audience to review the *Handbook for Unclassified Information Sharing (UIS)*; however, the risk-management concept underlying this device clearly struck a jarring chord among the OPT and illuminated the continuing undercurrent of discomfort with the unconditional release of unclassified information. This discomfort with unconditional release of information was observed during OPT discussions throughout the experiment play and during the after action review.

Finding: OPT members have a strong desire to share information with mission partners, but are confused about the requirements for releasing information to mission partners. As a course of habit and due to this confusion, unclassified information is withheld. Fear of reprimand or breaking legal barriers may significantly add to the culture of withholding information.

Recommendations: A pre-planned release matrix needs to address the following points regardless of the form adopted:

- The review authority for potentially sensitive unclassified information must be unambiguously defined in terms of duties and the authorities. Those duties need not reside with the FDO; the OPSEC Manager may be a better option. In any case, the misconception that it is the FDO's function to review unclassified information prior to its release should be dispelled by clear delineation of FDO duties and through training of the larger staff.
- The distinction should be made between unclassified information having sensitivities defined by law, information specifically identified as "not for public release," and what could be valuable information having no such sensitivities except to require sufficient review. As stated in President Obama's January 21, 2009 Memorandum for the Heads of Executive Departments and Agencies regarding the Freedom of Information Act (FOIA), unclassified information should not be withheld from release "merely because public officials might be embarrassed by disclosure, because errors and failures might be revealed, or because of speculative or abstract fears."

A culture of risk management vice risk aversion should be instilled into personnel. This culture change could be accomplished through policy revisions and training.

Mechanisms, such as the pre-planned release matrix introduced at the Analytic Seminar, to accommodate risk management should be put in place and implemented through policy and

procedure changes. Additionally, these risk management mechanisms should be incorporated into exercises and training.

6.2. Unclassified Information Storage (Solution 1-1b)

This solution included processes and procedures for expedited release of controlled unclassified information in a crisis response situation. This solution element focused on unclassified information storage on an UISC and included associated business rules.

The impetus for this solution was the lack of a networked unclassified information sharing system at USAFRICOM; however, the IMISAS project team also evaluated the general utility of a web-based storage system, and corresponding business rules, as a document exchange mechanism with external partners.

Observation: At their home organizations, 5 of 17 OPT respondents reported using a publicly accessible unclassified information storage location for sharing documents without release restrictions. Among Response Cell participants, 10 of 18 reported using such storage.

Pre-Q4, RC4-Q3: Does your organization have a publicly accessible unclassified storage location for sharing documents without release restrictions?			
Survey Group	Number of "Yes" Responses	Number of "No" Responses	Total Responses
Response Cell	10	8	18
OPT	5	12	17
Composite	15	20	35

The next three observations (survey responses) below are only from those respondents who had unclassified storage locations. Of note, the Response Cell was predominantly populated with non-military personnel.

Observation: The non-military personnel of the Response Cell whose organization had unclassified storage locations felt their storage locations were easily accessible.

Pre-Q4b, RC4-Q3b: It is easy to access the unclassified information stored in my organization's storage locations.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Response Cell	1	0	0	1	3	5	10	0.0%	99.6%
OPT	0	0	1	1	1	2	5	7.8%	68.3%
Composite	1	0	1	2	4	7	15	0.1%	99.6%

Observation: The non-military personnel of the Response Cell whose organizations had unclassified storage locations felt their storage locations were managed effectively.

Pre-Q4c, RC4-Q3c: In my organization's unclassified information storage location the information is effectively managed (adequate use of time stamps, authorship, version control, etc.).									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Response Cell	1	0	1	3	2	3	10	1.0%	73.3%
OPT	0	0	1	2	2	0	5	7.8%	33.7%
Composite	1	0	2	5	4	3	15	0.8%	69.2%

Observation: The non-military personnel of the Response Cell whose organizations had unclassified storage locations felt their storage locations were well structured.

Pre-Q4d, RC4-Q3d: In my organization's unclassified information storage location, the information directory is well structured, making it easy to locate information of interest.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Response Cell	0	0	0	3	4	3	10	0.0%	94.5%
OPT	0	0	1	2	1	1	5	7.8%	33.7%
Composite	0	0	1	5	5	4	15	0.0%	90.5%

Observation: Observed comments from the OPT and Response Cell coupled with survey responses indicated a preference for commercial data storage systems such as Googledocs, Dropbox, and YouSendIt, along with other web portals such as www.cimicweb.org, www.acaps.org, www.unitar.org, and EuShare. Interestingly, three of the Response Cell members cited APAN as a preferred storage system.

Findings: The low numbers of OPT participant responses to some survey questions make it difficult to draw comparative conclusions, but the data does suggest that Response Cell members enjoyed greater satisfaction, with ease of data retrieval and the management and organization of that data, than the OPT members. This view would be consistent with a less restrictive enterprise approach to information storage and Response Cell members' observations that field work during complex emergencies places a premium on tools with low learning overhead and effective content organization.

Recommendations: Design and implement UISC storage sites that are more attuned to the flatter and more collaborative methods used by external partners. The UISC should include a location for sharing information with a managed set of trusted partners.

Multiple vehicles for file sharing exist on the open internet and can serve the needs of both groups even in the absence of a dedicated UIS tool suite.

6.3. Business Rules for Cross-domain Transfer (Solution 1-2)

This solution focused on business rules governing the expedited transfer of unclassified information from classified networks to non-classified networks, primarily via manual cross-domain transfer processes. Due to security policy constraints at the experiment facility, this solution was not formally evaluated in the Analytic Seminar. The project team, however, was able to solicit some participant comments assessing the perceived benefits of the proposed cross domain procedure.

Observation: OPT members generally agreed that the cross domain transfer process would accelerate the sharing of documents with partners.

Period 2/4-Q1: Compared to current cross domain transfer processes, the proposed centralized cross domain transfer solution will accelerate the sharing of documents with partners.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	5	0	0	5	8	0	18	0.0%	90.2%

Observation: OPT members indicated that the proposed centralized review process would most likely ensure greater protection against inadvertent release of classified information.

Period 2/4-Q2: If implemented at my organization, the centralized review described in the recommended cross domain transfer solution would ensure a greater degree of protection against spills									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	6	0	1	4	6	1	18	0.2%	84.2%

Observation: The next two survey responses were from the Pre-Experiment Survey prior to the commencement of experiment play. Participant responses indicated a wide variance in the expected time required for transferring documents between different classification networks, indicated by the sample statements below:

- Varies – 1 response
- Hours to days – 9 responses
- Unsure – 4 responses.

Observation: Participant statements below also indicated a broad range of perceptions about, or lack of familiarity with, their organizations' approved cross-domain transfer procedures currently in place and the administrative process owner. Process ownership results below:

- Someone, but did not cite a position – 4 responses
- Either FDO or Security Manager – 4 responses
- The individual – 2 responses
- Ask a superior – 1 response

Observation: Risk assessments of OPT members' current cross-domain transfer procedures ranged from small ("only select personnel were allowed to conduct the transfer") to moderate, where burning the wrong information to CD-ROM or missing steps in the process were cited as specific potential modes of failure. One respondent noted they were able to conduct a cross domain transfer of information via email, presumably via an established High Assurance Guard, while another commented that the transfer procedure is not the issue, but rather the lack of a codified process for what, when, and how the DOD can share information.

Findings: Rules encouraging the maximum use of unclassified networks for the conduct of unclassified work are not expected to completely solve the information sharing problem. A

certain amount of military preparatory work in support of crisis response operations must be conducted on classified networks, if for no other reason than the COCOMs will receive much of their requisite information over those networks.

Participants moderately agreed that cross-domain transfer procedures similar to those found in the *Handbook for Unclassified Information Sharing (UIS)* would offer a method for accelerating the movement of that information to unclassified networks in a way that minimizes the risk. However, the particulars of the physical cross domain procedures, including the establishment of guards, are the prerogative of the operating command, and should also conform to United States Cyber Command policies.

OPT members' survey responses also suggest a strong recommendation for process standardization, generalized staff training, and focused training for the reviewers.

Recommendations: Centralize the resources and process points for cross domain transfers. Regardless of the solution employed, recommend that the solution be standardized across the command and regular training be conducted on the relevant procedures. Where an enterprise cross domain solution is available, it should be used preferentially; however, the proposed centralization of resources and manpower makes no assumptions on the exact mechanism of transfer.

This solution offers a potential method to solve the cross-domain issue; however, it does require further examination. One possible method could be to incorporate the solution into COCOM sponsored exercises.

6.4. Guide to Enable UIS with Mission Partners via a UISC (Solution 1-5)

This solution involved tailored guides to enable information sharing with mission partners and included processes and procedures to effectively engage non-military mission partners (e.g., U.S. Interagency, HN, multinational/coalition partners, IGOs and NGOs) as well as non-DOD staff and liaison personnel. Although similar in some degree to solution 1-8, this solution focused on the "how" of sharing information with partners.

The *Handbook for Unclassified Information Sharing (UIS)* included this guidance to enable information sharing with mission partners via a UISC.

Observation: Survey responses tended to be neutral with regard to the guide's effectiveness in explaining how to determine the means of sharing unclassified information and what unclassified information to share with external mission partners.

Period 2/4-Q10: The guide to non-DOD mission partners (Handbook Section 3.2.4 and Annex A) helped me to understand how to determine the means of sharing unclassified information with our external mission partners.

Survey Group	Number of Responses							Confidence Level	
	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	1	0	4	7	6	0	18	4.6%	26.4%

Period 2/4-Q8: The guide to non-DOD mission partners (Handbook Section 3.2.4 and Annex A) helped me to understand how to determine what unclassified information we need to share with our external mission partners.

Survey Group	Number of Responses							Confidence Level	
	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	1	1	4	5	7	0	18	12.6%	44.8%

Observation: Comments regarding the effectiveness with which Annex A to the *Handbook for Unclassified Information Sharing (UIS)*, Guide to Selected non-DOD Mission Partners, addressed the rationale for sharing and the span of mission partners with whom there was a need to share were neutral with a slightly positive bias.

Period 2/4-Q9: The guide to non-DOD mission partners (Handbook Section 3.2.4 and Annex A) improved my understanding of the rationale for sharing unclassified information with our external mission partners.

Survey Group	Number of Responses							Confidence Level	
	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	1	0	1	9	7	0	18	0.0%	44.8%

Period 2/4-Q11: The guide to non-DOD mission partners (Handbook Section 3.2.4 and Annex A) improved my understanding of the span of external mission partners with whom we need to share unclassified information.									
Survey Group	Number of Responses							Confidence Level	
	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	1	0	3	7	7	0	18	1.2%	44.8%

Observation: Substantive changes recommended by the OPT in open-ended survey questions related to Annex A to the *Handbook for Unclassified Information Sharing (UIS),* Guide to Selected non-DOD Mission Partners, were:

- To correct some inaccuracies
- To more fully develop descriptions of the various organizations' corporate cultures and their likely perception of the U.S. military
- To include more information on the United Nations
- To add detail to the role descriptions for the Bureau of Population, Refugees, and Migration (PRM)
- To broaden the Inter-Governmental Organizations section to include International Organizations (IOs) such as International Organization for Migration, International Committee of the Red Cross, and International Federation of Red Cross and Red Crescent Societies
- To add thematic organization to the NGO section and a description of why each of those bodies is important to the Commander or staff
- To add OneResponse (Office for the Coordination of Humanitarian Affairs site), Virtual On-Site Operations Coordination Centre Global Disaster Alert and Coordination System, and the NATO Euro Atlantic Disaster Relief Coordination Centre (EADRCC)
- To discuss DOD restrictions on information sharing with the various partners. Of particular note, three separate respondents recommended using the U.S. Army's and USAID's DOD Support to FDR Handbook for JTF Commanders and Below as a template for the guide

Observation: A key question addressed during OPT discussions was when best to introduce those external partners into the planning process. No clear consensus was reach; however, the

considerations underlying this question could be an excellent addition to the *Handbook for Unclassified Information Sharing (UIS).*

Observation: A non-military OPT member recommended early collaborative sessions during steady state operations among the COCOM and its partners in order to make a first collective estimate of needs, resources, and ground situation in the interests. These collaborative sessions would avoid or reduce delay in taking action when required. Establishing knowledge of common goals and objectives among the partners would also be an important outcome of the early collaboration.

Finding: In addition to the recommendations made for content additions and corrections to the guide, much valuable discussion transpired during the experiment regarding the "who, what, why, when, where, and how" of effective information sharing with external partners. These questions were the essence of solution 1-5, and observations relating to those questions are appropriate for consideration in recasting the Guide for Non-DOD Mission Partners. Among the key results were the following:

- Planning styles differ between the military and its non-military partners. The former tends to organize and interact hierarchically, and to focus internally during the initial stages of planning; exactly the opposite is often true in both respects for the latter. Those entities may want to engage early, and without their input – as cited during the Analytic Seminar as well as during Process Documentation Event interviews – the COCOM may not know what it doesn't know without that information, and waste resources in having to re-plan.

The importance of developing relationships and following up on communication was a salient point during the experiment and the after action review and is most appropriate to stress in the *Handbook for Unclassified Information Sharing (UIS).* As pointed out several times during the Analytic Seminar, "posting is not sharing". "Fire and forget" habits or posting artifacts without context or explanation can be seen as dismissing the recipients' value.

Recommendation: Implement the participant's suggestions to improve the guide and, as appropriate, with the *DOD Support to FDR Handbook for JTF Commanders and Below:*

- Further develop partner description and a ".org culture"
- Include more information on the UN
- Broaden the IO section
- Include thematic NGO descriptions and their importance to the mutual mission
- Add suggested information sites
- Address DOD restrictions to information sharing

Recommendation: Establish a posture for relationship building and an approach for effective information sharing with a broad range of potential mission partners that recognizes differences

in planning styles, accommodates preferences for engagement timing, seeks the "win-win" space among partner goals and objectives, and continually reinforces the importance of feedback and reciprocation in information sharing.

6.5. Information Management and Knowledge Management Business Rules for Unclassified Information Sharing (Solution 1-7)

This solution involved staff procedures and best practices focusing on information management and knowledge management (IM/KM) business rules while working with partners in non-DOD collaboration environments.

Observation: OPT members' basic knowledge of external partner collaboration needs and preferences were predominantly neutral.

Pre-Q14: I have a sufficient understanding of my mission partners' preferred collaboration tools and information sharing sites or venues.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	0	0	3	8	6	0	17	1.2%	26.4%

Observation: Most OPT members and Response Cell members agreed that inviting external mission partners to suggest their most familiar, or most comfortable, collaboration venues and tools would improve effective collaboration.

Post-Q17, RC5-Q4: Inviting non-military partners (via the RFI/RFA tools) to suggest venues and tools for collaboration will improve the effectiveness of that collaboration.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Response Cell	1	2	0	4	4	7	18	0.2%	96.5%
OPT	0	0	0	3	3	6	12	0.0%	98.5%
Composite	1	2	0	7	7	13	30	0.0%	99.8%

Observation: The value of the Annex D to the *Handbook for Unclassified Information Sharing (UIS)*, Expanded IM/KM Best Practices for UIS, was evaluated as neutral with a slightly positive bias.

Post-Q16: The information management best practices I used this week increased my understanding of how to collaborate with mission partners on their preferred collaboration tools and within their									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	0	0	0	7	5	0	12	0.0%	43.8%

Observation: Observations of OPT and Response Cell members' discussions during the Analytic Seminar reinforced many of the survey-generated observations. Notably, issues of communication degradation and limitations surfaced in regard to Adobe Connect Online (ACO) connectivity among non-DOD partner organizations. Other concerns included information security restrictions and the limited span of tools possessed by some organizations, which may be limited to Facebook or Twitter. Also, due to a multiplicity of collaboration methods, an Analytic Seminar observation strongly recommended a formalized tracking system for information requests. At the OPT Chief's recommendation, a similar capability was employed for handling the Department of State email requests from field agencies while using the UISC proxy system.

Observation: One of the most frequently cited impediments to information sharing during the experiment was the use of military-specific jargon, a lapse committed by the *Handbook for Unclassified Information Sharing (UIS)* and technical framework authors themselves in the request for information (RFI) tool. Chat protocol issues outlined in the *Handbook for Unclassified Information Sharing (UIS)* also surfaced during the Analytic Seminar, where participants cautioned against a 'staff action posted/staff action completed' mentality.

Findings: Common fixtures in both business and government work, IM plans can only succeed with consistent application and constant reinforcement to become a part of the organization's habit patterns and collective consciousness. USEUCOM and USAFRICOM both have IM/KM processes and procedures in place.

Using mission partner information sharing venues and tools may improve effective collaboration with mission partners.

There exists an overuse and misuse of military jargon of which personnel must be cognizant.

Recommendations: Implement training on the command's Information Management plan. Use the *Handbook for Unclassified Information Sharing (UIS)* to supplement the command's Information Management plan where useful, and stress the need for a more collaborative outreach with external partners.

Conduct regular and interactive training that focuses on those underlying organizational culture issues that can often impede information sharing, rather than on purely technical aspects of the UISC.

6.6. Quick-reference Guide to Potential non-DOD Mission Partners (Solution 1-8)

This solution involved quick reference guides for the roles, responsibilities and general information requirements of potential non-DOD mission partners (e.g., U.S. Interagency, HN, IGOs, NGOs). Although similar in some degree to Solution 1-5, this solution focused on a detailed description of non-military organizational roles, responsibilities and information requirements. During the experiment, perspectives on the "who, what, why, when, and where" of effective information sharing with external partners included the discussion of information exchange requirements.

The "Guide to Potential non-DOD Mission Partners" was included in the *Handbook for Unclassified Information Sharing (UIS)* to provide military staffs essential information about partner organizations.

Observation: OPT members indicated a slightly negative viewpoint that their current organization had adequate reference materiel and databases for identifying the capabilities and limitations of potential mission partners. The one member who felt positively towards his organization's reference materiel and databases for identifying the capabilities and limitations of potential mission partners was a non-DOD OPT member.

Pre-Q15: My organization's current reference material and databases are adequate for identifying the capabilities and limitations of potential mission partners.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	0	3	3	10	0	1	17	26.4%	0.0%

Observation: OPT members indicated a slightly negative viewpoint that their current organization had adequate reference materiel and databases for identifying roles and responsibilities of potential mission partners. One of the two members who felt positively was a non-DOD OPT member.

Pre-Q16: My organization's current reference material and databases are adequate for identifying the roles and responsibilities of my potential mission partners.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	0	3	3	9	2	0	17	26.4%	0.2%

Observation: OPT members agreed on the accuracy of the information found in the Guide to Potential non-DOD Mission Partners.

Post-Q18: The descriptions of partners' roles and responsibilities found in the guide to non-DOD mission partners (Handbook Section 3.2.4 and Annex A) were accurate to my knowledge.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	1	0	0	2	9	0	12	0.0%	99.4%

Observation: A small majority of OPT members agreed that the information found in the Guide to Potential non-DOD Mission Partners was sufficiently detailed.

Post-Q19: The descriptions of partners' roles and responsibilities found in the guide to non-DOD mission partners (Handbook Section 3.2.4 and Annex A) were sufficiently detailed to enable me to quickly establish contact with mission partners of interest.

Survey Group	Number of Responses							Confidence Level	
	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	1	0	0	5	6	0	12	0.0%	75.3%

Observation: The OPT members were generally neutral with a slightly positive bias regarding the robustness of the information found in the Guide to Potential non-DOD Mission Partners.

Post-Q20: The descriptions of partners' roles and responsibilities found in the guide to non-DOD mission partners (Handbook Section 3.2.4 and Annex A) were sufficiently robust to account for the range of mission partners with whom I needed to collaborate.

Survey Group	Number of Responses							Confidence Level	
	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	1	0	0	7	4	0	12	0.0%	29.6%

Findings: Current command reference materiel regarding roles and responsibilities, and capabilities and limitations of potential mission partners is viewed negatively.

The Quick Reference Guide was generally viewed in a positive manner, but it was noted that there is room for improvement.

Suggested improvements to the Quick Reference Guide included:

- "Consider changing the term 'partner' to another term as some mission partners may not wish to [be] seen as partners."
- "Add a list of information sharing websites that may be useful during crisis response operations."
- "Add additional information concerning the United Nations."
- "Add a section to include information concerning International Organizations."
- "Avoid military jargon or acronyms."

Recommendations: Increase the accuracy and utility of the guide while developing a feedback and review process to continuously update the guide.

Make the following changes to the *Handbook for Unclassified Information Sharing (UIS)*, concerning non-DOD mission partner information, to include the following:

- Add fully develop descriptions of the various organizations' corporate cultures and their likely perception of the U.S. military
- Include more information on the United Nations
- Add detail to the role descriptions for the Bureau of Population, Refugees, and Migration (PRM)
- Broaden the Inter-Governmental Organizations section to include International Organizations such as IOM, ICRC, and IFRC
- Add thematic organizations to the NGO section and a description of why each of those bodies is important to the Commander or the staff
- Add OneResponse (OCHA Site), Virtual OSOCC GDACS, and the NATO Euro Atlantic Disaster Relief Coordination Centre (EADRCC)
- Discuss DOD restrictions on information sharing with the various partners
- "Avoid military jargon or acronyms"

6.6.1. Information Exchange Requirements (IER) Matrix

Observation: Comments made during the experiment indicated that the IER matrix, suggested in section 3.2.7 of the *Handbook for Unclassified Information Sharing (UIS)*, was neither well understood by the experiment audience nor used with any consistency. Five respondents reported referencing the IER matrix one to two times during the event, while three others reported referencing it three to four times. Fewer participants reported actually updating the matrix in response to changes in collaborative capabilities or preferences across the partner base.

Observation: Specific open format feedback indicated that the matrix was neither explained well nor introduced effectively. Likert Scale responses indicate that some participants had reviewed this section of the *Handbook for Unclassified Information Sharing (UIS)*; however, no significant result beyond neutrality was noted with regard to its perceived utility in informing the means of collaboration.

Period 3/5-Q4: During the seminar today, the IER matrix provided an improvement over the normal means of deciding how best to collaborate with external partners in a dynamic environment.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	2	0	1	10	3	0	16	0.1%	4.0%

Observation: There was no indication that the "alternative method of collaboration field" provided in the IER matrix was useful, as the survey results were neutral.

Period 3/5-Q4c: The "alternative method of collaboration" field in the IER matrix is useful to have when primary collaboration means are unsupportable.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	2	0	0	10	3	1	16	0.0%	12.4%

Observation: No substantive recommendations were provided for additional fields within the IER matrix; however, most of the feedback in this section simply reiterated confusion as to the purpose of the matrix. One reviewer did recommend synchronizing the IER matrix with FDO matrices.

Observation: OPT member comments made during the experiment proved more revealing than the survey instruments. Some indicated that the IER matrix was neither well understood nor used with any consistency during the Analytic Seminar. OPT member comments revealed that five respondents had referenced the IER matrix 1-2 times during the event, while three others reported referencing it 3-4 times. Still fewer participants reported updating the matrix in response to changes in collaborative capabilities or preferences across the partner base. Of particular note, three separate respondents recommended using the *DOD Support to Foreign Disaster Relief Handbook for Joint Task Force Commanders and Below*[3] as a template for the Guide.

[3] A joint U.S. Army and U.S. Agency for International Development publication, on March 25, 2011, version 3.0 of *The DOD Support to Foreign Disaster Relief Handbook for the Joint Task Force Commander and Below*, was distributed to stakeholders for comment.

Finding: Although the IER Matrix was received with significant uncertainty, discussions during the experiment clearly indicated that both the OPT and Response cell were concerned with the information attributes specified in the matrix, including the desirability of identifying multiple paths for communication.

Recommendation: The IER Matrix requires further study as the examination during the Analytic Seminar was inadequate. The recommendation is to clarify the explanation and presentation of the IER matrix in the *Handbook for Unclassified Information Sharing (UIS)*. This artifact may have been better understood and more resonant with the concerns of all participants had they been presented with a more straightforward explanation of how the IER matrix could enable more efficient information sharing and focus collaboration expectations. The concept is not a novelty, but rather a well-established staple of the DOD Architectural Framework, and thus is easily cited for authoritativeness and integrated into other codified command and control architectures.

7. Materiel Solutions

The IMISAS project team explored ten materiel solutions, listed in the table below, during the five technical spirals and the Analytic Seminar.

Table J-2 – IMISAS Project Materiel Solutions

Solution		Elements	
***1-3**	Pre-defined template and business rules for the establishment of UISC work sites	**1-3a**	UISC work site template • UISC collaboration tools (e.g., wikis, blogs and widgets)
		1-3b	Business rules to support UISC work site • Portal establishment • Work site management
3-1	Business Rules to define data types, standards, metadata requirements that facilitate posting, transfer and use of data	• Standardized metatags • Business rules to standardize the tagging of documents, blogs, and forums	
4-1	UISC to make automatic bandwidth recommendations in a restricted communications environment	• Redirect mobile or low bandwidth device users to site with limited rich content • Develop appropriate business rules and procedures	
4-6	Graduated user account permissions and procedures for anticipated and unanticipated users to facilitate allocating access to different levels of unclassified information based on trust	• Emulate a granular permission structure from within APAN • Develop business rules and procedures	

Table J-2 – IMISAS Project Materiel Solutions		
Solution		**Elements**
4-7	A rapid user registration system with the capability and capacity to support expansion of the UISC COI in crisis response	• Scaled down UISC registration process to limit the use of personally identifiable information (PII)
4-8	UIS capability to push or post aggregated data from dynamic sources to mission partners	• UISC to push and receive really simple syndication (RSS) feed • Business rules and procedures for the tagging of RSS feed data • Social media, hotlines, news
4-9	UIS capability to capture, sort, categorize, filter information in the public domain	• Business rules for data tagging to support filtering and categorizing public domain data that is brought into UISC
4-10	Business rules to maximize current automatic trust center capability including: rating, recommendations, and level of confidence	• APAN "Star" rating system • Telligent "points" system potential use • Business rules
4-11	Source authenticity and information reliability capability for UISC use in filtering and verification of real-time data from channels such as Twitter, SMS, email and RSS feeds	• Source authenticity and information reliability capability (e.g., SwiftRiver) • Business rules and a set of protocols for determining the source authenticity and information reliability
4-12	UIS search capabilities (federated or integrated)	• Currently APAN has capability to search blogs, wikis, forums • Use of filters (Ifilter) to search Office 2003/2007 products and PDF files within the media gallery(if functional) • Standardized metatags

* Note – Solution 1-3 is both a materiel and non-materiel related.

The Analytic Seminar event provided a valuable test-bed for continued analysis of technical capabilities initially evaluated in the technical spirals by subjecting the capabilities to operationally, realistic, functional stresses and overlaying the human interaction element between two significantly different organizational cultures (i.e., OPT and Response Cell). As expected, strong viewpoints prevailed in the open-ended survey responses, reflecting the evident cultural divide. Conversely, many Likert Scale survey responses reflected a more balanced consensus, with generally equal distributions for agreement and disagreement between the groups.

7.1. Work Site Template (Solution 1-3a)

This broad solution focused on defined templates and business rules for the establishment of work sites on a UISC platform. This solution element identified collaboration tools (e.g., wikis, blogs and widgets) and other key features that should be included in any UISC work site. While

the format of the template used during the experiment was specific to APAN, the content recommendations are applicable to other information sharing portals.

This solution was assessed during the technical spirals and the Analytic Seminar.

7.1.1. Overall Usability

Observation: As shown in the survey responses below, the results were generally neutral regarding the degree of sufficiency of information types supported on the UISC. However, positive responses outnumbered negative responses for both OPT and Response Cell members.

RC5-Q2, Post-Q4: The range of information types that I used on the IMISAS Experiment site this week was sufficient for me to perform my job.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Response Cell	0	1	4	5	8	0	18	9.4%	56.3%
OPT	0	1	1	6	4	0	12	2.0%	22.5%
Composite	0	2	5	11	12	0	30	1.7%	43.1%

Observation: The OPT provided a large number of criticisms and recommendations for improvement regarding the UISC experimentation site's capabilities. They were neutral with a slight bias toward agreement regarding the general usefulness of the site in crisis response.

HF4-Q6: The IMISAS Experimentation site helps me to achieve my given tasks/goals.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	0	0	2	7	6	0	15	0.5%	40.3%

Observation: The OPT and Response cell were generally neutral regarding the UISC experimentation site's applicability to crisis response operations. Response Cell member comments were about evenly balanced between agreement and disagreement, while the OPT leaned more toward agreement.

Period 2/4-Q4, RC5-Q3: The capabilities hosted by the IMISAS Experimentation site are directly applicable to the conduct of crisis response operations.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Response Cell	0	0	9	1	5	3	18	73.7%	56.3%
OPT	1	1	0	8	6	2	18	0.0%	64.1%
Composite	1	1	9	9	11	5	36	5.8%	70.0%

Observation: Both the OPT and Response Cell members commented in the open-format Analytic Seminar survey questions that they found the UISC portal's user interface to be slow, cumbersome, and unintuitive, and felt that those accustomed to commercially available tools would lose patience with the DOD-provided tool set. In Likert Scale survey question responses, the OPT members were neutral leaning slightly toward agreement regarding ease of information access using the UISC portal, while the Response Cell responses were predominantly neutral. One difference was that the two strongly negative responses came from the OPT and the two strongly positive responses from the Response Cell.

Period 2/4-Q3, RC5-Q1: It was easy to access information using the tool sets on the IMISAS Experimentation site.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Response Cell	0	0	6	4	6	2	18	20.9%	56.3%
OPT	1	2	4	2	9	0	18	26.4%	80.1%
Composite	1	2	10	6	15	2	36	19.5%	80.7%

Observations: Feedback on the performance of the specific tools supporting the UISC was mixed, but largely influenced by "bugs" in the particular network instantiation and in some cases by a lack of familiarity with the interfaces. An OPT member commented that APAN provided a good medium for participating organizations to share information, while another mentioned being able to "connect up with the UN and NGOs faster than before". One Response Cell member commented that APAN continues to present "a very good suite of communication and

collaboration tools that enables great point-to-point communication and collaboration". There were also several negative comments. Among these were observations that APAN was currently a "poor vehicle for connecting, collecting, disseminating, and analyzing information"; a necessary UISC solution whose current approach is nonetheless unacceptable; and a site that is good for military use but which NGOs will not use. An OPT member remarked during the AAR meeting that external partners would not go to a military site that did not provide real value, and that the hosted Adobe Connect Online (ACO) collaboration tool apparently had such value, being used frequently and effectively with those partners. There were multiple OPT member comments that, effectively serving the needs of the COCOMs' external partners, would require designing more to their practices, "catching up with the development of real world [applications]", avoiding military-centric terminology and presentation of information, and facilitating their needs rather than leading the development in a pre-conceived direction.

Observation: While one OPT member indicated the span of tools hosted on the UISC to be limited, a Response Cell member believed there to be an overabundance of communication methods. Two OPT members mentioned that many of the demonstrated capabilities were redundant conduits for the same information, one pointing out the resulting bandwidth inefficiency and the other cautioning against the potential for source ambiguity. Another OPT Member disputed the need for complex interfaces, recommending a non-structured approach to information sharing. The expediency of a telephone was cited as necessary and sufficient, by two Response Cell members. On the other hand, when respondents were asked what tools sets were most useful in the performance of their jobs, both OPT and Response Cell members cited blogs, chat, wikis, other websites, email, social media platforms, and tools either contained within or accessible to the UISC. Google voice, Short Message Service (SMS), Drop Box, Yousendit and professional online platforms such as LinkedIn were also mentioned. Moreover, one Response Cell member commented that much of the functionality provided by APAN would be useful if exercised.

Observation: Comments made during the Analytic Seminar illustrated the critical role of KM in the maintenance of a UISC technical solution. A Response Cell member cited the need for additional forums for "facts", analysis, and risk assessment as distinct from RFIs/RFAs. Balancing this need for specificity was a suggestion to avoid proliferation of non-authoritative information, and limit the reviewer's requirement to visit a multiplicity of information stores. The need for KM was heavily cited in discussions of the RFI/RFA tool, the conduit that handled the vast majority of information posted to the UISC proxy. Specific concerns were how best to manage and prioritize the volumes of incoming requests and whom to assign responsibility for responding to them. Other feedback included dissatisfaction with the filtering and verification capabilities, and the lack of a logical sequence to the presentation of threads. Another respondent pointed out that the effective management of RFIs requires the reception of alerts as entries are posted. In APAN, the only way the OPT found to do this was to set up subscriptions for alerts to RFIs via email. The difficulty with this workaround was that they were unable to

respond to them in the same way that the alerts were sent via email. A final KM-related recommendation was for the use of a moderated forum to assist with the input from outside participants.

Observation: Specific recommendations for UISC improvements included:

- More informative, visual layouts with a review pane or other mechanism for new posts or hot topics
- Alerts directing users' attention to such postings
- Better organization of hosted tools and documents
- Standardized placement of controls leading to the same information stores
- A point of contact utility
- The capability to add greater visibility of key comments, buttons, icons, and links
- Simplify site navigation
- Include the provision of a "drag and drop" capability for file movement between modules

Findings: The capability package demonstrated by APAN generated widely mixed responses with respect to usefulness and applicability in crisis response situations. In spite of cited system latencies, survey responses indicated that the UISC proxy provided moderately easy access to information. There were disparate viewpoints regarding the number of collaboration tools provided in a centralized scheme. While the need to simplify the user interface was a common theme, the union of tool sets normally used by both the OPT and the Response Cell closely matches the suite of capabilities provided by APAN. It is also significant that ACO itself, a centralized and integrated set of collaboration tools, was well received by both the OPT and the Response Cell. UISC tools used most frequently used throughout the experiment periods were RFI/request for assistance (RFA) forum, media galleries, and ACO.

The range of opinions on the adequacy of APAN for information sharing and the contrast between what the OPT thought and what non-DOD participants wanted is significant. This difference reinforces the need for continued DOD coordination and information exchange as was highlighted in the non-technical solution analysis section of in this report.

Bridging the gap between both military and non-military organizational communication styles places design constraints on a UISC that are not levied on most commercial tools providing a smaller span of capabilities, and that the multi-functionality should be expected to incur developmental hurdles. The sheer volume of substantive recommendations for improvements to the UISC proxy suggests an interest in further development of the model.

Recommendations:

- The UISC must include:

- A continued development process for an integrated template of multimedia collaboration tools to serve the needs of both military and non-military partners.
- A simplified user interface, optimized for speed.
- Ability to send alerts to users who subscribe to automated information feeds.
- Tool definitions and descriptions that eliminate military specific terminology.
- Provision for robust KM support to include active moderation of user roles and inputs
- A web-based collaboration venue (such as Adobe Connect Online)that accommodates active moderation using rules of order.
- A dedicated question and answer (RFI, or simply "query") tool with the following features :
  - Filterable;
  - Can be grouped by topic and is easily searchable; and
  - Capable of organizing and linking RFIs;
- A forum tool that allows multiple instantiations for segregating discussion areas.

- Create a governance body to maintain configuration management of the UISC tools and capabilities, develop training on provided tools, implement business rules, charter a user/operating system group forum, and establish enterprise control to include future planning and an international consortium or steering group.

7.1.2. File Management

Observation: During one of the technical spirals, most users agreed that it was easy to post documents to APAN.

TS1: It was easy to post the document to APAN.								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	1	2	2	7	2	14	4.0%	94.2%

Observation: During the Analytic Seminar AAR, the OPT discussed several features that would be useful for file and document management. Those features are included in the recommendation below.

Findings: Documents were easy to post but additional capabilities are needed to make this tool more useful to the operators.

Recommendations: A UISC must have a file management capability to include the following:

- A multi-tiered folder structure for the storage of data or files
- A user friendly means to upload files
- Version control with the capability to check-out, revert, and compare previous versions in history
- Drag and drop functionality
- A simple sort, search, and retrieval utility
- Support for simple standard tagging and naming conventions
- A means of designating a single source point for authoritative documents (with links to other areas if required)

7.1.3. Document Collaboration

Observation: The majority of technical spiral participants agreed that the document collaboration tool was easy to use.

TS3: The document collaboration capability was easy to use.								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	1	0	1	6	1	9	1.0%	97.5%

Observation: During the Analytic Seminar AAR session, the OPT determined that having an area for document collaboration would be useful and suggested several features that would improve this capability. These features are included in the recommendation below.

Findings: Document collaboration was easy to use and useful in a crisis response environment. Additional capabilities are needed to make this tool more useful to the operators.

Recommendations: A UISC must have a document collaboration capability enabling simultaneous, multi-user contributions which should include the following features:

- Version control

- History comparison
- Moderation (as required)
- Draft document (work area and publish control capability)
- Publish capability
- Graduated access
- Subscription/alerts when content is updated/changed
- Rich text editor with spell check

7.1.4. Chat

Observation: The UISC chat functionality (APAN peer-to-peer chat and group chat) received mixed responses during both the technical spirals and the Analytic Seminar, with group chat receiving the greatest number of negative comments. During both events, there were participants who reported communicating effectively over chat, and at least understanding the utility of group chat even if they were unable to get it to work. The capability most cited during the technical spirals as a desirable feature was chat, and according to the surveys, both modes of chat (group and peer-to-peer) saw a marked increase in the level of use during the course of the Analytic Seminar. One participant during the technical spirals preferred ACO chat capability due to its more robust set of features. Specific drawbacks cited for group chat during the technical spirals were the need for a capability to define individual groups and the requirement, in one instance, to place Internet Explorer 9 into compatibility mode to make the capability work. During the Analytic Seminar, two OPT members had difficulty using chat. Another felt that the person-to-person chat capability was acceptable, but that group chat was unacceptable because the chat window was not visible unless the page to which it was associated was active. In any case, the automatic logout feature did not alert the user of the automatic action, an anomaly cited as particularly nettlesome because the auto-logoff feature deactivates some capabilities such as data entry while preserving the appearance that the user is still fully active.

TS1: It was easy to chat with other APAN users.								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	1	2	2	6	3	14	4.0%	94.2%

Findings: Chat is a capability cited both by the OPT and Response Cell as being regularly used, and given its familiarity among a large set of internet users and its low bandwidth consumption, it would seem an obvious choice for inclusion among the UISC tools. The criticisms of the chat utilities demonstrated during the technical spirals and Analytic Seminar were related to the user interface ("ability to sustain chat visibility like on [Facebook]", etc.) rather than on its acceptability among the other tools provided. The data indicate that usage rose sharply upon the audience's acclimation to the chat utilities.

Recommendations: The UISC must include an XMPP chat capability with the following features:

- The capability of running a chat process independently of the active UISC window
- Automatic logging, archiving, and exporting of chat for historical use
- Automatic alerts to annunciate when other participants are away, idle, and active
- Automatic alerts for users of new messages via a visual and/or audible cue
- Notification of user's "log-on" status
- The capability to converse with an entire group or privately with an individual
- The capability to create and use multiple chat rooms
- The capability to restrict access to different chat rooms

7.1.5. Mapping

Observation: The OPT responded mostly negatively to a survey question regarding the utility of MapView as hosted on the UISC proxy; however, most technical spiral participants found MapView easy to use and potentially of value in crisis response operations.

Post-Q12: MapView hosted on the IMISAS Experiment site provided a capability that would be useful during crisis response operations.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	0	5	1	4	1	1	12	66.5%	2.0%

TS4: MapView in APAN was easy to use.								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	0	1	1	4	3	9	1.0%	97.5%

TS4: MapView in APAN provided a capability that would be useful in crisis response								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	0	1	0	7	1	9	1.0%	99.6%

Observation: The results of both the Analytic Seminar and the technical spirals were consistent in their agreement on the usefulness of crowd mapping to crisis response operations.

Period 3/5-Q10a: "Crowdmapping" (organizing crowd-sourced information into interactive maps and timelines) provides a capability to view data that would be useful in a crisis response.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	0	0	0	4	5	1	10	0.0%	83.4%

TS4: Crowdmapping provides a capability to view data that would be useful in a crisis								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	0	0	1	6	2	9	0.0%	99.6%

Observation: Survey responses from the technical spirals regarding the ease of use of GeoCommons and MapView were positive; however, the group observed that limitations in internet access and requisite bandwidth for map uploading could reduce the usefulness of these applications during crisis response operations. This group also noted that the capabilities are not immune to inaccuracies or incompleteness in information. During the Analytic Seminar, the OPT Chief related a UN finding that the sheer volumes of information produced by crowd sourcing posed challenges to filtering it. Another respondent from the seminar noted that unverified reports from a crowd map could misdirect planning and waste time and asset resources.

Observation: Other OPT observations were more positive, recognizing the ability of crowd mapping to directly influence how the COCOMs might respond to host nation requests. Crowd mapping could support operations "on the leading edge of a constantly changing situation" by providing a continuously prioritized stream of key information. OPT members commented that crowd mapping facilitates the determination of response needs and priorities through the accumulation of multi-source input; the identification of areas that require the most assistance and that can leverage ongoing relief efforts; the confirmation of planning assumptions through the provision of real-time, targeted information; and the accelerated establishment of situational awareness.

Observation: MapView overlays or layers considered useful by the OPT included those providing real-time location of troops and other responders on the ground, streets, factories, critical infrastructure, administrative boundaries, incident reports, locations and capabilities of aid teams, medical stations, transport services, communications facilities, food stations, refugee camps, infrastructure outages, downed power lines, and washed out roads. One respondent reiterated the observation that validating the information contained on the map is important.

Findings: Notwithstanding the technical problems encountered in support for MapView and GeoCommons software during the Analytic Seminar, support for the utility of the mapping capabilities to crisis response operations was clearly positive.

Recommendations: A UISC must have a robust, easy to use mapping utility with the following features:

- The capability to pull and push data among other sites in a variety of formats (e.g., Keyhole Markup Language (KML), Really Simple Syndication (RSS), Geographic RSS (GeoRSS), Web Map Service (WMS))
- The capability to activate and deactivate layers, change base maps, modify zoom levels, drill down into map elements, and attach time, date, imagery and video to map elements
- The capability to sequence content in time
- Compatibility with current ".mil" security requirements

- Implement a methodology for mitigating the potential information overload associated with mapping source information, and a means of establishing an acceptable "false positive rate" to guide decisions on committing scarce resources based on incomplete or unverified reports.

7.1.6. Email

Observation: APAN mail, the UISC proxy email capability, received several criticisms during the Analytic Seminar due to an awkward window sizing interface for reading emails, an auto-logout function that required excessive user interaction, lack of automatic real-time updating of the user's mail repository, and the requirement for a separate password entry for the email application.

Finding: The experiment audience used E-mail on a regular basis as a method for unclassified information sharing among mission partners. Email will remain a method for unclassified information sharing among mission partners. The UISC, however, does not require an embedded email capability, but it must have the ability to send out alerts to users who subscribe to a UISC feed. Mission partners should be able to use their regular email addresses for this purpose.

Recommendation: UISC should limit the use of email to encourage posting information to locations that are searchable by and available to the larger community. Educate personnel to be cognizant of mission partners' communication methods and adapt to the mission partner's email system. This may include use of alerts or establishing a host nation email address for use during an operation.

7.1.7. Training

Observation: Respondents from both the technical spirals and the Analytic Seminar indicated that APAN, as a UISC technical solution, was significantly more difficult to become familiar with than many commercial information sharing tools. Survey responses from both the technical spirals and the Analytic Seminar indicated a requisite "critical mass" of familiarity, after which APAN's utility became evident. Other survey questions administered during the Analytic Seminar indicated that the lack of advanced training generated substantial frustration. Both groups suggested that training, either via documentation or a "guided tour," would help new users gain proficiency.

Findings: A requisite "learning curve" is associated with the UISC and presumably with any similar suite of centralized and integrated collaborative tools. While earlier observations and findings support the investment of time and effort in gaining familiarity with the UISC, other observations on user expectations suggest that the perceived marginal utility of the portal may rapidly evaporate with user frustration in learning its interface. Significant attention should

therefore be given to crafting a training interface that accelerates user familiarity as much as possible.

Recommendation: A UISC must institute a continuous, feedback-based program of user training on the UISC tools, capabilities, and business rules.

7.1.8. Network

Observations: Security settings on the NIPRNet proxy server and security policy preventing use of ActiveX controls on that network prevented the effective caching and presentation of crowd maps in both MapView and Geocommons environments, to the extent that none of these capabilities were ever employed on NIPRNet workstations during the Analytic Seminar. The OPT KM representative was able to establish a crowd mapping connection via GeoCommons over a commercial connection, and displayed the map on the common OPT screen. There was much discussion concerning the inability to add applications and browser plug-ins in a timely manner to work with mission partners.

Observation: Uploading video was not functional during the Analytic Seminar on the laptops given to the OPT while other NIPRNet machines functioned well. The inability to load a sample video is believed to have been due to network security protocol settings for YouTube.

Findings: To effectively use the UISC and access the open Internet, users' computers need to have adequate access to the internet sites and tools required for the operation.

Recommendations: A UISC must establish policies, processes and procedures to enable crisis responders to access resources on the open internet by facilitating the following:

- A relaxed security environment
- The capability to install required applications and browser plug-ins used to work with partners
- Provision of commercial-off-the-shelf clients and commercial internet as an alternative to configurable clients and connectivity via the NIPRNet

7.2. Business Rules for the UISC Work Site (Solution 1-3b)

This solution involved business rules for the implementation and use of the unclassified information sharing site template. During the Analytic Seminar, participants primarily used the business rules when posting requests for information (RFIs).

This solution was assessed in the Analytic Seminar.

Observation: Survey responses indicated general agreement that the business rules for posting an RFI/RFA were easy to use.

Period 2/4-Q5: The business rules found in the Handbook at Annex E for posting a request for information (RFI) or request for assistance (RFA) were easy to use.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Response Cell	5	0	1	3	8	1	18	0.1%	96.8%
OPT	1	0	1	6	10	0	18	0.0%	90.8%
Composite	6	0	2	9	18	1	36	0.0%	99.2%

Observation: OPT responses were neutral, tending toward agreement, that business rules for situational reports would enhance the situational awareness of external partner organizations.

Period 3/5-Q5: The business rules found in the Handbook for situation reports will enhance the situational awareness of partners collaborating on the IMISAS Experimentation site.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	1	0	0	7	8	0	16	0.0%	78.7%

Observation: Both OPT and Response Cell respondent surveys indicated nearly equal distributions of positive, negative, and neutral agreement regarding expectations that RFI/RFA business rules will improve the relevance of responsiveness to user requests. Regarding the degree of responsiveness provided by the business rules, the Response Cell provided mixed but generally neutral responses, while the OPT response was neutral tending somewhat toward agreement.

Period 2/4-Q7, RC5-Q7: Using the RFI/RFA business rules found in the Handbook at Annex E will improve the relevance of responses.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Response Cell	5	1	3	5	4	0	18	16.9%	16.9%
OPT	1	0	5	6	6	0	18	12.6%	26.4%
Composite	6	1	8	11	10	0	36	9.4%	17.6%

Period 2/4-Q6, RC5-Q6: Using the RFI/RFA business rules found in the Handbook at Annex E will provide a high degree of responsiveness to partner requests.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Response Cell	5	1	2	7	3	0	18	5.8%	5.8%
OPT	1	0	4	5	8	0	18	4.6%	64.1%
Composite	6	1	6	12	11	0	36	1.7%	29.1%

Observation: OPT responses were generally neutral, tending toward disagreement, with regard to the helpfulness of the document naming convention in locating specific data within a field of search results.

Post-Q10: The document naming convention implemented for the IMISAS Experiment site facilitates finding specific data within a field of search results.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	0	1	3	6	2	0	12	22.5%	2.0%

Observation: Open format survey responses during the Analytic Seminar event indicated that APAN's document location processes were confusing. One participant commented that the "miscellaneous" category in particular invited "lazy" storage practices and prevented rapid and easy identification as well as access to critical documents.

Observation: Open format survey responses suggested a set of business rules for message posting. Another recommendation advocated document handling rules contained in the *DOD Support to Foreign Humanitarian Assistance (FHA) Handbook for JTF Commanders and Below*.

Observation: The RFA/RFI tool was the most heavily used capability in the UISC tool suite during the last three experimentation periods, and observations indicate that significant effort was expended in ensuring requests were answered in the forum. The OPT Chief recognized the need to respond to requests from the external partners, but he and others also recognized the potential for information overload and the need to assign a team to manage the forum. Specific business rules designated by the OPT Chief were:

- The PAO should release information representing a command position but should not be otherwise involved.
- Information derivative to previously stated command positions should be exempt from PAO review.
- The team should verify and validate the information.
- RFI/RFAs should be routed to the appropriate subject matter experts and any other stakeholders identified.

Requests from the Department of State appeared to be handled via email rather than the RFI/RFA forum. The OPT Chief recognized the challenge inherent in sifting through the body of information transacted over the RFI/RFA tool, and cited the need for a tool to discern which entries were important. A non-DOD representative specifically cited the difficulty of gleaning pertinent information from the threads developed in the forum. While a USAFRICOM observer noted the need for some kind of tool for handling requests and gathering information from the broader base of partners, an OPT representative questioned the need for a new and dedicated process for this activity.

Findings: The magnitude of the information management challenges quickly became apparent as experiment play progressed and emphasized the need for business rules for use of the UISC tool suite. There is an apparent need for closer coupling of external partner equities to internal OPT processes. The RFA/RFI tool was a suggested methodology for achieving that close coupling and capturing reciprocal gains in the OPT's own situational awareness. The RFI/RFA tool, properly managed to ensure responsiveness and relevance of responses to partner needs, would seem to be a reasonable candidate for this function, both prior and subsequent to the "boots on ground" phase of operations. The business rules for use of the UISC will require updating or adaption to meet the needs each crisis.

Recommendations:

- The UISC must include business rules that allow for:
    - The rules to be derived for, trained on, and used by future warfighters.

- The adjudication, managing or moderating of site transactions, standardized naming conventions and other processes.
- Continual review to ensure both the warfighter and the mission partners' benefit from the information and collaboration on the UISC.

7.3. Business Rules for Data and Metadata Standards (Solution 3-1)

This solution proposed business rules to define data types, standards, and metadata requirements that facilitate posting, transfer and use of data (e.g., documents, blogs, and forums) through standardized content tags and search capabilities.

This solution was assessed during a technical spiral and the Analytic Seminar.

Observation: During the Analytic Seminar event, surveys responses by the UISC proxy system users were generally neutral, tending toward agreement, regarding the value of data tagging business rules to ensure the relevance of information found in searches and received by partners.

Site User-Q1: The data tagging business rules found in the Handbook will ensure the relevance of information retrieved by partners.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
APAN Users	0	0	4	7	6	3	20	1.6%	59.6%

Site User-Q3a: The data tagging business rules should significantly increase the amount of germane information found in searches.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
APAN Users	0	1	0	10	5	4	20	0.0%	59.6%

Observation: The OPT respondents found the UISC proxy system's data tagging function easy to use; a result consistent with the technical spirals.

Post-Q9: It was easy to tag documents that I posted to the IMISAS Experiment site.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	1	0	0	2	7	2	12	0.0%	99.4%

TS3: Tagging collaboration document was easy.								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	0	1	2	4	2	9	1.0%	90.1%

Observation: The extent of data tagging during the Analytic Seminar appeared uneven, at least temporally, although during the AAR meeting, the OPT felt that data tagging was one of the functions that performed well. Participants generally agreed on the positive value of data tags. A non-DOD representative attested to the utility of data tagging and aggregating data for a better understanding. Another representative stated that data tagging was the only way to sort and find information covering a wide-range of issues. The OPT suggested that individuals who post information should tag the information appropriately. Realizing that this may not always be done, one OPT representative suggested that a designated person should act as a screener to ensure that all the information is tagged. Another representative suggested that the United Nations Institute for Training and Research (UNITAR) Operational Satellite Applications Programme (UNOSAT) role player used tags for RFI/RFA responses, acknowledging the value of a standard data tagging framework, and sharing that the UN tagging convention was not always unified in its approach.

The most useful tags for crisis response operations, based on the APAN Users survey responses included the following:

Tag	Number of Responses
Logistics	16
Medical	16
Health	14
Refugees	14
Map	14
Infrastructure	13
Transportation	13
Imagery	13
Emergency Shelter	11
Water Sanitation Hygiene	11
Emergency Telecommunications	10
Protection	10
Camp Coordination	9
Camp Management	8
Nutrition	7
Utilities Electric	6
Video	4
Education	3
Utilities Fossil Fuel	3
Agriculture	2
Early Recovery	2

Findings: Correct tagging of information is of great importance to those researching information as a method of categorizing data, creating mappings among thematically related material, and ultimately supporting the construction of ontologies that enable organizations, however dissimilar in charter, to locate information hosted at partner sites. Lack of tagging greatly inhibits mission partners and internal personnel from finding relevant data. In particular, utilities such as Google search, that index the contents of a file, will not flag the file unless the keyword is present within the text, nor will it index non-textual files like .jpg images. Incorrect tagging will also inhibit efficient information searches. Using a standard tagging framework assists in both organizing information and making relevant information discoverable by both internal personnel and mission partners, including those cases where such discovery might not otherwise be possible.

Recommendation: The UISC must employ a robust tagging mechanism for all content, based upon a standard tag library, configurable at the group or site level at a minimum, and automatically available to every module or capability. Tagging must enable different organizations to locate information hosted at partner sites. Military training focused on standardized tagging practices must be provided.

7.4. Accommodating Disadvantaged Users (Solution 4-1)

This solution focused on the disadvantaged (low bandwidth/technology) users, by making automatic bandwidth recommendations in a restricted communications environment and redirecting mobile or low bandwidth device users to a site with limited rich content. This solution was evaluated only during the technical spirals.

This solution was assessed during one of the technical spirals.

Observations: A majority of respondents agreed the modified APAN system's (APAN Lite) capability had adequate functionality for use in crisis response operations.

TS5: The APAN Lite site I used today has adequte functionality for use in crisis response								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	1	0	2	2	2	7	2.8%	71.0%

Observation: A significant majority of the respondents agreed that the APAN Lite response time was adequate and that posting an image was easy using that capability.

TS5: The response time with the APAN Lite site was adequate.								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	1	0	1	3	2	7	2.8%	90.4%

TS5: It was easy to post the image to the APAN Lite site.								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	1	0	1	3	2	7	2.8%	90.4%

Observation: Nearly all the respondents agreed it was easy to access information from the RFI forum using the modified APAN system.

TS5: It was easy to access the information from RFI using APAN Lite.								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	0	0	1	2	4	7	0.0%	98.1%

Observation: The majority of respondents agreed they would be comfortable using the information posted to APAN Lite in a crisis response operation.

TS5: I would be comfortable using this information from the APAN Lite capability in a crisis response operation.								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	1	0	1	3	2	7	2.8%	90.4%

Observation: Respondents observed that the types of information they felt comfortable posting to the modified APAN site encompassed most of the normally shared types of unclassified information cited during the Analytic Seminar event.

Observation: Other testing done by the IMISAS team demonstrated capabilities using multiple browsers, operating systems, and mobile devices.

Observation: During the Process Documentation Event interview, a USAFRICOM participant noted that infrastructure limitations are frequently a key aspect of crisis response operations. For example, during the 2010 Haiti earthquake aftermath, a large proportion of initial field information came from locals using text capability on mobile devices.

Findings: The utility of a service supporting low bandwidth devices appear obvious, and the capability provided by the UISC proxy would seem to provide that utility.

Recommendations: A UISC must have disadvantaged/low-bandwidth rich content user service with the following support and features:

- The capability to search and join new groups/sites of interest
- The capability to work with the latest internet browsers and client operating systems
- Continuous review to ensure optimized speed and user experience
- The capability to post messages via short message service (SMS) and multimedia messaging service (MMS)

7.5. Graduated User Accounts (Solution 4-6)

This solution involved graduated user account permissions and procedures to facilitate allocating access to different levels of unclassified information based on trust. All users initially had "read only" access to the site and after being granted full-site membership, participants were able to post information as well.

This solution was assessed in the technical spirals and was discussed during the MPC, FPC and the Analytic Seminar.

Observations: During the MPC and the FPC, it was determined that the UISC proxy site for the experiment would be completely open for read-only access, but that an APAN account and IMISAS project site membership would be required to post information. It was also determined that a controlled access site would not be needed. This capability was reviewed during the technical spiral. Initially the participants did not have membership to the IMISAS project site, and it was shown that they were able to view the content but not post any information. They then requested site membership, and members were immediately able to post information to the site. The participants observed that it was easy to join groups/sites and post information. However, during the Analytic Seminar, participants repeatedly cited the need for a "fenced-off" area for unclassified documents in preparatory stages of release. During the Analytic Seminar, the OPT created such a group.

Findings: The use of a graduated user account capability was clearly stated and desired by the OPT members.

Recommendation: The mature UISC requires a multi-level access capability to work with DOD and non-DOD partners. Further investigation is needed on specific requirements for this capability.

7.6. Rapid User Account Registration (Solution 4-7)

This solution explored a revised, rapid user registration system during one technical spiral with the capability and capacity to support expansion of the UISC COI in crisis response situations. This capability was identified during the early stages of the project and a revised registration system was put in place and tested during a technical spiral.

This solution was examined during one of the technical spirals.

Observations: Participants strongly agreed about the appropriateness of information requested in the account registration process.

TS1: The user account registration process you used today asked appropriate questions.								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	0	1	1	11	1	14	0.1%	99.9%

Observation: Participants moderately disagreed that the account registration process required too much detail.

TS1: The user account registration process you used today required too much detail.								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	0	7	5	1	1	14	69.2%	0.8%

Observation: Participants generally agreed that it was easy to join the UISC proxy system. One participant commented on the helpfulness of the "forgotten password" feature.

TS1: It was easy to join the IMISAS Experimental Site which I was looking for.								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	0	2	2	9	1	14	0.8%	98.2%

Observation: During the course of the IMISAS project, the APAN administrators revised the account registration process to accommodate this solution.

Findings: The user account registration process was straightforward, asked appropriate questions requisite to access, and required minimal information.

Recommendation: The UISC must have a streamlined registration process to allow the maximum participation by non-DOD partners.

7.7. Pushing and Posting Data from Dynamic Sources (Solution 4-8)

This solution involved the capability to push or post aggregated data from dynamic sources such as Facebook and Twitter to mission partners, using business rules and procedures for pushing content to social media sources.

This solution was assessed during one of the technical spirals and in the Analytic Seminar.

Observation: Despite special considerations involved with publishing information to social media channels, there appeared to be general acceptance of the practice by military members for the purpose of collaboration with external partners.

Observation: The majority of survey responses during the Analytic Seminar agreed on the benefits of pushing HA/DR-related information to mission partners via social media streams, even when compared against the risk of inadvertent release of sensitive information and the necessary training and implementation costs.

Site User-Q4: The benefits of a concerted effort to "push" HA/DR related information to mission partners outweigh the risks of inadvertent release of potentially contentious or unvetted information.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
APAN Users	0	0	2	6	9	3	20	0.1%	94.3%

Site User-Q5: The benefits of a concerted effort to "push" HA/DR related information to mission partners outweigh the necessary implementation and training costs.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
APAN Users	0	1	1	7	7	4	20	0.1%	87.2%

Observation: The ease of transferring information between the UISC proxy system and Facebook received neutral evaluations during the Analytic Seminar, with one strongly negative response, while the same question posed during the technical spirals received more positive responses (with five positive responses and one "Strongly Disagree" response).

Post-Q8: It was easy to transfer information from the IMISAS Experimentation site to the social media site "Facebook".									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
OPT	6	1	0	5	0	0	12	4.7%	0.0%

TS3: Transferring information from the APAN portal; via a situation report blog post, to the social media site "Facebook" was easy.								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	1	0	3	4	1	9	1.0%	73.3%

Observation: Participant comments and survey responses indicated that these capabilities were not significantly used during the Analytic Seminar event. However, OPT members did provide valuable feedback on potential consequences of posting information to social media streams and the types of information they would expect to post during a crisis response operation. Potentially undesirable consequences included:

- Inadvertent release of internal USG documents and draft policy determinations
- Potential endangerment of U.S. personnel
- The potential for misinterpretation of the information (particularly the U.S. military's role) coupled with the inability to shape the message once released
- The ability for the mass media or the uninformed to add to the post and potentially misshape the perceived meaning or bury it in "chaff"

- The danger of projecting the appearance of working documents as official DOD/USG positions
- The potential for creating confusion regarding the degree of response support being provided by the USG
- The possible exacerbation of existing points of friction with public agencies or groups

The group conjectured that attaching caveats to the posted information may help mitigate these issues.

Observation: Respondents indicated that the types of information or files they envisioned posting to social media sites when working in a crisis response operation included:

- Any openly available information
- Status and update to information like supplies, roads, bridges and other critical infrastructure
- Locations of meeting, hospitals
- Information supporting evacuee operations and refugee camps or other assemblages of victims
- Links to other reports from other agencies
- Logistic sites
- Analyses of situations or host nation needs
- UN and OFDA situation reports
- Press releases
- Anticipated arrival time of resources
- Imagery and video from government and commercial sources
- Geodetic data such as vector overlays and point data
- Information best provided or exclusively provided by the community (i.e., crowd sourced information)

Further, the types of information posted to social media sites would depend upon the particulars of the crisis and the security situation in the region. Another concern was the time required for posts to appear, with some respondents citing delays of several hours, a latency which could render the information obsolete in a real-world situation.

Observation: One respondent commented that social media should not be the first information tool in crisis response operations. Others were even more restrictive in their outlook, recommending against the posting of USG documents in social media channels, other than those

vetted by the PAO. Two respondents pointed out that the pitfalls of posting to social media channels can be mitigated through the use of legal disclaimer statements such as "currently available information indicates…." , a common mechanism other organizations use to shape messages to broader groups over which they exercise no control.

Findings: The experimental audience stated clear benefits to pushing information to social media sites, particularly as part of the humanitarian assistance and disaster relief scenario.

Some concerns about posting of information to social media sites, including the potential:

- To confuse the public over DOD's role in crisis.
- For misinterpretation of information causing friction with mission partners.

Recommendations: The mature UISC requires the capability and associated procedures to push and post information to external social media sites in real-time. The use of common disclaimers should be considered as a means for message shaping and expectation management.

7.8. Capturing, Sorting, and Categorizing Information (Solution 4-9)

This solution involved the capability to capture, sort, categorize, and filter information in the public domain by capturing and sorting the content from social media sources. This solution was assessed in a technical spiral and the Analytic Seminar. Observations from the Process Documentation Event were also used to support the assessment.

Observations: A majority of the participants in the Analytic Seminar agreed that the benefits of receiving information from social media sources outweigh the risks and justify the management burden. However, there are certain inherent aspects to social media information that must be considered when using this information. Social media sites can assist the military in gaining information from mission partners that either choose not to collaborate with or would prefer not to be seen as collaborating with military organizations.

Site User-Q10: The benefits of subscribing to social media information streams from within the IMISAS Experiment site outweigh the risks.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
APAN Users	0	0	1	7	8	4	20	0.0%	94.3%

Site User-Q11: The value of information derived from social media streams justifies the work necessary to manage and assign reliability levels to the information.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
APAN Users	0	2	0	6	6	6	20	0.1%	94.3%

Observation: Analytic Seminar responses regarding the effectiveness of the demonstrated technical interface for pulling in social media streams were neutral, trending toward the negative.

Site User-Q13: The IMISAS Experiment site capability for presenting information from social media streams was effective.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
APAN Users	0	2	6	7	5	0	20	41.6%	5.1%

Observation: Analytic Seminar participants were asked to suggest social media or dynamic internet sites (beyond Facebook) which would be useful to link to the UISC proxy system in a crisis response operation. Responses included:

- Telecoms Without Borders, a body similar to Doctors Without Borders that stages in difficult areas in advance of the United Nations
- AllAfrica.com, a website having the broadest overarching news from Africa
- The websites of cell phone providers in Africa
- Other country-specific websites and applications
- The specific, crisis response UISC proxy established by the lead humanitarian agency in a crisis (most likely established by UN OCHA)
- SMS groups
- Local community sites
- ReliefWeb
- LinkedIn (for reaching NGO and other business leaders in affected areas)

Observation: Participants noted that information conduits for social media were situation dependent, and that users should avoid fixation on any particular vehicle.

Observation: Participants discussed the types of social media-derived information and files deemed useful to crisis response operations during the technical spirals. Responses included any information having geographic location or other relation to the mission; hints for responding to emergency situations; validated eyewitness information (i.e., photos, descriptions, or landmarks); infrastructure, injury, weather and security reports; locations of affected people; and status of infrastructure. Participants indicated that information posted to social media sites is probably not sufficient to perform mission analysis and planning, but it can help focus initial inquiries in order to gain verifiable information. Participants suggested establishing relationships with known entities, a network of trusted colleagues or noting the frequency of a given event being reported as ways to improve confidence in social media information sources.

Observation: During the Analytic Seminar, participants expressed concerns about committing scarce resources to act upon information derived from social media, given the sheer volume of that data. Several respondents stressed the need to cross-validate information among various sources, despite tendencies for social media information to converge on ground truth over time. One respondent noted that DOD may not be able to corroborate some social media derived information, and that risk management would be necessary in such cases. Two respondents cited the need for vetting social media derived information with trusted colleagues, and another suggested checking the frequency of similar information and the degree of information provided about the source.

Observation: Information considered not reliable by some OPT members (although not restricted in the subject survey question to social media) included locations, intent, mission updates, effects, numbers of affected persons, assertions of future political decisions or government commitments, non-substantiated assessments, and information having various sensitivities. On the other hand, another respondent to the same question pointed to the complementary nature of such information, noting that USAID and the United Nations (UN) each provide unique perspectives not standard within the DOD.

Observation: During a Process Documentation Event interview, a USAFRICOM member cited that using social media may fill a critical gap where the OPT "doesn't know what it doesn't know", thereby preventing commitment to a potentially untenable course of action.

Findings: Although several limitations of information gleaned from social media were discussed during the experiment, the Likert Scale questions clearly indicate that the information provided by this source is perceived as providing utility. As with information provided by USAID or the UN, it is information of notably different character than that traditionally acted upon by the military. However, in that very sense, it is mitigation against "groupthink". Information posted to social media sites is probably not sufficient to perform mission analysis and planning, but it can help focus initial inquiries in order to gain verifiable information. Given

that mechanisms can be put in place to vet and weight the information – efforts indicated by the OPT respondents as justified – it simply does not make sense to ignore it, especially given that capturing the information is a purely passive activity. Establishing relationships with known entities, using a network of trusted colleagues, or noting the frequency of a given event being reported are ways to improve confidence in social media information sources.

Recommendation: The mature UISC requires the capability to subscribe to "easy to read" social media feeds and generate alert notifications when external content is posted to the UISC.

7.9. Business Rules for Automatic Trust Center Capability (Solution 4-10)

This solution involved business rules to maximize an automatic trust center capability (e.g., rating, and a level of confidence). This solution was assessed during a technical spiral and observations were made during the Analytic Seminar that supported this assessment.

Observations: The automatic trust center used business rules to rate, recommend, and characterize confidence levels in data entered into APAN. The most accepted reliability mechanism for generating confidence level ratings was by far source identification attribution or knowing who or which organization authored the information. Other rating approaches, such as "Star" ratings and knowing the author's activities generated a moderate level of confidence. Knowing the author's favorites and email address did not provide much confidence in posted information.

Observation: During the technical spirals, a majority of respondents agreed it was easy to use APAN's "Star" rating feature.

TS2: I found the 'star' rating easy to use.								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	0	1	1	8	3	13	0.1%	99.9%

Observation: A majority of the respondents agreed that verification of an RFI answer was a useful UIS system capability.

TS2: The verification of an answer to a RFI/Question is a useful capability in unclassified								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	0	0	3	9	1	13	0.0%	99.2%

Observation: The level of trust in "Star" ratings was neutral or weak.

TS2: How trusting are you of 'star' ratings?								
							Confidence Level	
Survey Group	Not at all	Some-what trusting	Neutral	Very trusting	Always	Total	Disagree	Agree
Tech Spiral	1	4	7	1	0	13	35.3%	0.1%

Observation: OPT discussions indicated that on the RFA/RFI tool and social media streams, some mechanism for rating content is pointedly needed due to the potential for information overload and acting upon erroneous or incomplete information.

Findings: The ability to drill down into the information posters' background to include the author and organization is useful.

The "Star" rating, while easy to use, was not the most trusted capability for attaining source reliability and trustworthiness. Nonetheless, a mechanism for rating content is required.

Recommendation: The mature UISC requires a content rating capability that provides descriptions of how ratings are obtained, the number of ratings applied to content, and visibility into the profiles of content raters.

7.10. Source Authenticity and Reliability Rating (Solution 4-11)

This solution involved source authenticity and a reliable information capability for the UISC to use in filtering and verification of real-time social networking data. The source identification solution was not fully examined due to limited access to the "SwiftRiver" tool.

Finding: Data was collected for other technical solutions that referenced the need for a source reliability mechanism.

Recommendation: Although the source reliability and verification system concept is promising, further research is needed in this area.

7.11. UISC Search Capabilities (Solution 4-12)

This solution proposed involved searching across all UISC tools to include content and standard tags searches. This solution was assessed during a technical spiral and the Analytic Seminar.

Observations: During the Analytical Seminar, survey responses were mixed among members of the APAN Users Group regarding ease of use of APAN's search capability. During a very limited evaluation of the search capability in one technical spiral, the respondents agreed it was easy to use.

Site User-Q3b: The search capability on the IMISAS Experiment site was easy to use.									
	Number of Responses							Confidence Level	
Survey Group	Did not use	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
APAN Users	2	2	5	6	4	1	20	37.4%	9.4%

TS5: The search capability in APAN was easy to use.								
							Confidence Level	
Survey Group	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Disagree	Agree
Tech Spiral	0	0	0	4	2	6	0.0%	99.6%

Observation: During the Analytic Seminar event, there was little discussion about APAN's internal search function and no observed indications of Google searches in the UISC proxy system space. One participant criticized APAN's capability to search critical information as weak; however, another survey respondent noted acceptable results when searching for information on the UISC proxy system's blogs and posts.

Observation: A non-DOD representative observed that APAN did not appear to search substrings because a space is counted as an integral part of a tag. During the Analytic Seminar,

this limitation prevented one participant from finding a posted map and location information for a Pepsi Cola plant.

Findings: Guidelines, business rules and appropriate education concerning the search methods could enhance the use of the search capability.

No single search capability may be able to satisfy the requirements of an OPT or other organizations using a UISC. A search capability is critical to effective information sharing.

Searching capabilities were found to be easy to use during the technical spiral but were problematic during the Analytic Seminar. This was due to the inconsistency of tagging during the Analytic Seminar and lack of current APAN capability for partial or approximate queries when searching.

Recommendations: The mature UISC requires a robust capability. UISC search capabilities need to be capable of exact, approximate, and partial logic queries.

Appendix A – Binomial Significance Test

The number of responses to Likert Scale questions was insufficient in terms of evaluating statistical significance to meet the hypotheses for a parametric test such as a Student's T-test. Moreover, time constraints prevented gathering data in a standard control group approach that supported comparisons of results with and without applied treatments. To evaluate statistical significance of responses under these limitations, the Analysis Team used a binomial significance test, dividing the responses to each Likert Scale question (posed as positive statements) into two mutually exclusive binomial "success" and "failure" categories with respect to the question under consideration. If that question was whether there was significant agreement to the statement posed, then the "success" category encompassed the "Strongly Agree" and "Agree" responses, while the "failure" category encompassed the "Neither Agree nor Disagree", "Disagree" and "Strongly Disagree" responses. Likewise, if the question were taken as whether significant disagreement existed, then the "success" category corresponded to "Strongly Disagree" and "Disagree" responses while the "failure" category corresponded to "Neither Agree nor Disagree", "Agree", and "Strongly Agree" responses.

To facilitate evaluating significance of responses, the "control" or "baseline" for the question was based upon a notional random assignment of responses among the Likert Scale categories. With the success and failure categories thus defined, response data could be looked upon as a simple binomial experiment where evidence to reject a hypothesis of no significant agreement (or disagreement) would accrue with increasing unlikelihood that the results could have stemmed from random assignment of responses. As the construct is a binomial experiment by definition, the only underlying distribution assumed is binomial and the questionable results of assuming normality or applying a T-test with too few data points are avoided.

An example of applying the binomial statistical test (quoted from Devore[4]) follows:

- "~" means "distributed as":
- P([event]) signifies the probability of that event:
- Bin(n, p) refers to the binomial distribution based on n trials and success probability p: and
- B(s; n, p) denotes the binomial cumulative distribution function with the given parameters; that is, the probability of observing at most s successes in a binomial experiment of n trials having success probability p.

A certain type of automobile is known to sustain no visible damage 25% of the time in 10-mph crash tests. A modified bumper design has been proposed in an effort to increase this percentage. Let p denote the proportion of all 10-mph crashes with this new bumper that result

[4] (Devore, 1995, p. 308)

in no visible damage. The hypotheses to be tested are H_0: p = 0.25 (no improvement) versus H_a: p > .25. The test will be based on an experiment involving n = 20 independent crashes with no visible damage.

Test statistic: X = the number of crashes with no visible damage.

Rejection region: R_8 = {8, 9, 10, …, 19, 20}; that is, reject H_0 if $x \geq 8$, where x is the observed value of the test statistic.

This rejection is called upper-tailed because it consists only of large values of the test statistic.

When H_0 is true, X has a binomial probability distribution with n = 20 and p = 0.25. Thus,

α = *P(type I error) = P(H_0 is rejected when it is true)*

= *P($X \geq 8$ when $X \sim Bin(20, 0.25)$) = 1 – B(7; 20, 0.25)*

= *1 – 0.898 = 0.102.*

That is, when H_0 is actually true, roughly 10% of all experiments consisting of 20 crashes would result in H_0 being incorrectly rejected (a type I error).

Modifying the example for our Likert Scale responses, the probability p of observing agreement (or disagreement) in the notional "control" case would be 0.4, or the proportion of "Agree" and "Strongly Agree" (or "Disagree and "Strongly Disagree") responses that would result from an infinite number of random assignments of responses. Where the rejection region in the above example was selected as 8 or greater, we take our rejection region to be the number of observed agreements (or disagreements) or some greater number. This allows us to construct the following table for α, or 1 – B(s, n, 0.4), where "s" represents the number of agreements (or disagreements) and n represents the total number of responses.

Number of Trials (n)	Number of Successes (s)																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	0.400	0.000																		
2	0.640	0.160	0.000																	
3	0.784	0.352	0.064	0.000																
4	0.870	0.525	0.179	0.026	0.000															
5	0.922	0.663	0.317	0.087	0.010	0.000														
6	0.953	0.767	0.456	0.179	0.041	0.004	0.000													
7	0.972	0.841	0.580	0.290	0.096	0.019	0.002	0.000												
8	0.983	0.894	0.685	0.406	0.174	0.050	0.009	0.001	0.000											
9	0.990	0.929	0.768	0.517	0.267	0.099	0.025	0.004	0.000	0.000										
10	0.994	0.954	0.833	0.618	0.367	0.166	0.055	0.012	0.002	0.000	0.000									
11	0.996	0.970	0.881	0.704	0.467	0.247	0.099	0.029	0.006	0.001	0.000	0.000								
12	0.998	0.980	0.917	0.775	0.562	0.335	0.158	0.057	0.015	0.003	0.000	0.000	0.000							
13	0.999	0.987	0.942	0.831	0.647	0.426	0.229	0.098	0.032	0.008	0.001	0.000	0.000	0.000						
14	0.999	0.992	0.960	0.876	0.721	0.514	0.308	0.150	0.058	0.018	0.004	0.001	0.000	0.000	0.000					
15	1.000	0.995	0.973	0.909	0.783	0.597	0.390	0.213	0.095	0.034	0.009	0.002	0.000	0.000	0.000	0.000				
16	1.000	0.997	0.982	0.935	0.833	0.671	0.473	0.284	0.142	0.058	0.019	0.005	0.001	0.000	0.000	0.000	0.000			
17	1.000	0.998	0.988	0.954	0.874	0.736	0.552	0.359	0.199	0.092	0.035	0.011	0.003	0.000	0.000	0.000	0.000	0.000		
18	1.000	0.999	0.992	0.967	0.906	0.791	0.626	0.437	0.263	0.135	0.058	0.020	0.006	0.001	0.000	0.000	0.000	0.000	0.000	
19	1.000	0.999	0.995	0.977	0.930	0.837	0.692	0.512	0.333	0.186	0.088	0.035	0.012	0.003	0.001	0.000	0.000	0.000	0.000	0.000
20	1.000	0.999	0.996	0.984	0.949	0.874	0.750	0.584	0.404	0.245	0.128	0.057	0.021	0.006	0.002	0.000	0.000	0.000	0.000	0.000

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions Project (IMISAS)

Annex K - IMISAS Analytic Seminar (AS): DEU Human Factors Analysis (HFA)

IMISAS Analytic Seminar (AS): DEU Human Factors Analysis (HFA)

Version 1.1b
As of 22 August 2011

Authors:
LTC (GS) Soenke Marahrens, Airforce, Concept Developer and German FLO, JCS DD J7 JCW
Dr. Ulfert Rist, IABG, Ottobrunn, DEU IMISAS Lead Analyst
Corinna Semling, IABG, DEU IMISAS Analyst
Nikolaus Wlczek, IABG, DEU IMISAS Analyst

Point of Contact:
Dr. Ulfert Rist
DEU IMISAS Lead Analyst
IABG mbH
Competence Center – CC70
Systemic Analysis and Human Factors
Einsteinstr. 20
D-85521 Ottobrunn

Tel.: +49 - 89 – 6088 - 2885
Fax : +49 - 89 – 6088 - 2454
E-Mail: rist@iabg.de

Content

Acronyms **7**
Executive Summary **8**
Introduction **9**
IMISAS Problem Statement, Hypotheses, and Analytic Questions **10**
Human Factors Analysis (HFA) **10**
Data Sensors and Analysis Plan **12**
Motivation, Attitudes, and Information Sharing **12**
Analytic Approach **16**
Knowledge of Mission Partners **16**
Motivation of Mission Partners **20**
Cultural Differences of Mission Partners **23**
Coordination of and Collaboration with Mission Partners **23**
Policies of Mission Partners **25**
Procedures of Mission Partners **26**
Perceived Usefulness of the IMISAS Experimentation Site **27**
Information Sharing with Mission Partners **34**
Other Results and Findings **38**
Shared Situational Awareness (SSA) **42**
Mission partner´s network **42**
Quality of Information Exchange **47**
Assessing the Situational Picture by using Information Classes **50**
Summary of Human Factor Analysis **58**
Principles of cooperative information sharing **58**
Building shared situation awareness **59**
Cultural factors **60**
Motivation of Mission Partners **60**
Technical support for UIS and civil-military cooperation **61**
References **61**
Annexes **65**
Annex A: HF Survey Questions (SQ) **65**
Question – Period –Matrix **66**
Topic 1: Information Sharing (IS) **67**
Topic 2: Shared Situation Awareness (SSA) **72**
Annex B: HF Interviews **74**
Annex B.1: Motivation Interview **74**
Annex B.2: MCSSA Interview **82**
Annex C: Survey Questions on UIS Handbook **88**
Annex D: HFA Template for Observations of Communications **91**
Annex E: DEU Analytic Hierarchy for Motivation, Attitudes, and IS **92**
Annex F: IMISAS Solutions and HFA **98**
Annex F.1 IMISAS Solutions **98**
Annex F.2: HFA and IMISAS solutions **99**
Annex G: HFA Data **102**
Annex G.1: Motivation, Attitudes, and Information Sharing **102**

Annex G.2: Shared Situational Awareness 186
Annex H: Discussion of High-Level, Experimental Hypotheses 187
High-Level, Experimental Hypothesis 1 187
High-Level, Experimental Hypothesis 2 188
High-Level, Experimental Hypothesis 3 188
Analytic Break-Down 189

Table of Figures

Figure 1: Stations of Action Organization 11
Figure 2: Communication, coordination, and cooperation 14
Figure 3: TAM 1 15
Figure 4: TAM 2 16
Figure 5: Knowledge of Own Task 19
Figure 6: Satisfaction with own Work 23
Figure 7: Fast, stable, and technically mature aspects of site 27
Figure 8: Usefulness of Information 30
Figure 9: Relevance of Information 30
Figure 10: Completeness of Information 31
Figure 11: Reliability of Information 32
Figure 12: Trustworthiness of Mission Partners 35
Figure 13: Give-and-take Basis 38
Figure 14: Effectiveness of that Collaboration via the RFI/RFA 39
Figure 15: RFI/RFA Business Rules are easy to use 40
Figure 16: Business Rules and SA (OPT) 41
Figure 17: I experienced disruptions in coordination between my mission partners and my own organization. 48
Figure 18: Our mission partners provided all their information that was relevant for my organization's mission. 49
Figure 19: Our mission partners provided us with significant amounts of information that was not relevant for our mission 49
Figure 20: Occasionally my mission partners confused me due to their method of sharing information. 50
Figure 21: Despite the time shift between operational days I maintained an understanding of the operational situation. 51
Figure 22: Concept of Information Classes 52
Figure 23: SSA Chart; n=8 54
Figure 24: SSA Chart Clipping of Situational Cue 1 55
Figure 25: SSA Chart Clipping of Situational Cue 3 55
Figure 26: SSA Chart Clipping of Situational Cue 2 56
Figure 27: SSA Chart Clipping of Situational Cue 4 56
Figure 28: SSA Chart Clipping of Situational Cue 5 57
Figure 29: Influence Diagram H1 187
Figure 30: Influence Diagram H2 188
Figure 31: Influence Diagram H3 189

Acronyms

AOR	Area of Responsibility
AOI	Area of Interest
AQ	Analytic Question
AS	Analytic Seminar
AWG	Analytic Wargame
DoC	Department of Commerce
DoD	Department of Defense
EoE	End of Experiment
HBQ	UIS Handbook Question
HF	Human Factors
HFA	Human Factors Analysis
HLH	High-level Hypothesis
IMISAS	Interagency and Multinational Information Sharing Architecture and Solutions
IQ	Interview Question
IS	Information Sharing
MCSSA	Multilevel Comprehensive Shared Situational Awareness
OODA	Observe, Orientate, Decide, Act
OPT	Operational Planning Team
PAO	Public Affairs Officer
POLAD	Political Advisor
RC	Response Cell
RFA	Request for Assistance
RFI	Request for Information
SQ	Survey Question
SOP	Standing Operating Procedure
SSA	Shared Situational Awareness
UIS	Unclassified Information Sharing
UISC	Unclassified Information Sharing Capability
USEUCOM	United States European Command
WH	Work Hypothesis

Executive Summary

DEU Human Factors Analysis (HFA) highlighted two fields of interest in support of the USA Analysis:

The investigation of motivation and attitudes towards Information Sharing (IS) can be summarized by two significant findings.

- Analytic Seminar (AS) participants where highly motivated to interact (to coordinate and to collaborate) with their mission partners in order to respond to a given crisis situation according to mission objectives. They mostly agreed that a balanced give-and-take-basis of shared documents and information were given. AS participants also appeared to be highly motivated in order to fulfill their tasks in order to achieve mission objectives.
- The IMISAS Experimentation site[1] needs to be optimized regarding velocity, stability, technical maturity, and ergonomics. Especially, from the viewpoint of perceived usefulness of this information sharing mechanism the quality of information (usefulness, relevance, completeness, and reliability) appears to be a key factor which was not really given. Perceived usefulness of the IMISAS Experimentation site also lacked of sufficient access to information. Therefore, an information exchange site has to offer all modern software capabilities. Otherwise users will get back and use their own software applications on the web.

The investigation of Shared Situation Awareness (SSA) can be summarized by two significant findings.

- The need for a common operational picture was limited. But the analysis of goal awareness on the OPT level and situational picture of the DEU response cell shows that basic and original information from the ground is important for being aware of the ongoing situation on a higher echelon.
- Especially between civilian and military partners teambuilding processes in the OPT are necessary to build a so called team or partners mental model of common roles, responsibilities and shared objectives. This cognitive structure builds the underlying structure for developing SSA. This significant process of sharing knowledge might be part of interagency exercises or pre-deployment trainings but it might be more realistic to integrate teambuilding as a part of common working procedures “on the job”.

[1] The APAN software has been taken as an example for realization of functional requirements. Here, as an Information Sharing mechanism it is denoted as IMISAS Experimentation site.

Introduction

The US invited Germany to provide an analytic look at Human Factors (HF) in order to complement the USA analysis as a multinational IMISAS partner in a pragmatic way: „Products resulting from this effort will include a handbook and policy, doctrine and technical enhancement recommendations.“[2]

The main objective of Information Sharing (IS) from the viewpoint of the consumer (e.g., military user) is being described as follows: „The objective of the Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) project is to improve information sharing between the United States (U.S.) Department of Defense (DOD) and a wide variety of non-military mission partners, who may include civilian U.S. government agencies, other nations, inter-governmental organizations, and nongovernmental organizations.”[3]

Therefore, the scope of the US CD&E project/IMISAS Analytic Seminar (formerly designated as wargame) is being defined as follows: „The wargame will examine a set of proposed solutions designed to improve unclassified information sharing between the U.S. Department of Defense and a wide variety of non-military partners, who may include civilian U.S. government agencies, other nations, inter-governmental organizations, and nongovernmental organizations. The primary focus of the event is on staff policy, process, and procedures to enable effective unclassified information sharing across organizational, security, and to a limited extent, network domain boundaries.“[4]

The IMISAS AS is “focused on planning and coordinating USAFRICOM support to a notional multinational, civilian-led humanitarian assistance and disaster relief operation in Central Africa.“ It “will be an unclassified event consisting of an introductory scene-setter and two separate scenario vignettes. The vignettes provide context for examining IMISAS solutions dealing with unclassified information sharing among mission partners. The vignettes would direct the seminar participants to address a specific information-sharing challenge using the proposed solutions. Participants may also anticipate opportunities for discovering other unanticipated solutions during the course of the wargame.”[5]

Heaps of data have been collected during the IMISAS AS by data collectors, analysts, and observers. This report has been worked out within two weeks because of given conditions of the DEU IMISAS supporting project. From the viewpoint of DEU HF analysis, the given data and related possible insights appear most valuable and are worth to be looked at in a more intensified manner for all intents and purposes in order to detect more complex and subtle aspects of UIS.

[2] [Smith 2011].
[3] [IMISAS ED 2011], p. 4.
[4] [IMISAS AWG Overwiew 2011].
[5] [IMISAS AWG Overview 2011].

IMISAS Problem Statement, Hypotheses, and Analytic Questions

In order to explain HFA in the context of the IMISAS project, a brief presentation of the IMISAS problem statement and related hypotheses will be given. IMISAS is intended to generate pragmatic insights for the optimization of future Information Sharing: „The approach will include an assessment of current capabilities and on-going activities (such as the OSD NII Information Sharing Implementation Plan, Multi-National and other Mission Partner (MNMP) C2 Information Sharing Capability Definition Package (CDP), and the Unclassified Information Sharing Capability) being developed to allow real-time information sharing and collaboration across domains with a range of partners.“ [Smith 2011]
The IMISAS problem statement ([IMISAS ED 2011], p. 1) describes a capability gap which is being used to derive solution oriented hypotheses and analytic questions:

> Combatant Commands (COCOMs) lack a coherent framework / capability to share information and collaborate across multiple domains with a broad range of mission partners (government / interagency, multi-national, multi-lateral & private sector) due primarily to restrictive policies, conflicting authorities, ad hoc / non-existent procedures, business rules and non-interoperable networks and systems.

This problem statement allows to derive “high-level, experimental hypotheses“, and broken-down analytic questions [IMISAS ED 2011]. In Annex H an analytic discussion of these high-level hypotheses is prepared for interested readers.

Human Factors Analysis (HFA)

The general objective of Human Factors Analysis (HFA) is observing the impact of work and organizational design on human performance and well-being. Here, HFA is based on the so called psychological 'action organisation theory' of Prof. Dietrich Dörner[6] (see figure below, following [Dörner 2007]). It offers an empirically well-founded approach to the explanation of human behaviour, errors and fallacies in complex crisis environments. The empirical approach is usually implemented through different methods of data collection, such as participatory observation, survey study, content analysis and interviews.

[6] See [Bresinsky et al. 2008], [Dörner 2007] pp. 67 f., see also [Kannheiser 1992].

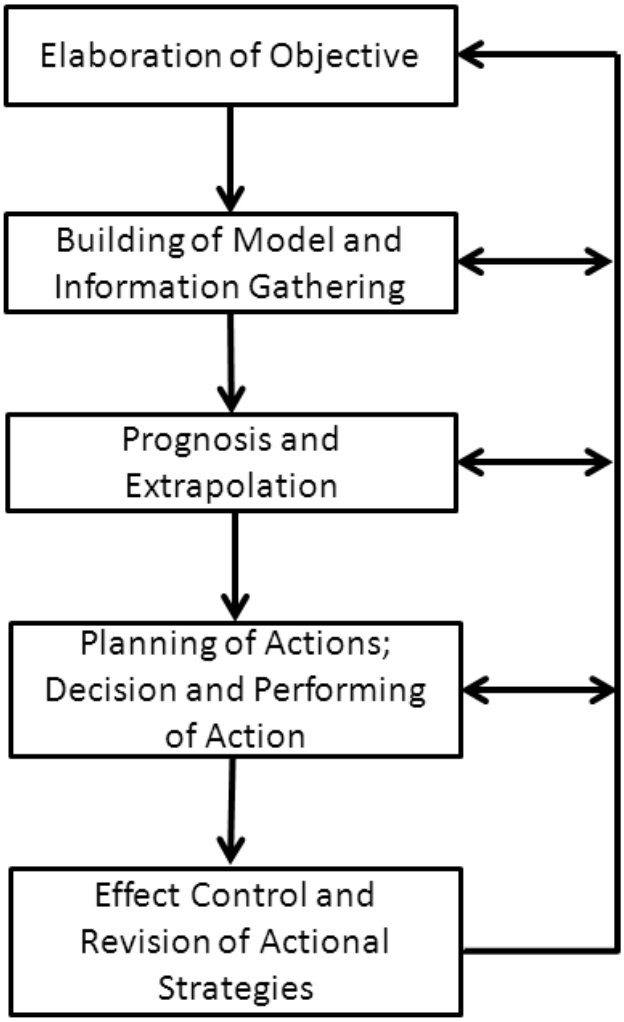


Figure 1: Stations of Action Organization

Each of these action stations has effects on motivation, like e.g., a sound elaboration of group and mission objectives (see section on motivation of mission partners below). Action stations can easily be related to military management processes such as to John Boyd's OODA loop ([Bresinsky et al. 2008]).

From the HFA perspective there are two research issues mostly applicable to IMISAS, understanding that it will not be the main analysis effort:

(1) exploring the impact of motivation and attitudes towards civil-military / interagency cooperation on information sharing requirements using web-based platforms/tools, and

(2) building and developing intra-group and inter-organizational shared situational awareness (SSA).

Following [Badke-Schaub et al. 2008a], the general Idea regarding human factors science can be described in the following manner: "Human factors science or human factors technologies is a multidisciplinary field incorporating contributions from psychology, engineering, industrial design, statistics, operations research and anthropometry. It is a term that covers:

- The science of understanding the properties of human capability (Human Factors Science).
- The application of this understanding to the design, development and deployment of systems and services (Human Factors Engineering).
- The art of ensuring successful application of Human Factors Engineering to a program (sometimes referred to as Human Factors Integration). It can also be called ergonomics."[7]

Accordingly, [Badke-Schaub et al. 2008a] define Human Factors as "all physical, psychological and social characteristics of humans, if they influence the acting in or with socio-technical systems or are influenced by them."[8]

DEU HFA covers many implications and findings to parts of the high-level, experimental hypotheses H1 to H3 in Annex H (e.g., situational understanding of responders in H1, information accessibility of an HA /DR response in H3). In terms of a complementary view regarding limited resources and given conditions, the intended contribution to USA analysis can be seen as realized.

Data Sensors and Analysis Plan

Before AS, HFA employed the following methods/tools, tailored to the specific conditions at the respective locations (coordinated with the USA experiment lead):

- Incorporation of a limited number of HFA specific items into the USA surveys (see Annex A);
- Administering additional HFA questionnaires, if required and appropriate (see Annex B);
- Conducting limited individual interviews with selected representatives of the experiment audience outside AWG period execution hours;
- Participation in experiment control meetings (incl. the provision of immediate HFA feedback);
- Development of survey questions on the UIS handbook on request (Annex C)
- HFA Observation template for quick notices (see Annex D);
- Evaluation of written AS material (e.g., JOT observations, ACO chats, OPT briefings).

According to given settings of the Analytic Seminar and to the USA DCAP[9], and due to the schedule, time restrictions and planning by the contractor, the range of DEU analysis (wording of questions, number of survey questions, frequency of survey questions, possibility to conduct interviews, possibility to administer questionnaires) had to be adjusted/downsized several times.

Motivation, Attitudes, and Information Sharing

The key point regarding Information Sharing (IS) using the web-based IMISAS experimentation site[10] from the viewpoint of HF is that certain mental states and dynamics –

[7] [WP HF 2011].
[8] Translated by the author.
[9] [IMISAS ED 2011].
[10] Functionally realized and demonstrated with APAN.

human factors – influence related technical and social activities with effects on collaboration and cooperation: “In general, a human factor is a physical or cognitive property of an individual or social behavior which is specific to humans and influences functioning of technological systems as well as human-environment equilibriums.”[11]

Therefore, if Information Sharing (IS) is being looked at as communicative act with its social implications, then the involved humans and their mindset have to be looked at in detail, focusing on conditions which have an impact on quality and quantity of Information Sharing: “In social interactions, the use of the term human factor stresses the social properties unique to characteristic of humans.”[12] Accordingly, the following explanation of HFA highlights two major components: “User Analysis, where data about the users, and their current and future environments, is collected, and Usability Testing which measures the effectiveness of users who complete tasks in current and future environments.”[13]

Regarding technical capabilities of the communication tool of interest (IMISAS Experimentation site), procedures (e.g., SOP) and policies of organizations, these humans are related to, have to be considered in terms of conditions for IS.

According to [Badke-Schaub 2008], group phenomena have to be considered in comprehensive contexts of situational requirements, attributes of humans, attributes of the group(s), attributes of processes, and in work results. Group members who struggle for a common objective, will seek for information in the beginning and whenever needed. Information exchange between group members needs communication acts. Communication is essential in order to transform information to coordinated activities, and to initiate cooperative activities. Objectives of groups or teams should be in concordance with objectives and needs of group members. The following figure shows main factors of a structural model as foundation for common activity in the context of Information Sharing (IS).[14]

[11] [WP HF 2011].
[12] [WP HF 2011].
[13] Internet: http://it.toolbox.com/blogs/enterprise-solutions/human-factors-analysis-18818, seen 11 August 2011.
[14] Following [Badke-Schaub 2008].

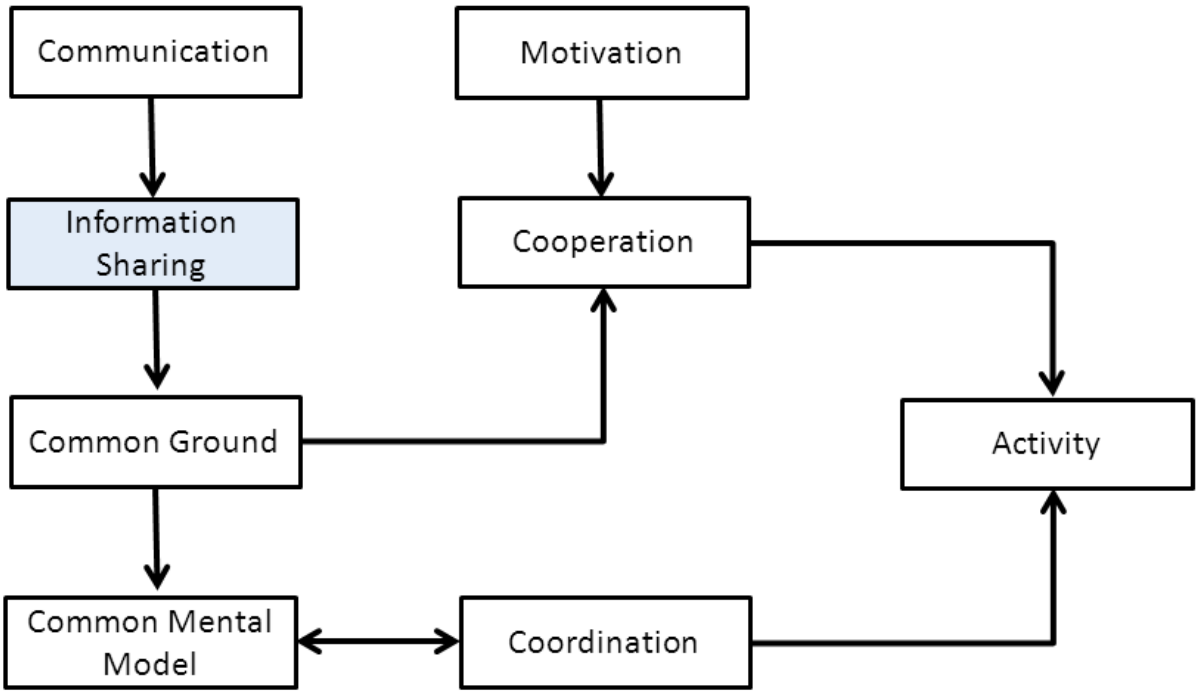


Figure 2: Communication, coordination, and cooperation

To establish a common understanding within a group the elaboration of a shared frame of reference or common ground can be used as precondition. In the case of information sharing of group members a shared understanding will be the result, evoking a common mental model. Now communication is necessary to continuously keep all group members and the common mental model up to date.[15]

Information Sharing will occur with certain quality and quantity in order to achieve certain objectives. Consequently, conditions of motivation, cooperation and coordination have to be considered in order to foster the understanding of their reversed impact on information sharing, the related IMISAS solutions and the UIS Handbook. E.g., external conditions are given by technical and functional capabilities of the IMISAS experimentation site, relational internal conditions by procedures, policies, organizational cultures, and the organizational structure of a future UIS cell. From the viewpoint of the IMISAS project, pragmatic learning is intended regarding these conditions: „The focus of the effort will include development of processes, procedures and policy and technical enhancement recommendations to enable effective information sharing and collaboration across organizational and security boundaries. Procedural and technical enhancement recommendations will be validated during field experimentation with US Africa Command, US European Command[16], and multiple non-DOD mission partners.“ [Smith 2011]

---

[15] See [Badke-Schaub 2008].

[16] “The United States European Command [USEUCOM] primary mission in support of NATO is to provide combat-ready forces to support U.S. commitments to the NATO alliance. Although planning for NATO conflict is first priority at USEUCOM, consideration is also given to unilateral and multilateral contingency planning. This includes providing forces to other unified command, and ranges from humanitarian relief to support of friendly governments with supplies. The area of responsibility (AOR) of the United States European Command includes 51 countries and territories. This territory extends from the North Cape of Norway, through the waters of the Baltic and Mediterranean seas, most of Europe, and parts of the Middle East. Prior to the formation of Africa Command in October 2008 the

Following [Badke-Schaub et al. 2008a], Human Factors Analysis (HFA) can be applied to individuals, groups, and organizations. Besides technical aspects, HFA can cross-sectionally be related to e.g., cultural phenomena (e.g., language barriers), to phenomena which arise from policies of involved communication partners, and to procedural phenomena.

A closer look has to be taken at the perceived usefulness of the experimented Information Sharing mechanism, the IMISAS Experimentation site. Therefore, coming from communication science and looking at acceptance of information, related factors like usefulness and relevance of information are extremely important for mission partners. Regarding limited resources in a crisis situation, like time, full technical acceptance has to be given. The so-called "Technology Acceptance Model" (TAM) aims at analyzing related factors: "Computer systems cannot improve organizational performance if they aren't used. […] To better predict, explain, and increase user acceptance, we need to better understand why people accept or reject computers. This research addresses the ability to predict peoples' computer acceptance from a measure of their intentions, and the ability to explain their intentions in terms of their attitudes, subjective norms, perceived usefulness, perceived ease of use, and related variables." [Davis et al. 1989] The following figure depicts the TAM.[17] Perceived usefulness covers the perceived usefulness of available information and perceived ease of use.

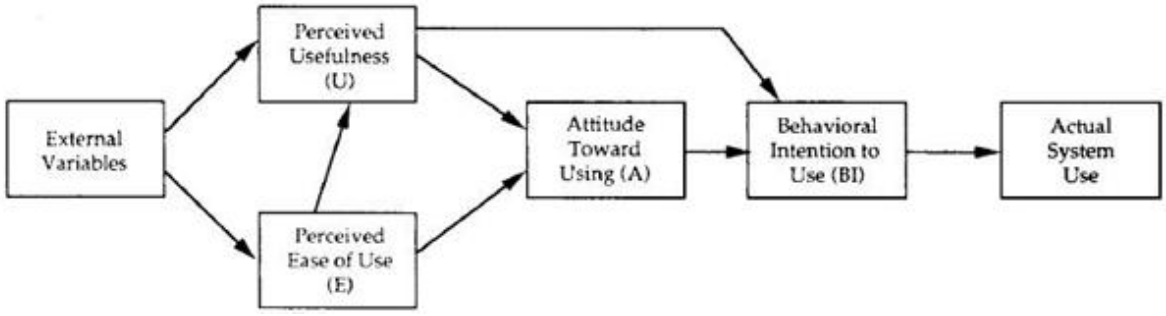


Figure 3: TAM 1

[Venkatesh/Davis 2000] elaborated the TAM towards an extended model, TAM 2: "The present research develops and tests a theoretical extension of the Technology Acceptance Model (TAM) that explains perceived usefulness and usage intentions in terms of social influence and cognitive instrumental processes. […] Both social influence processes (subjective norm, voluntariness, and image) and cognitive instrumental processes (job relevance, output quality, result demonstrability, and perceived ease of use) significantly influenced user acceptance. These findings advance theory and contribute to the foundation for future research aimed at improving our understanding of user adoption behavior." Output quality (degree to which an individual believes that the system performs his or her job tasks well[18])

---

area of responsibility (AOR) of the United States European Command covered more than 13 million square miles and included 91 countries and territories. This territory extends from the North Cape of Norway, through the waters of the Baltic and Mediterranean seas, most of Europe, parts of the Middle East, to the Cape of Good Hope in South Africa. Several other countries and territories were considered to be part of the USEUCOM area of interest (AOI)." (Internet: http://www.globalsecurity.org/military/agency/dod/eucom.htm, seen 10 August 2011)

[17] Internet: http://www.vvenkatesh.com/it/IT%20Images/tam.gif, seen 20 August 2011.

[18] Internet: http://www.vvenkatesh.com/it/organizations/Theoretical_Models.asp#Con=structdefs, seen 20 August 2011.

appears as influencing factor for perceived usefulness. Therefore, related information quality is a key factor. The following figure depicts TAM 2 ([Venkatesh/Davis 2000]):

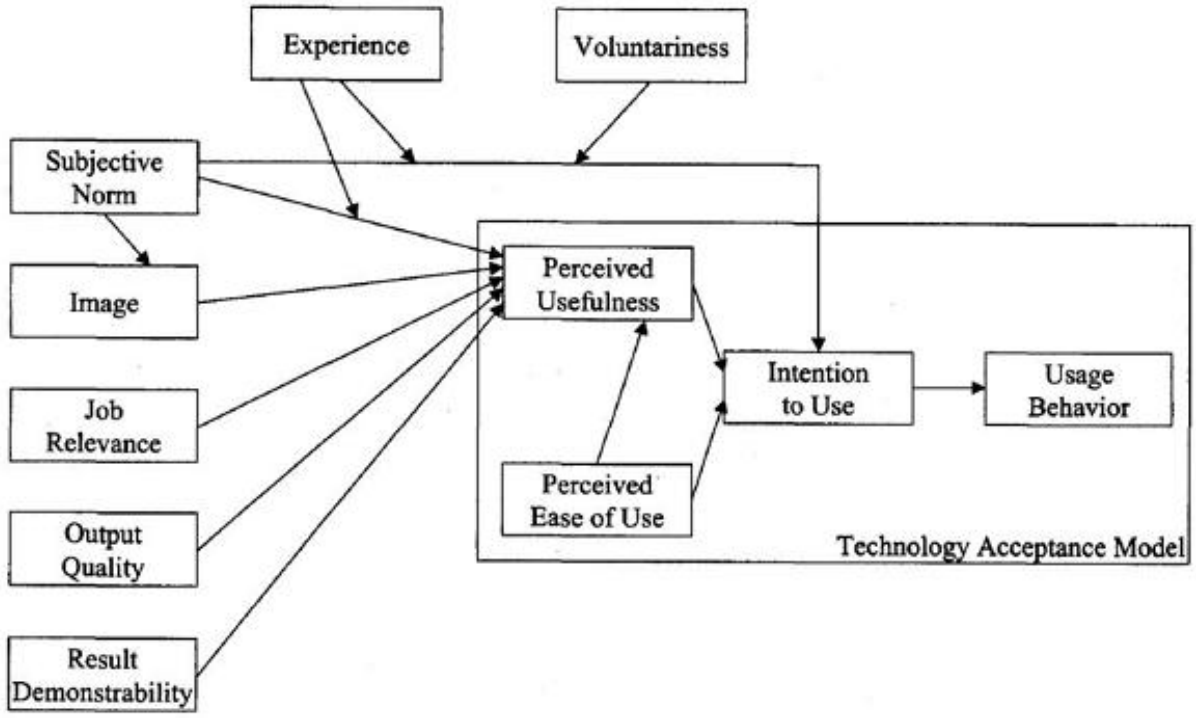


Figure 4: TAM 2

As can be seen in the figure above the perceived ease of use has impact on perceived usefulness. This issue will be considered when looking at capabilities of the IMISAS Experimentation site.

Analytic Approach

An analytic hierarchy of HF statements and questions has been derived from the referenced theoretical background (see Annex E). Due to aggregation level and restrictions of resources only numbered questions were intended and allowed for surveys (e.g., “SQ01”) or interviews (e.g., ”IQ01”).

A HF high-level hypothesis (HLH) served as starting point[19] of analysis:

Changes of motivation cause changes in quality and quantity of Information Sharing, coordination, and cooperation in the group of mission partners, which result in a change of achievement of objectives.

This HLH has been broken down systematically in the direction of survey questions and interview questions (see Annex E: DEU Analytic Hierarchy for Motivation, Attitudes, and IS).

The table in Annex F.2 (HFA and IMISAS solutions) shows links of HF questions to IMISAS solutions and issues of interest with regard to contents.

Knowledge of Mission Partners

[19] Interpretation of [Badke-Schaub 2008].

It is essential and indispensable for success under collaborative conditions that mission partners have sufficient knowledge on the mission, mission objectives, and their own tasks.

AS mission partners have been asked about knowledge on their assigned role and tasking for the AS:[20] OPT came up with clear answers on the role ("Dep OPT Lead Planner", "OPT Lead", "Deputy OPT", "J2 rep", "J4 logistics", "J35", "EUCOM Public Affairs representative", "Foreign disclosure officer", "INFORMATION SECURITY OFFICER", "J6/Communications and Information Planner", "Knowledge Management Officer") with given/implicit/hidden conception about associated tasking on one hand, and with vague descriptions (e.g., "Still trying to figure that out - J5 role not clear.", "??? Great Questions... Create dialogue I guess", "legal advisor, should issues of a legal nature arise. So far, just functioning as a joint planner, as no real legal issues have come up.") on the other hand.
More AS mission partners have been asked about their assigned role and tasking:[21]

- OPT Stuttgart:
  - "I am responsible for providing public affairs guidance and recommendations on what can / should be put in the public domain."
  - "Develop security guidance and procedures for the information to be shared."
  - „Operational planning team leader"
  - I provide a DOC perspective + champion DOC equities in the command; I also outreach to public and private non-federal entities for partnerships."
- RC Stuttgart:
  - "Representing the NATO Civil-Military Fusion Center (CFC) to simulate real-world support to a HA / DR mission."
  - "I am seeded by ACAPS to OCHA to coordinate a provide technical support to humanitarian assessments."
  - "Respond on behalf of WHO Headquarters Communications."
  - "Project - assistant ACAPS - development of situation reports in first 72 hours after a crisis."
  - "mapping and satellite imagery analysis for UN partners and NGOs"
- RC Ottobrunn:
  - "Roleplayer BW Ops J9"
  - "J Med is the senior medical officer and med advisor of Com MONUSCO"
  - "As GIZ we conduct long-term development projects."
  - "Provide civilian knowledge / skills to the scenario, represent the capabilities / agenda of a NGO"
  - "Coordination of DEU activities / invitation to an emerg. Coord. Meeting in Goma"
  - "Playing J9 of an UN force with all the duties and responsibilities as a CIMIC guy e.g. civil situation, assessment, J9-Staff work."

According to the experiment manning list and associated roles, most of the AS role players/mission partners appeared to be clear about their assigned roles and tasks; others had to find out by communication with their leaders. To be clear: Just telling a role will not automatically include a job description, especially in an experimental environment where future tasks are being performed.

[20] SQ12: "What is your assigned role and tasking for the Analytic Seminar?" (see table in Annex G.1.1, SQ12)
[21] IQ01: "Describe your activities and your area of responsibility." (see tables in Annex G.1.2, IQ01)

Knowledge on Mission Objectives

Knowledge of mission objectives is indispensable for a successful break down of tasks at tactical level and related individual acting.

AS mission partners have been asked about their contribution to mission partners in order to achieve their mission objectives:[22]

- OPT Stuttgart:
  - „Limited. More focused on advising our team.“
  - „Develop a security classification“
  - „Develop an coordinated US military response to the HAIPR event“
  - “This experiment is great for that as this is one of the issues the J9 in AFRICOM is trying to determine; I believe one of my mission contributions can be to help the command out much to useful info partners and work in concert with them in selected areas. However this has proven difficult in HA / DR situations. In fact there may be no role for my office J9 to play in these situations - I am trying to formulate this.”
- RC Ottobrunn:
  - „Injects according MSEL“
  - „Capacity building and strengthening of good gov as a prediction for long term stabilization.“
  - NGO capable to provide tents / engineering skills
  - “I try to coordinate DEU (gov + ngo) activities by bringing them on the table”
  - “Advise on expertise "how-to"”

Differences between civilian and military participants have been observed: "DART member states difference between civ/mil: Military prefers to know simply what the mission is (and will accomplish) whereas Civilian entities tend to prescribe to requirements details, such as specific number of trucks that can be provided." [IMISAS AS JOT 2011]

Obviously, contribution to mission partners has been perceived as understanding of own role, not as relational specification of an own task.

Knowledge on Own Tasks

The understanding of a task depends on given conditions like job description, but also on interpretation of things that have to be done in direction of organizational objectives and mission objectives.[23] The evaluation of own work depends on how clear the conditions, the task, and objectives have been given in order to support orientation and feedback sections of the stations of action organization following [Dörner 2007].

---

[22] IQ02: “What is your contribution to mission partners in order to achieve their mission objectives?” (see tables in Annex G1.1.2, IQ02).

[23] "OPT Chief explained to the OPT members that he wants them to push the envelope on sharing information and don`t get hung up on products. He explained that currently, the military over-classifies and we need to find ways to share more information. This was primarily a pep talk to get the team focused upon the reason for being here which is to find better ways to share information with mission partners." [IMISAS AS JOT 2011]

Most of the AS mission partners only sometimes agree that they know exactly what to do and how to do it in order to achieve mission objectives.[24]

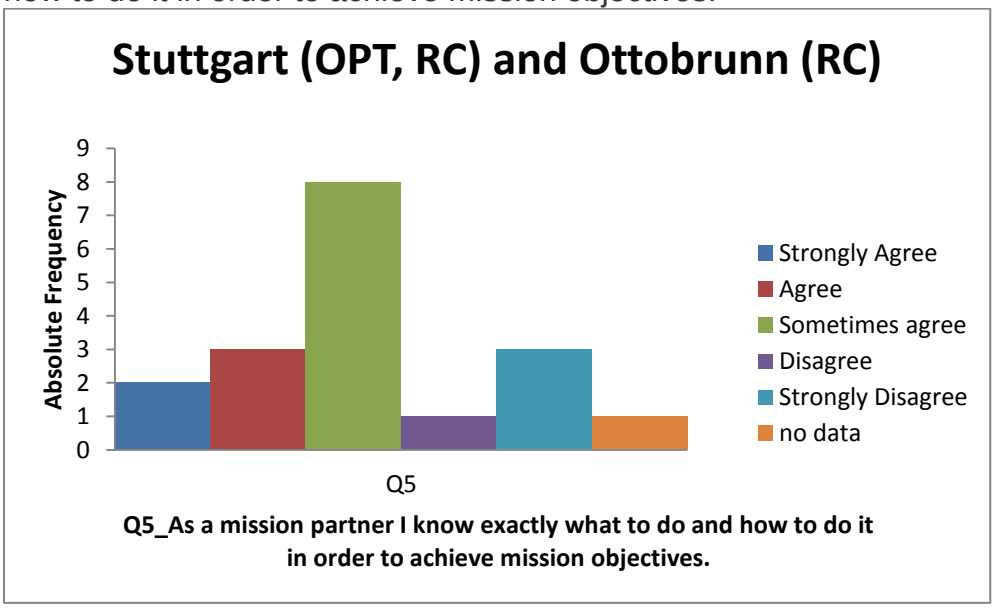


Figure 5: Knowledge of Own Task

The following statements have been given:

- OPT Stuttgart:
  - „In my lane, yes; overall could be more clear."
  - "Initial … are always nebulous - as the project moves forward is goals"
  - "We are still learning"
  - "no training on the military planning process has hampered my ability to know when and how to effectively contribute."
- RC Stuttgart:
  - "The CFC's role is clear and will do it to best of own ability."
  - "CFC main aim is to facilitate information sharing."
  - "It is not my objective to achieve someone else's mission objectives"
- RC Ottobrunn:
  - "It seems to me that the mission is a one way mission, Information sharing is rarely observed."
  - „As a NGO I'm following my own agenda."

Perception and Evaluation of Work of Mission Partners

AS mission partners are not being seen to work very hard in order to achieve mission objectives.[25]

[24] IQ05: "As a mission partner I know exactly what to do and how to do it in order to achieve mission objectives." (see figures in Annex G.1.2, IQ05)
[25] IQ06: "My mission partners always work hard in order to achieve mission objectives." (see figures in Annex G.1.2, IQ06)

On the contrary from an own perspective, mission partners strongly believe to always work hard in order to achieve mission objectives.[26] AS mission partners stated the following reasons:[27]

- OPT Stuttgart:
  - "To the extent they are in my lane and clear"
  - "conflicting goal and priorities can skew mission objectives"
  - "I often feel disheartened by the process but never disengaged."
- RC Ottobrunn:
  - „Information were pasted but no answer at all from the audience but the US response cell"

Motivation of Mission Partners

Motivation can be seen as relational category that drives certain issues in the field of information sharing, e.g., willingness to coordinate and to collaborate with mission partners, and to use communication tools like the IMISAS Experimentation site.

Motivation research has a long scientific history in psychology. Therefore, in scientific literature, a number of motivational theories exist: "Expectancy theory, need theories, equity theory and goal-setting theory are each different interpretations within motivation. Expectancy theory suggests that high levels of motivation occur when employees believe they can get the task done, believe they are capable of performing at high levels, and desire the outcomes. For example, pay or bonuses can be a desired outcome. Several need theories exist, but all of these theories have a common definition. Managers must determine the needs of their employees within an organization. They are responsible for ensuring that people receive outcomes to satisfy needs when performing at high levels. Equity theory suggests that managers promote high levels of motivation by ensuring people believe in the outcomes. For example, salaries are distributed in proportion to inputs, such as time and effort. Goal-setting theory suggests that specific and difficult goals lead to high motivation and success."[28] Most AS mission partners have the perception to be acting on specific goals.[29]

AS mission partners strongly agree to believe to be capable of performing at high levels. [30]

Most AS mission partners strongly have the perception to be acting on difficult goals.[31]

In order to cover different aspects of views on the concept of motivation, in this supportive study survey questions (SQ), interview questions (IQ), and UIS handbook questions (HBQ) have been derived from different motivation theories in a trans-disciplinary way which aims at pragmatic but theory-based insights and solutions.

---

[26] IQ07: "As a mission partner I always work hard in order to achieve mission objectives." (see figures in Annex G.1.2, IQ07)

[27] IQ07.2: "As a mission partner I always work hard in order to achieve mission objectives." (see figures in Annex G.1.2, IQ07)

[28] Internet: http://www.ehow.com/about_5387352_definition-employee-motivation.html, seen 2011-07-31.

[29] IQ10: *"As a mission partner I act on specific goals."* (see figures in Annex G.1.2, IQ10)

[30] IQ14: "As a mission partner I believe I am capable of performing at high levels." (see figures in Annex G.1.2, IQ14)

[31] IQ11: *"As a mission partner I act on difficult goals."* (see figures in Annex G.1.2, IQ11)

Following [Dörner 1998], “behavioral tendencies result of unspecific motivations, knowledge about the current surrounding (situational picture), knowledge about reality, and knowledge on possibilities on how to act in reality.”[32] Therefore, a closer look at motivation regarding certain aspects of interaction of participants of the IMISAS Analytic Seminar (AS) with mission partners (role players in the IMISAS AS) will support understanding of contextual aspects of the willingness of participants to engage in comprehensive Information Sharing. “Behavior is directed by intentions, wishes, motives, objectives, and performances. That what a person wishes, or is willing, or decides to do, regulates his or her behavior. Thus, the knowledge of own objectives and motives serves as a relevant ingredient of regulation of behavior.”[33]
For example, empirical studies show that there are two kinds of leakage of motivation[34]:

- *Social loafing*: less readiness/willingness if own contribution is not visible (see survey question SQ14 in Annex G.1.1, and result on this section 5.2.5 below)
- *Diffusion of responsibility*: lower individual take-over of responsibility if there are many other individuals present who are capable of acting (see survey question SQ15 in Annex G.1.1, and result on this section 5.2.5 below)

[Badke-Schaub 2008] describes two motivators for group members:

- If a group member recognizes own objectives in the commonly defined objective, it will share his or her abilities and knowledge with the group. The underlying motivation in this case is motivation for competence and control. Otherwise, if the common objective is not visible to a group member, motivation will decrease
- The need for affiliation can be described as a need for social contact, precisely for signals of legitimacy. The group member acts as information deliverer and reflection organ for the group in order to optimize the acting of the group.

“Motivated employees always look for better ways to do a job. Motivated employees are more quality oriented. Motivated workers are more productive.”[35] Accordingly, „In the motivation equation, input, performance and outcome are key factors that contribute to high motivation. Inputs are anything an employee contributes to the job or organization, such as time, effort, education and experience. Outcomes are anything an employee gets from a job or organization, such as pay, job security and benefits. Organizations hire based on inputs. High performance levels contribute to the organization's efficiency, effectiveness and overall goals. Managers use outcomes to motivate people to contribute inputs.“ [36] “Jones and George list direction of behavior, effort and persistence as key components toward motivation. The behavior that a person chooses is direction of behavior. Effort measures how hard an

[32] Translated by the author.
[33] [Dörner 1998], translated by the author.
[34] [Badke-Schaub 2008].
[35] Internet: http://en.wikipedia.org/wiki/Motivation, seen 2011-07-31.
[36] Internet: http://www.ehow.com/about_5387352_definition-employee-motivation.html, seen 2011-07-31.

employee works. Persistence occurs when an employee continues trying in the face of difficulties, instead of giving up." [37]

Most AS mission partners believe that mission partners always continue trying in the face of difficulties, instead of giving up.[38]
From an own perspective, most AS mission partners always strongly continue trying in the face of difficulties, instead of giving up.[39] Mission partners had the following insights:[40]

- OPT Stuttgart;
  - "If I give up the mission could fail"
  - "This question directly assesses internal fortitude"
  - "However I am concerned that this trying should ultimately end up as a helpful thing rather than an non-helpful one"
- RC Stuttgart:
  - "CFC understands complexities of Civil-Military Interaction as not all partners are "willing or able" to share information and / or work together."
  - "It depends on the cost effectiveness of continuing"
- RC Ottobrunn:
  - "Which mission objectives? I as a NGO, following own agenda /objectives might be different from "mission objectives""

Most AS mission partners strongly agreed to always look for better ways to do a job.[41]
Most AS mission partners strongly agreed to believe that they can get their job done.[42]

AS mission partners mostly really desire the results of their work in the mission.[43]

Regarding the perceived satisfaction with own results of work the following chart came up:[44]

[37] Internet: http://www.ehow.com/about_5387352_definition-employee-motivation.html, seen 2011-07-31.
[38] IQ08: "My mission partners always continue trying in the face of difficulties, instead of giving up." (see figures in Annex G.1.2, IQ08)
[39] IQ09.1: "As a mission partner I always continue trying in the face of difficulties, instead of giving up" (see figures in Annex G.1.2, IQ09.1)
[40] IQ09.2: "Please comment" (see tables in Annex G.1.2, IQ09.2)
[41] IQ12: "As a mission partner I always look for better ways to do a job." (see figures in Annex G.1.2, IQ12)
[42] IQ13: "As a mission partner I believe that I can get my job done." (see figures in Annex G.1.2, IQ13)
[43] IQ15: "As a mission partner I desire the results of my work in the mission." (see figures in Annex G.1.2, IQ15)
[44] IQ16: "As a mission partner the results of my work in the mission give me full satisfaction." (see figures in Annex G.1.2, IQ16)

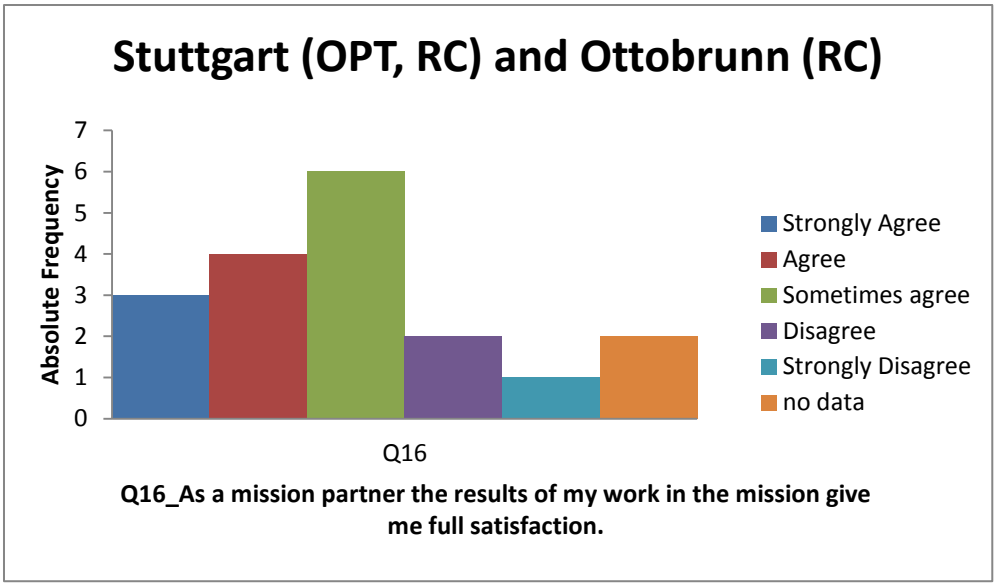


Figure 6: Satisfaction with own Work

In a very impressive way AS mission partners indicated to agree and strongly agree to fully support the mission objectives.[45]

Finding: AS mission partners appeared to be highly motivated to fulfill their tasks in order to achieve mission objectives. They were not fully satisfied by results of their work.

Cultural Differences of Mission Partners

Differences between civil-military, organizational, national, and other cultures can lead to misunderstanding and misconception, and may block intercultural relations within staffs and organizations. Therefore, the related cultural bound understanding of language was a main subject when the OPT started their work.[46]
Following [Badke-Schaub et al. 2008a], cultural phenomena can be divided into geographic cultural (e.g., national) and organizational cultural (e.g., civil and military, governmental, non-governmental) affiliation. Cultural phenomena also cover lingual, ethic, and regarding factors which aim at cognition, emotion, and behavior.

From start of the OPT work during IMISAS AS civil participants complained about special military terms, abbreviations, and acronyms they could not understand. Civil-military cooperation often suffers from different technical terminology and regarding mindsets.

Coordination of and Collaboration with Mission Partners

[45] IQ04: “As a mission partner I fully support the mission objectives.” (see figures in Annex G.1.2, IQ04)
[46] "group discusses and underlines that civ, mil, gov are talking completeley different languages; proposal to implement a lexicon for common understanding of terms for mission partners. E.G. the acronym "RFI" would not be accaptable in the civil world" [IMISAS AS JOT 2011]

Following [Badke-Schaub 2008], coordination of humans and processes, like the gathering of knowledge, experience, and competence, will be conducted by explicit communication of group members. In most cases, an active lead for initiation and control of leading processes will be needed, especially for risky and time-critical actions. Therefore, successful groups develop additional implicit (indirect, diplomatic) coordination mechanisms.

Most members of OPT and RCs clearly indicated that they fully support coordination with their mission partners.[47]

Following [Badke-Schaub 2008], regarding the group dynamics of Tuckmann (1965), efficient cooperation cannot be conducted before the group phases forming, storming, norming and performing have been run through. Good cooperation covers assistance and mutual aid, and it implies mutual appreciation and a minimal level of trust.

Group dynamics have been observed when OPT started working. First, the group had to learn about own abilities and functional roles: "Role players openly discuss face to face how to organize themselves - try to develop and establish guidelines/understanding for own role play" [IMISAS AS JOT 2011]

Cooperation of mission partners has been double checked in the interview questionnaire: In general, most members of OPT and RCs stated that they strongly agree to fully support cooperation with their mission partners. [48] [49] A slight tendency can be observed that civilian mission partners are perceived more supportive than military mission partners.

Regarding the Comprehensive Approach, OPT members clearly agreed and strongly agreed that their support of civil-military cooperation is important.[50]

Especially regarding interagency cooperation, OPT members very clearly and strongly agreed that they believe that interagency cooperation is important.[51]

Two de-motivators according to [Badke-Schaub 2008] have been tested (see section on motivation in 5.2.3 above):

- Social loafing and effort of mission partners: Many OPT members agreed that mission partners tend to slowly decrease their effort when they cannot identify their own contributions on the IMISAS Experimentation site, whether some of them were not sure about that.[52] This issue has to be considered in the course of optimizing an information sharing site.
- Diffusion of responsibility of mission partners: Most of the OPT members neither agreed nor disagreed that mission partners take less responsibility when there are other capable mission partners present in a collaborative situation (e.g. ACO, chat), and many agreed

[47] IQ26: "As a mission partner I fully support coordination with my mission partners." (see figures in Annex G.1.2, IQ26)
[48] IQ03: "As a mission partner I fully support cooperation with my (civ, civ-ngv, civ-gov…) mission partners." (see figures in Annex G.1.2, IQ03)
[49] IQ27: "As a mission partner I fully support cooperation my with mission partners." (see figures in Annex G.1.2, IQ27)
[50] SQ08: "My support of civil-military cooperation is important." (see figure in Annex G.1.1, SQ08)
[51] SQ09: "I believe that interagency cooperation is important." (see figure in Annex G.1.1, SQ09)
[52] SQ14: "Mission partners tend to slowly decrease their effort when they cannot identify their own contributions on the IMISAS Experimentation site." (see figure in Annex G.1.1, SQ14)

or disagreed. There was no A clear tendency on this issue and therefore cannot be observed.[53]

Finding: The willingness to cooperate with mission partners is not critical for OPT.

Policies of Mission Partners

Following [Badke-Schaub et al. 2008a] policies can be seen also as result of cultural factors. On individual level of acting humans and organizational bodies these factors are more or less operative. It has to be critically examined in which way policies are being formulated and to what extent they are being realized.
Accordingly, "A policy is typically described as a principle or rule to guide decisions and achieve rational outcome(s). The term is not normally used to denote what is actually done, this is normally referred to as either procedure or protocol. Whereas a policy will contain the 'what' and the 'why', procedures or protocols contain the 'what', the 'how', the 'where', and the 'when'. Policies are generally adopted by the Board of or senior governance body within an organisation whereas procedures or protocols would be developed and adopted by senior executive officers. A Policy can be considered as a "Statement of Intent" or a "Commitment". For that reason at least, we can be held accountable for our "Policy". The term may apply to government, private sector organizations and groups, and individuals. Presidential executive orders, corporate privacy policies, and parliamentary rules of order are all examples of policy. Policy differs from rules or law. While law can compel or prohibit behaviors (e.g. a law requiring the payment of taxes on income), policy merely guides actions toward those that are most likely to achieve a desired outcome.
[…] Policies can be understood as political, management, financial, and administrative mechanisms arranged to reach explicit goals."[54]
Mission partners mostly agreed and strongly agreed that they would provide every required unclassified information to their mission partners.[55]

Furthermore, AS mission partners declared:[56]

- OPT:
  - "There is no requirement for this at EUCOM."
- RC Stuttgart:
  - "Some sensitive info is not released if they can damage the organization. This would be reviewed by PAO / POLAD prior to release."
- RC Ottobrunn:
  - " Depends on quality of information."

It is clear that policy conditions always have some influence on the communication of members of organizations regarding other organizations. Here, no special constraint

[53] SQ15: "Mission partners take less responsibility when there are other capable mission partners present in a collaborative situation (e.g. ACO, chat)." (see figure in Annex G.1.1, SQ15)

[54] Internet: http://encyclopedia.thefreedictionary.com/Policy, seen 04 July 2011.
[55] IQ25: "My policy allows that I provide every required unclassified information to my mission partners." (see figures in Annex G.1.2, IQ25).
[56] IG25.8: „Please comment" (see tables in Annex G.1.2, IQ25.8).

of policy on Information Sharing can be observed, may be as a result of internalized policy in the course of organizational socialization.

Procedures of Mission Partners

Procedures support the handling of certain recurrent situations: “A set of established forms or methods for conducting the affairs of an organized body such as a business, club, or government.”[57] Procedures reflect policies and cultural phenomena. Non-observance of given procedures will normally be sanctified. Military Standing Operating Procedures (SOPs) in special are “[…] a set of fixed instructions or steps for carrying out usually routine operations.”[58]

Having asked AS mission partners, the provision of unclassified information to mission partners appears not to be a problem (of procedures) – most of them strongly agreed.[59] Of course, the military partners tend to be more restrictive at this point (ibd.). This has a tremendous effect on the mechanism of Information Sharing which should be working on a balanced give-and-take basis. Otherwise mission partners will become disappointed over time with related negative effect on motivation.

Processes of UIS appear to have to be adjusted to processes and procedures of regular general staff work:

- "A little stress and confusion of what can be posted to APAN without going through processes and procedures and gaining approval. Generally, it was determined that if it is already out in the public or has been passed to OPT via open source, then it can be posted to APAN without further approval." [IMISAS AS JOT 2011]
- "discussion on pricipal planning styles and procedures. differences between military and gov" [IMISAS AS JOT 2011]
- "usage of powerpoint and group discussion for planning appears to be ineffective to civ group member: "planning goes to the slides, not to reality"" [IMISAS AS JOT 2011]
- "The USAID and Commerce rep are using their own seperate process for vetting information for posting, but not interested in the handbook." [IMISAS AS JOT 2011]

Furthermore, AS mission partners declared:[60]

- OPT:
  - “Regardless of who the partner is - certain aspects of CUI cannot be shared without a specific need to know.”
  - “The process is still unclear and not the same from COCOM to COCOM.”[61]
  - “Not sure what you mean by required.”
- RC Ottobrunn:
  - “To be honest, NGOs don't have classification on their information, they decide case by case.”
  - “Working CIMIC is working open source!”

[57] Internet: http://www.thefreedictionary.com/procedure, seen 04 July 2011.
[58] Internet: http://universalium.academic.ru/201893/standard_operating_procedure, seen 04 July 2011.
[59] IQ24: “My procedures (e.g., SOPs) allow that I provide every required unclassified information to my mission partners.” (see figures in Annex G.1.2, IQ24).
[60] IG24.8: „Please comment“ (see tables in Annex G.1.2, IQ24.8).
[61] Unreadable statement has been interpreteted here by the author.

Processes and procedures were a point of discussion as OPT examined structures of a future UIS Cell (see section 5.2.10.3 below).

Perceived Usefulness of the IMISAS Experimentation Site

The APAN software has been taken as an example for realization of functional requirements. It is denoted as IMISAS Experimentation site.

Software Capabilities and Ergonomic Aspects

Following [Badke-Schaub et al. 2008a], ergonomic requirements are being formulated from the German Institute for Standardization[62] in the following three dimensions:

- Compatibility related to abilities of humans
- Compatibility related to expectations of the user (conformity of expectations)
- Compatibility related to tasks (appropriateness of tasks)

Therefore, regarding survey questions on ergonomics and usability of the IMISAS Experimentation site have been developed. AS mission partners have been asked on speed, stability, and technical maturity of the IMISAS Experimentation site:[63]

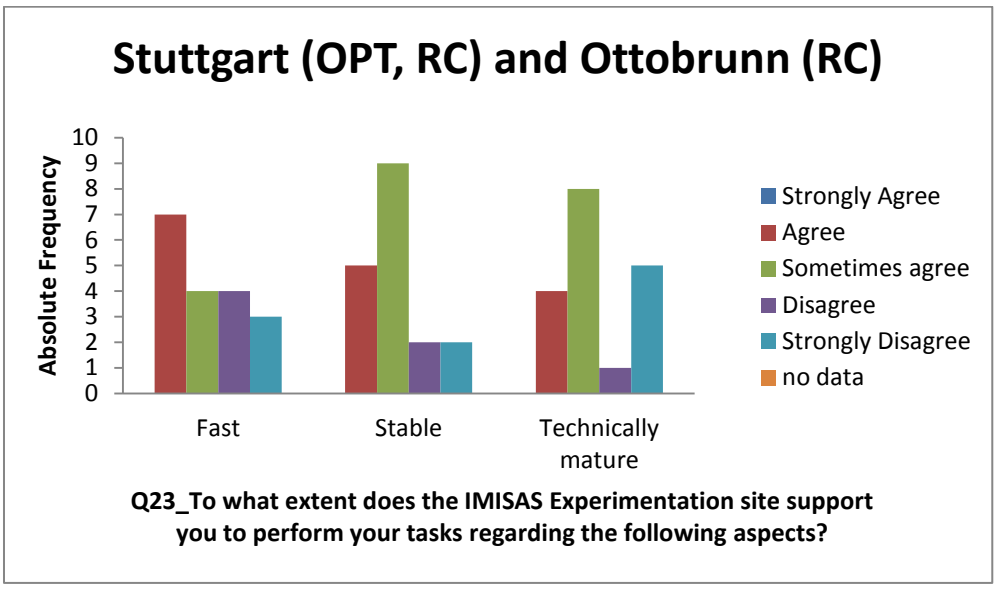


Figure 7: Fast, stable, and technically mature aspects of site

[62] (DIN EN 894-1, 1997). "DIN, the German Institute for Standardization, offers stakeholders a platform for the development of standards as a service to industry, the state and society as a whole. A registered non-profit association, DIN has been based in Berlin since 1917. DIN's primary task is to work closely with its stakeholders to develop consensus-based standards that meet market requirements. Some 26,000 experts contribute their skills and experience to the standardization process. By agreement with the German Federal Government, DIN is the acknowledged national standards body that represents German interests in European and international standards organizations. Ninety percent of the standards work now carried out by DIN is international in nature." (Internet: http://www.din.de/cmd?level=tpl-bereich&menuid=47566&cmsareaid=47566&languageid=en, seen 14 August 2011)

[63] IQ23: ""To what extent does the IMISAS Experimentation site support you to perform your tasks regarding the following aspects?" (see figures in Annex G.1.2, IQ23)

Several times the bandwidth was a point of discussion: "Discussion of how best to communicate with mission partners revealed that many would prefer to use DSL to establish the UISC. Actually, a person's home, hotel room, or commercial coffee shop would provide easier information sharing than the firewalls and NIPRNet. Consideration should be given to using DSL for the UISC." [IMISAS AS JOT 2011]

The IMISAS Experimentation site needs to be optimized regarding velocity, stability, and technical maturity.

Usage of Software Features

Some features of the IMISAS Experimentation site have been used mostly during the AS. According to cooperation with the USA analysis team question SQ11 has been re-engineered like follows:

> Please select the five features/functionalities of the IMISAS Experimentation site that you used the most in order to perform your tasks during this experiment period. (If you used less than five of the features/functionalities, please select those you did use.)
>
> □ Did not use any functions of the IMISAS Experimentation Site
> □ Situation Report (SITREPs) Blog
> □ Files and Imagery – Media Galleries
> □ Map View User of Defined Operational Picture (UDOP)
> □ Forum
> □ Group Chat
> □ Help Function
> □ Email
> □ One to One Chat
> □ Document Collaboration Wiki
> □ Group Activity Log
> □ Adobe Connect Online (ACO)
> □ Quick Launch Links ("Start here")
> □ Social Media Feeds
> □ Search
> □ Weather
> □ Group Members Listing
> □ Validity and Rating of Information Posted on UIS Sites
> □ Access, Permissions and Graduated Access

According to scenario period 2 to 5, the following features have been mostly used:[64]

(x) = competitive items

	P2	P3	P4	P5

[64] See figures in Annex G.1.1, SQ11.

Did not use any functions				
Questions…[65]		x	x	x
Situation Report (SITREPs) Blog	x	(x)	x	(x)
Files and Imagery – Media Galleries	x	x	x	x
Map View User of Defined Operational Picture (UDOP)				
Forum	x	(x)		
Group Chat		(x)		x
Help Function				
Email	x		x	
One to One Chat			x	(x)
Document Collaboration Wiki				
Group Activity Log				x
Adobe Connect Online (ACO)	x	(x)		
Quick Launch Links (“Start here”)				
Social Media Feeds				
Search				
Weather				
Group Members Listing				
Validity and Rating of Information Posted on UIS Sites				
Access, Permissions and Graduated Access				

Not surprisingly, “Files and Imagery – Media Galleries”, “Situation Report (SITREPs) Blog”, and “Questions” are the features of most interest. Therefore, a powerful retrieval functionality should be implemented in order to increase the quality of busy user’s found information.

Quality of Shared Information

The concept of quality of information is being modeled according to the Technical Acceptance Model (TAM, see above in section 5.2.1) with the following factors:

Usefulness of Information: Most members of OPT and RCs had the impression to only sometimes get useful information from mission partners, but many agreed to get useful information.[66]

[65] This category appeared without notification to the DEU analysis time at period 3.
[66] IQ19: “My mission partners provide useful information to me.”(see figures in Annex G.1.2, IQ19)

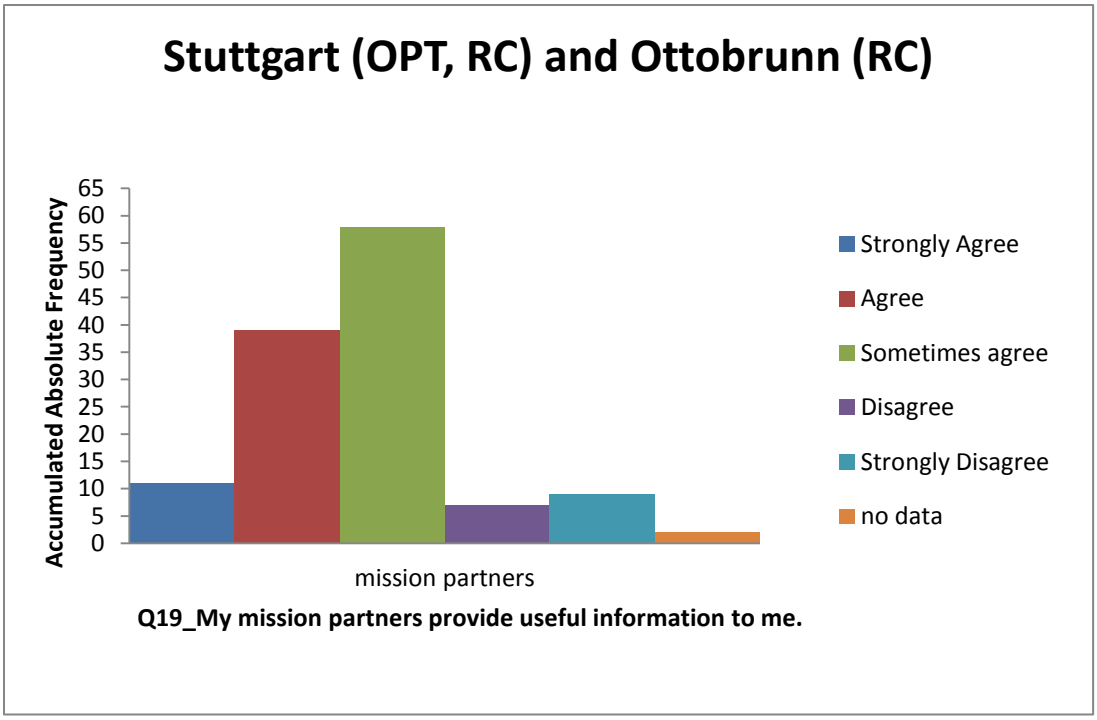


Figure 8: Usefulness of Information

Relevance of Information: Most members of OPT and RCs had the impression to only sometimes get relevant information from mission partners, but many agreed to get relevant information.[67]

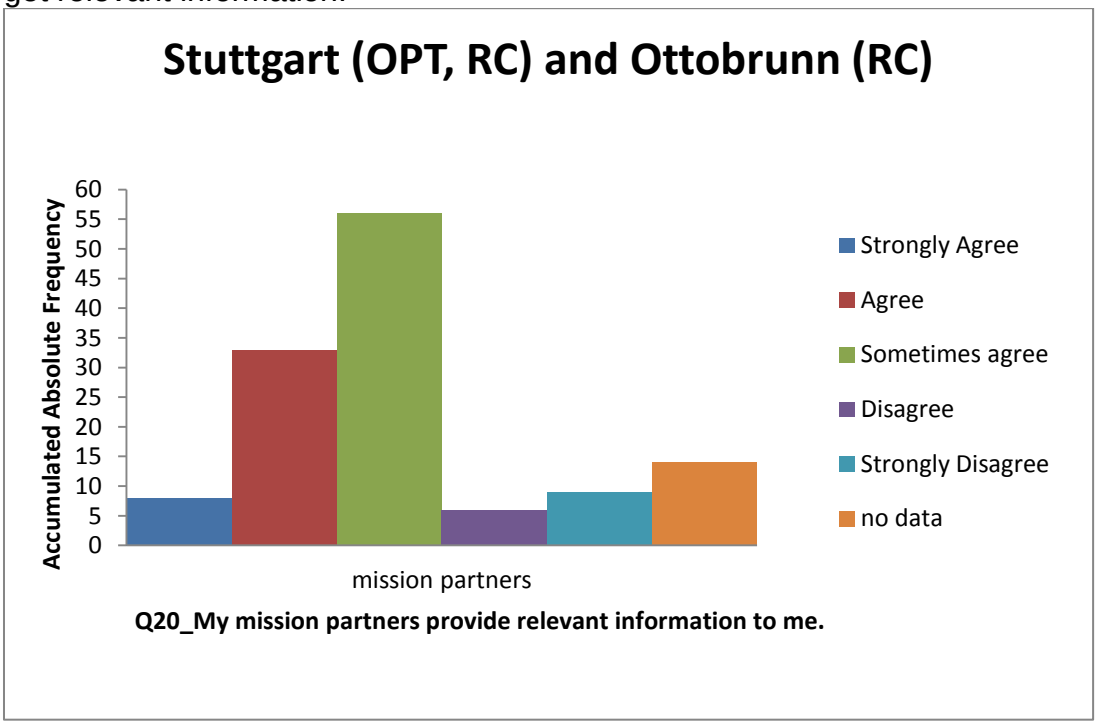


Figure 9: Relevance of Information

[67] IQ20: "My mission partners provide relevant information to me." (see figures in Annex G.1.2, IQ20)

Completeness of Information: Most members of OPT and RCs had the impression to only sometimes get complete information from mission partners, many disagreed to get complete information.[68]

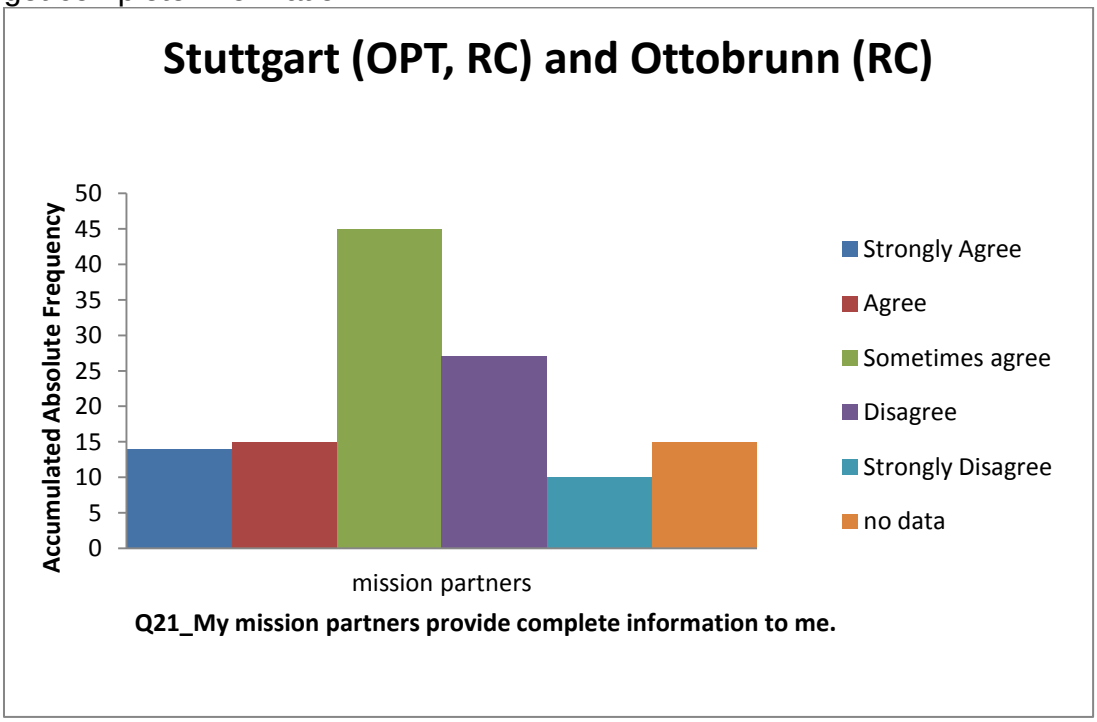


Figure 10: Completeness of Information

Reliability of information: Most OPT members agreed – with a slight tendency to disagree – that information from their mission partners is reliable.[69] When looking at all AS mission partners, most members of OPT and RCs only for sometimes agree that mission partners provide reliable information to them, see figure below.[70] A rating system for reliability of provided information of mission partners can be a step forward at this critical point.

[68] IQ21: "My mission partners provide complete information to me." (see figures in Annex G.1.2, IQ21)

[69] SQ07: "Information from my mission partners is reliable." (see figure in Annex G.1.1, SQ07)

[70] IQ22: "My mission partners provide reliable information to me." (see figures in Annex G.1.2, IQ22)

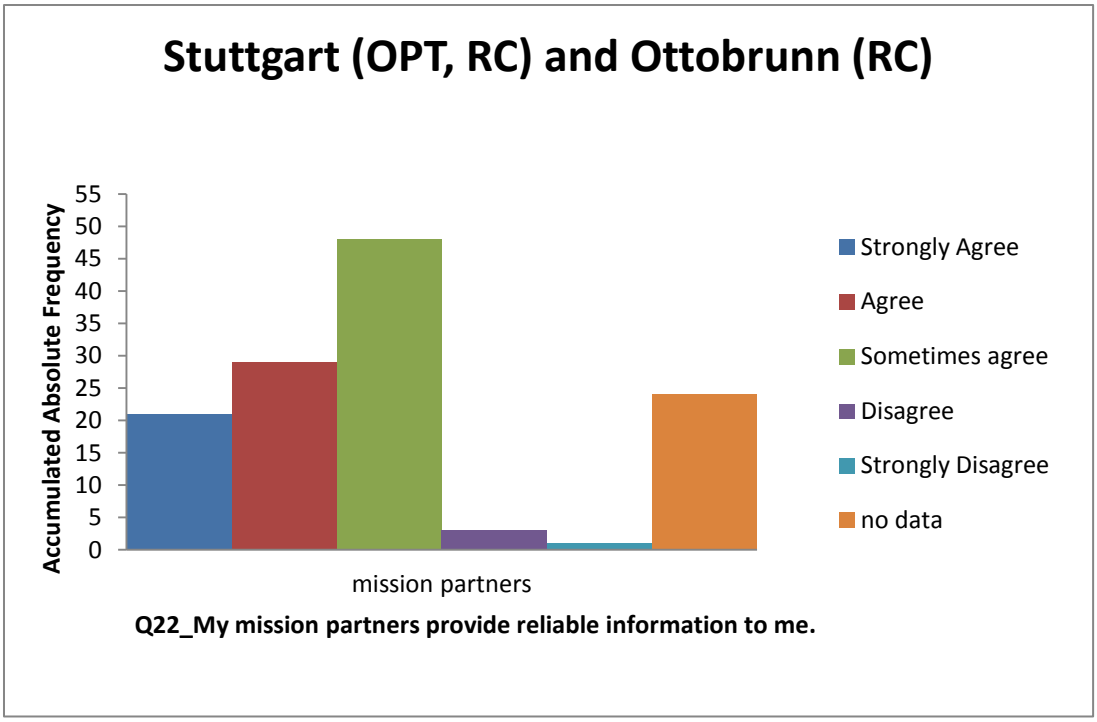


Figure 11: Reliability of Information

Quality of information (general usefulness, relevance, completeness, reliability) appears to be a key problem for perceived usefulness of the IMISAS Experimentation site.

Achievement of Mission Objectives

Members of the OPT didn't really have the feeling that the IMISAS Experimentation site helped them to achieve given tasks/goals.[71]
The following questions came up with reasons.
Regarding perceived benefits to use the IMISAS Experimentation site OPT members stated:[72]

- "UIS is certainly a required capability but current version approach is not acceptable"
- "Provided a collaborative planning venue"
- "Opportunity to shape information for use by an OPT"
- "Hands-on training with group interaction"
- "It taught me that DoD does NOT know how to plug into operations they don't have the authority to take charge. We flop around and I'm sure outsiders just shake their heads . . ."
- "provided a good medium that all participating could access and share info"
- "none"

[71] SQ16: "The IMISAS Experimentation site helps me to achieve my given tasks/goals." (see figure in Annex G.1.1, SQ16)
[72] SQ17.1: "Based upon your experience this week and your role and responsibilities in the experiment, what were the benefits to using the IMISAS Experimentation site?" (see table in Annex G.1.1, SQ17.1)

These statements appear not too enthusiastic about the IMISAS Experimentation site in order to achieve mission objectives.
AS OPT mission partners also had the opportunity to name drawbacks of the IMISAS Experimentation site:[73]

- "The site was difficult to use at best if the tools functioned."
- "Limited to the tools available on APAN"
- "APAN was very slow and not reactive . . . so slow that sometimes I'd get something out there, then forget what I was doing because the page would take so long to update."
- "some of the functions where hard to navigate and you had to dig to find posts containing info I needed"
- "cumbersome, not intuitive, too many ways to get to the same information, labeled areas not clear enough, too military-focused"
- "The system was not intuitive and in today's computer savvy world, if you can't figure it out with a few clicks then it takes too long."
- "Innaccesibility / slow functioning of the site. Poor access to broad set of information."
- "Too complex. There is no need to "pretty up" an APAN site. Users need to be comfortable sharing information in a non-structured manner. Renaming menus and trying to shape every website to look "SharePoint like" isn't actually improving how we share information."
- "Many. Functionality didn't work well -- things weren't intuitive -- you don't have time to learn to use the tool the tool has to be accessible and intuitive. It takes too long to load, it's poorly organized and key information does not float automatically to the top like it can in social media. It's hard to keep track, too many clicks between functions and too many passwords. It needs to be facilitated not lead in a particular direction."
- NONE (three times)

Communication with Mission Partners

How about the capabilities of the IMISAS Experimentation site to support communication with mission partners?
OPT Stuttgart described the benefits as follows:[74]

- "Provides a collaborative environment"
- "Provides a starting point and place for us to publish out information."
- "It throws some of the issues out there that we can see, but when there isn't a clear place that I can direct traffic I feel I can cause more harm and confusion. If we use the concert analogy, I know how to play my instrument, but I'm not familiar with the instruments around me and everyone sounds like they are just making sound and it is NOT pretty."
- "It has explored the direct issues I think we will encounter"

[73] SQ17.2: "Based upon your experience this week and your role and responsibilities in the experiment, what were the drawbacks to using the IMISAS Experimentation site? " (see table in Annex G.1.1, SQ17.2)
[74] SQ10: "How does the IMISAS Experimentation site benefit communication with mission partners?" (see table Annex G1.1, SQ10)

- "Theoretically, it allows a single question to be responded to by the group or at least come to the attention of the subject matter expert who the question submitter did not know existed."
- "provides good forum to communicate within specific areas"
- "Serves as a tool for collaboration"
- "In theory it is creates an open forum for discussion but DoD intent for the site is not defined on whether it should be used to collaborate or just to post information for military transparency issues"
- "Centralized place to communicate."
- "Provides a free and open location for communication / collaboration. Some artificiality in this as many mission partners will not come to a MIL site for collaboration but expect MIL to come to their sites."
- "Well the jury is still out on that. It seems to be difficult to use and there seems to be much more information out there in other capabilities. I also find it very difficult to master the tech issues involved with the site. At this level it seems to cut off information sharing in the room not enhance it."
- "Uncertain at this time"
- "For me it has not enhanced anything."
- "none" (two times)

The IMISAS Experimentation site appears not to perform too overwhelming regarding these perceived "benefits".

Information Sharing with Mission Partners

Information Sharing (IS) can be seen as integrated concept in the context of this analysis report. Since concepts like motivation, and constraints like procedures and policies, can been looked at in a relational way in order to describe how current Unclassified Information Sharing Capability (UISC) can be optimized, a support for the further evaluation of IMISAS solutions and products is being provided.

Without mentioning any conditions, the OPT appears highly motivated to share information with mission partners.

- Most OPT members believe that mission partners are willing to share information with them.[75]
- From their own perspective, most OPT members tell they are willing to share information with their mission partners, some even strongly.[76]

All AS mission partners had the following impression of trustworthiness of other mission partners:[77]

[75] SQ03: "My mission partners are willing to share information with me." (see figure in Annex G.1.1, SQ03)
[76] SQ04: "I am willing to share information with my mission partners." (see figure in Annex G.1.1, SQ04)
[77] IQ17: "My mission partners appear to be trustworthy to me." (see figures in Annex G.1.2, IQ17)

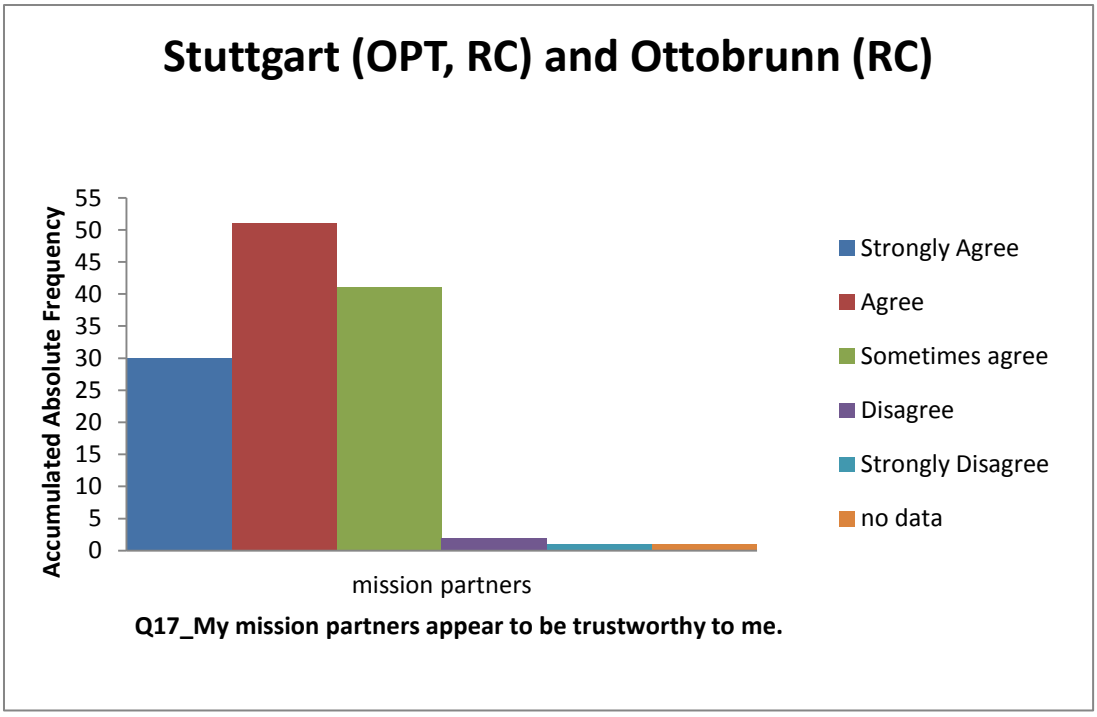


Figure 12: Trustworthiness of Mission Partners
Most mission partners are perceived trustworthy.

If an Information Sharing mechanism was mentioned in the survey question in concert with the general willingness to share all available information, then the readiness for information sharing decreases.

- Most OPT members would feel comfortable providing all available unclassified Information requested by their mission partners on a site similar to the IMISAS Experimentation site.[78] On the other hand, some of them neither agree or disagree, some disagree or strongly disagree. No one strongly agrees.
- From their own perspective, most OPT members would provide all available unclassified Information requested by their mission partners regardless of the information sharing mechanism.[79]

Open OPT members had the following proposals for improvement of information sharing with mission partners:

Better communication:[80]

- "The interaction is good."
- "We need better essay where they post and share their info."
- "NONE, most of my issues are on our DOD side of the house"
- "I really don't know - in DoD I feel stuck behind a huge wall of barriers. I can see there are real problems and there should be ways for DoD to assist, but bringing those

[78] SQ05: "I would feel comfortable providing all available unclassified Information requested by my mission partners on a site similar to the IMISAS Experimentation site." (see figure in Annex G.1.1, SQ05)
[79] SQ06: "I will provide all available unclassified Information requested by my mission partners regardless of the information sharing mechanism." (see figure in Annex G.1.1, SQ06)
[80] Open SQ01 "What could the mission partners do to better communicate with you?" (see table in Annex G.1.1, SQ01)

together is very disjointed. To me, it's not what mission partners need to do to better communicate with us, it's us that needs to make our people and processes more accessible to them. Truly a spider web that won't go away."

- "Provide a time period that they need the information. Groups on the ground and such can respond MUCH quicker than the COCOM. At the COCOM level, we operate at a glacial pace."
- "They could include BASIC biographical information in their profiles so we know who we're dealing with in what section of their organization."
- "I think communication needs to improve on my end, I did not check blogs/posts often enough."
- "I can't speak for mission partners. We (DOD) need to solve our own internal communications issues first."
- "Provide more specific feedback that has actionable information. Additionally, a mission partner posted a question specific to another individual in the comment section under the Concept of Operation document -- not the best way to reach a specific individual."
- "Military partners could ask for input from me. Specify to other partners when they should come to me. Communicate by "human" means rather than have the primay means of input be an internal planning process for a bunch of slides to give to the Commander."
- None (five times)

Fundamental improvements:[81]

- "A new tool...at least the front end."
- "Learning the social sites and terminology, then ensuring you have the technology to maximize its use"
- "go to where they are, use the sites they use"
- "The USG / US military cannot expect our mission partners to come to us. Many are hesitant / unwilling to do so. Many don't know how. Our significant mission partners expect the USG / US military to interact with their own information sharing sites. USG needs to find a way to strike a balance and not expect / require all mission partners to interact with OUR information sharing applications at all times."
- "Better training, more finite acceptable levels of familiarity with technology on the part of the partici-pants. I don't have time for people that can't navigate websites or adapt to technology in a rapid manner."
- "a new exercise that would actually get to the issues of information sharing in a productive manner and not one that disregards expertise in the room."
- "I don't know but APAN is too painful to use in a real world situation unless it's all you have and the military is running the show. We need to meet with and exchange information with IOs and NGOs and other partners on a face to face basis before crisis hit. Information sharing is only as good as the networking that underlies it. I believe as does much of this group that a separate cell for unclassified information sharing should be created in phase 0 of a potential operation. Some in the room think this should be staffed and run by operational people. However I believe that a more horizontal functional team outside and not driven by the military process would provide much richer data for the military to work from in forming their responses to a disaster. The mission statement for this cell would be to create "a data rich redundant

[81] SQ13: "What fundamental improvements to information sharing with mission partners would you recommend?" (see table in Annex G.1.1, SQ13)

site which is a USG site which provides a detailed up to date picture of the crisis for broad consumption that is responsive to but not driven by military planning". I would also not ask the operations people to "lead" this you need a facilitator not a leader. The lead of the OPT has to be its on event not drive the information creation and sharing."

- None (seven times)

What were the impressions of the AS mission partner OPT of the IMISAS Experimentation site to give good results?[82]

- "Gave me feedback that DoD really does not know how to plug into an operation led by another agency, nor how to work within the larger IO, NGO, HA community."
- "On the ground information, in real time once I made the right connections
- being able to upload information worked well as long as it was not a video"
- "None...fair at best. File sharing was ok."
- "RFI processing", "RFI, once objective understood by team"
- "search for information on blogs and posts"
- "Document storage, tracking of site activity."
- "When used as described in the handbook."
- "I was able to connect up with UN and NGOs faster than before."
- NONE (four times)

Of special interest was the question regarding perspective change: "„If you were your mission partner, what would you propose in order to change your own way of information sharing in order to achieve mission objectives?"[83]

- OPT Stuttgart:
  - "There is limited applicability on information sharing in public affairs. I think we share info in our lane appropriately."
  - "Improve communication(s) infrastructure that can handle large bandwidths to facilitae sharing speed."
  - "They must realize the military is only there to help as they are and we are prone to make the same mistakes they are"
  - "more training on military procedures for CONOPs; work with military individuals who shared some of my concerns and use them as entry ways for my info"
- RC Stuttgart:
  - "Develop stronger personal and organizational relationships."
  - "Exchanging information instead of only "asking" of them."
  - "A more pro-active approach needed; more info-sharing instead of obtaining info from other actors"
  - "I would do more training to understand military roles and procedures"
- RC Ottobrunn:

[82] Open SQ02.1: "In which situations did the IMISAS Experimentation site give you good results?" (see table in Annex G.1.1, SQ02)
[83] IQ28, see table in Annex G.1.2, IQ18.

- "If I were the training audience I would answer the requests / I would try to get in contact with other forces / players in theatre."
- „For the time being, there is no two-way info flow yet."
- "Force everyone to have a Facebook and Twitter account."

It is necessary to consider the balance of the give-and-take-basis of mission partners:[84] AS mission partners mostly agree that a give-and-take-basis sometimes is given, many of them only sometimes agree:

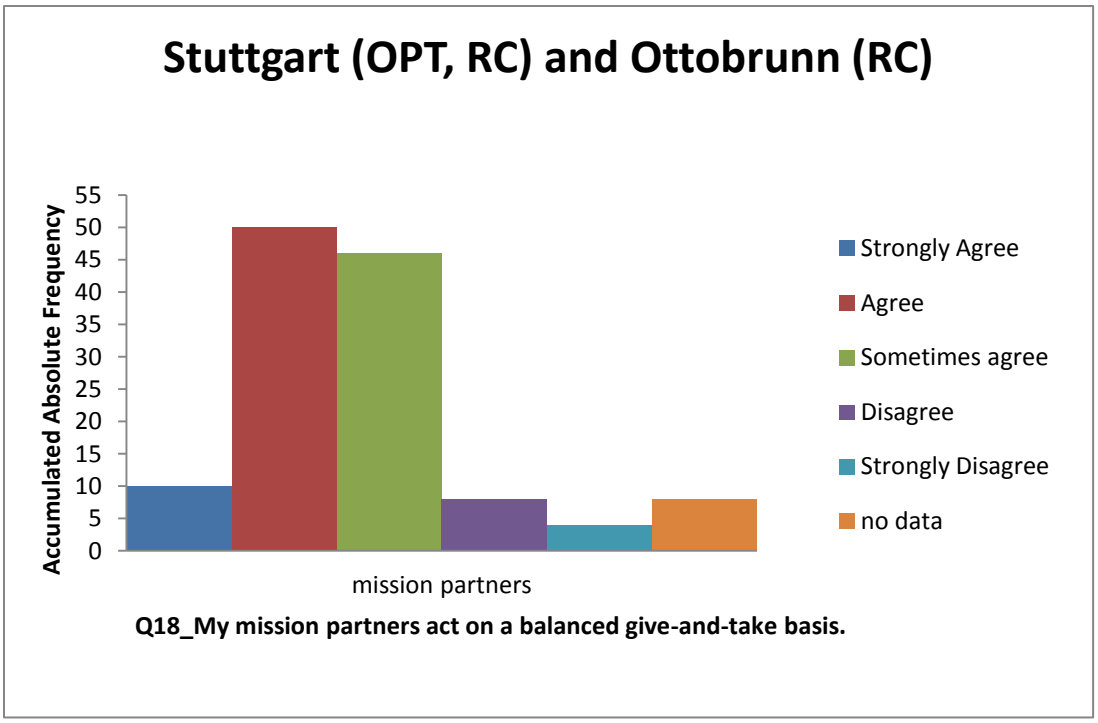


Figure 13: Give-and-take Basis

Other Results and Findings

Planning of Mission Partners

The US comprehensive approach aims at bringing military, civil- governmental and civil non-governmental organizations together.
Differences between civilian and military planning brought up a discussion on related planning styles and process within the OPT.

RFI / FRA

The handling of RFI and RFA popped up several times in OPT discussions. Besides given procedures, regarding management has to be supported by advanced software capabilities: "RFI/RFA management. Group is trying to determine how best to manage the RFI/RFA site.

[84] IQ18: "My mission partners act on a balanced give-and-take basis." (see figures in Annex G.1.2, IQ18)

They are reviewing the Hand Book and checking APAN. Report will be at 1430. The group does not appear to be pleased with the APAN `blog.` Also the threads do not appear to line up in a logical manner and the verify items do not seem to do much for their comfort level." [IMISAS AS JOT 2011]

RC participants agreed that inviting non-military partners (via the RFI/RFA tools) to suggest venues and tools for collaboration will improve the effectiveness of that collaboration [IMISAS AS RC P5 2011]:[85]

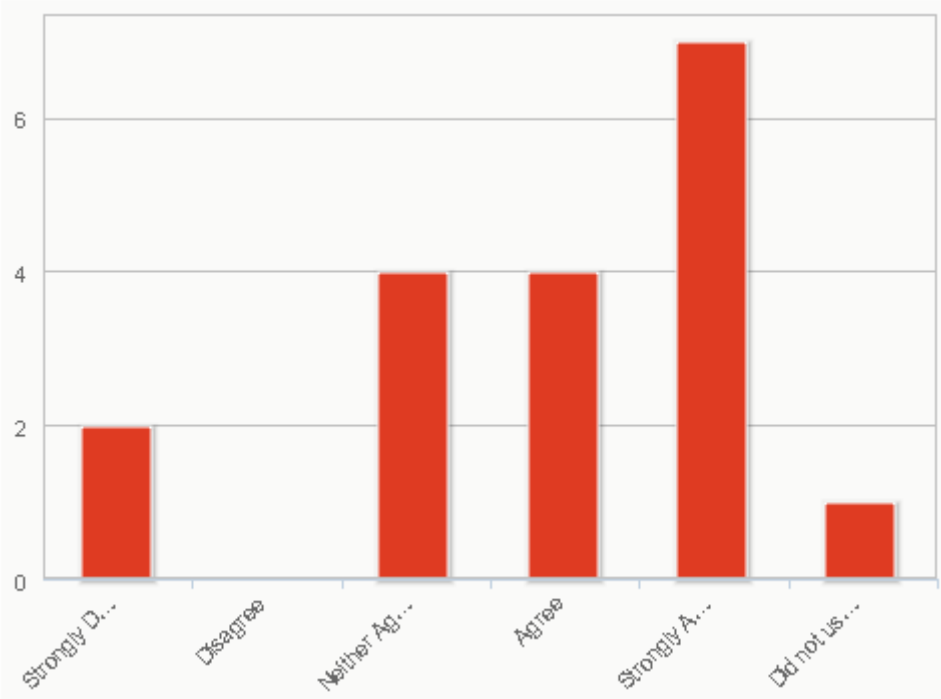


Figure 14: Effectiveness of that Collaboration via the RFI/RFA

RC participants also mostly found that the business rules found in the Handbook at Annex E for posting a request for information (RFI) or request for assistance (RFA) were easy to use [IMISAS AS RC P5 2011]:[86]

[85] "Inviting non-military partners (via the RFI/RFA tools) to suggest venues and tools for collaboration will improve the effectiveness of that collaboration."
[86] "The business rules found in the Handbook at Annex E for posting a request for information (RFI) or request for assistance (RFA) were easy to use."

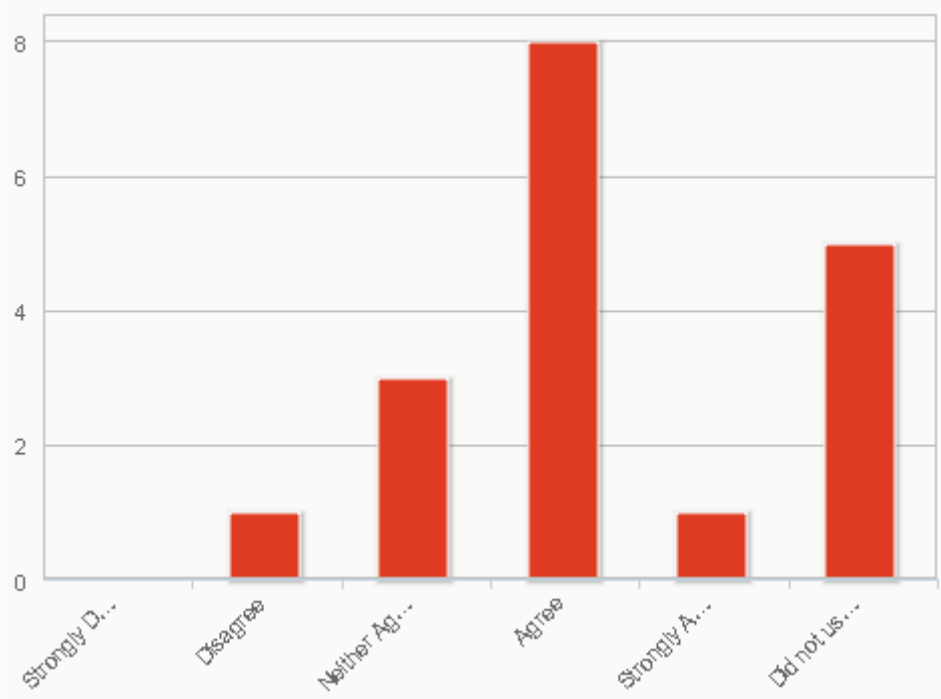


Figure 15: RFI/RFA Business Rules are easy to use

UIS Handbook and software capabilities are on track but need to be more developed.

Structure of a Future UIS Cell

In the OPT, there occurred a discussion on how a future UIS Cell should be structured. A consensus between civil and military members of the OPT emerged the following insight: The UIS Cell should act upon integrated knowledge and experience from both civilian and military experts, handling unclassified information in a constructive and unfiltered way. OPT also emphasized that a purely military UIS Cell will not provide the appropriate mindset for the UIS tasks because of a tendency of using vertical/hierarchical-oriented thinking patterns versus needed horizontal/associative ones.

Observations:

- "opt group discusses best setting for uis process (who will be in the uis cell, what will they be doing), in order not to replicate what opt is doing" [IMISAS AS JOT 2011]
- "Consideration was given to the establishment of a core cell to establish the information sharing enterprise while an OPT forms. The OPT would use this core as the primary information sharing entity. One of the qualifications would be for personnel to not have pre-filtered ideas or positions on information that would reduce the sharing of information. SIPR would not be needed for this core group; however, having a reach back person with SIPR access would be needed. The leader of the core group must be a good facilitator. The leaders `day job` is not important as facilitation skills are most important." [IMISAS AS JOT 2011]

Relationship between OPT and RC

RC (Stuttgart and Ottobrunn) several times complained of not knowing what is going on in OPT.[87] They had the impression that OPT was not really interested in giving feedback on delivered products or ongoing planning or discussion. This appeared to be a typical phenomenon of dislocated reach back cells. This feeling of isolation of the RCs regarding OPT decreased motivation. Moreover, the limited knowledge of mission objectives and own tasks gave RC mission partners a low level of perceived appreciation.

Consequences for UIS Handbook

Business rules appeared to be easy to use for RC participants (see section 5.2.10.2 above).

After period 3, most of OPT members neither agreed nor disagreed – and some of them agreed or strongly agreed -- that the business rules found in the Handbook for situation reports will enhance the situational awareness of partners collaborating on the IMISAS Experimentation site. [IMISAS AS P3 2011]:

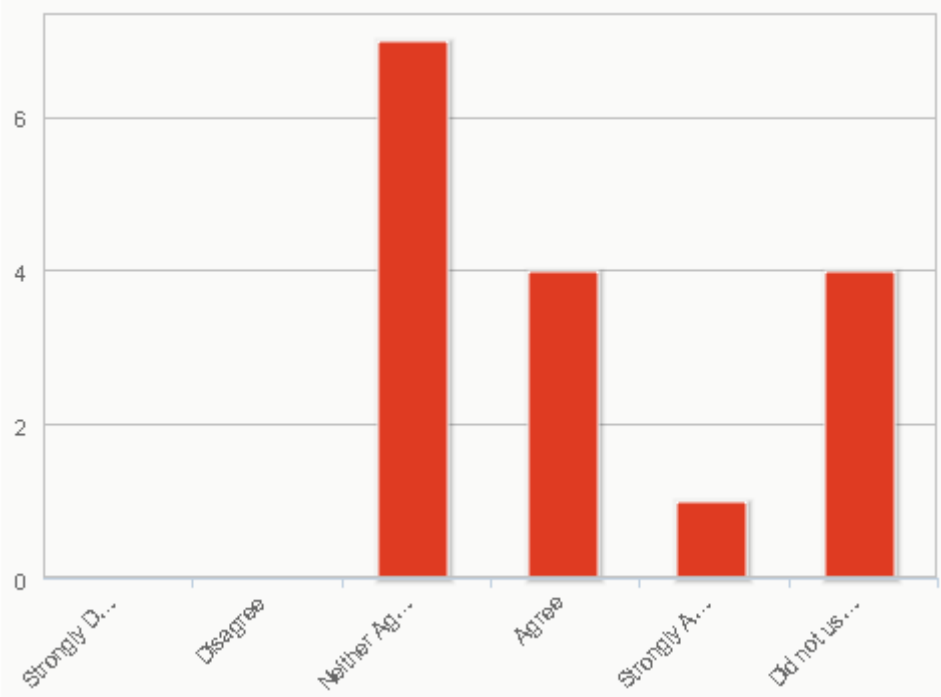


Figure 16: Business Rules and SA (OPT)

Many results of this analysis report provide practical hints for an updated version of the UIS Handbook.

Consequences for UIS Concept

Many results of this report provide practical hints for an updated version of the UIS Concept.

[87] "Role Player (JMED MONUSCO) perceives lack of feedback from OPT to own inputs. Used not only APAN but also facebook & email to get in contact." [IMISAS AS JOT 2011]

Shared Situational Awareness (SSA)

From a Human Factors perspective the term Shared Situation Awareness (SSA) has been proven as a very useful concept to explain a common understanding for mission´s development and mission partner´s action. The need for a well-developed SSA depends on the degree of shared goals and the necessity of coordinative action. The goal of the HFA in the IMISAS analytic seminar was to investigate the necessity of sharedness between the OPT and the external partners and the development of SSA. If there was a need for SSA our analysis should have been shown also driving and inhibiting factors to the processes of building a common situation picture and sharing information in order to build SSA between partners.
The IMISAS scenario required to deal with complex coordination between different civilian and military actors. For that reason there was a need for a good SSA from the very beginning. We assumed that teams or communities of shared interest show a well developed SSA when partners

- Share information in a timely manner
- Coordinate information sharing on a regular basis
- Evaluate or rate information and communicate their own interpretations to partners
- Being aware of each other's information needs and each other's goals
- And develop courses of actions together for the future development of the situation

These are the main characteristics of SSA. From the IMISAS experiment we collected data to show which actors need to develop this sort of sharedness and how this sharedness changed by routine and better understanding of each other's roles and responsibilities.
To draw conclusions on SSA we based this part of the HFA on three sources of data: the online survey in period 3 and 5 as well as on the online survey at the end of the analytic seminar, observation data from the OPT and the response cell in Ottobrunn and structured interviews with civilian actors from the response cells and the OPT[88].

Mission partner´s network

Interdependencies between partners
Our HFA shows the necessity of professional networks and social networks of the mission partners. Most of the OPT members coordinated and shared information with external partners. For gaining a first overview of the conducted tasks, planned actions , intentions successfully completed during the operation day the following table displays the results for the OPT.

[88] The analytic sources for HFA SSA are limited due to the fact that the online survey questions were not posed to the response cells. For that reason we cannot match the perception of shared goals and shared information between OPT and external actors.

Position	Period 3	Period 5	Need for Cooperation with external partners
J35 OPT TEAM Chief	Information sharing via APAN	Process for the leveraging the RFI/RFA tool	+
J35 OPT Deputy TEAM Chief	Submitted RFIs and received replies Continue to build SA	Refined information sharing processes branch and sequel planning	+
J4 Log / Transportation	Posted RFI's on the Questions site	Developed logistic Concept of Support for branch plans to support CO2 scenario	+
Foreign Disclosure Officer	Coordinating activities (RFI Process)	answering RFIs	+
Commerce	Coordinating activities (communication with external partners) Answering RFI	Answering and Rating RFIs Coordinating activities (communication with external partners)	+
J2 Planner	n/a	Answering RFI	+
PAO	provide Public Affairs perspective	answered or provided advice on responding to an RFI	-
Disclosure Officer	Coordinating activities (Complete SCG for signature)	n/a	-
KM / IM Officer	Review of CONOPS coordinating data storage	All of them except cross domain transfer.	-
Strategic Communication	None	None	-
J5 Plans	None	None	-
J5 Future Plans	none	n/a	-
J5 HA Programs / Disaster Preparedness planning officer	None	ALL	-
J6 Comms Planner	none	n/a	-

Table 1: Task interdependencies between OPT and external partners

First of all the table shows that collaboration between mission partner wasn´t as complex as it might be in a more realistic environment.

Despite this the OPT collaboration network changed slightly from period 3 to 5 and became even more differentiated. All of the relevant planning positions established more interdependencies with external agencies or civilian organizations. Only a few

of them had to develop real shared situation awareness due to their task requirements.

Goal awareness as basis for situation awareness

Concerning the awareness for mission partners´ goals the following table shows a quite positive final state: Most of OPT positions evoked a well developed insight in their partners´ actions and so far there should be a good sense for relevant information sharing. Support from external actors seems to lead to a better goal awareness for the OPT member. When OPT mentioned a good awareness for their partners´ goals the following driving factors could be observed:

- receiving feedback from the RFI process, even when it´s a negative response there should be a response
- passing information in an early mission period,
- using discussion forums,
- sharing and posting operational information,
- having open discussion of policy, information sharing issues, and personal understandings of the problem set.

The following table shows further the results from the online survey of OPT and displays the working interdependencies between external actors and the OPT positions. The main interesting part are the goal awareness rating of OPT positions. Additionally we asked for the external partners interdependencies this means the most important organizations, civilian or military, collaborating during the planning period 3 and 5.

OPT position	Goal Awareness (for partners´goals)	Goal Awareness (for partners´goals)	Partners network	Partners network
	Period 3	Period 5	Period 3	Period 5
J35 OPT TEAM Chief	Sometimes	Sometimes	Interagency partners	WHO DEU Mil
J35 OPT Deputy TEAM Chief	Sometimes	Most of the time	OCHA OFDA	OCHA OFDA NATO CIMIC
J35 OPT Deputy TEAM Chief	Most of the time	All of the time	DART Team	Civilian on the ground JTF fwd
J4 Log / Transportation	All of the time	All of the time	DART USAID	DART USAID/ OFDA NGO's/ IGO's
J5 Plans	Not at all	Not at all	DOS CP OCHA OFDA	OFDA
J5 HA Prgs. / Disaster Preparedness	Sometimes	Most of the time	DOS	DOS
Foreign Disclosure Officer	Sometimes	Sometimes	Civilian government members working in a military organization.	Civilian government members working in a military organization.
Commerce	Sometimes	Not at all	UNOSAT DOC/ NOAA US Embassy ACAPS	UNOSAT DOS DOD USAID RMT Companies
PAO	Sometimes	Sometimes	DOS	
Disclosure Officer	Most of the time	n/a	USAFRICOM	
KM / IM Officer	Most of the time	Most of the time		
Strategic Comms	Most of the time	Most of the time	None	None
J6 Comms Planner	All of the time	n/a	None	
KM / IM Officer	Sometimes	Most of the time	None	
J5 Future Plans	Not at all	n/a	None	

Table 2: Goal Awareness of OPT

Especially collaborating with partners highly involved in field actions positions (e.g. J4 and Monusco J-Med) seemed to develop a better awareness for their mission partners´ goals. One OPT member stated that valuable support from his partner was to hear about the situation on the ground in Goma, which he gained from DART and NGO/IGO's.
Besides this positive tendency there are two deviating data sets: J5 Plans and J5 Future Plans haven´t developed any awareness for their partners´ goals and the representative of Commerce changed from a satisfying awareness to none. First might be explained due to the fact that there was no collaboration required between J5 Plans and external instances. This fits well to the assumption that awareness can only be developed by collaboration and task oriented communication between partners. Switching partners in a time critical phase of operations should be avoided: “UN and NGO and companies and DOS were very supportive and answered quickly. Military was hard to work with as even when I made personal contacts and asked for specific information it was not forthcoming“. Despite the amount of external interdependencies the representative of commerce couldn´t build up an understanding of partners´ goals. Taking a closer look at the data a suitable explanation might be that commerce operated with completely different partner´s from period 3 to 5. Awareness and sharedness of goals can only be reached by a certain amount of collaboration time: “You cannot ask for 100 degree situational awareness without being interested in actually doing something about it”.
Concerning the awareness for each other´s goals the OPT improved between period 3 and 5. This might be due to the fact that the mental model of support from partner improved during the analytic seminar.
Also role players in the DEU Response Cell were asked for their awareness of their mission partners´ goal. Positions from J9 and J-Med are meant to coordinate their actions in line with OPT´s planning. The interview results indicate that there was less coordination than expected. If there was good goal awareness mentioned these positions had access to groups and organizations on the ground like NGO, embassy or GOs.

Support for building a mission partners´ network
Overall in the online survey from period 3 and 5 some supportive behavior and procedures were mentioned from the OPT to its mission partners. Also the OPT was quite aware of causing difficulties or problems for their partners with its own actions. Being supportive and avoiding problems in coordination and cooperation between partners could be improved by providing good technical or procedural solutions to the following aspects:

	What sort of problems do you think your mission partners had with your actions?
Lack of goal and role definition	- difficult time defining roles - disconnect on what the objective is and what is notional or suspended in reality - not knowing what the goals and objectives are or what is the expectation from each partner - partners role were not specified in conjunction with own mission
Lack in quality of information sharing	- civilian and military organizations being able to communicate in the same language - slow or no responses and partners have been moving on or slow down their pace to achieve their goals - one way flow of information - placing imagery without explanation social network site - loosing information connection with people “on the ground” - not understanding where we wanted different types of information leaded
Lack of partners´ awareness and reliability / lack of cooperation	- Not having their inputs taken serious or suggestions from non military members not incorporated into the discussion. - Lack of commitment to provide support, which can do during the planning phase - Military working their internal processes without regard to the greater need of the actual on the ground emergency situation.
Different tool-set and procedures	- Not using partners´ tools - Not understanding where different types of information leaded - Governmental organizations are too slow to embrace non-structured collaboration, leading to a decreased lack of interest in collaboration with us.
Errors	- Disrupting existing missions - actions could have been disruptive, could serve to predict in advance military actions

Table 3: Supportive Actions for civil-military cooperation

Quality of Information Exchange

The section above already mentioned some findings concerning information sharing in the IMISAS Analytic Seminar. There are some intangible aspects mentioned as well as some specific aspects handling the information flow:

- civilian and military organizations should be able to communicate in the same language
- information sharing should be a win-win situation for all partners
- giving explanation to operational information as imagery esp. when posted on blogs or social media
- establishing connectivity with people “on the ground”
- transparent ways of information flows and different information types

At the end of the analytic seminar OPT was asked to qualify their ways and procedures of information sharing with their mission partner. Posing questions about the information sharing quality we measured mission partners` understanding of OPTs tasks and information needs. These results are shown in the following sections.

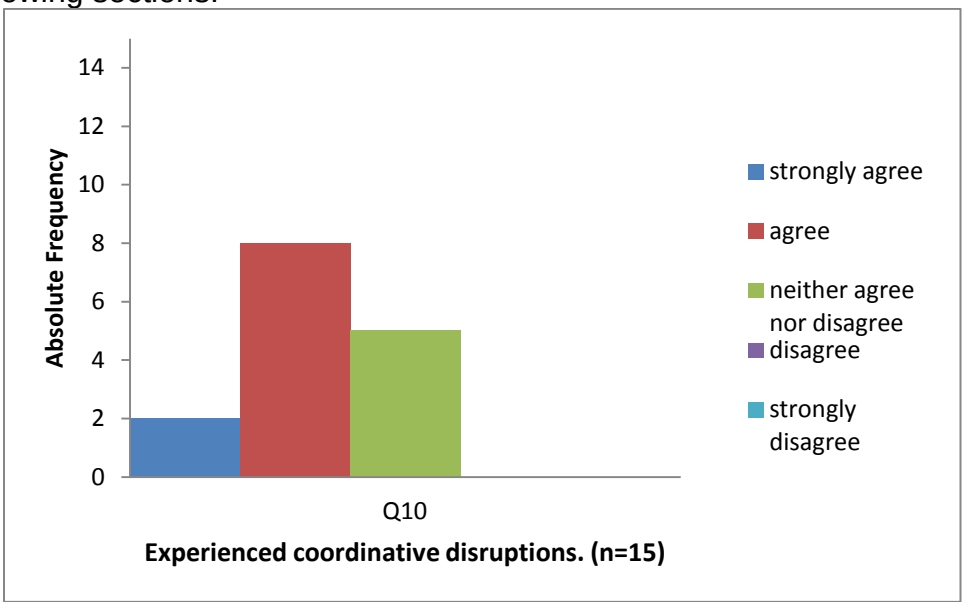


Figure 17: I experienced disruptions in coordination between my mission partners and my own organization.

The overall quality of coordination wasn´t sufficient: 10 out of 14 members of the OPT agreed on the statement that coordination was experienced as disruptive. Although there was a need for collaboration because of the operational situation, some organizations from MONUSCO and the OpsCmd couldn´t even report coordinative activities with the OPT.

This subjective perception could be supported by the lack of sharing relevant data. As the tables below show data provided to the OPT was only partly helpful or relevant. This might be a source for extra work and more effort in asking and searching for better data.

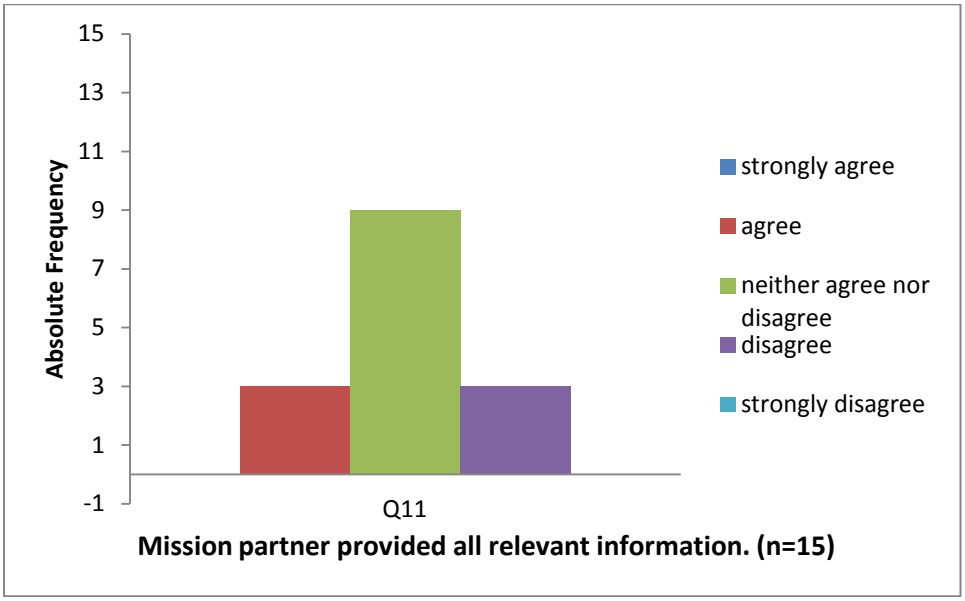


Figure 18: Our mission partners provided all their information that was relevant for my organization's mission.

The next figure also indicates that mission partner´s understanding of roles and information need could have been better: 11 participants of the OPT fully or partly agreed that information provided to them was not relevant for their tasks. In more a complex operational situation this lack of shared mental model could have been caused by information overload on the planning positions.

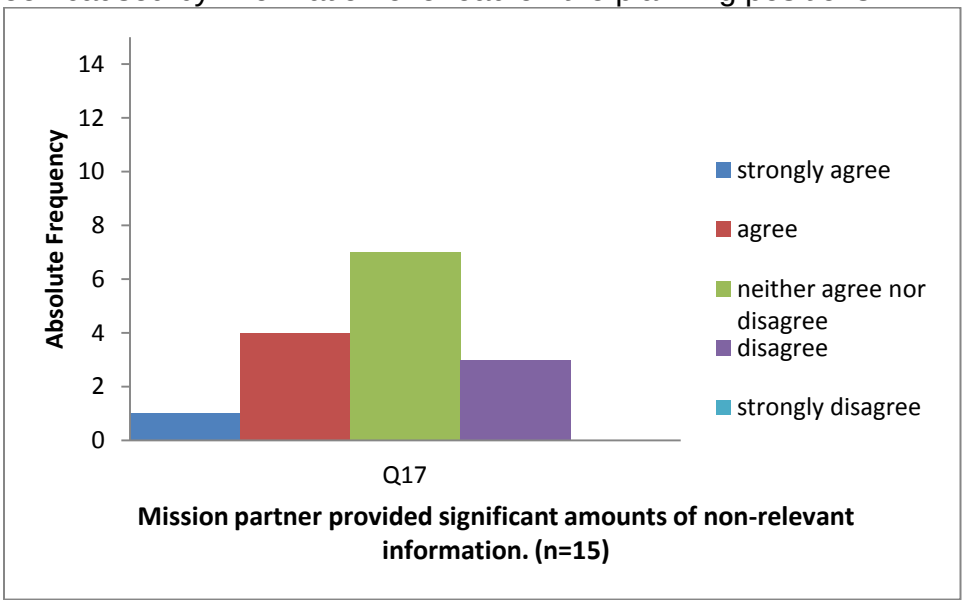


Figure 19: Our mission partners provided us with significant amounts of information that was not relevant for our mission

Knowing how team members share their information is also crucial for effective coordination. Some OPT members regarded the information sharing procedures as confusing as the following frequencies from the online survey indicate.

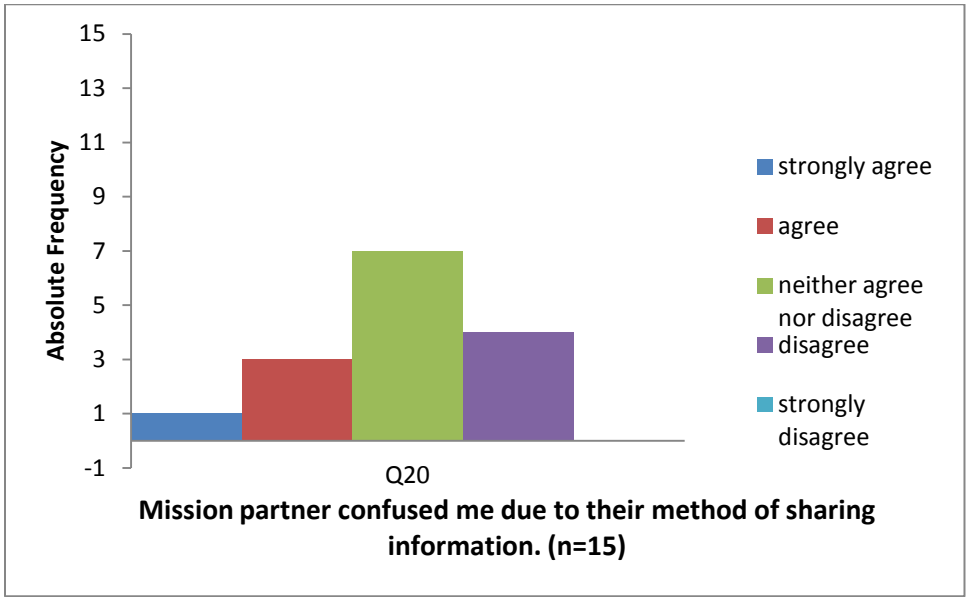


Figure 20: Occasionally my mission partners confused me due to their method of sharing information.

Assessing the Situational Picture by using Information Classes

A shared or common understanding between partners helps to deal with difficult and unclear situations in complex missions. It is often described as 'being aware' of the partner´s informational needs and good sense of the ongoing situation. In the IMISAS Analytic Seminar we measured individual situational awareness and mission needs by subjective statements and observations from the OPT.

The process of building an individual situational understanding or situational picture is supported by an easy access to task relevant information and clear and efficient way of information sharing. Results from the online survey suggest the opposite. Also quotations from interviews with civilian actors lead to the assumption that OPT had developed a shortened situational picture: "Military working their internal processes without regard to the greater need of the actual on the ground emergency situation. You cannot ask for 100 degree situational awareness without being interested in actually doing something about it". Civilian partners in the response cell also quoted their involvement as "unidirectional communication with US-partners" and experienced information exchange as "I have had the feeling that I always provided information with no pay back".

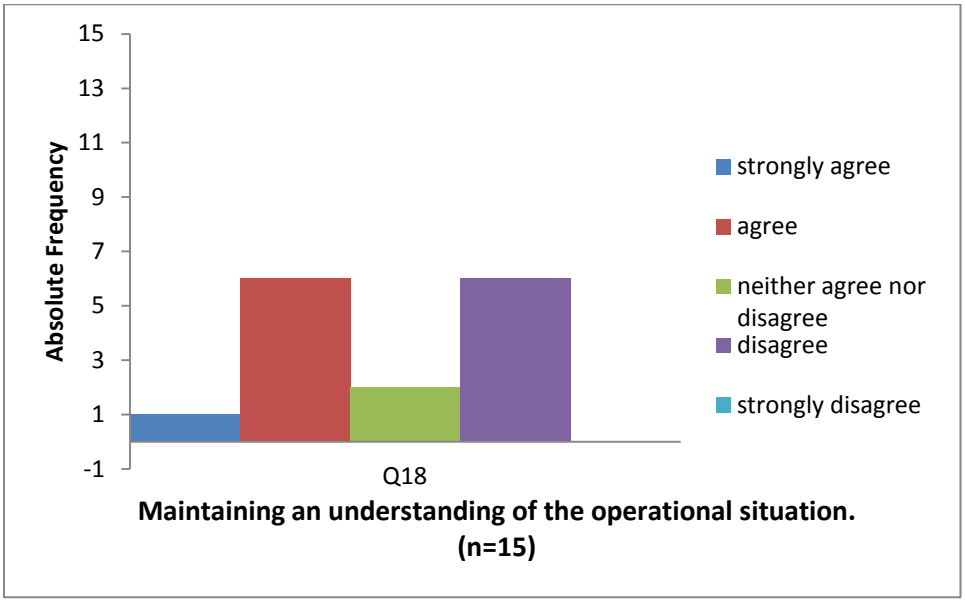


Figure 21: Despite the time shift between operational days I maintained an understanding of the operational situation.

In accordance with the latter interview quotations the self-rated understanding of the operational situations is fragmented. Half of the OPT members didn´t maintain a continuous situational understanding. The following quotation again stresses the importance of information from the lower or subordinated level to build an individual situational picture: “a lot of information from the ground did not get incorporated into the situational awareness of the group nor the site”. Military and governmental organizations should be aware of the high validity of information from local actors like embassies with a permanent office on the ground. Usually they have useful and well founded information about local political and governmental key player.

To facilitate another view on information processing, information requirements and its coverage, the method of information classes has been used.

Methodology

The concept of “information classes” has been developed due to the evaluation of shared situational awareness (SSA). The assessment of information is carried out only by the awareness if that information is available and required and is therefore classified by subjective viewpoints. Other attributes / parameters of information (e.g. actuality, reliability, accuracy etc.) are not nullified but completed by the concept of information classes.

Therefore it is possible to prove the existence of shared situational awareness or similar mental models and to evaluate them. It is also possible to draw conclusions on its transformation e.g. during the experiment. These aspects couldn’t be tracked at this point, as the method was based only on data acquisition by a questionnaire in the DEU Response Cell.

Figure 22 shows the classification key and names the information classes:

Information	Available	Not available
Required	Primary Information	Deficit Information
Not required	Shadow Information	None Information

Figure 22: Concept of Information Classes

Primary information (PI)

- Primary information is information that is available and required. It is important to actual problematic situation and problematic scenario. Especially missing agreements in the connection between leader and directee can show a missing shared situational awareness.

Deficit information (DI)

- Deficit information is information that is required but not available. Its importance is significant as well. Special information requirement can be derived from this information class (e.g. one team member should provide special information for the whole team). This allows conclusions on the distribution of information within the acting team. It is therefore a criterion of optimality.

Shadow information (SI)

- Shadow information is information that is available but not required for the current task. Be reminded that all evaluations on information by the individuals are subjective. If some members of the team classify information as shadow information and others as primary information one can conclude easily the absence of a shared situational awareness in this team.

None information (NI)

- None information is information that is neither available nor required. This can be owed to a lack of interest or to a missing understanding of the problem itself. If all team members classify information in this way, it can be abolished. If not, a precise analysis on this behavior has to be done (if necessary with expertise of Subject Matter Experts (SME)).

The existence and distribution of these information classes allow the conclusion on the degree of information coverage.

Method implementation

During the Analytic Seminar IMISAS this method was employed by using a questionnaire at the local facility in Ottobrunn.

The following information or situational cues, all taken from the IMISAS Master Scenario Event List (MSEL), should be evaluated by the polled role players. (The questionnaire "Information Assessment Sheer" can be found at the document's appendix):

1. The most recent eruption, prior to the disaster today, was 2002.
2. Mount Nyiragongo is located about 20 km north of the town of Goma.
3. At the beginning of the scenario a German NGO offered help soon/directly
4. CNN has announced a missing USGS Team.
5. An UNHCR fuel storage has been destroyed by lava.
6. The status of the lava-flow/eruption could have been followed also on facebook.
7. The department of foreign affairs has been concerned about the security situation.
8. There was a suspicious local NGO.
9. There have been several explosions at the airport.
10. MONUSCO Chief Meece declared MONUSCO Peacekeepers north of Goma out of contact since Saturday afternoon, 30 July 2011.
11. Several DEU NGO recognized necessity to go to GOMA in order to support UN HA/DR activities.
12. A warning by DEU has been announced on carbon dioxide around Lake Kivo.
13. A SME (professor) refused to use APAN because of ethical reasons (he doesn't want to cooperate with MIL). Instead, he prefers to use next door media like Facebook, Twitter, Skype, and EMail.
14. CNN journalists reported on small riots in the Goma suburbs, people blame UN Soldiers for the water contamination.
15. Flights to Sake, Kigali, Kampala and Gisenyi have been cancelled.

Table 4: Situational Cues of IMISAS MSEL

The following Table 5 illustrates an example for the implementation of the Information-Assessment:

Information	I had the information	I needed the information
Example: A disaster happened in Goma.	☑yes ☐ no	☑yes ☐ no

Table 5: example for implementation of the information- Assessment

All of the 15 situational cues were given for evaluation to such an extent and consequently located by every respondent in one of the information classes.

Graphical Data Evaluation

Through a graphical listing of all information classes and the number of respondents, who designated them, a SSA Chart has been created (please refer to Figure 23**Error! Reference source not found.**). For example, seven people assessed information one as primary information and one person as shadow information. The coloured scale shows a colour gradient from green to red and can be understood as a sign of common ground in the assessment of the information. The more green in one information class, the more participants assessed the information in the same class (the more red, in unison the less). The number shown in the boxes is the exact number of participants who assessed information xy in the respective class. In addition, rows with the number of the information and the information itself were added in favour of clarity.

SSA Chart

No	Information	PI	DI	SI	NI
1	The most recent eruption, prior to the disaster today, was 2002.	7		1	
2	Mount Nyiragongo is located about 20 km north of the town of Goma.	6	1	1	
3	At the beginning of the scenario a German NGO offered help soon/directly	7		1	
4	CNN has announced a missing USGS Team.	1	4	1	2
5	An UNHCR fuel storage has been destroyed by lava.	1	5	1	1
6	The status of the lava-flow/eruption could have been followed also on facebook.	2	3	2	1
7	The department of foreign affairs has been concerned about the security situation.	2	2	2	2
8	There was a suspicious local NGO.	1	5		2
9	There have been several explosions at the airport.	2	6		
10	MONUSCO Chief Meece declared MONUSCO Peacekeepers north of Goma out of contact since Saturday afternoon, 30 July 2011.	4	2		2
11	Several DEU NGO recognized necessity to go to GOMA in order to support UN HA/DR activities.	5	1	1	1
12	A warning by DEU has been announced on carbon dioxide around? Lake Kivo.	7		1	
13	A SME (professor) refused to use APAN because of ethical reasons (he doesn't want to cooperate with MIL). Instead, he prefers to use next door media like Facebook, Twitter, Skype, and EMail.	4		4	
14	CNN journalists reported on small riots in the Goma suburbs, people blame UN Soldiers for the water contamination.	3	4	1	
15	Flights to Sake, Kigali, Kampala and Gisenyi have been cancelled.	4	3		1

Figure 23: SSA Chart; n=8

Data Evaluation and implications on the basis of selected examples

The evaluation of Figure 23 allows drawing the following conclusions (the upcoming array will be explained with R (Response), E (Evaluation), C (Conclusion)). A clipping of the SSA Chart can be seen above every evaluation table:

Examples for an existent Shared Situation Awareness between the role players inside the DEU Response Cell

SSA Chart

No	Information	PI	DI	SI	NI
1	The most recent eruption, prior to the disaster today, was 2002.	7		1	

Figure 24: SSA Chart Clipping of Situational Cue 1

Situational Cue 1: The most recent eruption, prior to the disaster today, was 2002.

R	Seven out of eight respondents judged this information as Primary Information. Only one person chose a different class (Shadow Information).
E	This is an example for a good shared awareness about the importance of this information. Due to the preparation for the analytic seminar all of the participants have known this information, but one judged it as unimportant for his/her task fulfillment.
C	Basic information was well known to the role players.

SSA Chart

No	Information	PI	DI	SI	NI
3	At the beginning of the scenario a German NGO offered help soon/directly	7		1	

Figure 25: SSA Chart Clipping of Situational Cue 3

Situational Cue 3: At the beginning of the scenario a German NGO offered help soon/directly.

R	Seven out of eight respondents judged this information as Primary Information. Only one person chose a different class (Shadow Information).
E	This information has been discussed in the group of role-players why this high accordance could be established. Even if this is an experiment´s artificiality, it is a perfect evidence for the importance and quality of face-to-face communication to establish a useful SSA.
C	The discussion led here to the mindset. Apart from that, the same conclusions as shown above (information 1) are valid.

Examples for a none existent Shared Situation Awareness between the role players inside the DEU Response Cell

SSA Chart

No	Information	PI	DI	SI	NI
2	Mount Nyiragongo is located about 20 km north of the town of Goma.	6	1	1	

Figure 26: SSA Chart Clipping of Situational Cue 2

Situational Cue 2: Mount Nyiragongo is located about 20 km north of the town of Goma.

R	Six respondents assess this as PI, DI and SI were assessed each with one person.
E	Even if this information has been classified by the majority as important, there are two outliers. The fact is remarkable that these outliers have been the two German NGO with the specialty that NGO 1 needed the information, but did not have it and NGP 2 had the information and did not need it. Taking into account the comparably aim of the two NGOs this is a very good example what can occur with a lack of SSA.
C	At least two participants had no information exchange at all. Due to the fact that all of the others have seen it as primary information (the location of the volcano should be important for a helping organization) this should have led to an information exchange.

SSA Chart

No	Information	PI	DI	SI	NI
4	CNN has announced a missing USGS Team.	1	4	1	2

Figure 27: SSA Chart Clipping of Situational Cue 4

Situational Cue 4: CNN has announced a missing USGS Team.

R	Four respondents judged this information as DI, two as NI, and each with one as PI and SI.
E	This information has been published via RSS feed and has been missed by the

	majority of the role-players.
C	Eventually the RSS feed did not have the necessary distribution within the role-players. A reason could by the position of the RSS feed on the APAN site or problems could have occurred with the utilization of the APAN service itself. A position change of the feed could be a solution and should be tried, because DI has to be prevented as far as possible.

SSA Chart

No	Information	PI	DI	SI	NI
5	An UNHCR fuel storage has been destroyed by lava.	1	5	1	1

Figure 28: SSA Chart Clipping of Situational Cue 5

Situational Cue 5: An UNHCR fuel storage has been destroyed by lava.

R	Five of the respondents judged this information as DI, and each with one as PI, SI and NI.
E	Most of the role-players needed this information (six out of eight), but only one had it. For two it was not needed. The quality of the information channel did not reach the interested majority.
C	Facebook and APAN Maps did obviously not have the necessary coverage during the seminar.

Summary of Human Factor Analysis

Principles of cooperative information sharing

In crises situation time constraints cause pressure on Information Sharing. Coordination meetings have to be very efficient and should be a win-win situation for every participant - coordination means pulling all the partners together, respecting people if you bring in information. From the HFA some important principles of civilian-military Information Sharing can be summed up. At the beginning we stated that the following aspects are highly relevant to develop shared situation awareness in communities of interest. These aspects are still valid and can be differentiated for the IMISAS environment of crises response on a higher echelon planning team:

Feed-back and Feed-forward: Share information in a timely manner and coordinate Information Sharing on a regular basis

Especially in the early stage of crises handling the partners´ network has to be established. So far the RFI process has to be regarded as a performance critical process in organizing planning and should be handled carefully. Even when OPT work is distracted by team building processes RFI handling has to be a robust process to external partners.

Share information and feedback to requests in a timely manner is the important principle to integrate and to keep external partners in the planning process. Even when there is negative response to requests, all requests should be answered.

Some very simple principles should also be regarded when information requests are being answered: providing translation to military terms and explain the background of the request briefly.

From working environments like dislocated command posts it is already known that especially on collaboration platforms operational information as imagery when posted on blogs or social media need explaining additional information to reinforce the interpretation of the data in the right way. This mechanism of *feeding forward information* and especially *interpretation* makes collaboration smoother and avoids misunderstanding.

Team and Partner Mental Models: Evaluate or rate information and communicate their own interpretations to partners

Information Sharing depends on the clarity of responsibilities.

Most of the AS mission partners only sometimes agree that they know exactly what to do and how to do it in order to achieve mission objectives. Civilian partners in the planning staff missed the opportunity to introduce themselves and to communicate their responsibilities. This sort of *team mental model* should be established in any way at the beginning of the mission in order to support discussion of policy, information sharing issues, and personal understandings of the problem set. Besides the own role and responsibilities also the mission goals of partners should be discussed in an early stage of planning.

The quality of information sharing also depends on the awareness of each other's information needs and each other's goals. Not only OPT positions needs

a team mental model also the interdependent external partners and OPT need a *partners mental model* to facilitate an efficient information sharing. This could be realized with branch specific and Cdr specific partners checklists for Planning and Situation Assessment to organize partners network of “must actors”, “good to know” and “might be of occasionally use”.

Information sharing should be a win-win situation for all partners
Survey data and observations support the assumptions that even higher echelon units can benefit from connectivity with people “on the ground”. In military terms information sharing should be relevant to the organisational level means the higher in the organisational structure the more aggregated provided information should be. Our findings indicate that this rule of common relevant operational information sharing seems to be not applicable in the early stage of crises response. Staff on the higher echelon might get a better understanding of the ongoing situation and better background for interpreting their own planning intentions by having access to people on the ground.

Building shared situation awareness

Shared Situation Awareness between OPT and external actors
As a matter of principle, the evaluation of situational cues allows the conclusion that no SSA in the sense of a common understanding could be observed during IMISAS and was therefore not intended to be established by the response cells. Therefore it should be gone into detail with the information that has been assessed with a high grade of common ground (to identify lessons learned in a useful manner).
The information, which started a controversy (discussion or question about content or meaning) are more likely to be assed in the same way as important or unimportant by the whole group. The importance of the information itself (see situational cue “security concerns”) seems to play a secondary role. Next to this notable fact, the forwarding media plays a role in the information cognition. Twitter and Facebook News have a much lower common assessment than announcements via APAN. Due to the fact that APAN has been a prerequisite and the role-players do not have to use Facebook or Twitter this case could be an upcoming problem for a real emergency situation. When social media is used, conversational partner should be clear named (e.g. If you post in this group, you will reach person x on position y)[89].
Shared Situation Awareness in the civilian-military OPT
Similar to the SSA assessment in the response cell in Ottobrunn to build a common information space was already not required by the OPT players. Although they had one shared overall objective there was less common

[89] Due to limited resources it was not possible to collect data from Stuttgart with this method, so the outcomes are limited extractable and can only be seen as first suggestions for upcoming seminars.

discussion about relevant information or interpretation of crises development. This might happened due to the fact, that there was no common procedure and transparent ways of information handling for the outcomes of the planning process phases. Besides the lack of common civic-military planning routine the overall function of the OPT was also challenged during the analytic seminar. In conclusion the observations of the OPT are in line with the common Human Factors recommendations for performing teams: Without defining the team mental model in the sense of the common understanding and knowledge of each other's roles, responsibility and objectives the group is more focused on team processes than on performing and fulfilling their original task.
For the development of SSA there was one interesting finding: SSA on the strategic level also needs information from the ground to gain goal awareness. This seems to be in contrast to the general assumption that higher echelon needs aggregated information spaces instead. Another observation from the civilian partners in the OPT feeds this hypothesis. It seems to be a promising way to invite experts joining the OPT planning process to get detailed information and direct assessments.

Cultural factors

Differences between civil-military, organizational, national, and other cultures can lead to misunderstanding and misconception, and may block intercultural relations within staffs and organizations. Therefore, the related cultural bound understanding of language was a main subject when the OPT started their work.
Some differences in the underlying basic assumptions could have been observed in the analytic seminar. Civilian and military partners are different in handling their information sources. For civilian actors information is always connected with a person or an expert. For them to share information is always building a network of experts and managing the coordination between the experts. Military information handling is building a network of sensor and managing the data flow and integrating sensors in one network. As one of the civilian partners mentioned military staff acts like "we put the information out there and don´t care who works with it". On the other side information handling with civilian partners should be understood in the following way: "I would like to provide information to somebody who is going to act on it" or "one connection with one person". The technical and the social view of information management cause different ways of information handling: Managing information vs. managing expertise.
Differences between civilian and military planning caused a discussion on related planning styles and processes within the OPT.

Motivation of Mission Partners

Survey data and interview data clearly indicate that AS participants where highly motivated to interact (to coordinate and to collaborate) with their mission partners in order to respond to a given crisis situation according to mission objectives. AS mission partners mostly agreed that a balanced give-and-take-basis of shared

documents and information were given. AS mission partners also appeared to be highly motivated in order to fulfill their tasks in order to achieve mission objectives. However, they were not fully satisfied by results of their work.

Technical support for UIS and civil-military cooperation

However, from the viewpoint of perceived usefulness of the information sharing mechanism the quality of information (usefulness, relevance, completeness, reliability) and related rating appears to be a key factor which was not really given.
Perceived usefulness of the IMISAS Experimentation site also lacked of sufficient access to information. Furthermore, a collaborative environment should provide more information on other present participants. Participants agreed that inviting non-military partners (via the RFI/RFA tools) to suggest venues and tools for collaboration will improve the effectiveness of that collaboration.
An information exchange site should offer all modern software functionalities. Otherwise users will get back and use their own software applications on the web. Moreover, an information exchange mechanism should also be capable of tailoring the delegation of tasks, processes and business rules.
The IMISAS Experimentation site needs to be optimized regarding velocity, stability, technical maturity, and ergonomics. The related UIS Handbook has been perceived as a good start which needs more development.

References

[Badke-Schaub et al. 2008] Badke-Schaub, Petra; Hofinger, Gesine; Lauche, Kristina [Eds.]: Human Factors. Psychologie sicheren Handelns in Risikosituationen. – Heidelberg: Springer Medizin Verlag, 2008.
[Badke-Schaub et al. 2008a] Badke-Schaub, Petra; Hofinger, Gesine; Lauche, Kristina: Human Factors. – In: [Badke-Schaub et al. 2008], pp. 3-18.
[Badke-Schaub 2008] Badke-Schaub, Petra: Handeln in Gruppen. – In: [Badke-Schaub et al. 2008], pp. 113-130.
[Bresinsky et al. 2008] Bresinsky, Markus; Detje, Frank; Littschwager, Martin: Militär: Handeln in komplexen Problemlagen. – In: [HF 2008], pp. 244-255.
[Davis et al. 1989] Davis, F.D.; Bagozzi, R.P.; Warshaw, P.R: User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. - In: Management Science, 35, 1989, 982-1003. - Internet: http://www.vvenkatesh.com/IT/Abstract/FDetal1989.asp, seen 20 August 2011.

[Dörner 1998] Dörner, Dietrich: Wissen und Verhaltensregulation: Versuch einer Integration. – In: [Mandl/Spada 1998], pp.264-279.
[Dörner 2007] Dörner, Dietrich: Die Logik des Misslingens. Strategisches Denken in komplexen Situationen. – Reinbek bei Hamburg: Rowohlt, 2007.

[IMISAS Analysis 2011] Duncan, Jeff: IMISAS MPC - Analysis Overview. - Briefing, MPC, MITRE Building, Suffolk, 2011. - Filename: “(U)_IMISAS_MPC_D2-02_Analysis_20110419.ppt”
[IMISAS AS JOT 2011] USA Analysis Team: JOT data. - Filename: "IMISAS_AS_JOT_final.xlsx”

[IMISAS AS P2 2011] USA Analysis Team: USIMISAS Analytic Seminar Period 2 Survey Type: AS Period 2 Survey. Date: 8/3/2011 - Filename: "Results_imisas_analytic_seminar_period_2_survey_0803update.DOC"
[IMISAS AS P3 2011] USA Analysis Team: IMISAS Analytic Seminar Period 3 Survey Type: Analytic Seminar Period 3 Survey. Date: 8/3/2011 - Filename: "results_imisas_analytic_seminar_period_3_survey_updated0803.DOC"
[IMISAS AS RC P5 2011] USA Analysis Team: IMISAS AS Response Cell Survey Period 5 Type: IMISAS Response Cell Survey Per 5. Date: 8/4/2011 - Filename: "Results_imisas_as_response_cell_survey_period_5.DOC"
[IMISAS ASG 2011-07-14] N.N. (IMISAS Analysis Team): Analysis & Data Collectors Study Guide. - Analytic Seminar, August 1-4, 2011. - Unfertiges Arbeitsdokument, übersendet am 18.07.11 von Jeff Duncan (USA Analyse), TASC, 1040 University Blvd, Portsmouth, VA. - Filename "AS_Analysis_Study_Guide_7-14-11.doc"
[IMISAS AWG Overwiew 2011] N.N.: (IMISAS) Analytic Wargame, 1 – 4 August 2011. - o.O., 2011-05-24 (?). - Filename: “IMISAS_Analytic_Wargame_Overview_20110524.doc”
[IMISAS ED 2011] Hammack, Michael; Landino, Michael: Annex G to the End-to-End Experiment Plan - Analytic Seminar (AS) - Event Directive (ED). - Draft, Version 1.10, 13 July 2011. - Filename "(U-FOUO)_IMISAS_AS_ED_20110713_v1.1_w-Appendices.pdf"
[IMISAS HFA 2011-05-19] Westenkirchner, Peter; Semling, Corinna; Rist, Ulfert: IMISAS Human Factors (Analysis Concept – Synopsis) . Besprechungsergebnis. – Strausberg, ZTransfBw, 2011. - Filename: “2011-05-19_IMISAS_HumanFactorsAnalysis_Update.doc”
[IMISAS HF Survey P2 2011] USA Analysis Team: Human Factors Survey - Period 2. - Filename: "IMISAS Human Factors Survey - Period 2[1].pdf"
[IMISAS HF Survey P3 2011] USA Analysis Team: Human Factors Survey - Period 3. - Filename: "IMISAS Human Factors Period 3 Survey[1].pdf"
[IMISAS HF Survey P4 2011] USA Analysis Team: Human Factors Survey - Period 4. - Filename: "IMISAS Human Factors Survey Period 4[1].pdf"
[IMISAS HF Survey P5 2011] USA Analysis Team: Human Factors Survey - Period 5. - Filename: "IMISAS Human Factors Period 5 Survey[1].pdf"
[IMISAS HF Survey P6 2011] USA Analysis Team: Human Factors Survey - Period 6. - Filename: "IMISAS Human Factors End of Experiment Survey[1].pdf"
[IMISAS Results HF P2 2011] USA Analysis Team: IMISAS Human Factors Survey - Period 2 Type: HF Survey Per 2. Date: 8/2/2011. - Filename: "results_imisas_human_factors_survey_period_2_0802.ppt"

[IMISAS Results HF P2 2011a] IMISAS Human Factors Survey - Period 2. Type: HF Survey Per 2. Date: 8/2/2011 - Filename: "results_imisas_human_factors_survey_period_2_0802.ppt"
[IMISAS Results HF P3 2011] USA Analysis Team: IMISAS Human Factors Period 3 Survey Type: HF Period 3 Survey. - Filename: "results_imisas_human_factors_period_3_survey.ppt"
[IMISAS Results HF P4 2011] USA Analysis Team: IMISAS Human Factors Survey Period 4 - Type: Standard Report. Date: 8/4/2011 - Filename: "Report_imisas_human_factors_survey__period_4.ppt"
[IMISAS Results HF P4 2011a] USA Analysis Team: IMISAS Human Factors Survey Period 4 - Type: Standard Report. Date: 8/4/2011- Filename: "Results_imisas_human_factors_survey__period_4.doc"
[IMISAS Results HF P5 2011] USA Analysis Team: IMISAS Human Factors Period 5 Survey Type: HF Period 3 Survey. Date: 8/4/2011 - Filename: "results_imisas_human_factors_period_5_survey.ppt"
[IMISAS Results HF P6 2011] USA Analysis Team: IMISAS Human Factors End of Experiment Survey. Type: IMISAS HF End of Exp Survey Date: 8/4/201. - Filename: "results_imisas_human_factors_period_5_survey.ppt"
[IMISAS Results HF P6 2011a] USA Analysis Team: IMISAS Human Factors End of Experiment Survey. Type: IMISAS HF End of Exp Survey. Date: 8/4/2011 - Filename: "Results_imisas_human_factors_end_of_experiment_survey.doc"
[IMISAS Results AS P2 2011] USA Analysis Team: IMISAS Analytic Seminar Period 2 Survey. - Type: AS Period 2 Survey. Date: 8/3/2011 - Filename: "Results_imisas_analytic_seminar_period_2_survey_0803update.doc"
[IMISAS MPC Analysis Overview 2011] Duncan, Jeff: IMISAS MPC - Analysis Overview. - Briefing, MPC, MITRE Building, Suffolk, 2011. - Filename: “(U)_IMISAS_MPC_D2-02_Analysis_20110419.ppt”
[IMISAS Scenario v1.0 2011] US Joint Forces Command, Smith, Kathryn: Draft - Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS). - Disaster in Goma Scenario. - Version 1.0. - 11 May 2011. – Filename: “IMISASSCENARIO_v3_0518_2011_sdh_.docx”
[Kannheiser 1992] Kannheiser, Werner: Arbeit und Emotion. Eine integrierende Betrachtung. – München: Quintessenz, 1992.
[Mandl/Spada 1998] Mandl, Heinz; Spada, Hans [Eds.]: Wissenspsychologie. – München; Weinheim: Psychologie Verlags Union, 1988.
[Smith 2011] Smith, Kathryn (United States Joint Forces Command, IMISAS Project Lead): Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project. – File: “IMISASInfoPaper_7MAR2011.doc”
[UISC v0.6 2011] United States Joint Forces Command, Joint Concept Development and Experimentation (JCD&E), Smith, Kathryn J. (IMISAS/Project Lead); Sarcone, John (IMISAS/TASC Project Manager); Danks, Paul (Support/Transition Team Lead); Welshans, Jim (Support/Transition Team – Document Author): Unclassified Information Sharing (UIS). Unofficial Joint Operating Concept. Draft. - 26 May 2011, Version 0.6, Suffolk, VA.
[Ulich/Mayring 1992] Ulich, Dieter; Mayring, Philipp: Psychologie der Emotionen. – Stuttgart et al.: Kohlhammer, 1992.

[Venkatesh/Davis 2000] Venkatesh, V.; Davis, F.D.: A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. - In: Management Science, 46, 2000, 186-204. - Internet: http://www.vvenkatesh.com/IT/Abstract/14.asp, seen 20 August 2011.

[WP HF 2011] Wikipedia: Human Factors. – o.O., O.D. – Internet: http://en.wikipedia.org/wiki/Human_factors, seen 11 August 2011.

Annexes

Annex A: HF Survey Questions (SQ)

IMISAS AS – DEU Survey Questions
DEU Analysis Team @ IABG, Ottobrunn
Version 1.0 as of 29 July 2011 (DRAFT)
Authors: Lukas Bucher, Dr. Ulfert Rist, Corinna Semling, Nikolaus Wlczek

Question – Period –Matrix

Every “x” in the following table indicates, that the according question is supposed to be presented in the survey following the according period. This table indicates planning status as of 28 July 2011.

Color code: green = quick answer (seconds), yellow = middle answer (up to 30 seconds), blue = intensive answer (up to one minute), grey = up to two minutes

Topic	Question #	01 Aug – Period 1	02 Aug – Period 2	02 Aug – Period 3	03 Aug – Period 4	03 Aug – Period 5	04 Aug – Period 6
1: IS	SQ01				x		
	SQ02						x
	SQ03		x				
	SQ04		x				
	SQ05						x
	SQ06						x
	SQ07		x				
	SQ08		x				
	SQ09		x				
	SQ10				x		
	SQ11		x	x	x	x	
	SQ12		x				
	SQ13						x
	SQ14				x		
	SQ15				x		
	SQ16				x		
	SQ17						x
	SQ18					x	
2: SSA	1			x		x	
	2			x		x	
	3			x		x	
	4			x		x	
	5			x		x	
	6			x		x	
	7			x		x	
	8			x		x	
	9			x		x	
	10			x		x	
	11						x
	12						x
	13						x
	14						x
	15						x
	16						x

	17						x

Topic 1: Information Sharing (IS)

Part 1: Communication Issues

1. If you would have been your counterpart, what would you change / improve in information sharing? Please specify for civilian/non-governmental, civilian/governmental and military mission partners. [SQ01]
    a. civ/non-gov _____
    b. civ/gov _____
    c. mil _____

(updated and reduced [IMISAS Results HF P4 2011a]: "What could the mission partners do to better communicate with you? Please specify the mission partner in your answer. (If none, please enter 'NONE' in the box below.)")

2. In which situations did you experience best and poor results when using the IMISAS Experimentation site as platform for information sharing? [SQ02]
    a. Best results _____
    b. Poor results _____

(updated wording and structure [IMISAS Results HF P6 2011]:

SQ02.1: In which situations did the IMISAS Experimentation site give you good results? (If none, please enter 'NONE' in the box below.

SQ02.2: In which situations did the IMISAS Experimentation site give you poor results? (If none, please enter 'NONE' in the box below.)

3. My mission partners are ready to share information with me. [SQ03] (updated wording for the survey in cooperation with USA analysis team: "My mission partners are willing to share information with me.")
    a. civ/non-gov mission partners (scale 1=Strongly Disagree to 5=Strongly Agree)[90]
    b. civ/gov mission partners (scale 1=Strongly Disagree to 5=Strongly Agree)

[90] The following wording has been used by the USA team in the scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree nor Disagree, 4 = Agree, 5 = Strongly Agree .

c. mil mission partners (scale 1=Strongly Disagree to 5=Strongly Agree)
d. Do dou have comments?_____

(Annotation: open question d.) appears to have been skipped due to time restrictions)

4. I am ready to share information with my mission partners. [SQ04] (updated wording for the survey in cooperation with USA analysis team: “I am willing to share information with my mission partners.”)
   a. civ/non-gov mission partners (scale 1=Strongly Disagree to 5=Strongly Agree)
   b. civ/gov mission partners (scale 1=Strongly Disagree to 5=Strongly Agree)
   c. mil mission partners (scale 1=Strongly Disagree to 5=Strongly Agree)
   d. Do dou have comments?_____

5. I would provide every required unclassified Information to my mission partners. [SQ05] (updated wording [IMISAS Results HF P6 2011]: “I would feel comfortable providing all available unclassified Information requested by my mission partners on a site similar to the IMISAS Experimentation site.”)
   a. civ/non-gov mission partners (scale 1=Strongly Disagree to 5=Strongly Agree)
   b. civ/gov mission partners (scale 1=Strongly Disagree to 5=Strongly Agree)
   c. mil mission partners (scale 1=Strongly Disagree to 5=Strongly Agree)
   d. Which kind of information would you not provide to your mission partners? And why?
      _____

6. Regarding the technical security conditions of the IMISAS Experimentation site, I would provide every required unclassified information there. [SQ06] (updated wording [IMISAS Results HF P6 2011]: “I will provide all available unclassified Information requested by my mission partners regardless of the information sharing mechanism.”) (scale 1=Strongly Disagree to 5=Strongly Agree)
   a. Which kind of information would you not provide on the IMISAS Experimentation site? And why?
      _____

(updated wording and structure [IMISAS Results HF P6 2011]: “Which kinds of unclassified information would you not share with your mission partners on a site similar to the IMISAS Experimentation site? (If not applicable, please enter 'N/A' in the box below.))”

7. I recognize information from my mission partners as reliable. [SQ07] (updated wording cooperation with USA analysis team for the survey: “Information from my mission partners is reliable.”)
    a. civ/non-gov mission partners (scale 1=Strongly Disagree to 5=Strongly Agree)
    b. civ/gov mission partners (scale 1=Strongly Disagree to 5=Strongly Agree)
    c. mil mission partners (scale 1=Strongly Disagree to 5=Strongly Agree)
    d. Which kind of information would you not recognize as reliable from your mission partners? And why?

       _____

       (updated wording cooperation with USA analysis team for the survey: “What types of information from your mission partners are not generally reliable ? And why?”)

8. My support of civil-military cooperation is important. [SQ08] (scale 1=Strongly Disagree to 5=Strongly Agree)
    a. What is your attitude regarding civil-military cooperation?

       _____

    (SQ08a has been skipped due to time restrictions)

9. My motivation regarding interagency cooperation is important. [SQ09] (scale 1=Strongly Disagree to 5=Strongly Agree) (updated wording cooperation with USA analysis team for the survey: “I believe that interagency cooperation is important.”)
    a. What is your attitude regarding interagency cooperation?

       _____

    (SQ09a: own question and updated wording cooperation with USA analysis team for the survey: “Please explain your answer in Question (6) above regarding the importance of interagency cooperation.”)

10. Which additional benefit do you get when using the IMISAS Experimentation site (regarding other communication ways)? [SQ10]

11. Which five features/functionalities of the IMISAS Experimentation site did you use most in order to perform your tasks during the previous period? [SQ11]
    Please rank your answers according to importance.
    1 _____
    2 _____
    3 _____
    4 _____
    5 _____

Annotation:
SQ11 has been reengineered with the USA analysis team (Jim Dare) in the following way:
SQ11(update): Please select the five features/functionalities of the IMISAS Experimentation site that you used the most in order to perform your tasks during this experiment period. (If you used less than five of the features/functionalities, please select those you did use.)
□ Did not use any functions of the IMISAS Experimentation Site
□ Situation Report (SITREPs) Blog
□ Files and Imagery – Media Galleries
□ Map View User of Defined Operational Picture (UDOP)
□ Forum
□ Group Chat
□ Help Function
□ Email
□ One to One Chat
□ Document Collaboration Wiki
□ Group Activity Log
□ Adobe Connect Online (ACO)
□ Quick Launch Links (“Start here”)
□ Social Media Feeds
□ Search
□ Weather
□ Group Members Listing
□ Validity and Rating of Information Posted on UIS Sites
□ Access, Permissions and Graduated Access

Part 2: General

12. What is your given role and task in the Analytic Seminar (AS)? [SQ12] (updated wording cooperation with USA analysis team for the survey: "What is your assigned role and tasking for the Analytic Seminar?")

    _____ (open question)

13. If you could change something for fundamental improvements in information sharing in general with mission partners, what would it be? [SQ13] _____ (open question)

    (updated wording [IMISAS HF Survey P6 2011]: "What fundamental improvements to information sharing with

    mission partners would you recommend? (If none, please enter 'NONE' in the box below.)")

14. Is it the case that mission partners tend to slow down their effort when mission partners cannot identify their own contribution on the IMISAS Experimentation site? [SQ14] (updated wording: "Mission partners tend to slowly decrease their effort when they cannot identify their own contributions on the IMISAS Experimentation site." [IMISAS Results HF P4 2011]) (yes/no)

15. Is it the case that mission partners tend to take over less responsibility when there are other capable mission partners present in a collaborative situation (e.g. ACO, chat) on the IMISAS Experimentation site? [SQ15] (updated wording [IMISAS Results HF P4 2011]: "Mission partners take less responsibility when there are other capable mission partners present in a collaborative situation (e.g. ACO, chat)."") (yes/no)

16. The IMISAS Experimentation site helps me to achieve my given tasks/goals? [SQ16] (scale 1=Strongly Disagree – 5=Strongly Agree) [SQ16.1]
    a. What functionality in special?
       _____ [SQ16.2]

17. When you critically look at the IMISAS Experimentation site, what are the real benefits/draw backs regarding your given role and tasks? [SQ17]
    b. benefits _____ [SQ17.1]

c. draw backs _____ [SQ17.2]

(updated wording and structure:

SQ17.1: “Based upon your experience this week and your role and responsibilities in the experiment, what were the benefits to using the IMISAS Experimentation site? (If none, please enter 'NONE' in the box below.)”

SQ17.2: “Based upon your experience this week and your role and responsibilities in the experiment, what were the drawbacks to using the IMISAS Experimentation site? (If none, please enter 'NONE' in the box below.)”)

Part 3: Ergonomy

18. To what extent does the IMISAS Experimentation site support you to perform your tasks regarding the following aspects? [SQ18]
    a. clear arrangement (scale 1=Strongly Disagree – 5=Strongly Agree) [SQ18.1]
    b. capability for self-disclosure (scale 1=Strongly Disagree to 5=Strongly Agree) [SQ18.2]
    c. understandability (scale 1=Strongly Disagree to 5=Strongly Agree) [SQ18.3]
    d. information content (scale 1=Strongly Disagree to 5=Strongly Agree) [SQ18.4]
    e. chance for support (scale 1=Strongly Disagree to 5=Strongly Agree) [SQ18.5]

Topic 2: Shared Situation Awareness (SSA)

Part 1: Interdependencies

1. Which of your planned actions and intentions have you successfully completed during the operation day?

2. Which of the civilian agency or organization, military command or partners have been your main three mission partners in the operation day?

3. Were you aware of your mission partners goal achievement or plan realization during the operation day?
   A. All the time b: Most of the time C. Sometimes D. Not at all

4. Which of your own actions were mandatory for your mission partners’ achievement of plans/ activities/ targets?

5. Which of your mission partners’ actions have been supportive in fulfilling your own goals?

6. Which of your actions or options might endanger (hinder, constrain) your mission partners' target achievement?

7. Which of your mission partners' actions or options might endanger or hinder your organization's target achievement?

8. What have been the three main achievements of your mission partners during the operation day?

9. What kind of problems did you have with your mission partners? List the current three main problems experienced with your mission partner.

10. What kind of problems do you think had your mission partners? List the current three main problems experienced by your mission partner.

Part 2: Quality of Information Exchange

The following statements relate to your most important partner organization. For the most important partner organizations, the following statements should be rated on a scale:
(Scale = Strongly Disagree, Disagree, Netiher Agree or Disagree, Agree, Strongly Disagree, N/A)

11. I experienced disruptions in coordination between my mission partners and my own organization.
12. My mission partners gave us all their information that was relevant for my organization.
13. My mission partners provided us with a lot of information that was not relevant for my organization.
14. Despite the time shift between operation days I always had an overall picture of the situation.
15. I exchanged some thoughts / ideas about likely and unlikely crises development with my mission partners.
16. Occasionally my mission partners confused me by their way of sharing information.

Annex B: HF Interviews

Annex B.1: Motivation Interview

Annotation: Coding of Interview Questions (IQ) in brackets.

Interview IMISAS HFA

Responsible Analyst/Observer:
PLEASE FILL IN YOUR DATA !
Date and Time: _____ [IQ0.1]
Location: ❑ Response Cell OTN ❑ Response Cell STG ❑ OPT STG [IQ0.2]
Interview Partner, IMISAS Role and Name: _____ [IQ0.3], [IQ0.4]
Abbreviations:

civ	civilian organization (in general)
civ-gov	civ governmental
civ-ngv	civ non-governmental
civ-gvs	subordinated civ-gov department
mil	military
mn	multinational
nat	nat

1. Describe your activities and your area of responsibility. [IQ01]

   _____
   _____

2. What is your contribution to mission partners in order to achieve their mission objectives? [IQ02]

   _____
   _____
   _____

3. As a mission partner I fully support cooperation with my (civ, civ-ngv, civ-gov…) mission partners. [IQ03]

civ ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ03.1]
civ-ngv ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ03.2]
civ-gov ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ03.3]
civ-gvs ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ03.4]
mil ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ03.5]

mn ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ03.6]
nat ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ03.7]

4. As a mission partner I fully support the mission objectives.
   ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ04]

5. As a mission partner I know exactly what to do and how to do it in order to achieve mission objectives.
   ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ05.1]
   Please comment [IQ05.2]

6. My mission partners always work hard in order to achieve mission objectives. [IQ06]

civ ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ06.1]
civ-ngv ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ06.2]
civ-gov ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ06.3]
civ-gvs ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ06.4]
mil ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ06.5]
mn ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ06.6]
nat ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ06.7]

7. As a mission partner I always work hard in order to achieve mission objectives. [IQ07]
   ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ07.1]
   Please comment [IQ07.2]
   _____
   _____
   _____

8. My mission partners always continue trying in the face of difficulties, instead of giving up. [IQ08]

civ ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ08.1]
civ-ngv ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ08.2]
civ-gov ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ08.3]
civ-gvs ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ08.4]
mil ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ08.5]
mn ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ08.6]
nat ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ08.7]

9. As a mission partner I always continue trying in the face of difficulties, instead of giving up. [IQ09]

   ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ09.1]
   Please comment [IQ09.2]
   _____
   _____
   _____

10. As a mission partner I act on specific goals. [IQ10]
    ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ10]

11. As a mission partner I act on difficult goals. [IQ11]
    ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ11]

12. As a mission partner I always look for better ways to do a job [IQ12]
    ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ12]

13. As a mission partner I believe that I can get my job done. [IQ13]
    ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ13]

14. As a mission partner I believe I am capable of performing at high levels. [IQ14]
    ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ14]

15. As a mission partner I desire the results of my work in the mission. [IQ15]
    ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ15]

16. As a mission partner the results of my work in the mission give me full satisfaction. [IQ16]

❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ16]

17. My mission partners appear to be trustworthy to me. [IQ17]

civ ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ17.1]
civ-ngv ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ17.2]
civ-gov ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ17.3]
civ-gvs ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ17.4]
mil ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ17.5]
mn ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ17.6]
nat ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ17.7]

18. My mission partners act on a balanced give-and-take basis. [IQ18]

civ ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ18.1]
civ-ngv ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ18.2]
civ-gov ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ18.3]
civ-gvs ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ18.4]
mil ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ18.5]
mn ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ18.6]
nat ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ18.7]

19. My mission partners provide useful information to me. [IQ19]

civ ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ19.1]
civ-ngv ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ19.2]
civ-gov ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ19.3]
civ-gvs ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ19.4]
mil ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ19.5]
mn ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ19.6]

nat ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ19.7]

20. My mission partners provide relevant information to me. [IQ20]

civ ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ20.1]
civ-ngv ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ20.2]
civ-gov ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ20.3]
civ-gvs ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ20.4]
mil ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ20.5]
mn ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ20.6]
nat ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ20.7]

21. My mission partners provide complete information to me. [IQ21]

civ ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ21.1]
civ-ngv ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ21.2]
civ-gov ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ21.3]
civ-gvs ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ21.4]
mil ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ21.5]
mn ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ21.6]
nat ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ21.7]

22. My mission partners provide reliable information to me. [IQ22]

civ ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ22.1]
civ-ngv ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ22.2]
civ-gov ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ22.3]
civ-gvs ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ22.4]

mil ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ22.5]
mn ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ22.6]
nat ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ22.7]

23. To what extent does the IMISAS Experimentation site support you to perform your tasks regarding the following aspects? [IQ23]

Fast:

❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ23.1]

Stable:

❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ23.2]

Technically mature:

❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ23.3]

24. My procedures (e.g., SOPs) allow that I provide every required unclassified information to my mission partners. [IQ24]

civ ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ24.1]
civ-ngv ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ24.2]
civ-gov ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ24.3]
civ-gvs ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ24.4]
mil ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ24.5]
mn ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ24.6]
nat ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ24.7]

Please comment [IQ24.8]

_____
_____
_____

25. My policy allows that I provide every required unclassified information to my mission partners. [IQ25]

civ ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ25.1]
civ-ngv ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ25.2]
civ-gov ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ25.3]
civ-gvs ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ25.4]
mil ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ25.5]
mn ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ25.6]
nat ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ25.7]

Please comment [IQ25.8]

_____

_____

_____

26. As a mission partner I fully support coordination with my mission partners. [IQ26]

civ ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ26.1]
civ-ngv ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ26.2]
civ-gov ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ26.3]
civ-gvs ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ26.4]
mil ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ26.5]
mn ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ26.6]
nat ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ26.7]

27. As a mission partner I fully support cooperation my with mission partners. [IQ27]

civ ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ27.1]
civ-ngv ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ27.2]
civ-gov ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ27.3]
civ-gvs ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ27.4]

mil ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ27.5]
mn ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ27.6]
nat ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree [IQ27.7]

28. If you were your mission partner, what would you propose in order to change your own way of information sharing in order to achieve mission objectives? [IQ28]

_____
_____
_____
_____
_____

Annex B.2: MCSSA Interview

Interview and Observation Guideline MCSSA

Date: _____ Observer / Interviewer: _____
Location: ❑ Response Cell OTN ❑ Response Cell STG ❑ OPT STG
Observed or interviews IMISAS Role: _____

Part A: Information Exchange

1. Describe your activities and your area of responsibility.

   _____
   _____

2. Who are your civilian / military / governmental partners?

   A: Partners, you needed to get useful information?

   _____
   _____

   B: Partners, you worked with and provided own working results?

   _____
   _____

3. Were you aware of your organizations goal achievement during the operation day?
   A. All the time B. Most of the time C. Sometimes D. Not at all

   _____

4. In what form did you receive the information (i.e. written, oral, phone…)? Please rank your answer according to frequency

A _____
B _____
C _____

5. Please specify the content of your communication.

   _____

   _____

   _____

6. Describe the frequency of mutual Information exchange using the different communication lines.

   A _____: ❑ all the time ❑ most of the time ❑ sometimes
   B _____: ❑ all the time ❑ most of the time ❑ sometimes
   C _____: ❑ all the time ❑ most of the time ❑ sometimes

7. Observations:

Please note Critical Incidents or utterances concerning the ways and procedures of information exchange

Time	*Observation*

Part B: Quality of Information Exchange and Coordination

1. Describe the problems encountered during work. Have you expected these disruptions or obstacles?

   Please use the following categories:

   - ❑ Time delay: _____
   - ❑ Communication resources: _____
   - ❑ Voice: _____
   - ❑ Gestures: _____
   - ❑ Inexperienced Counterparts: _____
   - ❑ Contradictions of…: _____
   - ❑ Lack of situation awareness of your counterparts: _____
   - ❑ Unexpected ways of communication / information exchange: _____
   - ❑ Other:

     _____

     ____

2. How did you recognize the relevance of your mission partner´s information provided to you since the beginning of your interaction?

   _____

3. Observations:

Please note Critical Incidents or utterances concerning the quality of information exchange

Time	*Observation*

Part C: Situational Picture

1. Which content based on civilian / military / governmental information has become an **essential part** of your **current** situational picture?

   - ❑ A relevant information of the situational picture **for accomplishing my own tasks**_____
     _____
   - ❑ B relevant information of the situational picture **for gaining a comprehensive understanding** of the ongoing crises development
     _____
     ____

2. Which information helped you to gain **a comprehensive understanding for the development** of the ongoing situation in **the future**?

   - ❑ A relevant information of the situational picture **for accomplishing my own tasks**_____
     _____
   - ❑ B relevant information of the situational picture **for gaining a comprehensive understanding** of the ongoing crises development
     _____
     ____

3. Have you been thinking of likely and unlikely crises development together with your my mission partners (or at least on your own)?

   _____

4. How much effort did you spend on gaining a good understanding of the situation? Was it important for you?

   _____

5. And on the other side, do you think it was necessary to have a shared situation awareness between the mission partners?

_____

6. How far the time jumps between operation days had a negative impact on your overall picture of the situation?

_____

7. Critical Incident

A shared or common understanding between partners helps to deal with difficult and unclear situations in complex missions. It is often described as ‘being aware’ of the partner´s informational needs and good sense of the ongoing situation.

Have you been pleased by your partner´s information support in the operation day? Have you been disappointed by your partner at any time? *Please describe the situation briefly.*

Annex C: Survey Questions on UIS Handbook

Contextual information: Additionally to the request of experiment lead Kathryn Smith[91], specific and supportive HF questions on the UIS handbook have been developed by the DEU HF team in Stuttgart during the Analytic Seminar at night at 02 August and handed over from DEU lead analyst to USA study director per E-mail. In the next morning a selection of questions and word-smithing has been conducted.

UIS Handbook

1. In which situation are you supposed to use the UIS Handbook? [HBQ01]

Please specify

_____
_____
_____

2. In which way are you going to use the UIS Handbook? [HBQ02]

Please explain

_____
_____
_____

3. The usage of the UIS Handbook really helps me to achieve my mission objectives. [HBQ03]
   ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree

4. The usage of the UIS Handbook really helps me to conduct information sharing with my mission partners. [HBQ04]
   ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree

5. The UIS Handbook reflects real world conditions. [HBQ05]
   ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree

6. The UIS Handbook appears to be applicable to and consistent with given procedures (e.g., SOPs) of my organization to me. [HBQ06]

---

[91] Transmitted from LTC (GS) Soenke Marahrens at 02 August 2011: "I would be very interested in ensuring that we are capturing some of the human engagement in making decisions about how and when to use the handbook and use information sharing tools. I think we need those observations, because we aren't going to get them from the surveys."

❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree

7. The UIS Handbook appears to be applicable to and consistent with given policies of my organization to me. [HBQ07]
   ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree

8. The UIS Handbook appears to be applicable to given functionalities of the IMISAS experimentation site to me. [HBQ08]
   ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree

9. I would like to recommend the usage of the UIS Handbook to my mission partners. [HBQ09]
   ❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree

10. Being asked, the UIS Handbook could be updated and optimized in the following way. [HBQ10]

Please describe frankly regardless of rank, position, and organization

_____
_____
_____

Information Sharing Tools

11. In which situation and for what reasons are you supposed to use information sharing tools? [HBQ11]

Please specify

_____
_____
_____

12. In which way are you using information sharing tools? [HBQ12]

Please explain

_____
_____
_____

13. The usage of information sharing tools really helps me to achieve my mission objectives. [HBQ13]

❑ Strongly agree ❑ Agree ❑ Sometimes agree ❑ Disagree ❑ Strongly disagree

Annex D: HFA Template for Observations of Communications

An observation template has been created to be used by HF analysts (focus: motivation, attitudes, and information sharing) to quickly cover ad hoc observations.

IMISAS HFA Communications

Date and Time: _____, Analyst/Observer: _____

Location: ❑ Response Cell OTN ❑ Response Cell STG ❑ OPT STG

Date, Time	**Involved Role Players/Organizations**	**Activity, Topic, Issue, Content, Event**	**Description of Communication Channels (Docs, Chat, Phone, etc.)**	**Related Processes, Procedures, SOPs**	**Observed Difficulties, Problems, Success Stories etc.**	**Annotation**
Date: Time: Duration:						
Date: Time: Duration:						

Annex E: DEU Analytic Hierarchy for Motivation, Attitudes, and IS

In the outline (tree structure) the following abbreviations will be used: High-level hypothesis (HLH), Hypothesis (H), Working Hypothesis (WH), Analytic Question (AQ), Survey Question (SQ), and Interview Question (IQ).

1. High-level hypothesis (HLH): Changes of motivation cause changes in quality and quantity of information sharing, coordination, and cooperation in the group of mission partners, which result in a change of achievement of objectives.[92]
   - 1.1. Hypothesis (H): High motivation causes better quality and increased quantity of information sharing, coordination, and cooperation in the group of mission partners, therefore a better achievement of objectives will be the result.
     - 1.1.1. Working Hypothesis (WH): If high motivation causes better quality and increased quantity of information sharing in the group of mission partners, then a better achievement of objectives will be the result.
       - 1.1.1.1. Analytic Question (AQ): To what extent does motivation cause a better quality and increased quantity of information sharing in the group of mission partners?
       - 1.1.1.2. AQ: To what extent does a better quality and increased quantity of information sharing cause a better achievement of objectives?
     - 1.1.2. WH: If high motivation causes better quality and increased quantity of coordination in the group of mission partners, then a better achievement of objectives will be the result.
       - 1.1.2.1. AQ: To what extent does motivation cause a better quality and increased quantity of coordination in the group of mission partners?
       - 1.1.2.2. AQ: To what extent does better quality and increased quantity of coordination in the group of mission partners cause a better achievement of objectives?
     - 1.1.3. WH: If high motivation causes better quality and quantity of cooperation in the group of mission partners, then a better achievement of objectives will be the result.
       - 1.1.3.1. AQ: To what extent does motivation cause a better quality and increased quantity of cooperation in the group of mission partners?

[92] Interpretation of [Badke-Schaub 2008].

1.1.3.1.1. IQ: As a mission partner I fully support cooperation with my mission partners. (different mission partners and agreement scale)

1.1.3.1.2. SQ08: My support of civil-military cooperation is important. (agreement scale)

1.1.3.1.3. IQ/(before: SQ08a) What is your attitude regarding civil-military cooperation? (open question)

1.1.3.1.4. SQ09: My motivation regarding interagency cooperation is important. (agreement scale)

1.1.3.2. AQ: To what extent does better quality and increased quantity of cooperation in the group of mission partners cause a better achievement of objectives?

2. HLH: Certain conditions cause changes of motivation for quality and quantity of information sharing, coordination, and cooperation in the group of mission partners.

2.1. H: Favorable conditions cause a higher motivation for quality and quantity of information sharing in the group of mission partners.

2.1.1. WH: If favorable conditions cause a higher motivation, then a better quality and increased quantity of information sharing in the group of mission partners will be the result.

2.1.1.1. AQ: To what extent do inputs of mission partners (contributions to the mission, such as time, effort, education and experience) cause higher motivation for a better quality and increased quantity information sharing?

2.1.1.1.1. SQ12: What is your given role and task in the Analytic Seminar (AS)? (open question)

2.1.1.1.2. IQ04: As a mission partner I fully support the mission objectives. (agreement scale)[93]

2.1.1.1.3. IQ05: As a mission partner I know exactly what to do and how to do it in order to achieve mission objectives. (agreement scale)

2.1.1.1.3.1. IQ01: Describe your activities and your area of responsibility (open question)

2.1.1.1.3.2. IQ02: What is your contribution to mission partners in order to achieve their mission objectives? (open question)

[93] Individual attitudes regarding given objectives and mission partners influence the achievement of these objectives. See effort measure, [WP HF 2011].

2.1.1.1.4. IQ06: My mission partners work always hard in order to achieve mission objectives. (different mission partners and agreement scale) (see effort measure, [WP HF 2011])[94]

2.1.1.1.5. IQ07: As a mission partner I always work hard in order to achieve mission objectives. (agreement scale and open question)

2.1.1.1.6. IQ08: My mission partners always continue trying in the face of difficulties, instead of giving up. (different mission partners and agreement scale)[95]

2.1.1.1.7. IQ09: As a mission partner I always continue trying in the face of difficulties, instead of giving up. (agreement scale and open question)[96]

2.1.1.1.8. SQ14: Is it the case that mission partners tend to slow down their effort when mission partners cannot identify their own contribution on the IMISAS Experimentation site? (yes/no)

2.1.1.1.9. SQ15: Is it the case that mission partners tend to take over less responsibility when there are other capable mission partners present in a collaborative situation (e.g. ACO, chat) on the IMISAS Experimentation site? (yes/no)

2.1.1.2. AQ: To what extent do outcomes of mission partners (anything a mission partner gets from a job or organization, such as pay, job security, benefits, and awards) cause higher motivation for a better quality and increased quantity information sharing?

2.1.1.3. AQ: To what extent do high performance levels of mission partners (contributions to the mission's efficiency, effectiveness and overall goals) cause a higher motivation for a better quality and increased quantity information sharing?[97]

2.1.1.3.1. IQ10: As a mission partner I act on specific goals. (agreement scale)

2.1.1.3.2. IQ11: As a mission partner I act on difficult goals. (agreement scale)

[94] See persistent measure, [WP HF 2011].

[96] See persistent measure, [WP HF 2011].

[97] IQs reference different motivation theories.

2.1.1.3.3. IQ12: As a mission partner I always look for better ways to do a job.[98] (agreement scale)

2.1.1.3.4. IQ13: As a mission partner I believe that I can get my job done.[99] (agreement scale)

2.1.1.3.5. IQ14: As a mission partner I believe I am capable of performing at high levels. (agreement scale)

2.1.1.3.6. IQ15: As a mission partner I desire the results of my work in the mission. (agreement scale)

2.1.1.3.7. IQ16: As a mission partner the results of my work in the mission give me full satisfaction. (agreement scale)

2.1.1.4. AQ: To what extent do good relationships between mission partners cause a higher motivation for a better quality and increased quantity information sharing?

2.1.1.4.1. Q: Do you already know your mission partners?

2.1.1.5. AQ: Does the building and implementation of trust help to increase qualitative and quantitative information sharing with mission partners?

2.1.1.5.1. IQ17: My mission partners appear to be trustworthy to me. (different mission partners and agreement scale)

2.1.1.5.2. SQ01/IQ28: If you would have been your counterpart, what would you change / improve in information sharing? Please specify for civilian/non-governmental, civilian/governmental and military mission partners.

2.1.1.5.3. SQ03: My mission partners are ready to share information with me. (different mission partners and agreement scale)

2.1.1.5.4. SQ04: I am ready to share information with my mission partners. (different mission partners and agreement scale)

2.1.1.6. AQ: To what extent do good working conditions for mission partners cause a higher motivation for a better quality and increased quantity information sharing?

2.1.1.6.1. SQ10: Which additional benefit do you get when using the IMISAS Experimentation site (regarding other communication ways)?

2.1.1.6.2. IQ18: My mission partners act on a balanced give-and-take basis. (different mission partners and agreement scale)

---

[98] [WP HF 2011]

[99] "high levels of motivation occur when employees believe they can get the task done" [WP HF 2011]

2.1.1.6.3. SQ05: I would provide every required unclassified Information to my mission partners. Civ, mil

2.1.1.7. AQ: To what extent does the quality and quantity of provided information between mission partners cause a higher motivation for a better quality and increased quantity information.

2.1.1.7.1. IQ19: My mission partners provide useful information to me. (different mission partners and agreement scale)

2.1.1.7.2. IQ20: My mission partners provide relevant information to me. (different mission partners and agreement scale)

2.1.1.7.3. IQ21: My mission partners provide complete information to me. (different mission partners and agreement scale)

2.1.1.7.4. IQ22 My mission partners provide reliable information to me. (different mission partners and agreement scale)

2.1.1.7.5. SQ07: I recognize information from my mission partners as reliable.

2.1.1.7.6. SQ02: In which situations did you experience best and poor results when using the IMISAS Experimentation site as platform for information sharing?

2.1.1.8. AQ: To what extent do techniques and technologies for mission partners cause a higher motivation for a better quality and increased quantity information sharing?

2.1.1.8.1. SQ06: Regarding the technical security conditions of the IMISAS Experimentation site, I would provide every required unclassified information there.

2.1.1.8.2. SQ11: Which five features/functionalities of the IMISAS Experimentation site did you use most in order to perform your tasks during the previous period? Please rank your answers according to importance.

2.1.1.8.3. SQ16: The IMISAS Experimentation site helps me to achieve my given tasks/goals?

2.1.1.8.4. SQ17: When you critically look at the IMISAS Experimentation site, what are the real benefits/draw backs regarding your given role and tasks? benefits draw

2.1.1.8.5. IQ23: To what extent does the IMISAS Experimentation site support you to perform your tasks regarding the following aspects? fast, stable, technically mature (agreement scale)

2.1.1.8.6.

2.1.1.8.7. SQ18: To what extent does the IMISAS Experimentation site support you to perform your tasks regarding the

following aspects? a. clear arrangement (agreement scale); b. capability for self-disclosure (agreement scale); c. understandability (agreement scale); d. information content (agreement scale); e. chance for support (agreement scale)

2.1.1.9. AQ: To what extent do procedures (e.g. SOP) of mission partners cause a higher motivation for a better quality and increased quantity information sharing?

2.1.1.9.1. IQ24: My procedures (e.g., SOPs) allow that I provide every required unclassified Information to my mission partners. (different partners and agreement scale, and open question)

2.1.1.10. AQ: To what extent do policies of mission partners cause a higher motivation for a better quality and increased quantity information sharing?

2.1.1.10.1. IQ: My policy allows that I provide every required unclassified Information to my mission partners. (different partners and agreement scale, and open question)

2.1.1.11. AQ: General view on conditions:

2.1.1.11.1. SQ13: If you could change something for fundamental improvements in information sharing in general with mission partners, what would it be?

2.2. H: Favorable conditions cause a higher motivation for quality and quantity of coordination in the group of mission partners.

2.2.1. WH: If favorable conditions cause a higher motivation, then a better quality and increased quantity of coordination in the group of mission partners will be the result.

2.2.1.1.1. IQ26: As a mission partner I fully support coordination with my mission partners. (different partners and agreement scale)

2.3. H: Favorable conditions cause a higher motivation for quality and quantity of cooperation in the group of mission partners.

2.3.1. WH: If favorable conditions cause a higher motivation, then a better quality and increased quantity of cooperation in the group of mission partners will be the result.

2.3.1.1.1. IQ03/IQ27: As a mission partner I fully support cooperation my with mission partners. (different mission partners and agreement scale)

Annex F: IMISAS Solutions and HFA

Annex F.1 IMISAS Solutions

Solution		Element	
1-1	Process and procedures for the expedited release of controlled unclassified information (CUI) in a crisis response situation	**1-1a**	Pre-planned release matrix --Linked to Commander's release guidance --Release matrix applies risk management --Additional release authorities
		1-1b	Unclassified information storage – UISC --Business rules for storage of unclassified information on the UISC
1-2	Business rules governing the expedited transfer of unclassified information from classified networks to non-classified networks.	**1-2a**	Business rules for manual cross-domain transfer
1-3	Pre-defined template and business rules for the establishment of UISC work sites	**1-3a**	UISC work site template --UISC collaboration tools (e.g., wikis, blogs and widgets)
		1-3b	Business rules to support UISC work site --Portal establishment --Work site management
1-5	Guides to enable UIS with mission partners via a UISC	**1-5a**	Processes and procedures to effectively engage mission partners for information sharing --US Interagency, Host Nation (HN), multinational / coalition partners, IGOs and NGOs --Use of staff embeds / LNOs --Address all UIS capabilities (portal, email, phone, etc.)
1-7	Guides for staff use of UISC in support of operations	**1-7a**	Best practices to maximize use of UISC --IM / KM business rules

1-8	Quick reference guides for the roles, responsibilities and general information requirements of potential non-DOD mission partners	**1-8a**	Reference guide for mission partners --US Interagency, HN, IGOs and NGOs --Roles, responsibilities and general information requirements --Electronically searchable

Annex F.2: HFA and IMISAS solutions

The following table indicates contentwise relations of DEU survey questions (SQ), DEU interview questions (IQ), and DEU UIS handbook questions (HBQ) to IMISAS solutions from the viewpoint of HFA (focus motivations, attitudes and IS). Also, relations to issues of interest, like motivation, information sharing, procedures, and policies, are noted. By doing so, HF analysis results hopefully contribute to the USA analysis on IMISAS. Since solutions and solution elements are linked to the handbook and conceptual, the regarding CD&E process is being supported. Especially, the conceptual work on the Unclassified Information Sharing (UIS) Concept, [UISC v0.6 2011], might profit from HF findings and insights of this analysis report.

Code	S1-1	S1-2	S1-3	S1-5	S1-7	S1-8	Handbook	Objectives	Procedure	Policy	IMISAS site	IS	Trust	Knowledge	Motivation	Coordination	Cooperation	Task and Work
SQ01				x	x	x						x					x	
SQ02				x	x	x					x	x						
SQ03				x	x	x						x			x		x	
SQ04				x	x	x						x			x		x	
SQ05				x	x	x						x			x		x	
SQ06		x	x								x	x			x			
SQ07				x	x	x						x	x		x		x	
SQ08				x	x	x									x		x	
SQ09				x	x	x									x		x	
SQ10				x	x	x					x				x			
SQ11											x							x
SQ12				x	x	x								x				x

SQ13				x	x	x					x	x			x		x	
SQ14			x	x	x	x					x	x			x		x	
SQ15												x			x		x	
SQ16								x			x				x			x
SQ17			x	x				x			x							x
SQ18			x	x	x	x					x							
IQ01														x				x
IQ02								x									x	
IQ03															x			x
IQ04				x				x							x			
IQ05								x						x				x
IQ06								x							x			
IQ07								x							x			
IQ08															x			
IQ09															x			
IQ10				x	x	x		x										
IQ11				x	x	x		x										
IQ12															x			x
IQ13															x			x
IQ14															x			x
IQ15				x	x	x									x			x
IQ16															x			x
IQ17													x					
IQ18				x	x	x									x		x	
IQ19				x	x	x						x			x		x	
IQ20				x	x	x						x			x		x	
IQ21				x	x	x						x			x		x	
IQ22				x	x	x						x	x		x		x	
IQ23			x								x	x						x
IQ24	x								x			x						
IQ25		x								x		x						
IQ26				x	x	x									x	x		
IQ27				x	x	x									x		x	
IQ28				x	x	x		x				x						
HBQ01	x	x	x	x	x	x	x					x		x				x
HBQ02	x	x	x	x	x	x	x					x		x				x
HBQ03	x	x	x	x	x	x	x	x										
HBQ04	x	x	x	x	x	x	x					x			x		x	
HBQ05	x	x	x	x	x	x	x								x			
HBQ06	x						x		x									
HBQ07		x	x				x			x								
HBQ08							x				x							
HBQ09				x		x	x								x		x	
HBQ1	x	x	x	x	x	x	x											

0																		
HBQ11					x						x	x						x
HBQ12											x	x						x
HBQ13								x			x	x			x			

Annex G: HFA Data

Annex G.1: Motivation, Attitudes, and Information Sharing

The following table indicates the real life status of conducted HF survey questions due to adjustments of the USA analysis team during the Analytic Seminar because of limited time:

	P1	P2	P3	P4	P5	P6/EoE
SQ01				o		
SQ02						+ (splitted)
SQ03		o				
SQ04		o				
SQ05						o
SQ06						o (splitted)
SQ07		o				
SQ08		+				
SQ09		+				
SQ10				+		
SQ11		+	+	+	+	
SQ12		+				
SQ13						+
SQ14				+		
SQ15				+		
SQ16				+		
SQ17						+ (splitted)
SQ18 cancelled						
Group: N	OPT: 18 RCS: - RCO: -	OPT: 16 RCS: - RCO: -	OPT: 16 RCS: - RCO: -	OPT: 16 RCS: - RCO: -	OPT: 13 RCS: - RCO: -	OPT: 14 RCS: - RCO: -

Meaning of symbols:
Groups: OPT = Operational Planning Team Stuttgart, RCS = Response Cell Stuttgart, RCO = Response Cell Ottobrunn
+ = question conducted
o = question conducted in reduced form/no diversification (civ, mil, …) due to time constraints
- = no survey conducted due to time constraints

Annex G.1.1: Survey Questions (SQ)

SQ01

Period 4/OPT:
(1) HF Per 4: Better comms: (1) What could the mission partners do to better communicate with you? Please specify the mission partner in your answer. (If none, please enter 'NONE' in the box below.)

Response		
The interaction is good.		
We need better essay where they post an share there info.		
None		
NONE, most of my issues are on our DOD side of the house		
I really don't know- in DoD I feel stuck behind a huge wall of barriers. I can see there are real problems and there should be ways for DoD to assist, but bringing those together is very disjointed. To me, it's not what mission partners need to do to better communicate with us, it's us that needs to make our people and processes more accessible to them. Truly a spider web that won't go away.		
Provide a time period that they need the information. Groups on the ground and such can respond MUCH quicker than the COCOM. At the COCOM level, we operate at a glacial pace.		
They could include BASIC biographical information in their profiles so we know who we're dealing with in what section of their organization.		
I think communication needs to improve on my end, I did not check blogs/posts often enough.		
NA		
NONE		
NONE		
I can't speak for mission partners. We (DOD) need to solve our own internal communications issues first.		
none		
Provide more specific feedback that has actionable information. Additionally, a mission partner posted a question specific to another individual in the comment section under the Concept of Operation document -- not the best way to reach a specific individual.		
Military partners could ask for input from me. Specify to other partners when they should come to me. Communicate by "human" means rather than have the primay means of input be an internal planning process for a bunch of slides to give to the Commander.		
	Valid Responses	**15**
	Total Responses	**15**

[IMISAS Results HF P4 2011a]

SQ02

SQ02.1

Period 6, EoE/OPT:

6: (1) In which situations did the IMISAS Experimentation site give you good results? (If none, please enter 'NONE' in the box below.)

Response		
None...fair at best. File sharing was ok.		
RFI processing		
On the ground information, in real time once I made the right connections		
being able to upload information worked well as long as it was not a video		
RFI, once olbjective understood by team		
Gave me feedback that DoD really does not know how to plug into an operation led by another agency, nor how to work within the larger IO,NGO,HA community.		
search for information on blogs and posts		
NONE		
None		
Document storage, tracking of site activity.		
When used as described in the handbook.		
none		
none		
I was able to connect up with UN and NGOs faster than before.		
	Valid Responses	**14**
	Total Responses	**14**

[IMISAS Results HF P6 2011a]

SQ02.2

Period 6, EoE/OPT:

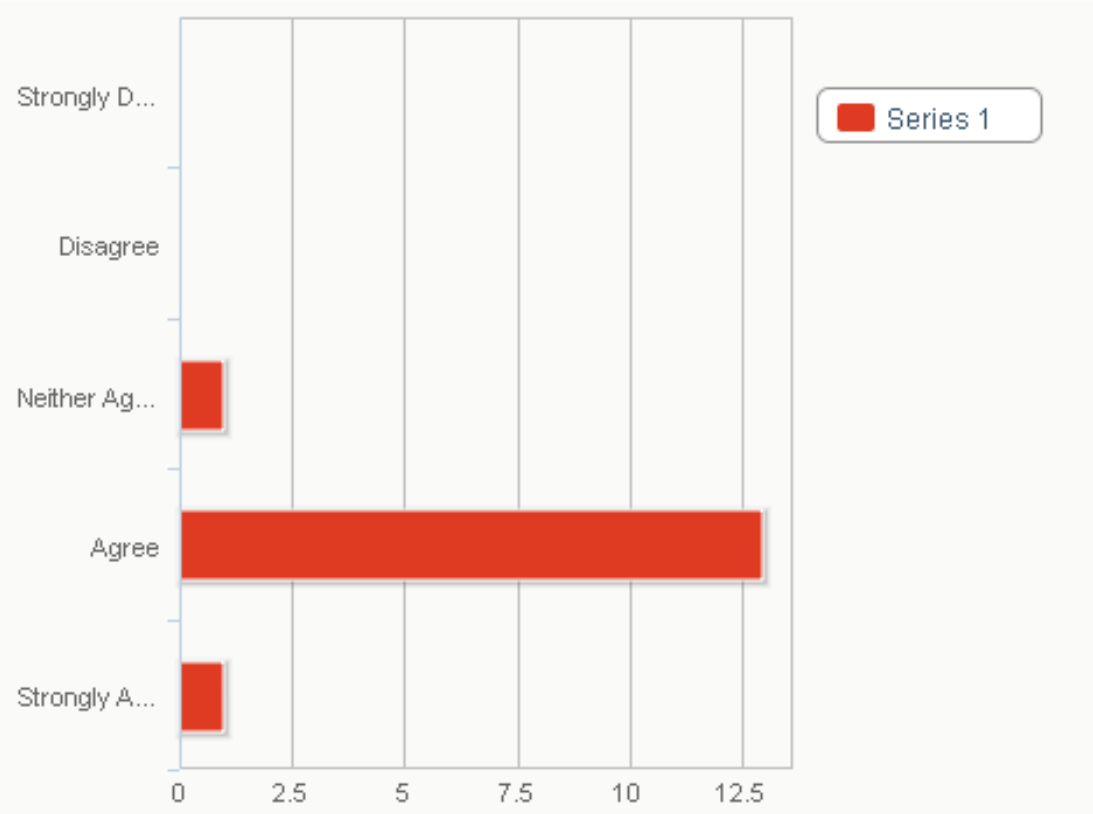
2: (2) In which situations did the IMISAS Experimentation site give you poor results? (If none, please enter 'NONE' in the box below.)

Response		
Among the worst were, chat, boards, and map.		
Establising a visual opertaing picture		
Some of the social media networks have a time-lag if the individual is not actively monitoring or using on the ground		
uploading video did not work		
The group identified areas of improvement		
none		
map view		
map wouldn't load people finder was cumbersome and not intuitive no clear place (and initially no ability to) post incoming information that did not fit into RFI/RFA		
mapping		
mapping, peer-to-peer chat, group chat, group collaboration, common operating picture.		
When utilized on the fly / ad hoc		
none		
from the beginning, there was no invitation, no agenda, no role provided. once involved, the structure was fluid and the participants hostile. there were very negative results in most of the situations.		
Its currently a poor vehicle for connecting, collecting, diseminating, and analyzing infor.		
	Valid Responses	**14**
	Total Responses	**14**

[IMISAS Results HF P6 2011a]

SQ03

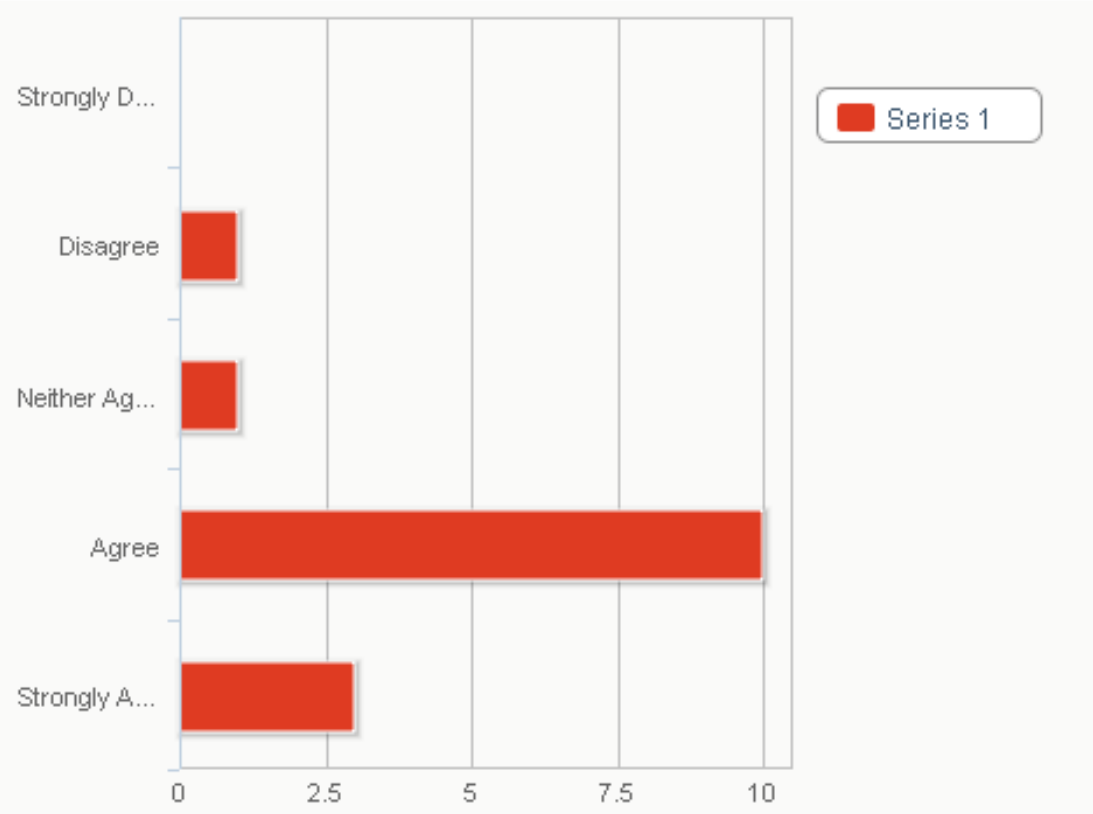
Period 2/OPT:
(1) HF Per2: Partner willingness:
(1) My mission partners are willing to share information with me.



[IMISAS Results HF P2 2011]

SQ04

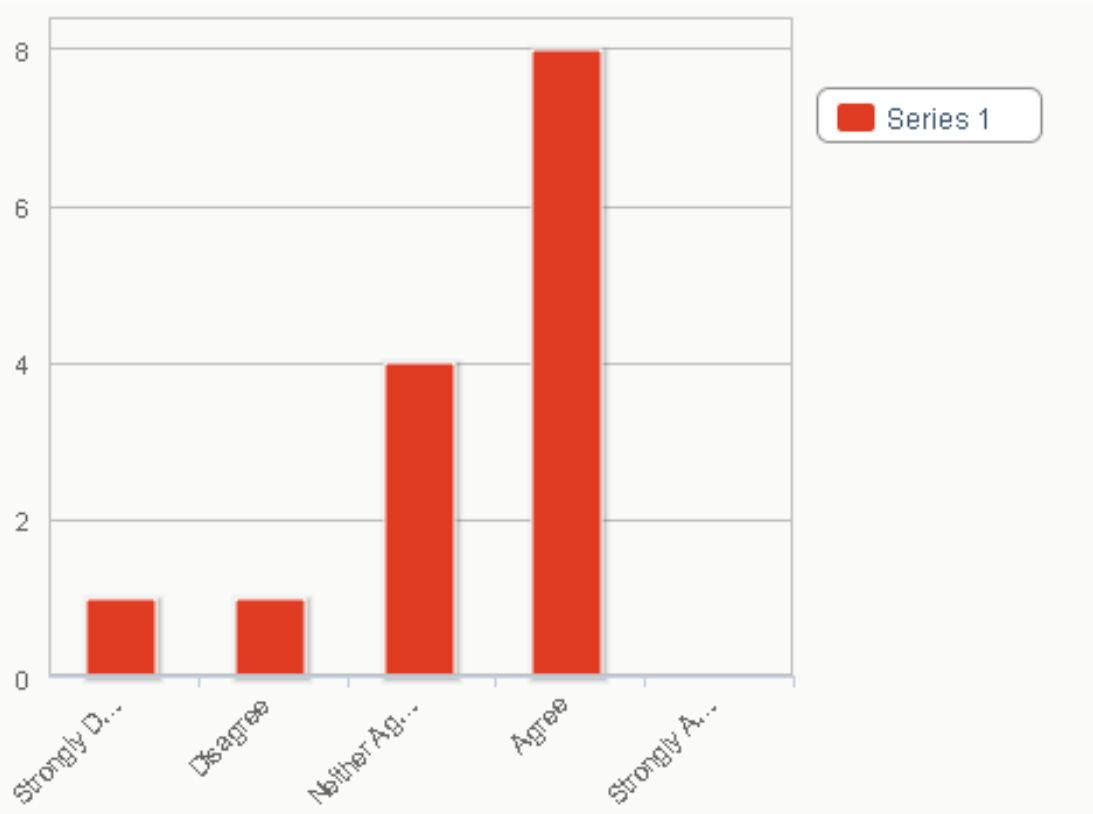
Period 2/OPT:
(2) HF Per2: My willingness:
(2) I am willing to share information with my mission partners.



[IMISAS Results HF P2 2011]

SQ05

Period 6, EoE/OPT:
(3) I would feel comfortable providing all available unclassified Information requested by my mission partners on a site similar to the IMISAS Experimentation site.

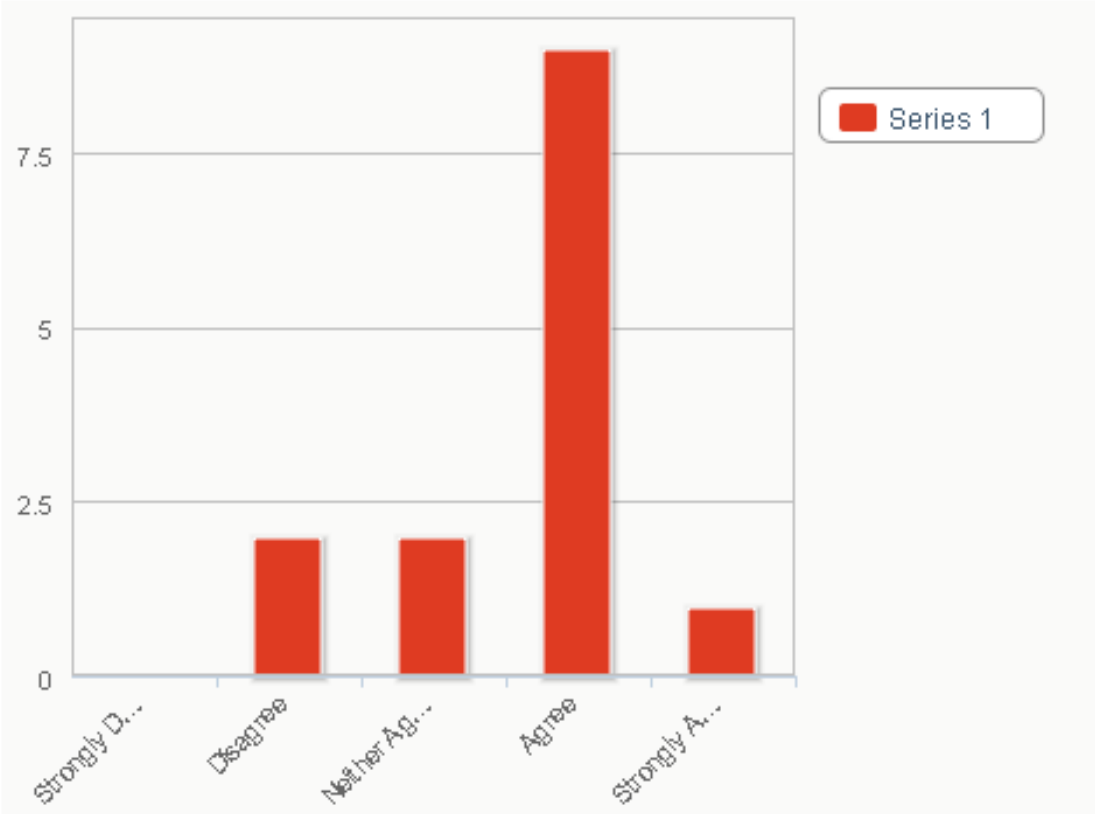


[IMISAS Results HF P6 2011]

SQ06

Period 6, EoE/OPT:

(5) I will provide all available unclassified Information requested by my mission partners regardless of the information sharing mechanism.



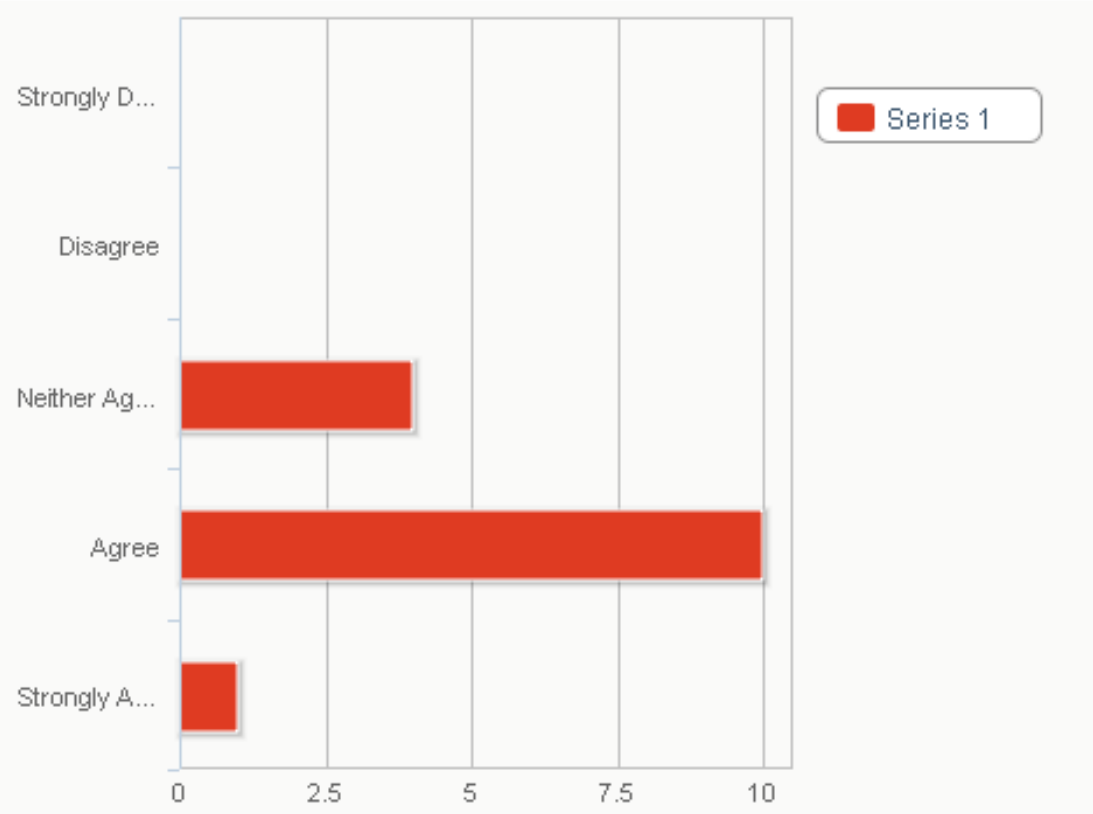
[IMISAS Results HF P6 2011]

SQ07

Period2/OPT:

(3) HF Per2: Info reliability:

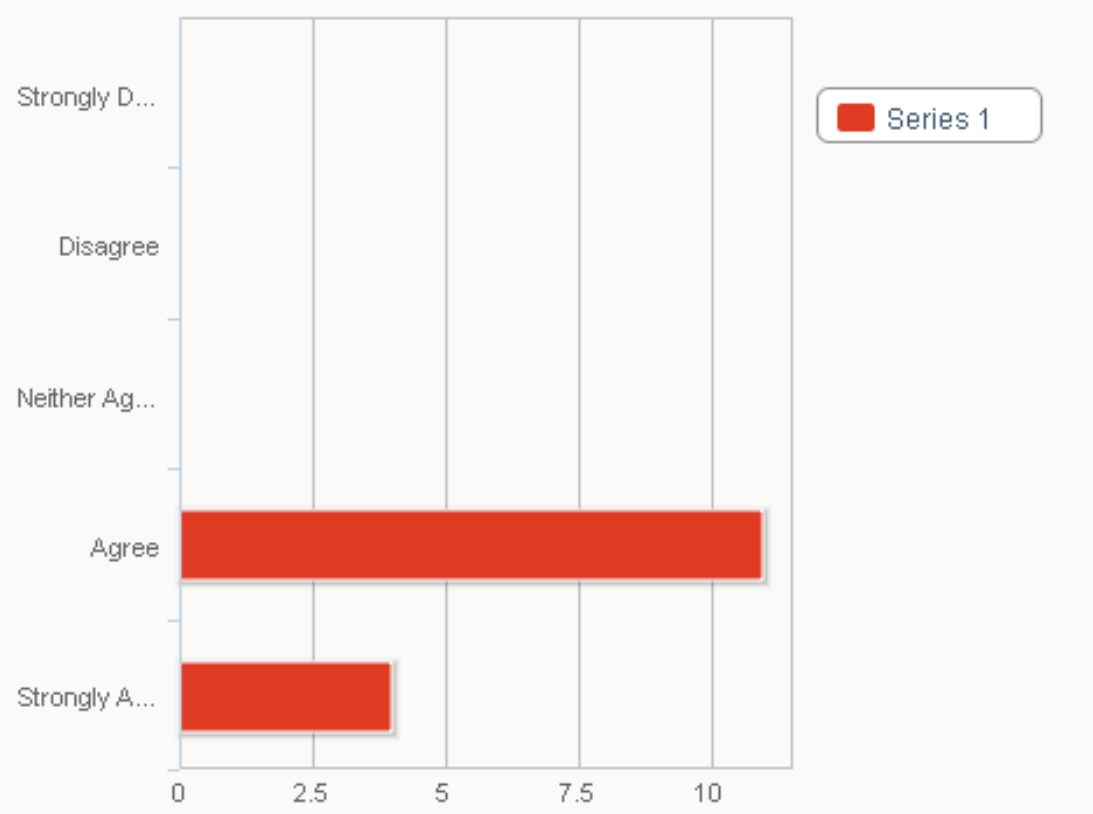
(3) Information from my mission partners is reliable.



[IMISAS Results HF P2 2011]

SQ08

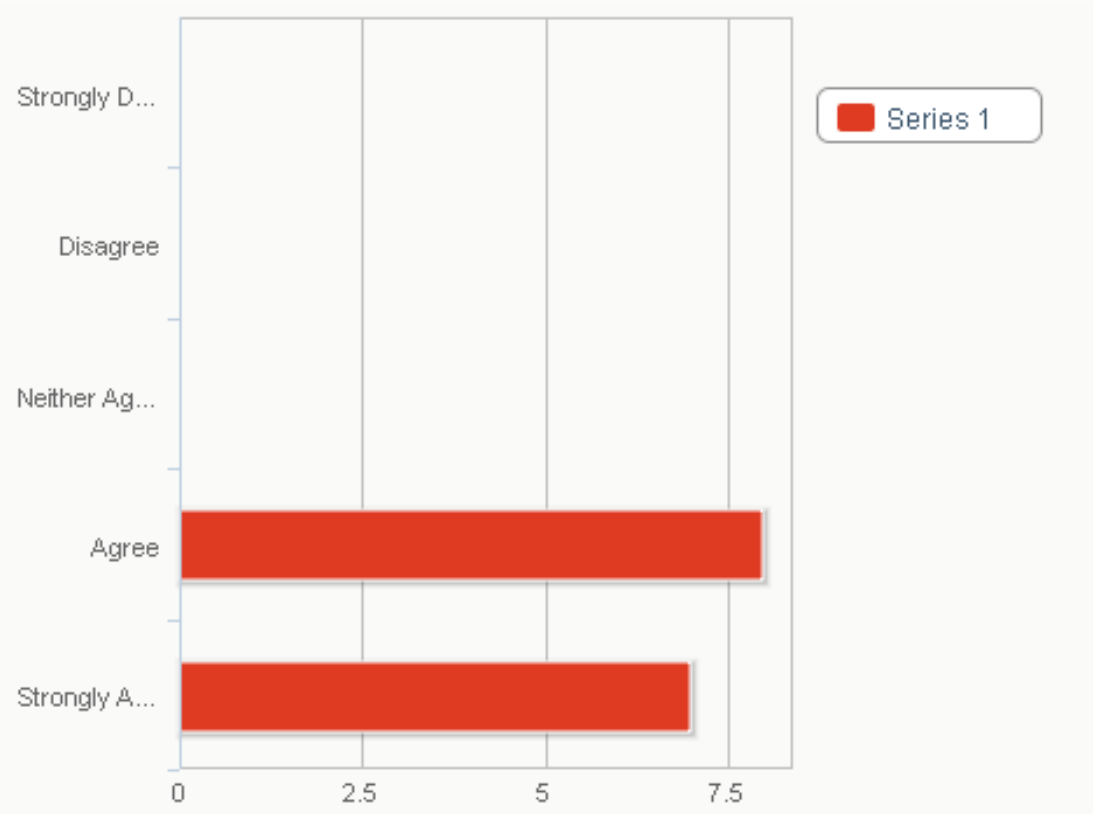
Period 2/OPT:
(5) HF Per2:Civmil importance:
(5) My support of civil-military cooperation is important.



[IMISAS Results HF P2 2011]

SQ09

Period 2/OPT:
(6) HFPer2: IA coop importance:
(6) I believe that interagency cooperation is important.



[IMISAS Results HF P2 2011]

SQ10

Period 4/OPT:
(2) HF Per4: Site benefits comms: (2) How does the IMISAS Experimentation site benefit communication with mission partners? (If none, please enter 'NONE' in the box below.)

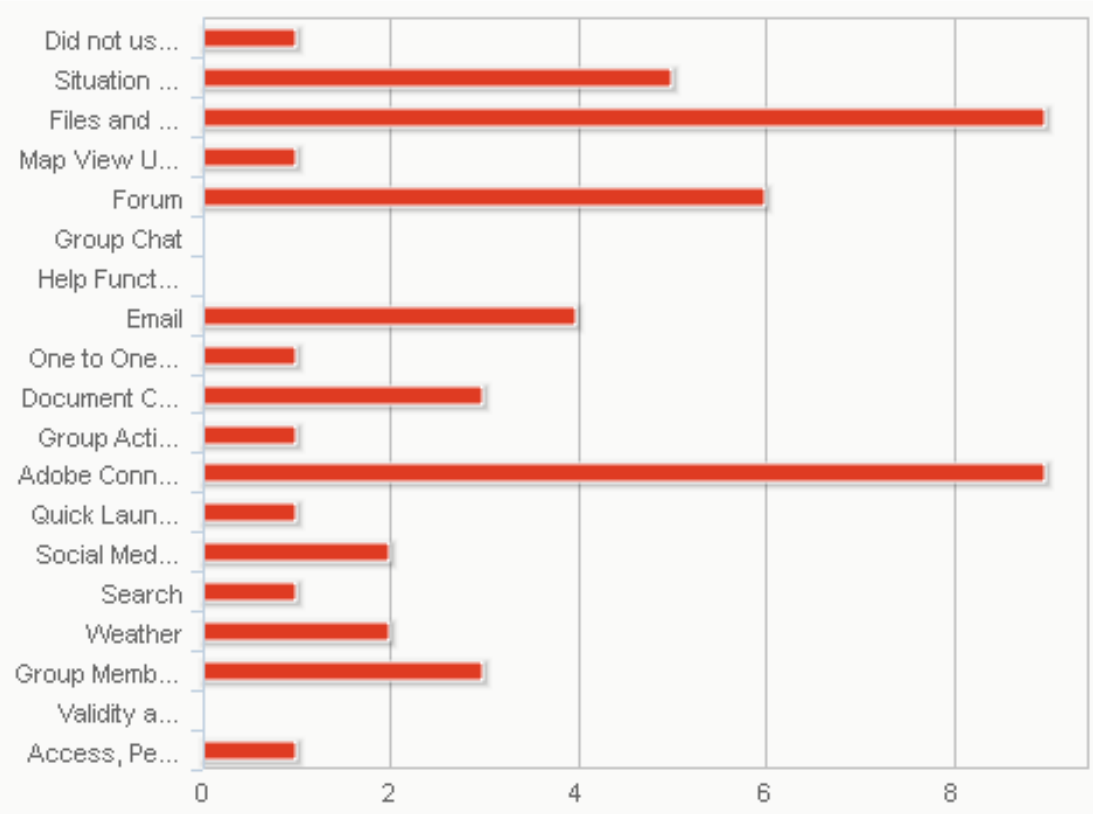
Response
Provides a collaborative environment
Provides a starting point and place for us to publish out information.
Uncertain at this time
It has explored the direct issues I think we will encounter
It throws some of the issues out there that we can see, but when there isn't a clear place that I can direct traffic I feel I can cause more harm and confusion. If we use the concert analogy, I know how to play my instrument, but I'm not familiar with the instruments around me and everyone sounds like they are just making sound and it is NOT pretty.
none

Theorhetically, it allows a single question to be responded to by the group or at least come to the attention of the subject matter expert who the question submitter did not know existed.		
provides good forum to communicate within specific areas		
Serves as a tool for collaboration		
In theory it is creates an open forum for discussion but DoD intent for the site is not defined on whether it should be used to collaborate or just to post information for military transparency issues		
For me it has not enhanced anything.		
Centralized place to communicate.		
none		
Provides a free and open location for communication / collaboration. Some artificiality in this as many mission partners will not come to a MIL site for collaboration but expect MIL to come to their sites.		
Well the jury is still out on that. It seems to be difficult to use and there seems to be much more information out there in other capabilities. I also find it very difficult to master the tech issues involved with the site. At this level it seems to cut off information sharing in the room not enhance it.		
	Valid Responses	**15**
	Total Responses	**15**

[IMISAS Results HF P4 2011a]

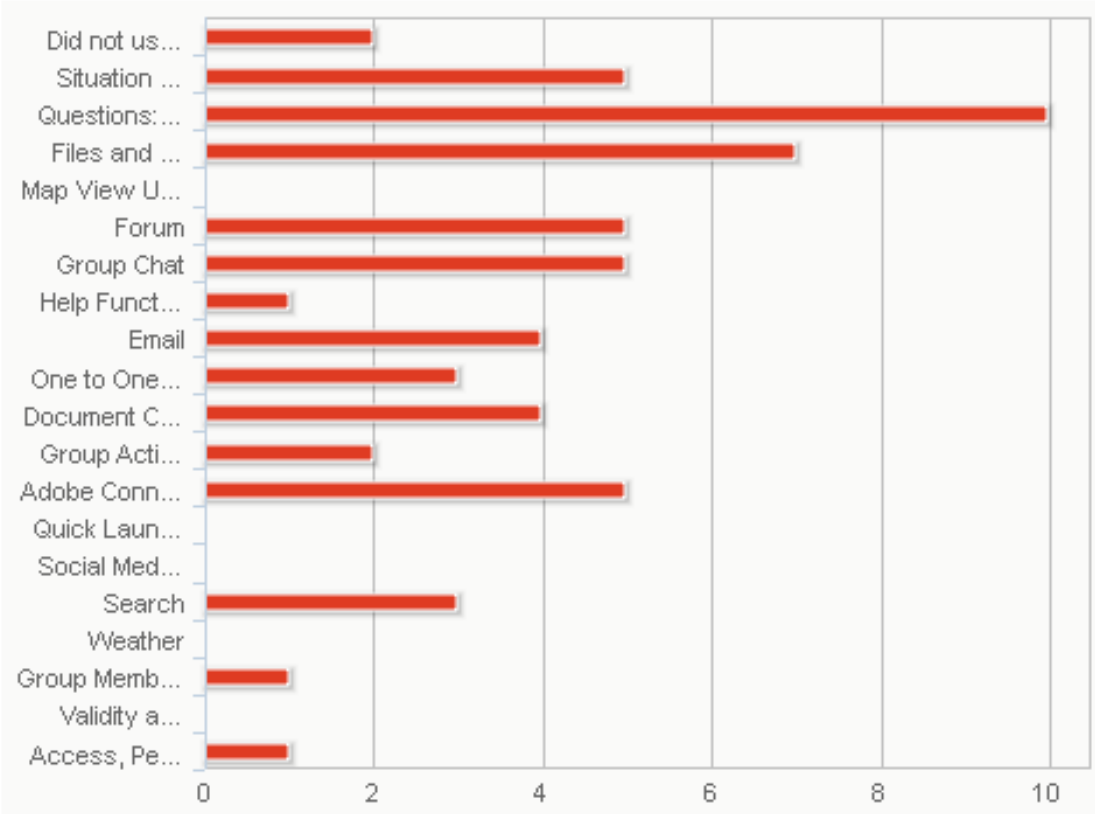
SQ11

Period 2/OPT:
(8) HF Per2: UISC features used:
(8) Please select the five features/functionalities of the IMISAS Experimentation site tha…during this experiment period. (If you used less than five of the features/functionalities, please select those you did use.)



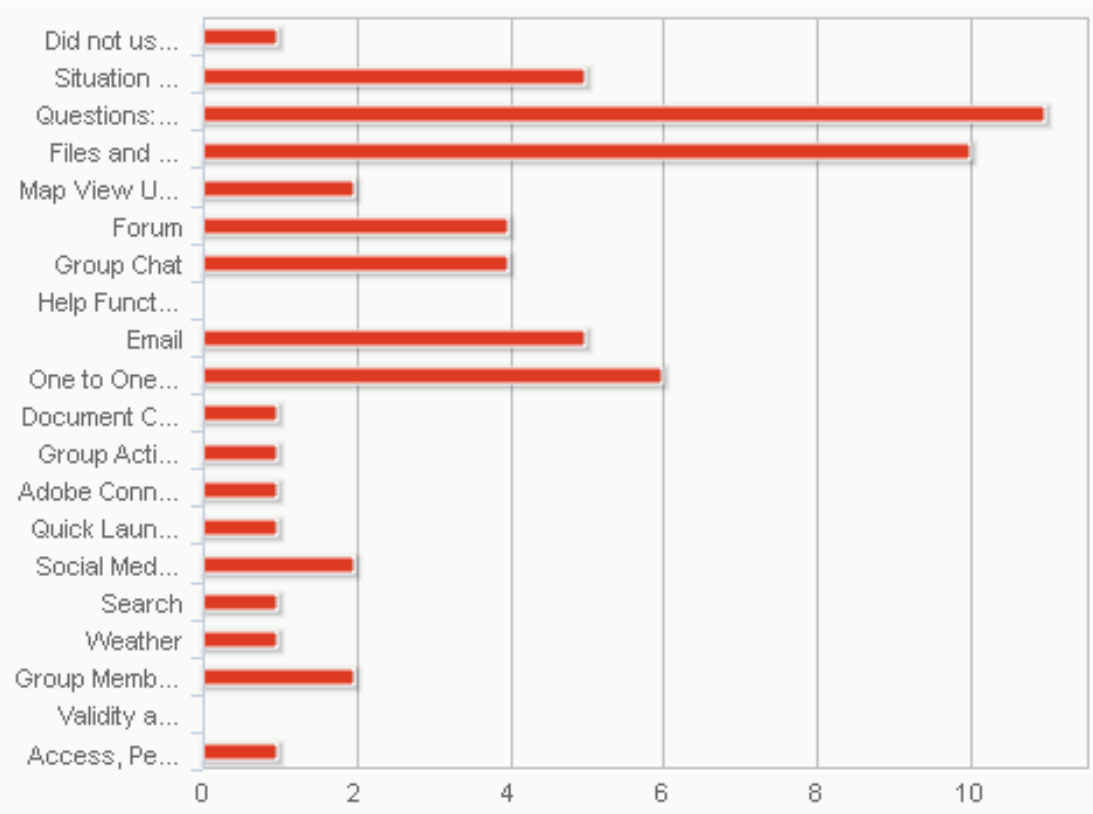
[IMISAS Results HF P2 2011]

Period 3/OPT:
(1) HF Per 3: Exp site use:
(1) Please select the five features/functionalities of the IMISAS Experimentation site that you …during this experiment period. (If you used less than five of the features/functionalities, please select those you did use.)



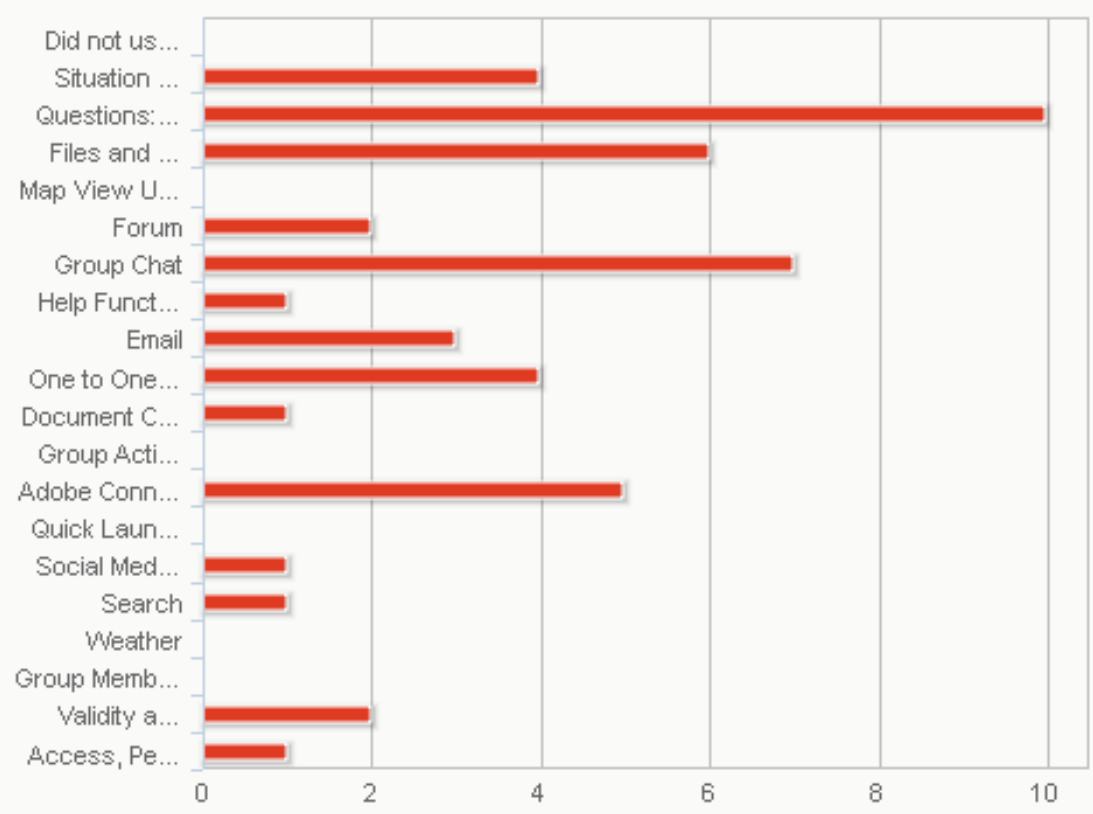
[IMISAS Results HF P3 2011]

Period 4/OPT:
(3) HF Per4: Exp site use:
(3) Which five features/functionalities of the IMISAS Experimentation site did you use most in o… list in order of importance. If you used less than five of the features/functionalities, please list the ones you did use.)



[IMISAS Results HF P4 2011]

Period 5/OPT:
(1) HF Per 3: Exp site use:
(1) Please select the five features/functionalities of the IMISAS Experimentation site that you …during this experiment period. (If you used less than five of the features/functionalities, please select those you did use.)



[IMISAS Results HF P5 2011]

SQ12

Period 2/OPT:
(9) HF Per2:AS role: (9) What is your assigned role and tasking for the Analytic Seminar?

Response
Dep OPT Lead Planner
OPT Lead
Deputy OPT
J2 rep
Still trying to figure that out - J5 role not clear.
??? Great Questions... Create dialogue I guess
legal advisor, should issues of a legal nature arise. So far, just functioning as a joint planner, as no real legal issues have come up.
J4 logistics

J35		
EUCOM Public Affairs representative		
Foreign disclosure officer		
INFORMATION SECURITY OFFICER		
J6/Communications and Information Planner		
Knowledge Management Officer		
OPT - KM Officer		
	Valid Responses	**15**
	Total Responses	**15**

[IMISAS Results HF P2 2011a]

SQ13

Period 6, EoE/OPT:
7: (7) What fundamental improvements to information sharing with mission partners would you recommend? (If none, please enter 'NONE' in the box below.)

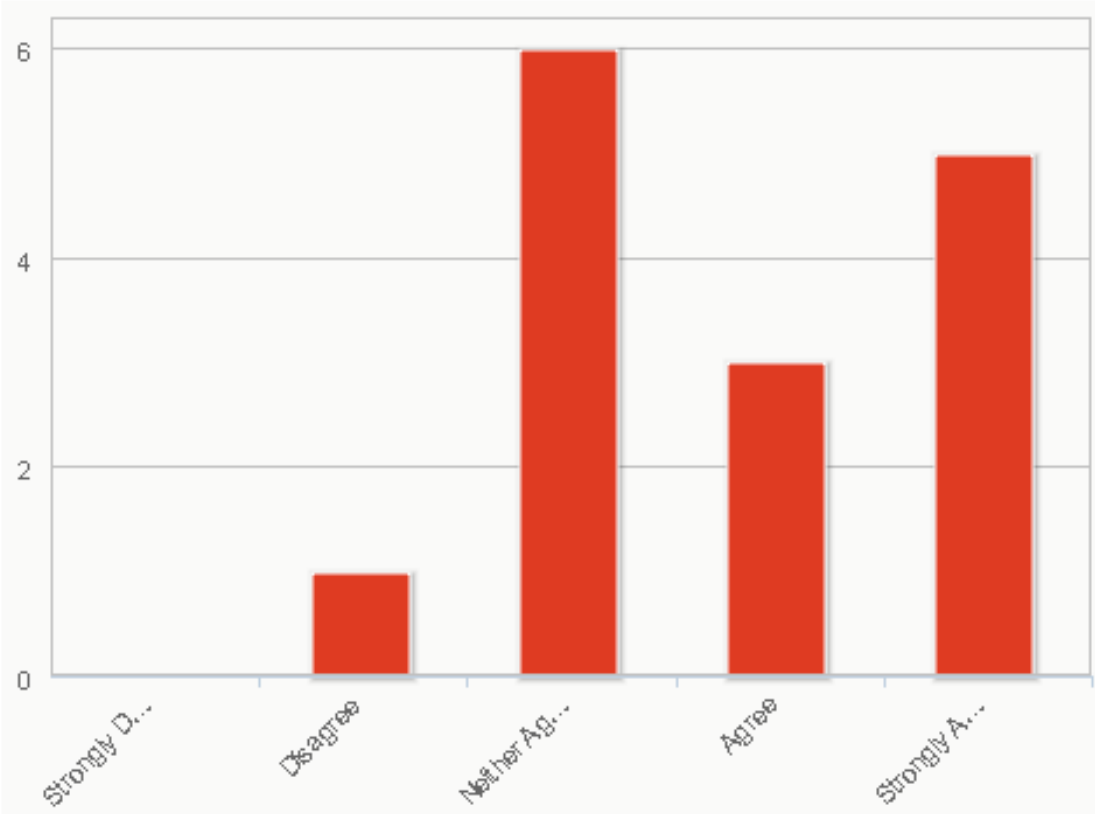
Response
A new tool...at least the front end.
None
Learning the social sites and terminolgy, then ensuring you have the technology to maximize its use
none
None
none
None
go to where they are, use the sites they use
NONE
The USG / US military can not expect our mission partners to come to us. Many are hesitant / unwilling to do so. Many don't know how. Our significant mission partners expect the USG / US military to interact with their own information sharing sites. USG needs to find a way to strike a balance and not expect / require all mission partners to interact with OUR information sharing applications at all times.

Better training, more finite acceptable levels of familiarity with technology on the part of the participants. I don't have time for people that can't navigate websites or adapt to technology in a rapid manner.		
none		
a new exercise that would actually get to the issues of information sharing in a productive manner and not one that disregards expertise in the room.		
I don't know but APAN is too painful to use in a real world situation unless its all you have and the military is running the show. We need to meet with and exchange information with IOs and NGOs and other partners on a face to face basis before crisis hit. Information sharing is only as good as the networking that underlies it. I believe as does much of this group that a separate cell for unclassified information sharing should be created in phase 0 of a potential operation. Some in the room think this should be staffed and run by operational people. However I believe that a more horizontal functional team outside and not driven by the military process would provide much richer data for the military to work from in forming their responses to a disaster. The mission statement for this cell would be to create "a data rich redundant site which is a USG site which provides a detailed uptodate picture of the crisis for broad consumption that is responsive to but not driven by military planning". I would also not ask the operations people to "lead" this you need a facilitator not a leader. The lead of the OPT has to be its on event not drive the information creation and sharing.		
	Valid Responses	**14**
	Total Responses	**14**

[IMISAS Results HF P6 2011a]

SQ14

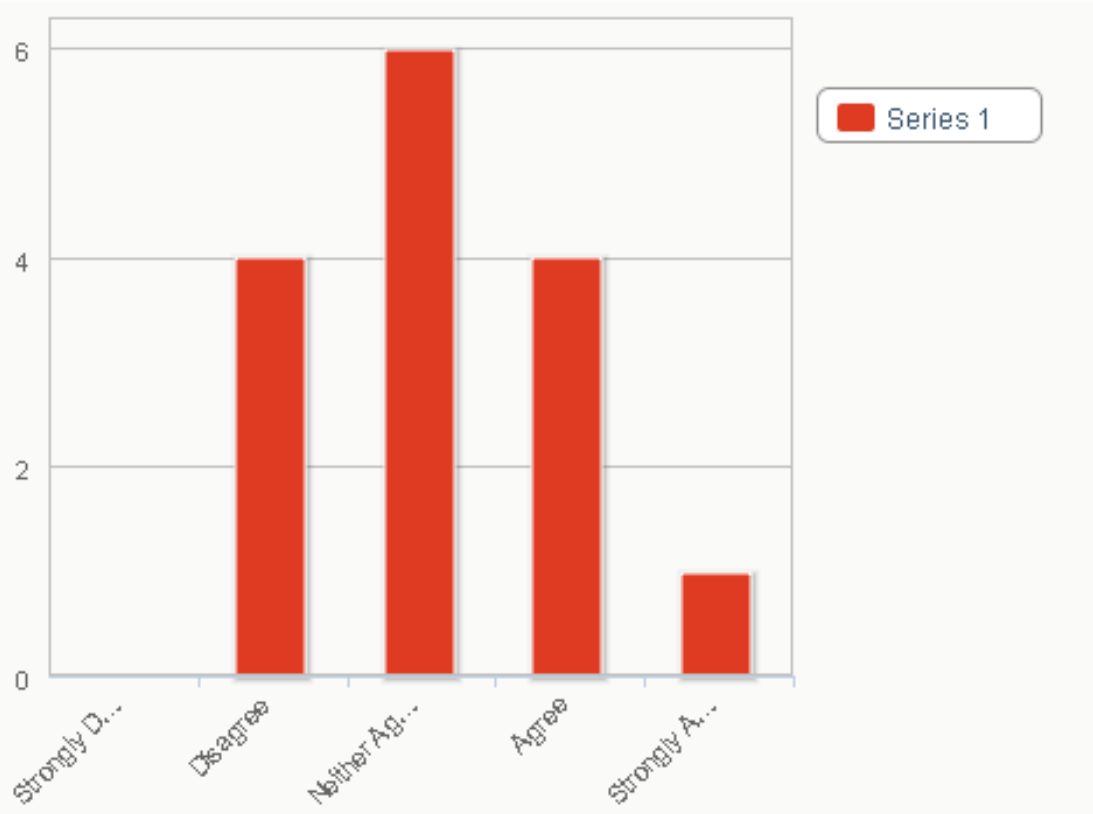
Period 4/OPT:
(4) HF4: Partners decrease effort:
(4) Mission partners tend to slowly decrease their effort when they cannot identify their own contributions on the IMISAS Experimentation site.



[IMISAS Results HF P4 2011]

SQ15

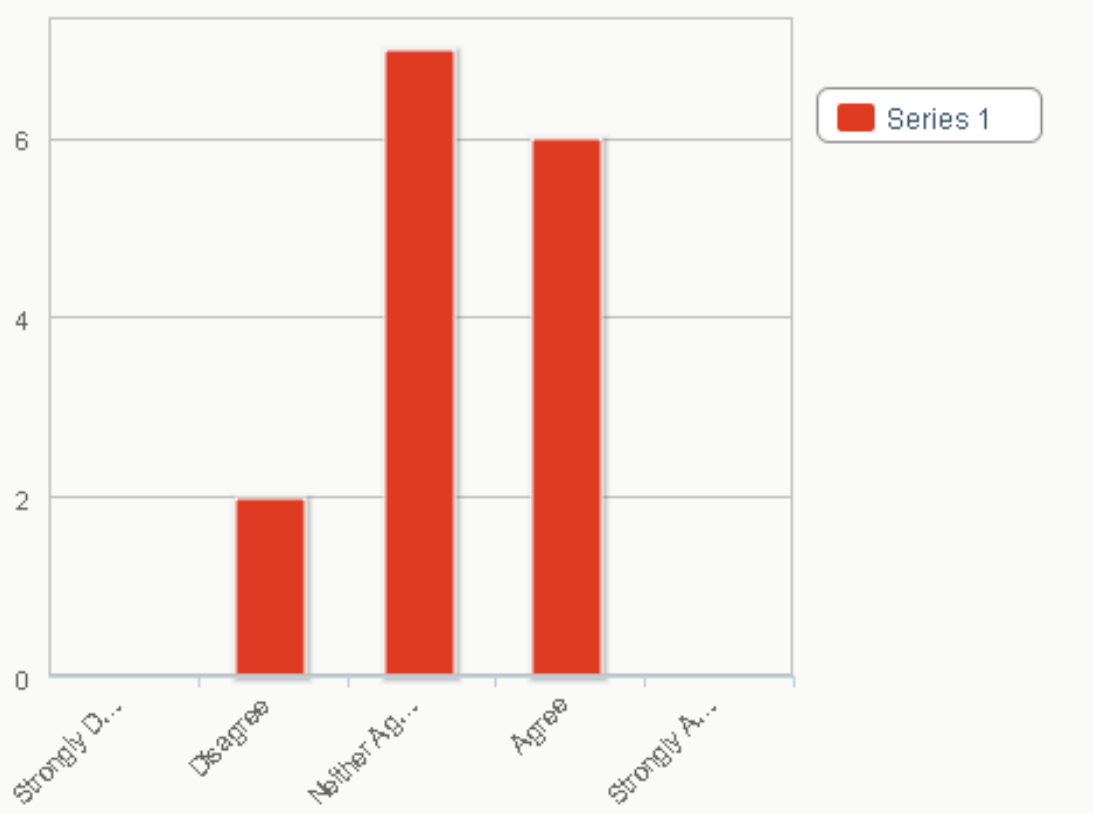
Period 4/OPT:
(5) HF Per4: Partners responsibility:
(5) Mission partners take less responsibility when there are other capable mission partners present in a collaborative situation (e.g. ACO, chat).



[IMISAS Results HF P4 2011]

SQ16

Period 4/OPT:
(6) HF Per4: Exp site achieves goals:
(6) The IMISAS Experimentation site helps me to achieve my given tasks/goals.



[IMISAS Results HF P4 2011]

SQ17

Splitted during Analytic Seminar.

SQ17.1

Period 6, EoE / OPT:

8: (8) Based upon your experience this week and your role and responsibilities in the experiment, what were the benefits to using the IMISAS Experimentation site? (If none, please enter 'NONE' in the box below.)

Response
UIS is certianly a required capability but current version approach is not acceptable
Provided a collaborative planning venue
Oportunity to shape information for use by an OPT
none
Hands-on training with group interaction
It taught me that DoD does NOT know how to plug into operations they don't have the authority to take charge. We flop around and I'm sure outsiders just shake their heads . . .

provided a good medium that all participating could access and share info
NONE
NONE
Identify the areas in which a UIS application is useful / requirements for a DoD wide system (should that be identified as the desired approach).
Exposed weaknesses in our policy and know-how
none
none
Its only place for this week that provided a shared area where we were looking to work together and I was able to be in contact with UN and NGO personnel working in the area as they self idenified and without APAN I would not be aware of nor have reached out to them. The same is true for some of the military personnel. As a discovery site for players on the ground it has potential but it has to attract them by being the best or one of the best organizations for them to use.

	Valid Responses	**14**
	Total Responses	**14**

[IMISAS Results HF P6 2011a]

SQ17.2

Period 6, EoE/OPT:
9: (9) Based upon your experience this week and your role and responsibilities in the experiment, what were the drawbacks to using the IMISAS Experimentation site? (If none, please enter 'NONE' in the box below.)

Response
The site was difficult to use at best if the tools functioned.
Limted to the tools av ailable on APAN
NONE
some aspects did not work....like the map
None
APAN was very slow and not reactive . . . so slow that sometimes I'd get something out there, then forget what I was doing because the page would take so long to update.
some of the functions where hard to navigate and you had to dig to find posts containing info I needed
cumbersome, not intuitive, too many ways to get to the same information, labeled areas not clear enough, too military-focused
The system was not intuitive and in today's computer savvy world, if you can't figure it out with a few clicks then it takes too long.
Innaccesibility / slow functioning of the site. Poor access to broad set of information.

Too complex. There is no need to "pretty up" an APAN site. Users need to be comfortable sharing information in a non-structured manner. Renaming menus and trying to shape every website to look "SharePoint like" isn't actually improving how we share information.		
none		
listed already		
Many. Functionality didnt work well -- things weren't intitutive -- you don't have time to learn to use the tool the tool has to be accessable and intitutive. It takes too long to load, its poorly organized and key information does not float automatically to the top like it can in social media. Its hard to keep track, too many clicks between functions and too many passwords. It needs to be facilitated not lead in a particular direction.		
	Valid Responses	**14**
	Total Responses	**14**

[IMISAS Results HF P6 2011a]

SQ18

Cancelled by USA analysis team during Analytic Seminar.

Annex G.1.2: Interview Questions (IQ)

In the following section the following coding has been used:

5 = Strongly Agree
4 = Agree
3 = Sometimes agree
2 = Disagree
1 = Strongly Disagree
0 = No data

civ = civil
civ-gov = civil governmental
civ-ngv = civil non-governmental
civ-gvs = subordinated civ-gov
mil = military
mn = multinational
nat = national

N = 18

IQ01

"Describe your activities and your area of responsibility."

OPT Stuttgart

I am responsible for providing public affairs guidance and recommendations on what can / should be put in the public domain.
Develop security guidance and procedures for the information to be shared
Operational planing team leader
I provide a DOC perspective + champion DOC equities in the command; I also outreach to public and private non-federal intities for partnerships

RC Stuttgart

Representing the NATO Civil-Military Fusion Center (CFC) to simulate real-world support to a HA / DR mission.
(?) Representing the NATO Civil-Military Fusion Center as an (???) knowledge manager
I am seeded by ACAPS to OCHA to coordinate a provide technical support to humanitarian assessments
Repond on behalf of WHO Headquarters Communications
Project - assistant ACAPS - development of situation reports in first 72 hours after a crisis
mapping and satellite imagery analysis for UN partners and NGOs

RC Ottobrunn

Roleplayer BW Ops J9
J Med is the senior medical officer and med advisor of Com MONUSCO
Aufbau der Verbindung mit US Regierungsorg., um eigene Ustg. anzubieten (konzentriert sich auf Wiederaufbau der Infrastruktur im Raum GOMA)
As GIZ we conduct long-term development projects.
Provide civilian knowledge / skills to the scenario, represent the capabilities / agenda of a NGO
Coordination of DEU activities / invitation to an emerg. Coord. Meeting in Goma
Entwicklungsorientierte Not- und Übergangshilfe, keine humanitäre Hilfe (observe and advise on activities of colleagues: AA, NGOs etc.)
Playing J9 of an UN force with all the duties and responsibilities as a CIMIC guy e.g. civil situation, assessment, J9-Staff work.

IQ02

"What is your contribution to mission partners in order to achieve their mission objectives?"

OPT Stuttgart

Limited. More focused on advising our team.
Develop a security classification
Develop an coordinated US military response to the HAIPR event
This experiment is great for that as this is one of the issues the J9 in AFRICOM

is trying to determine; I believe one of my mission contributions can be to help the command out much to useful info partners and work in concert with them in selected areas. However this has proven difficult in HA / DR situations. In fact there may be no role for my office J9 to play in these situations - I am trying to formulate this.

RC Stuttgart

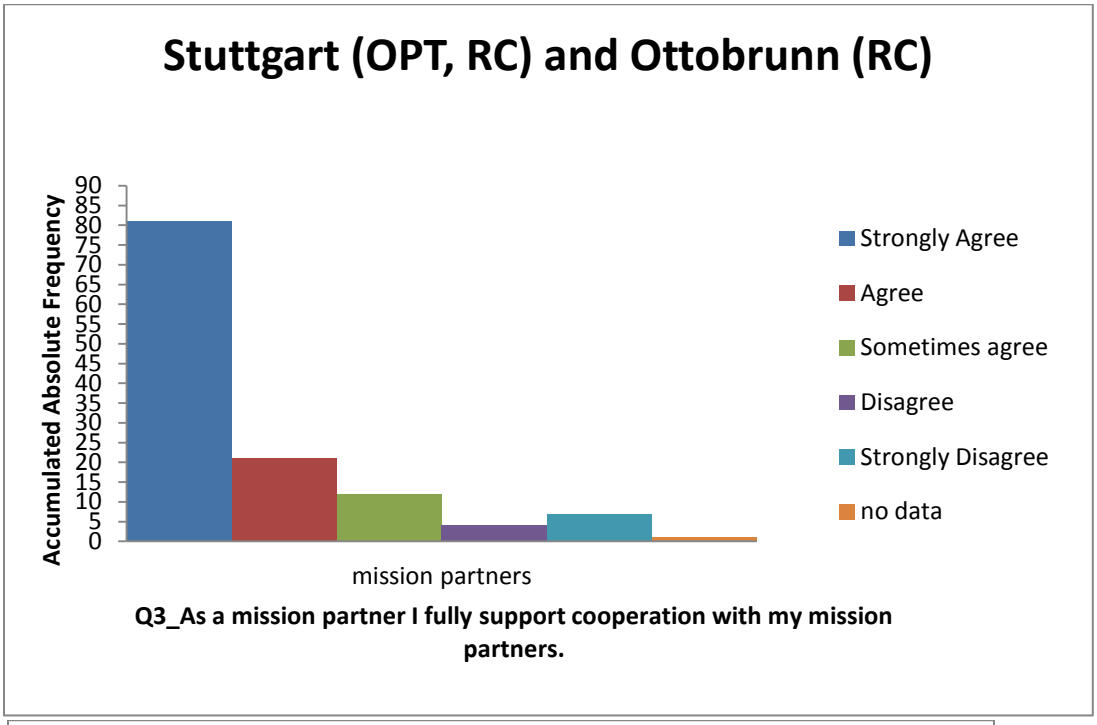
Representing the NATO Civil-Military Fusion Center (CFC) to simulate real-world support to a HA / DR mission.
(?) Representing the NATO Civil-Military Fusion Center as an xxx knowledge manager
I am seeded by ACAPS to OCHA to coordinate a provide technical support to humanitarian assessments
Repond on behalf of WHO Headquarters Communications
Project - assistant ACAPS - development of situation reports in first 72 hours after a crisis
mapping and satellite imagery analysis for UN partners and NGOs

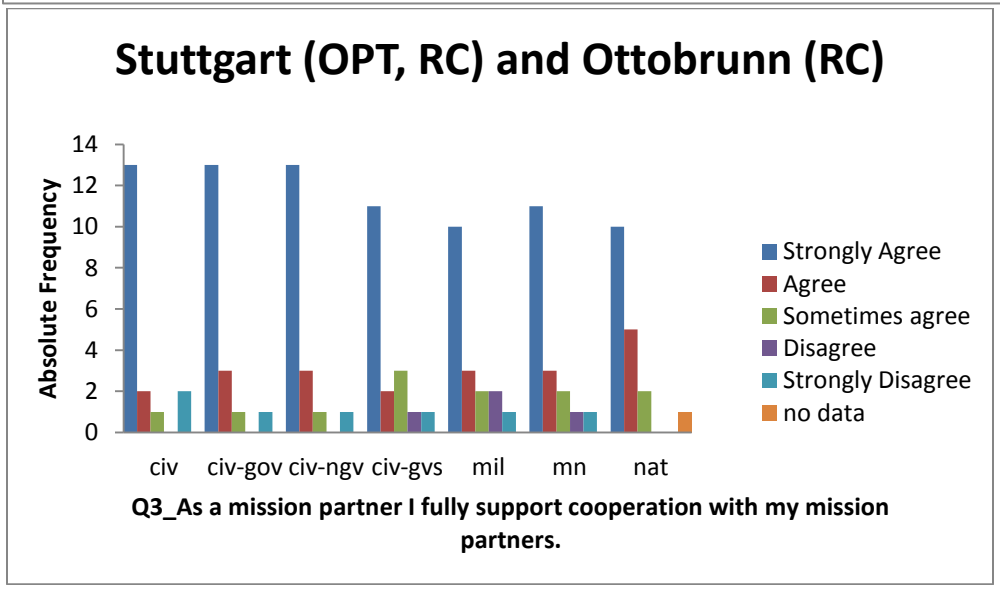
RC Ottobrunn

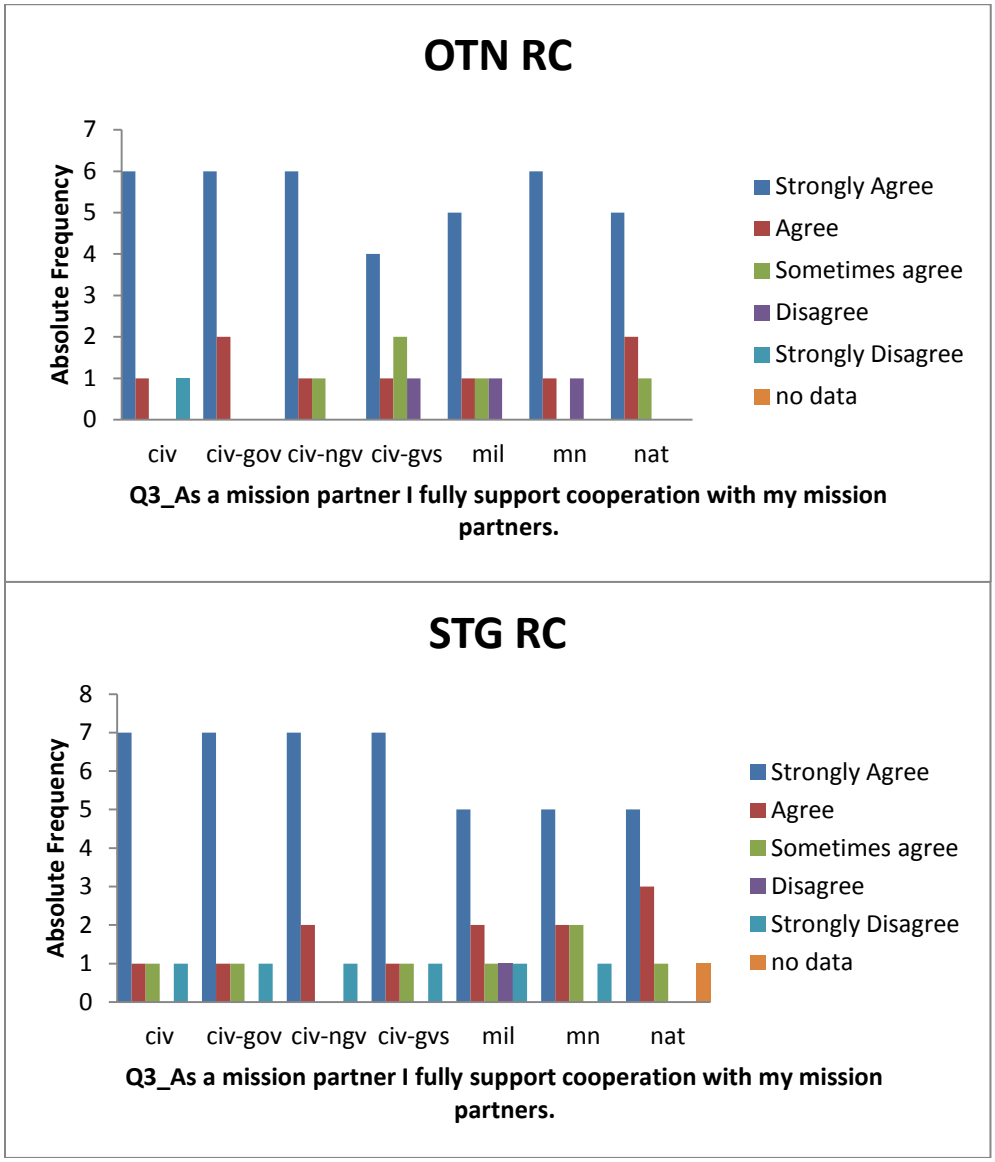
Injects according MSEL
(?) up to now no work; lot's of work / missions …additional COS+COM+HighRER Monusco FFFwd
Bereitstellen von Personal und Maschinen für den Wiederaufbau, Kontakt zu anderen NGOs aufbauen und halten, sowie Infos an US weitergeben)
Capacity building and strengthening of good gov as a prediction for long term stabilization.
NGO capable to provide tents / engineering skills
I try to coordinate DEU (gov + ngo) activities by bringing them on the table
Advise on expertise "how-to"

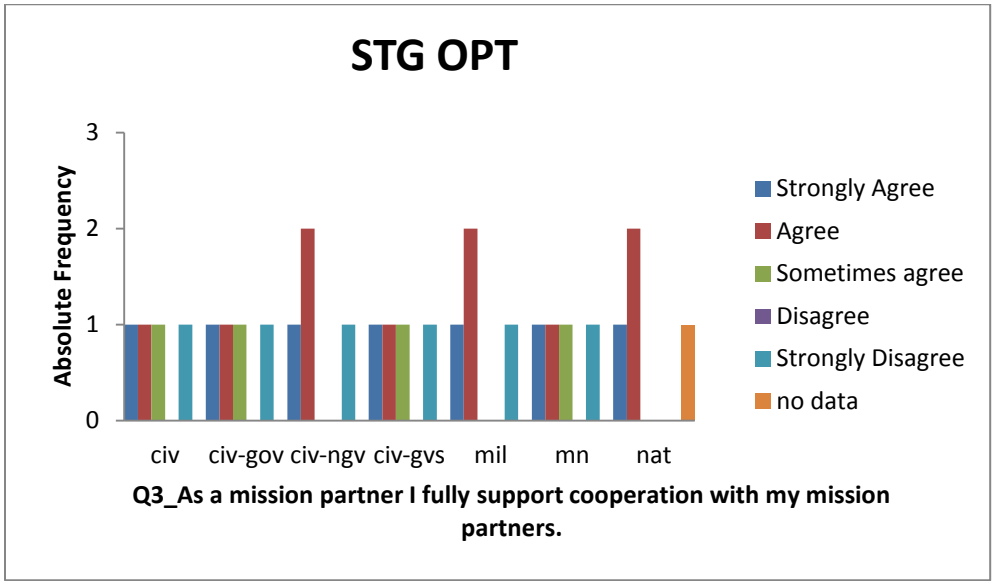
IQ03

"As a mission partner I fully support cooperation with my (civ, civ-ngv, civ-gov…) mission partners."


Stuttgart (OPT, RC) and Ottobrunn (RC)
Accumulated Absolute Frequency
90
85
80
75
70
65
60
55
50
45
40
35
30
25
20
15
10
5
0
mission partners
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q3_As a mission partner I fully support cooperation with my mission partners.

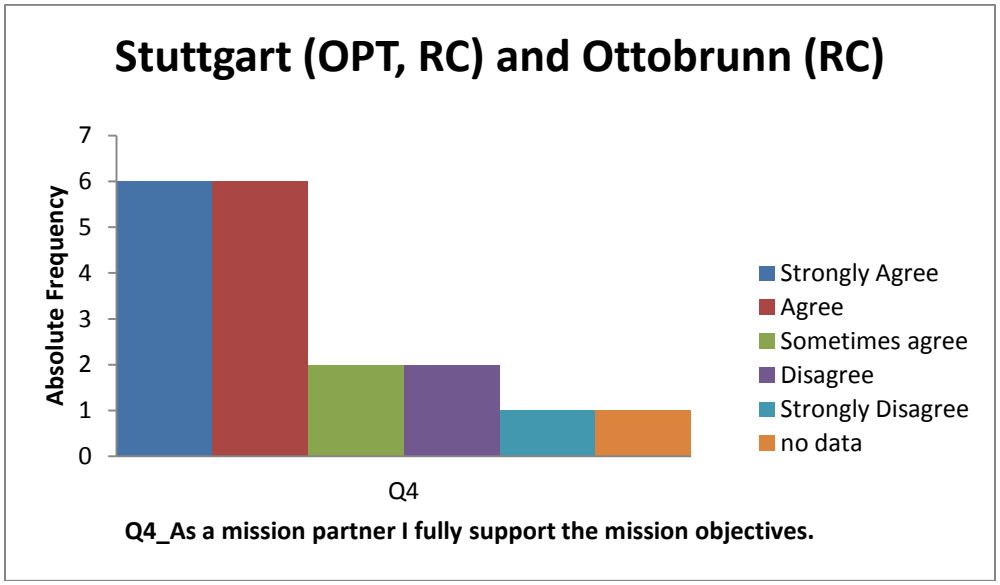

Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
14
12
10
8
6
4
2
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q3_As a mission partner I fully support cooperation with my mission partners.

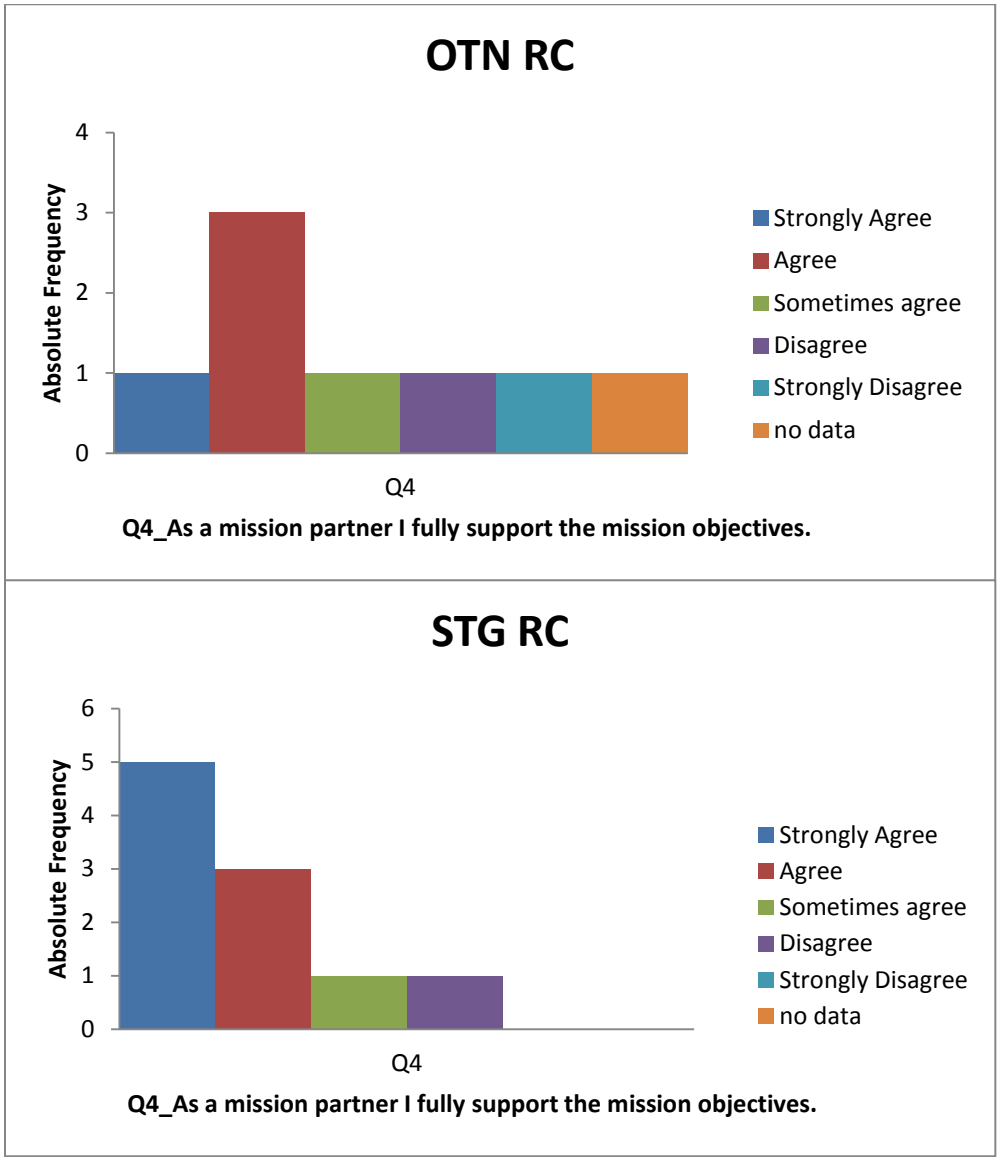

OTN RC
Absolute Frequency
0
1
2
3
4
5
6
7
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q3_As a mission partner I fully support cooperation with my mission partners.
STG RC
Absolute Frequency
0
1
2
3
4
5
6
7
8
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q3_As a mission partner I fully support cooperation with my mission partners.

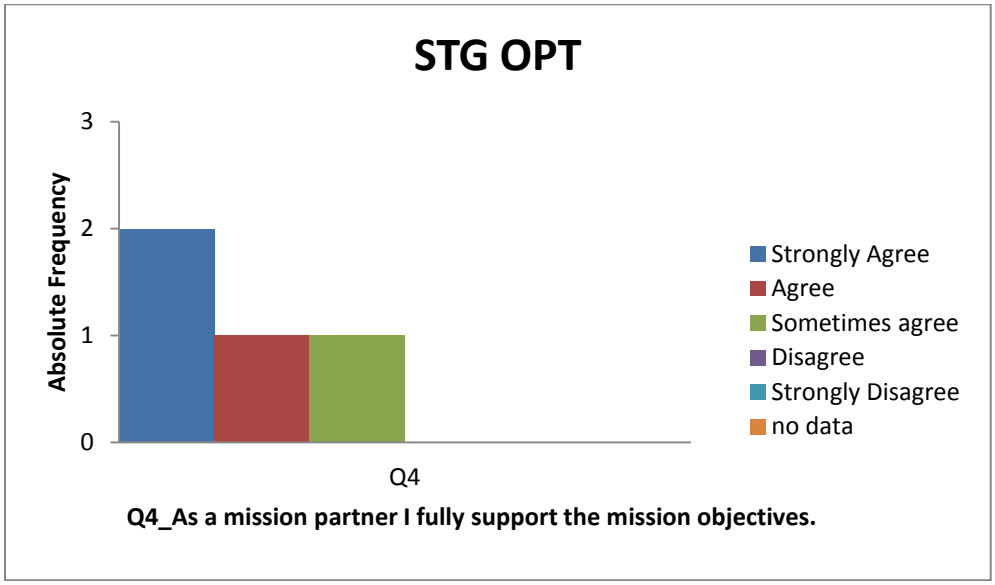


IQ04

"As a mission partner I fully support the mission objectives."



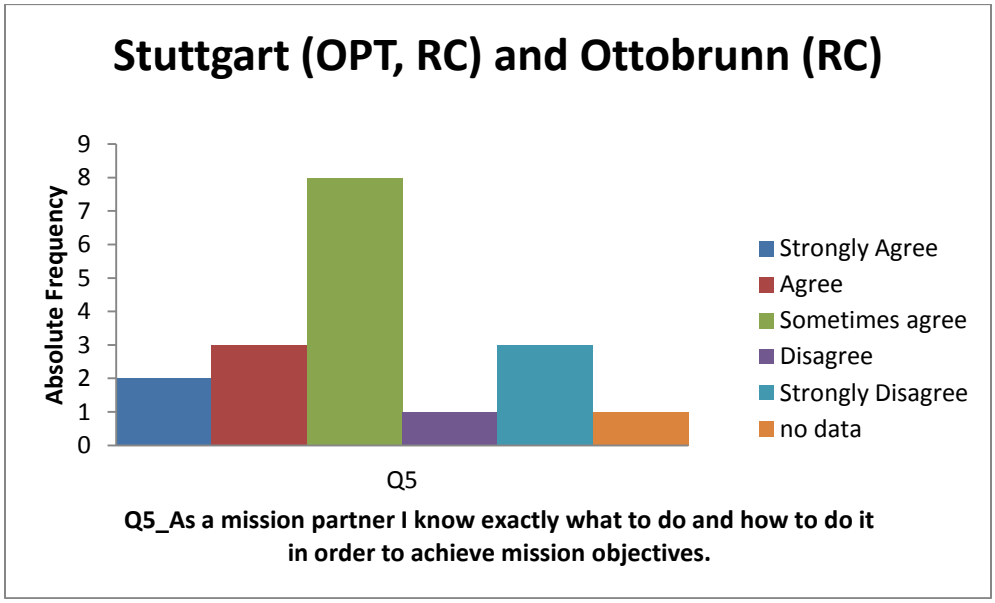

OTN RC
Absolute Frequency
4
3
2
1
0
Q4
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q4_As a mission partner I fully support the mission objectives.
STG RC
Absolute Frequency
6
5
4
3
2
1
0
Q4
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q4_As a mission partner I fully support the mission objectives.

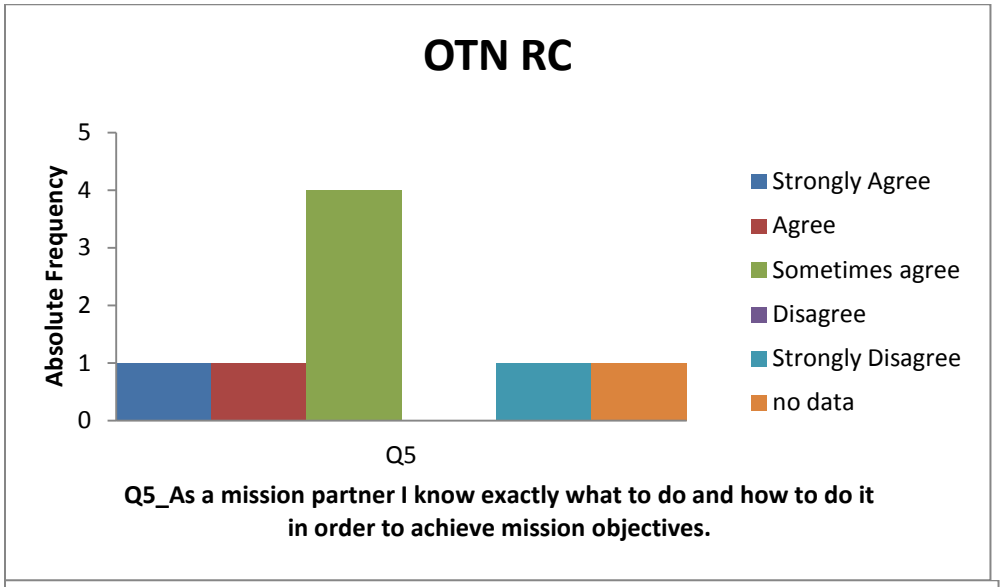


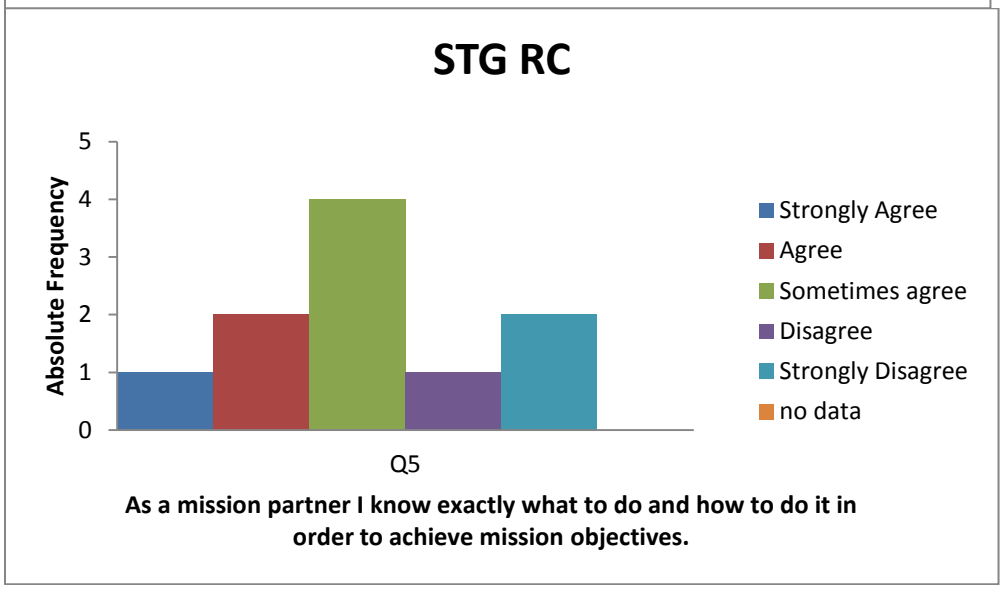
IQ05

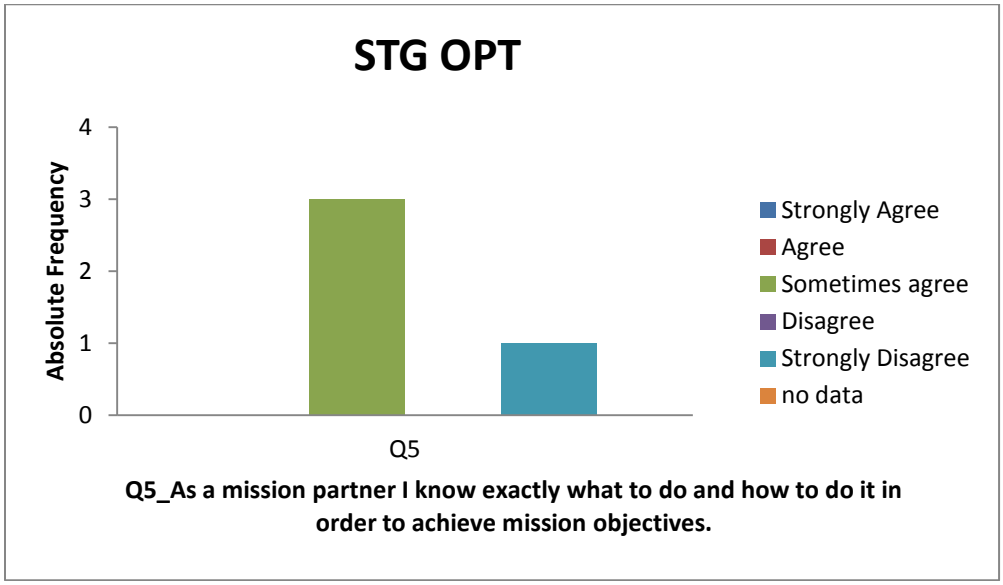
"As a mission partner I know exactly what to do and how to do it in order to achieve mission objectives."

IQ05.01




OTN RC
Absolute Frequency
5
4
3
2
1
0
Q5
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q5_As a mission partner I know exactly what to do and how to do it in order to achieve mission objectives.


STG RC
Absolute Frequency
5
4
3
2
1
0
Q5
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
As a mission partner I know exactly what to do and how to do it in order to achieve mission objectives.



IQ05.2

"Please comment"

OPT Stuttgart

In my lane, yes; overall could be more clear.
(?) Initial … are always nebulous - as the project moves forward is goals
We are still learning
See last page - no training on the military planing process has hampered my ability to know when and how to effectively contribute.

RC Stuttgart

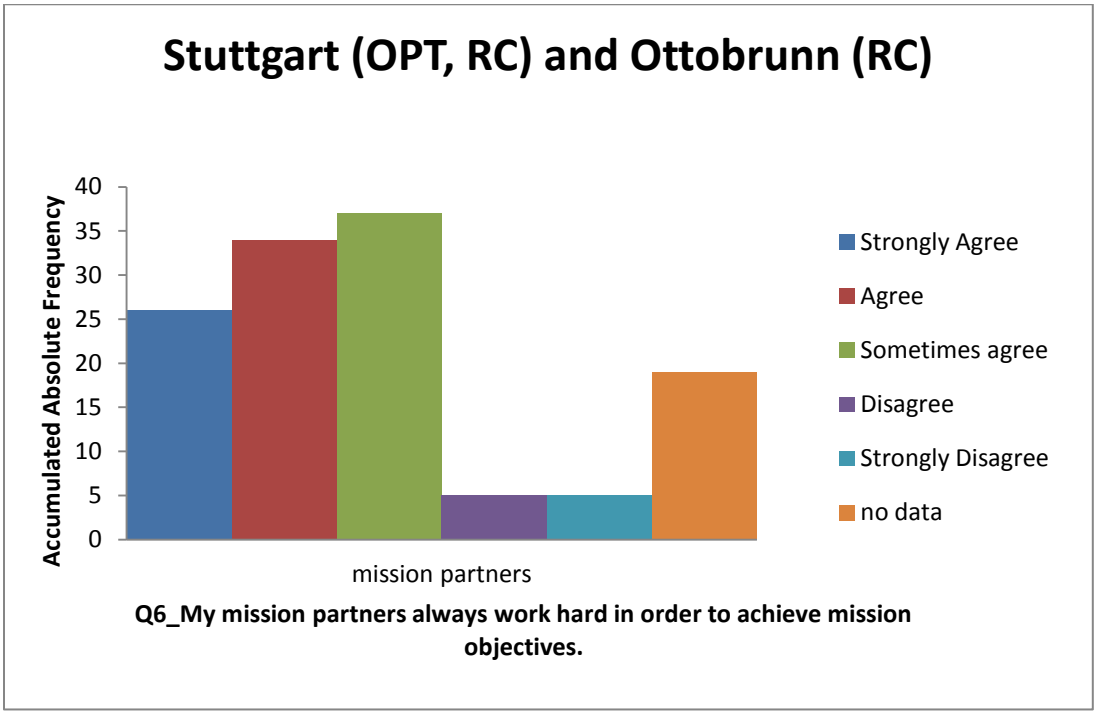
The CFC's role is clear and will do it to best of own ability.
CFC main aim is to facilitate information sharing.
It is not my objective to achieve someone else's mission objectives

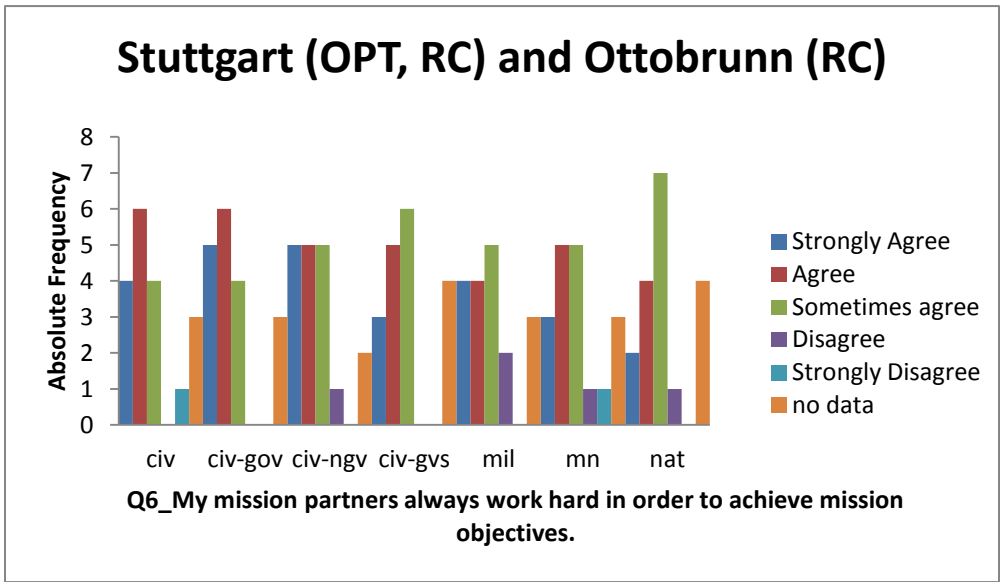
RC Ottobrunn

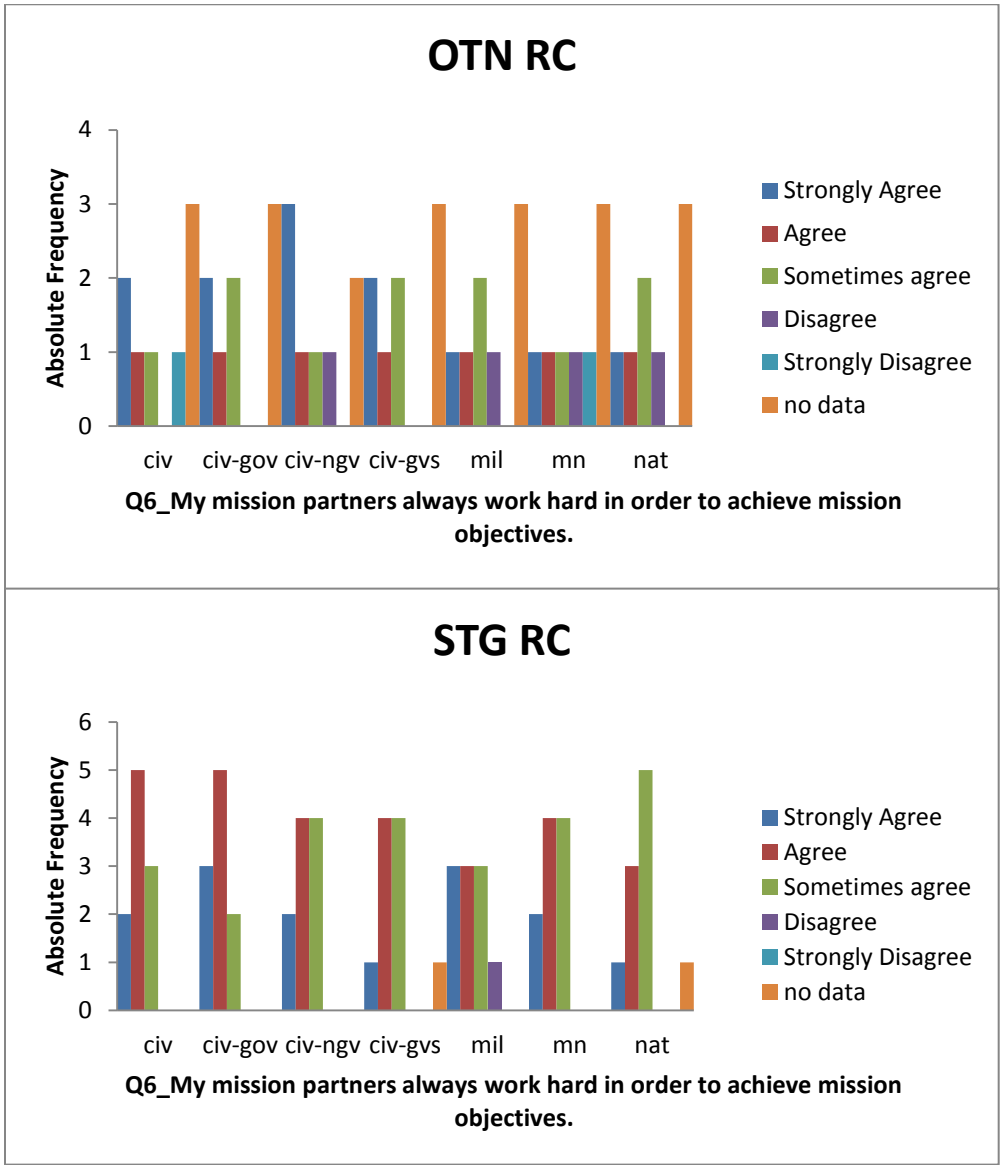
It seems to me that the mission is a one way mission, Information sharing is rarely observed.
Die Informationsträger sind nicht immer bekannt. Kontaktpartner antworten selten. Plattform der Infoübertragung ist hauptsächlich APAN mail.
how can I know
As a NGO I'm following my own agenda.

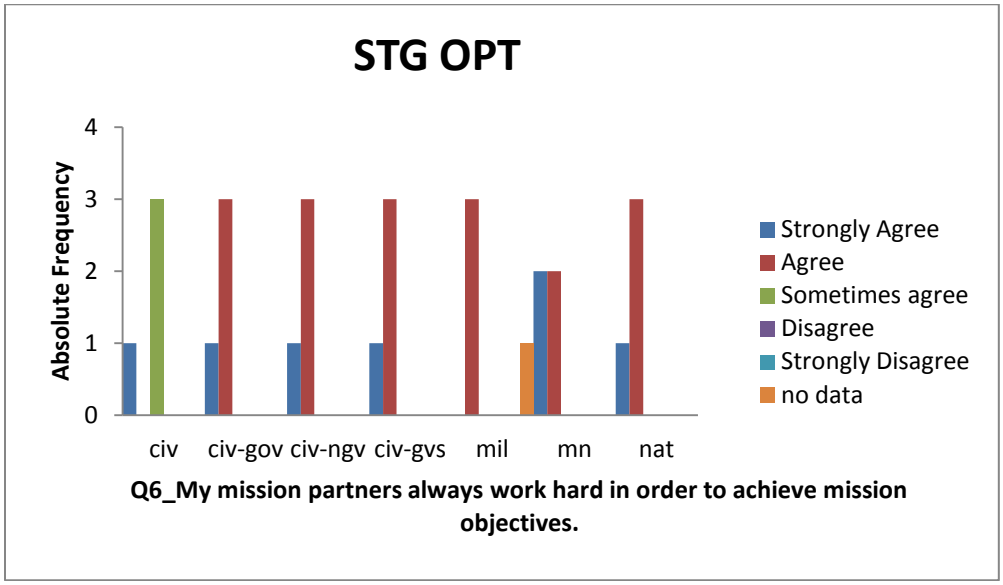
IQ06

"My mission partners always work hard in order to achieve mission objectives."


Stuttgart (OPT, RC) and Ottobrunn (RC)
Accumulated Absolute Frequency
40
35
30
25
20
15
10
5
0
mission partners
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q6_My mission partners always work hard in order to achieve mission objectives.


Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
8
7
6
5
4
3
2
1
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q6_My mission partners always work hard in order to achieve mission objectives.


OTN RC
Absolute Frequency
0
1
2
3
4
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q6_My mission partners always work hard in order to achieve mission objectives.
STG RC
Absolute Frequency
0
1
2
3
4
5
6
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q6_My mission partners always work hard in order to achieve mission objectives.

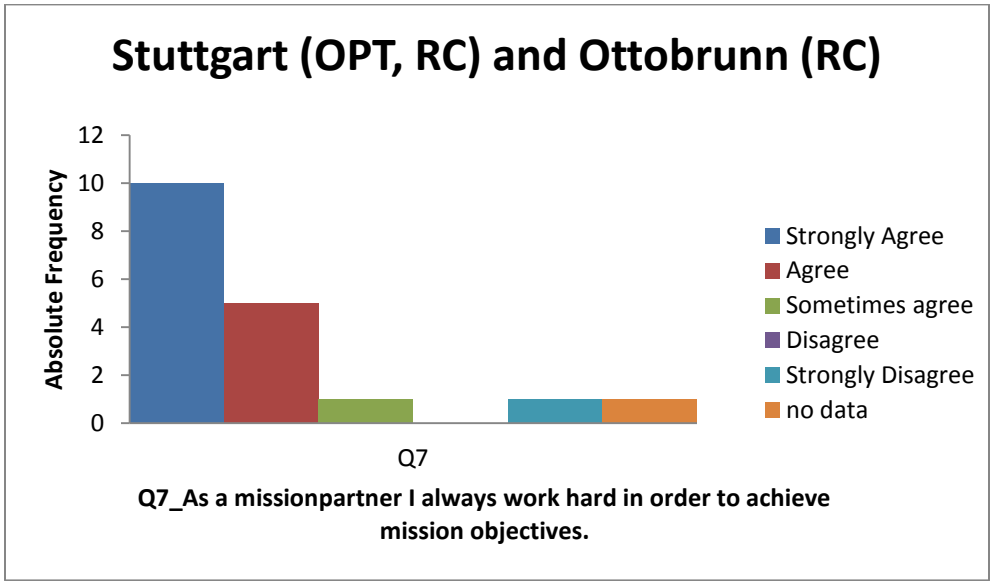


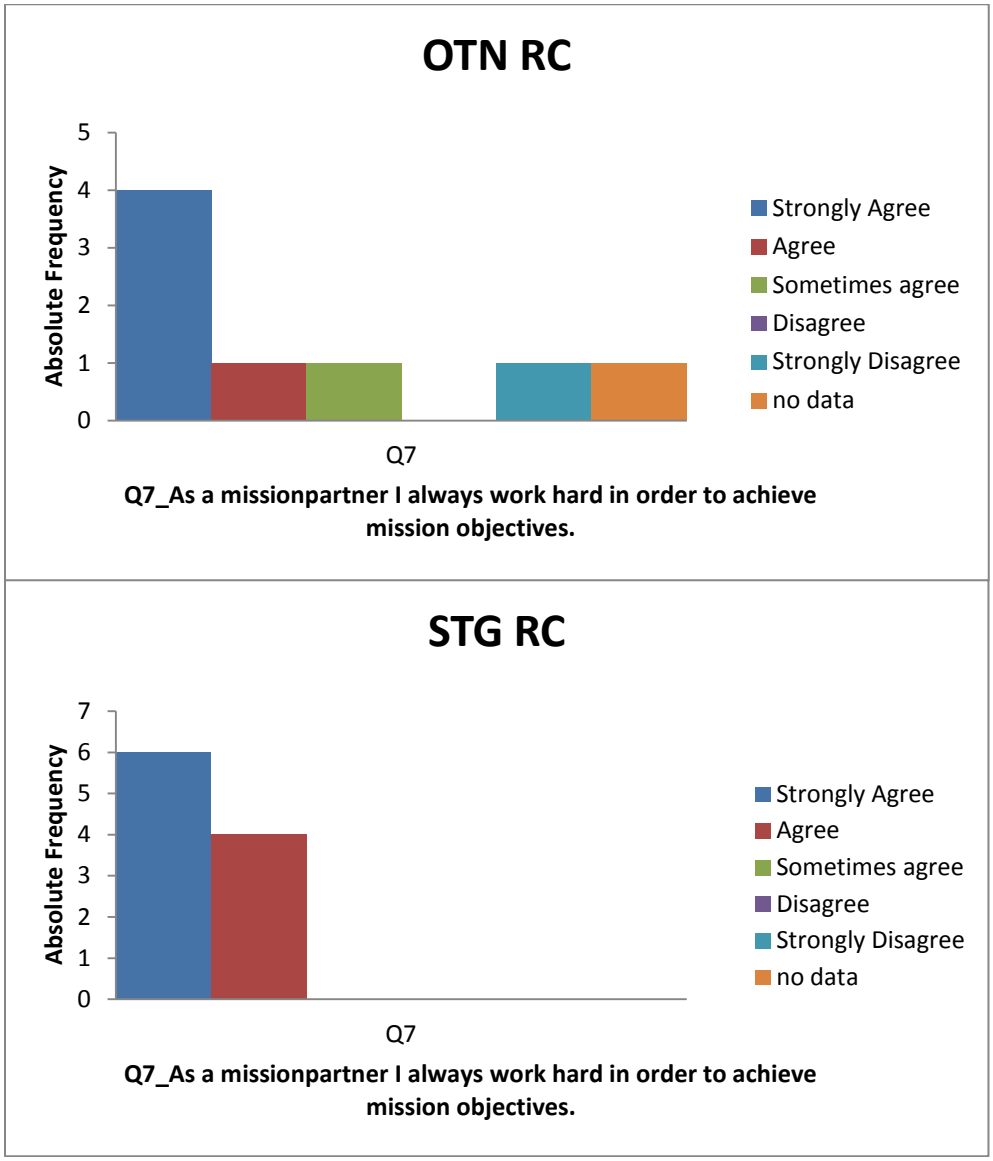
IQ07

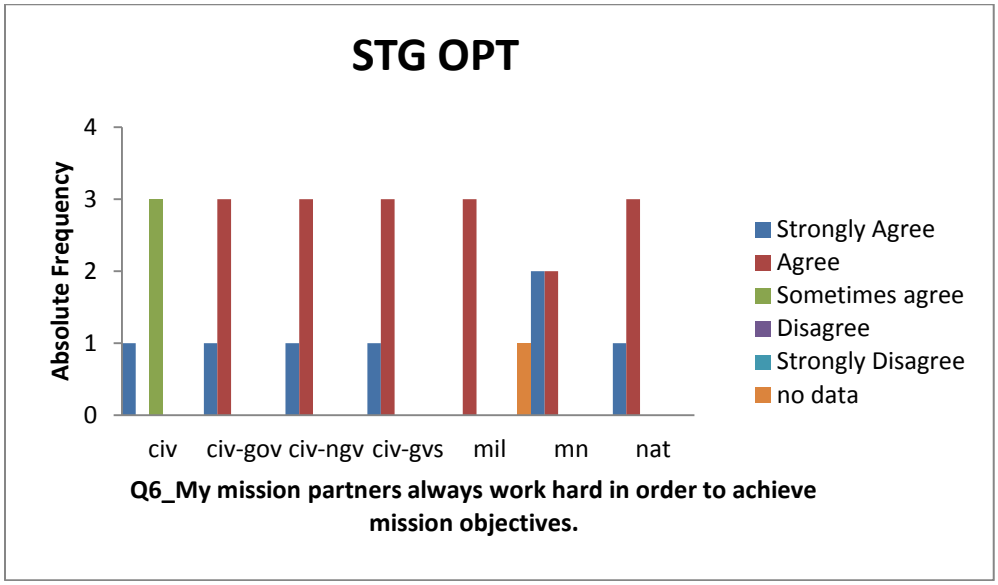
IQ07

"As a mission partner I always work hard in order to achieve mission objectives."

IQ07.1




OTN RC
Absolute Frequency
5
4
3
2
1
0
Q7
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q7_As a missionpartner I always work hard in order to achieve mission objectives.
STG RC
Absolute Frequency
7
6
5
4
3
2
1
0
Q7
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q7_As a missionpartner I always work hard in order to achieve mission objectives.



IQ07.2

"Please comment"

OPT Stuttgart

To the extent they are in my lane and clear
conflicting goal and priorities can skew mission objectives
I often feel disheartened by the process but never disengaged.

RC Stuttgart

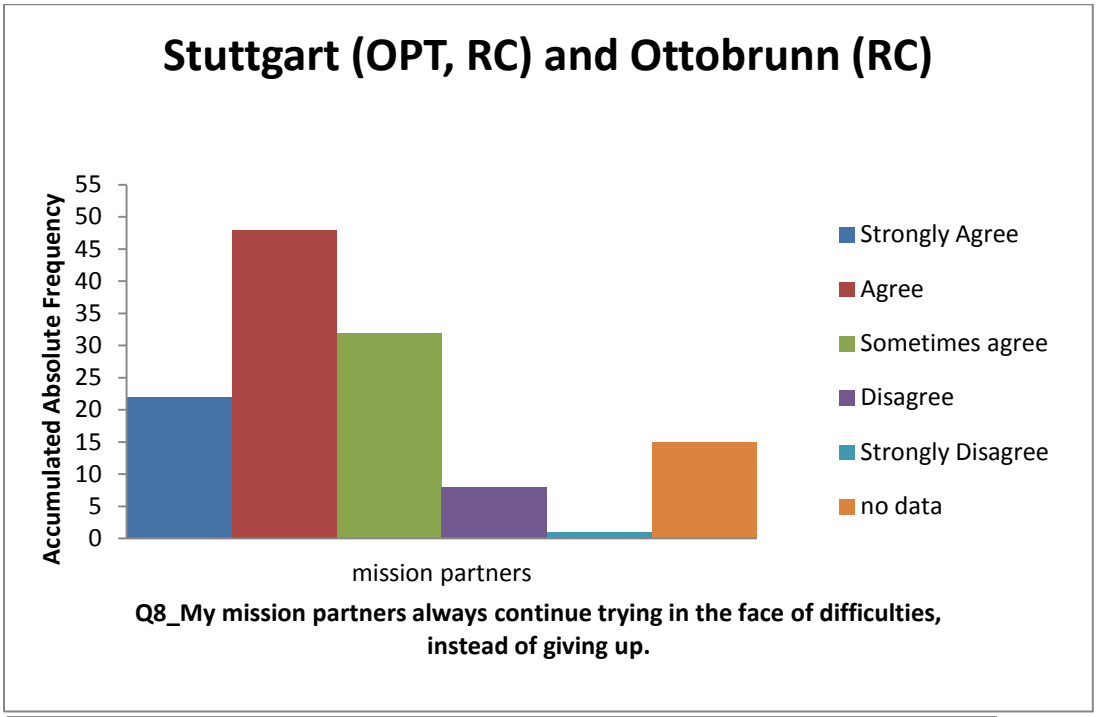
my mission objectives

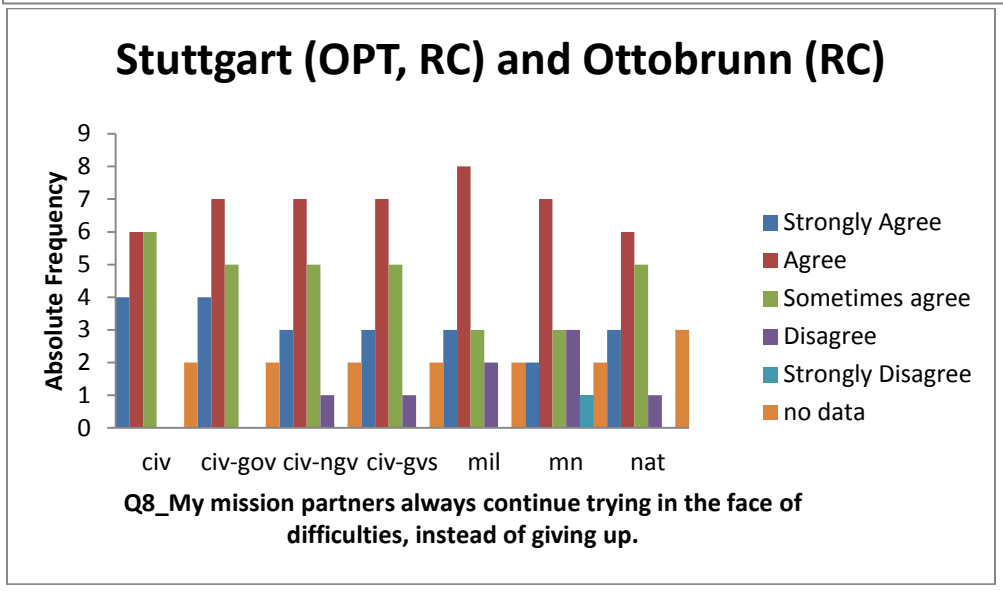
RC Ottobrunn

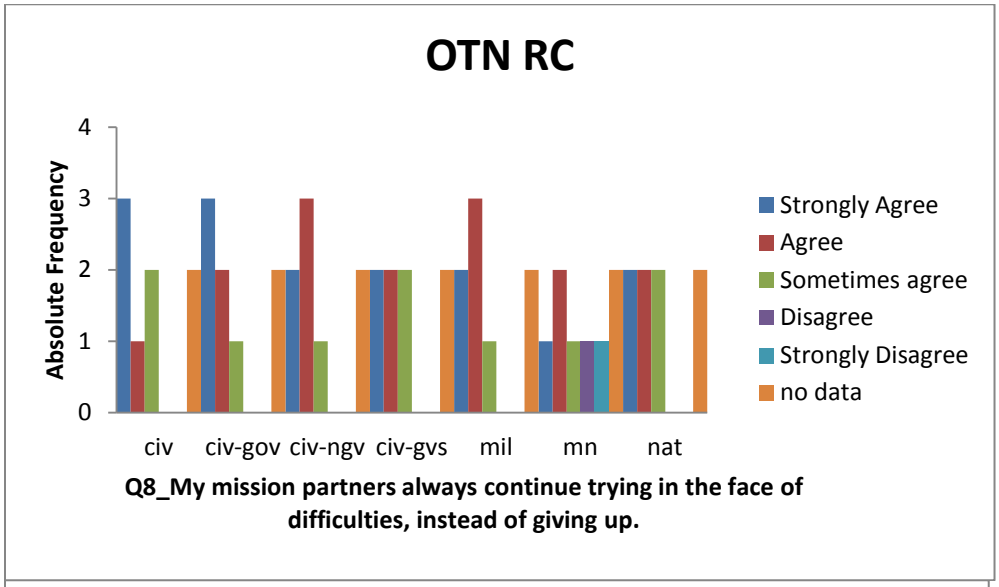
Information were pasted but no answer at all from the audience but the US response cell
Die Arbeit erfolgt schleppend, da Infos zu langsam weitergegeben werden oder Fragen nicht beantwortetet werden.
manipulating question!
My objectives.

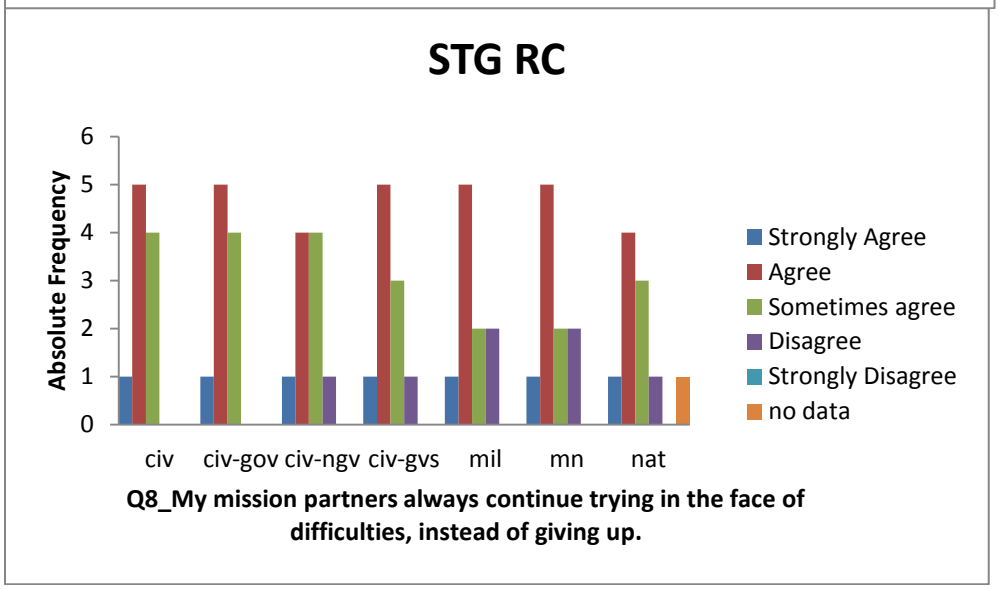
IQ08

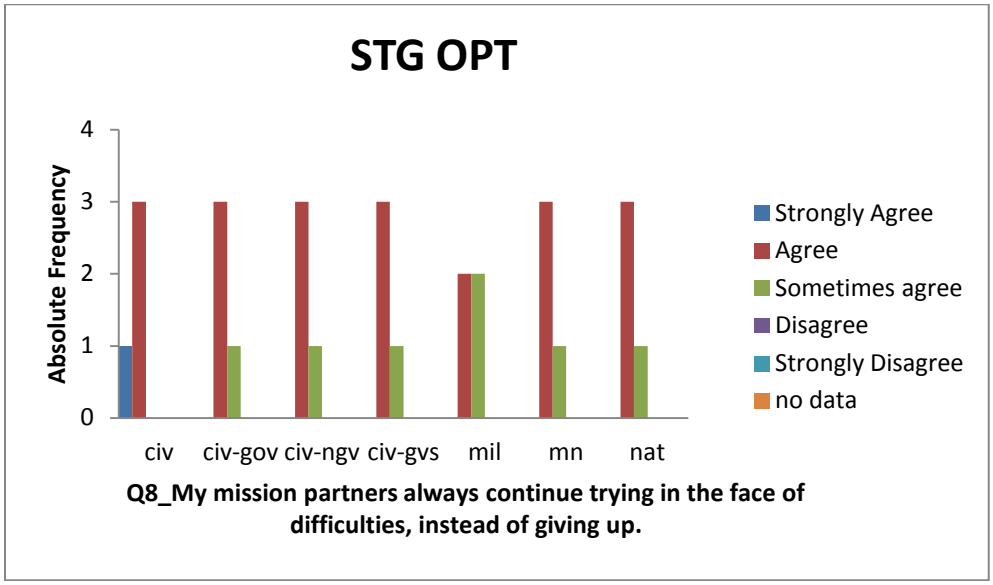
"My mission partners always continue trying in the face of difficulties, instead of giving up."


Stuttgart (OPT, RC) and Ottobrunn (RC)
Accumulated Absolute Frequency
55
50
45
40
35
30
25
20
15
10
5
0
mission partners
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q8_My mission partners always continue trying in the face of difficulties, instead of giving up.


Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
9
8
7
6
5
4
3
2
1
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q8_My mission partners always continue trying in the face of difficulties, instead of giving up.


OTN RC
Absolute Frequency
4
3
2
1
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q8_My mission partners always continue trying in the face of difficulties, instead of giving up.

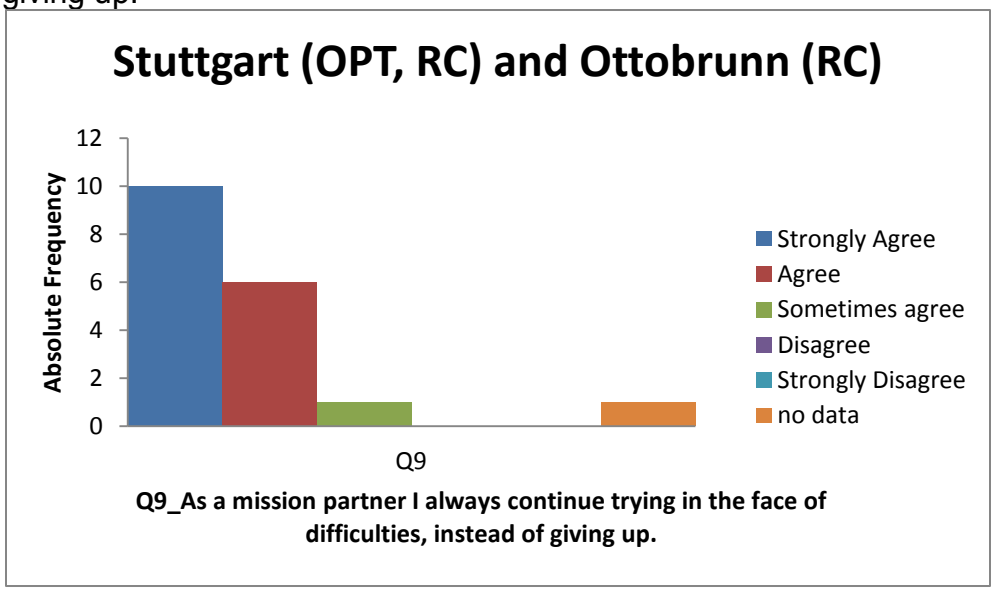

STG RC
Absolute Frequency
6
5
4
3
2
1
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q8_My mission partners always continue trying in the face of difficulties, instead of giving up.

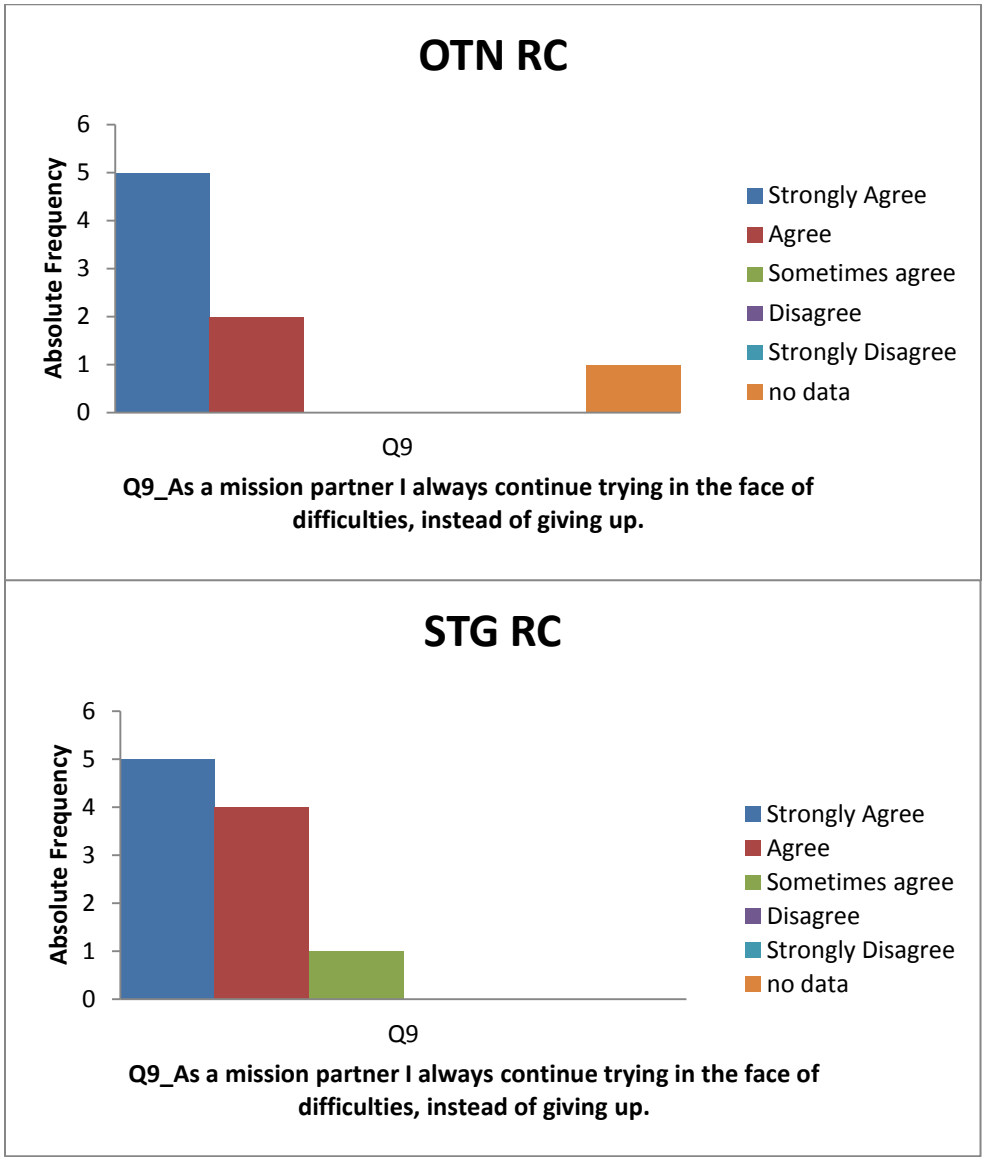


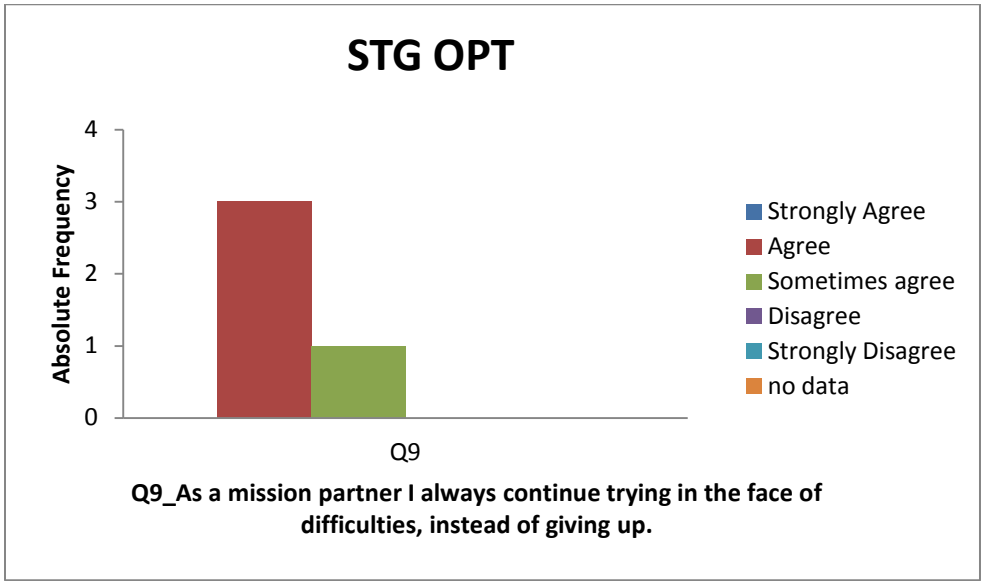
IQ09

IQ09.1

"As a mission partner I always continue trying in the face of difficulties, instead of giving up."




OTN RC
Absolute Frequency
6
5
4
3
2
1
0
Q9
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q9_As a mission partner I always continue trying in the face of difficulties, instead of giving up.
STG RC
Absolute Frequency
6
5
4
3
2
1
0
Q9
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q9_As a mission partner I always continue trying in the face of difficulties, instead of giving up.



IQ09.2

"Please comment"

OPT Stuttgart

If I give up the mission could fail
This question directly assesses internal fortitude
(?) We are pushing to coordinate…but don't always know who to contact or are (???) to do the wrong thing
However I am concerned that this trying should ultimately end up as a helpful thing rather than an non-helpful one

RC Stuttgart

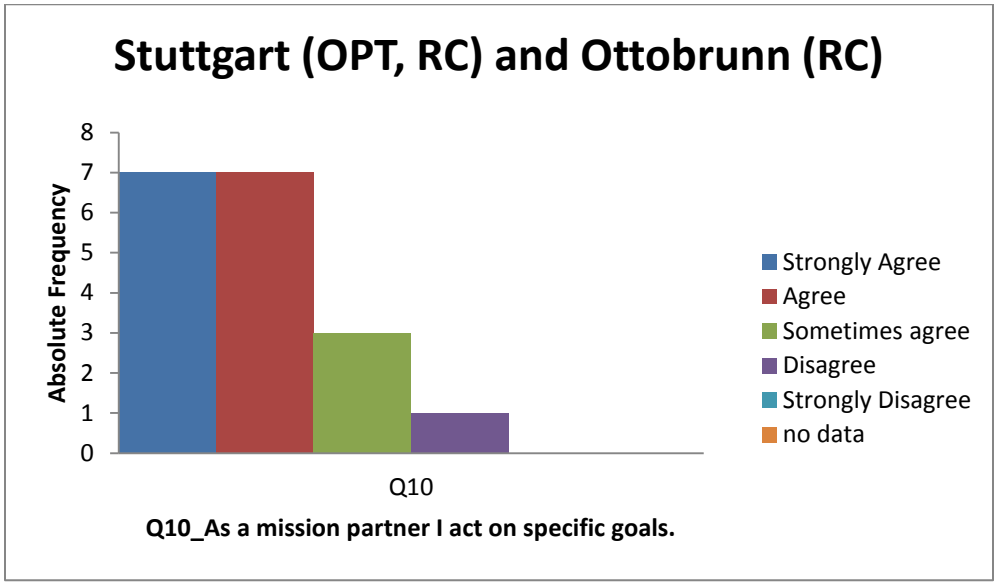
CFC understands complexities of Civil-Military Interaction as not all partners are "willing or able" to share information and / or work together.
It depends on the cost effectiveness of continuing

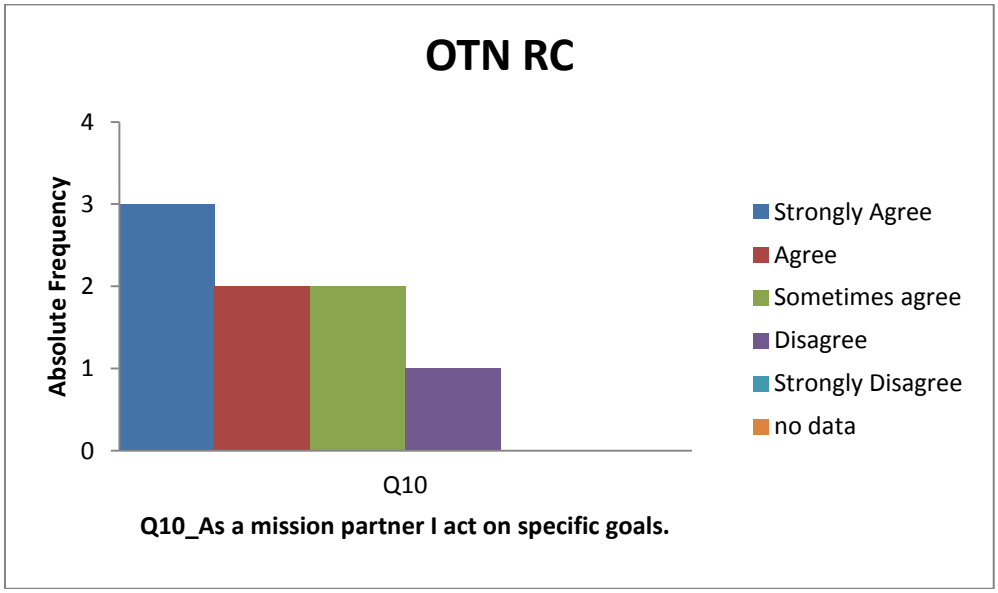
RC Ottobrunn

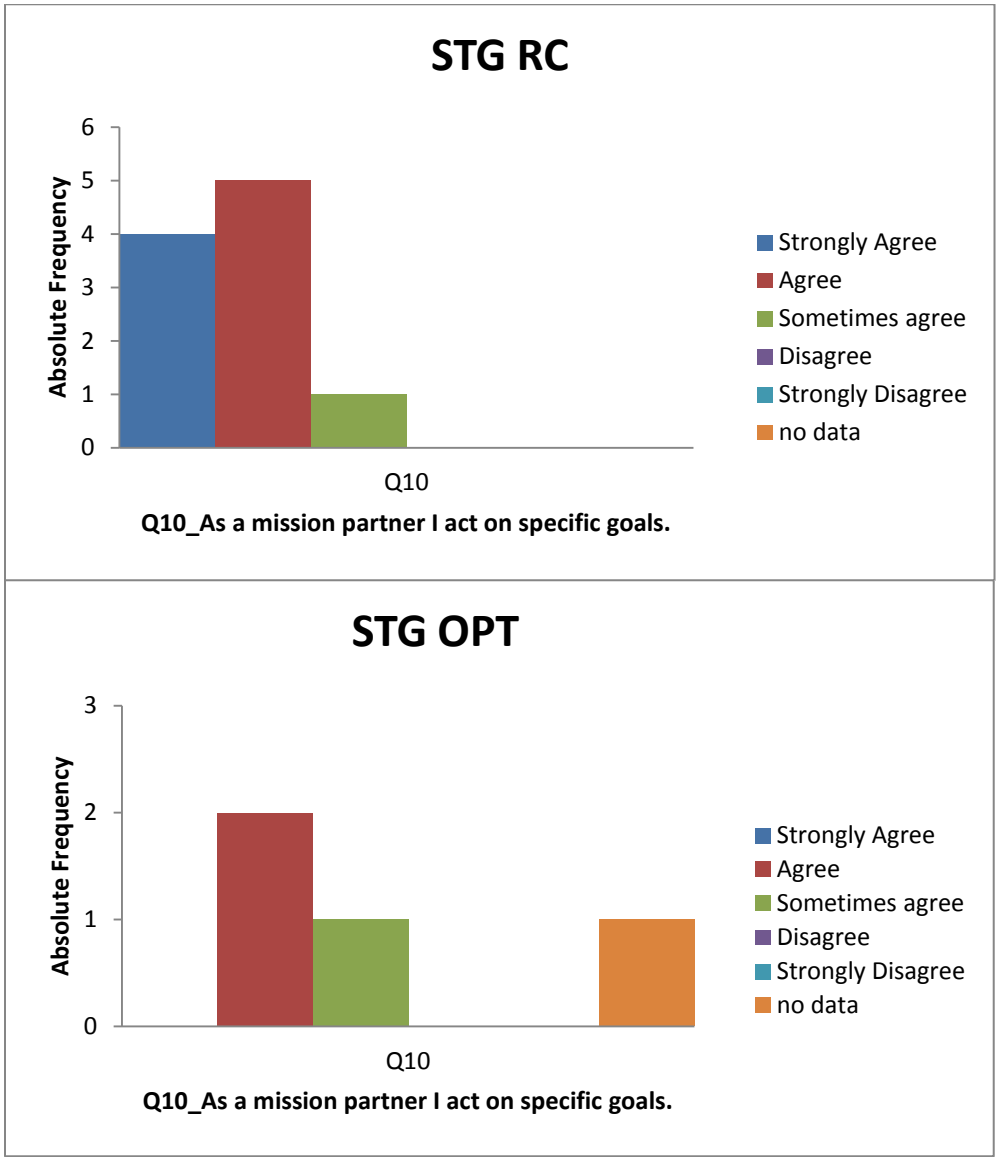
Which mission objectives? I as a NGO, following own agenda /objectives might be different from "mission objectives"

IQ10

"As a mission partner I act on specific goals."

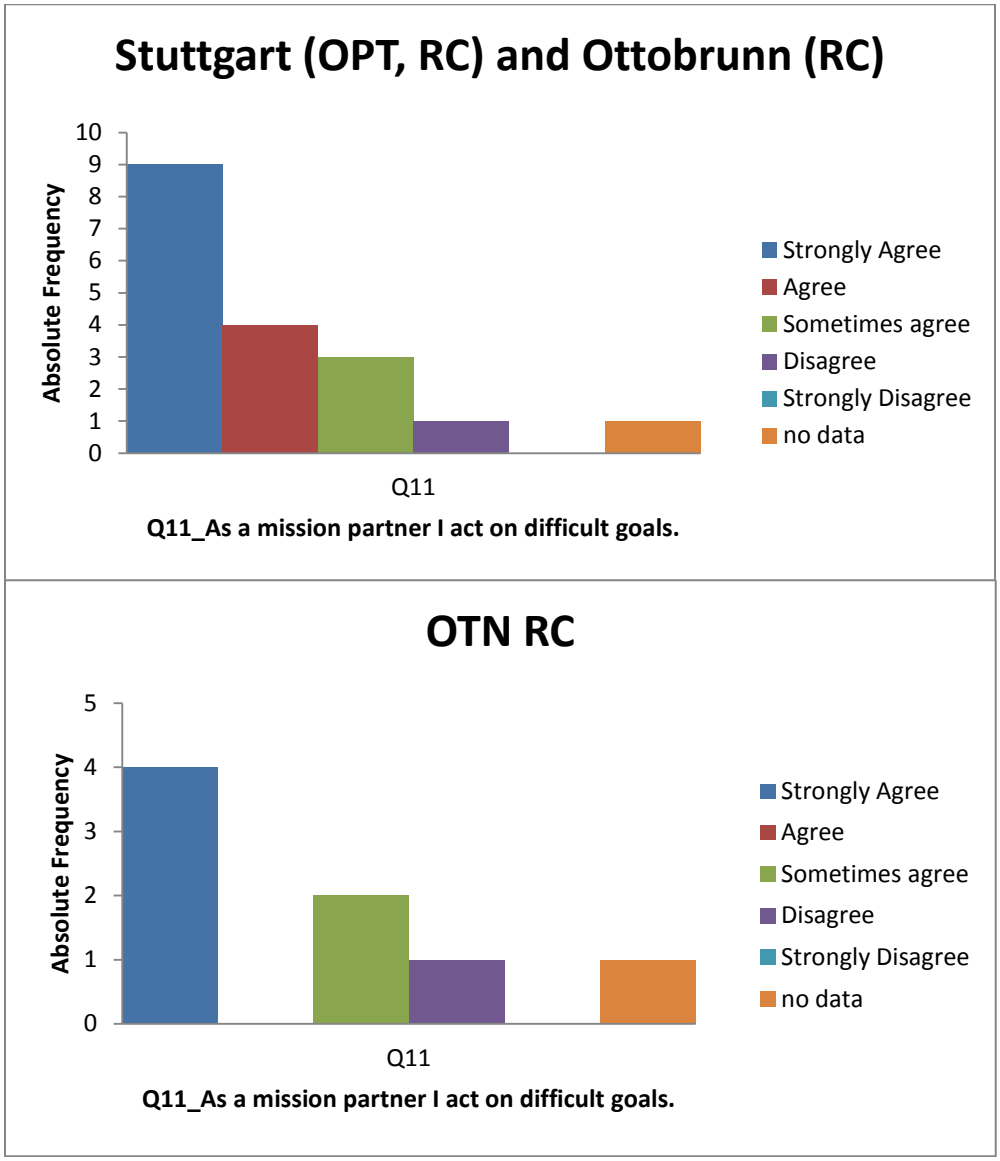

Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
8
7
6
5
4
3
2
1
0
Q10
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q10_As a mission partner I act on specific goals.

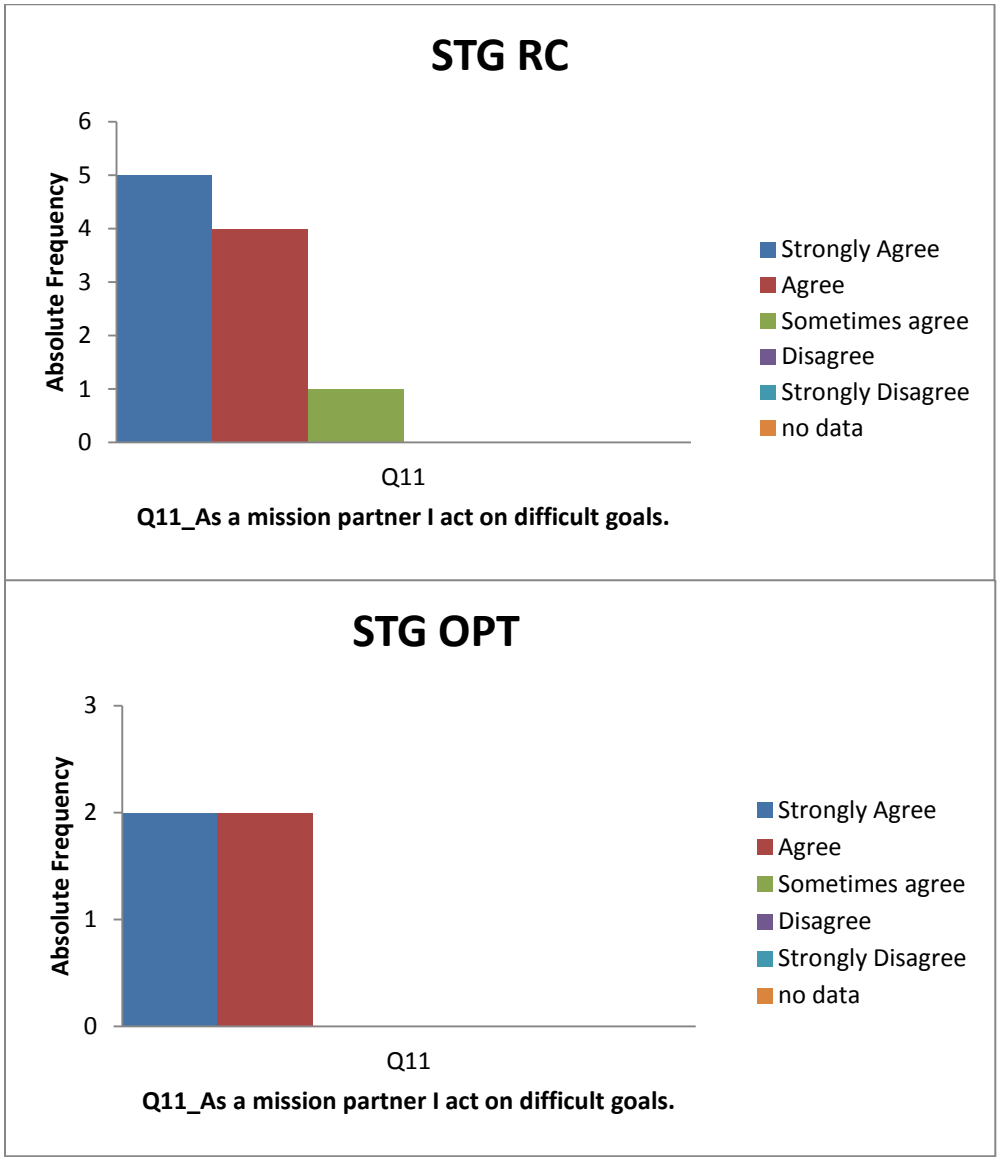

OTN RC
Absolute Frequency
4
3
2
1
0
Q10
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q10_As a mission partner I act on specific goals.



IQ11

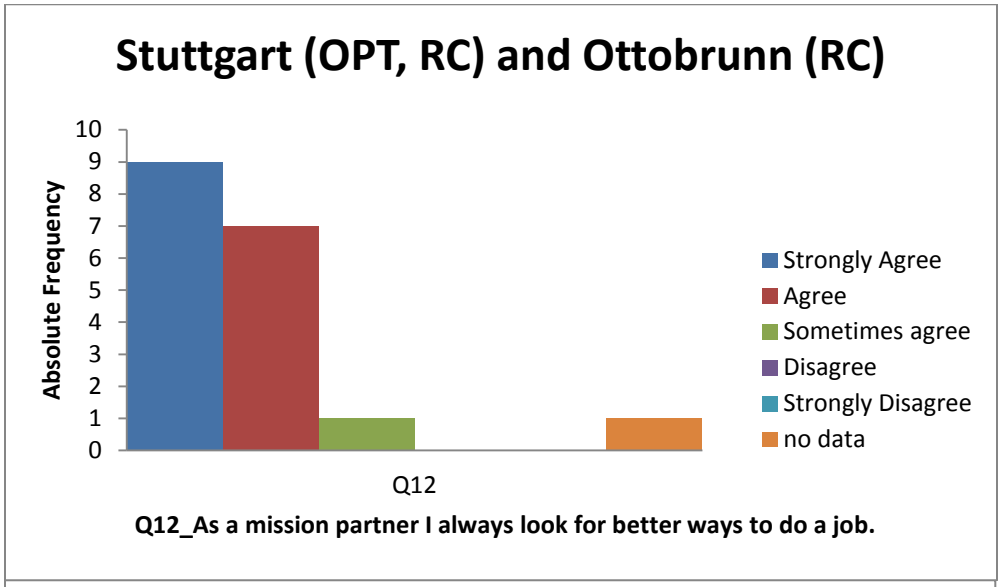
"As a mission partner I act on difficult goals."

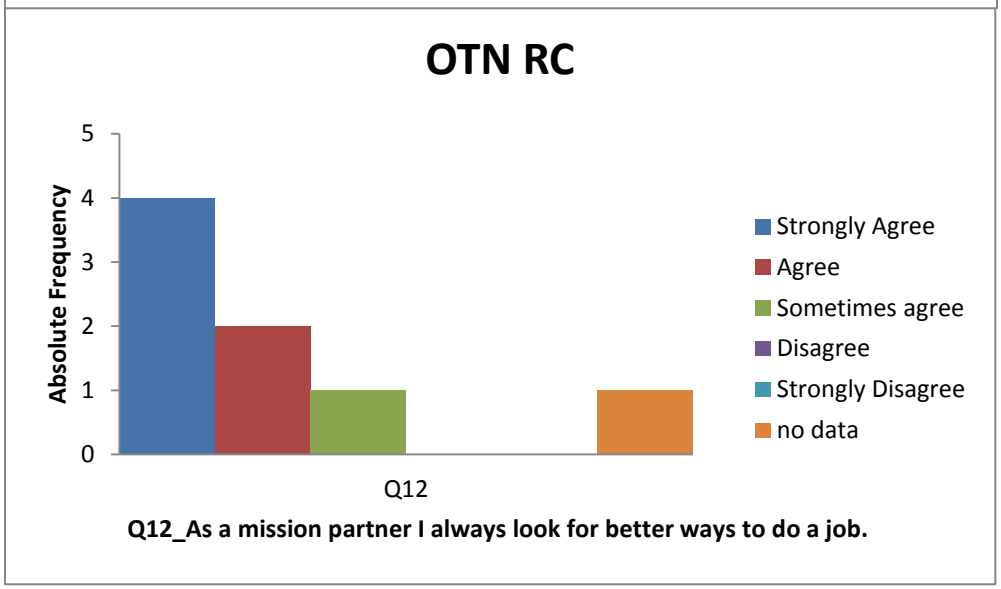

Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
10
9
8
7
6
5
4
3
2
1
0
Q11
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q11_As a mission partner I act on difficult goals.
OTN RC
Absolute Frequency
5
4
3
2
1
0
Q11
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q11_As a mission partner I act on difficult goals.

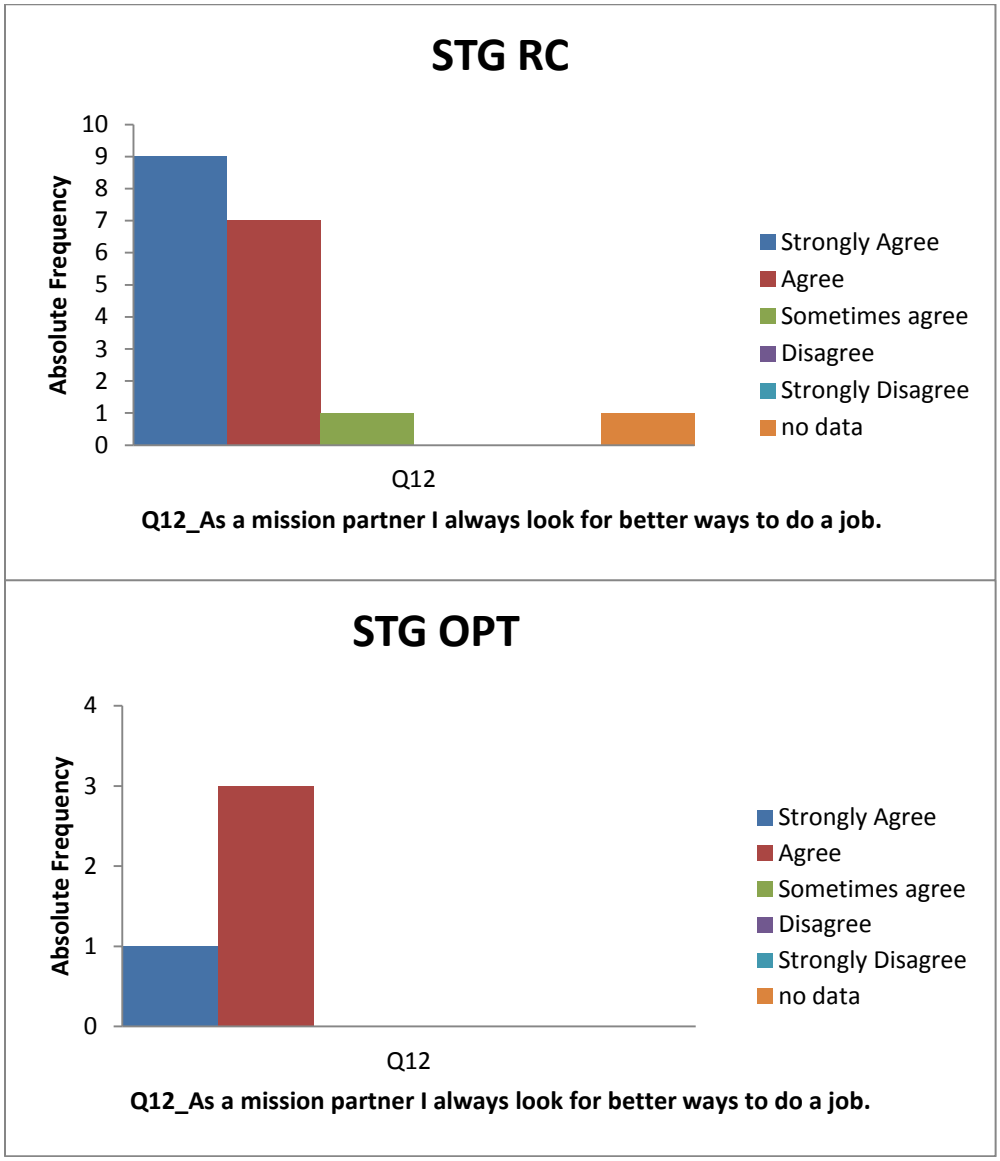


IQ12

"As a mission partner I always look for better ways to do a job."

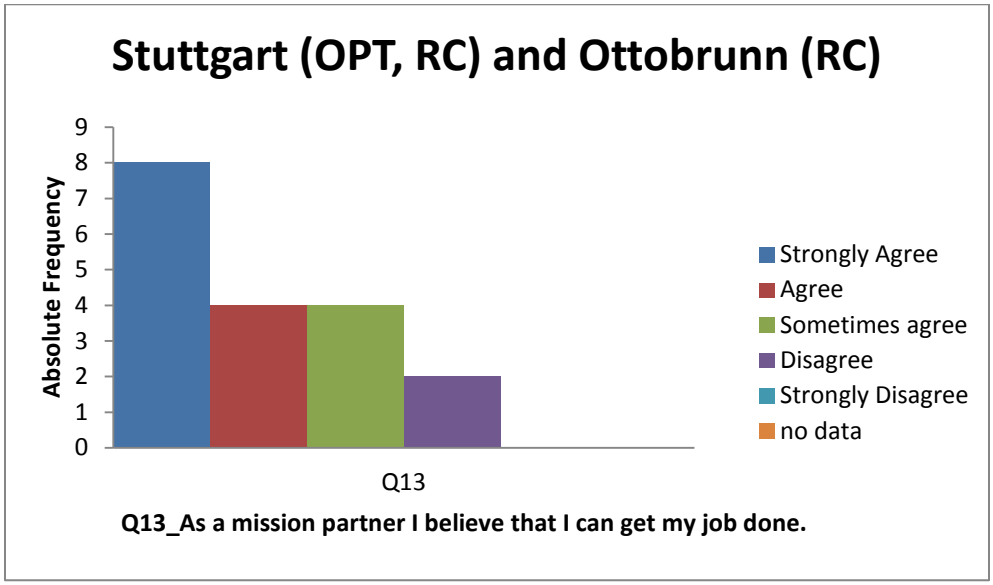

Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
10
9
8
7
6
5
4
3
2
1
0
Q12
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q12_As a mission partner I always look for better ways to do a job.

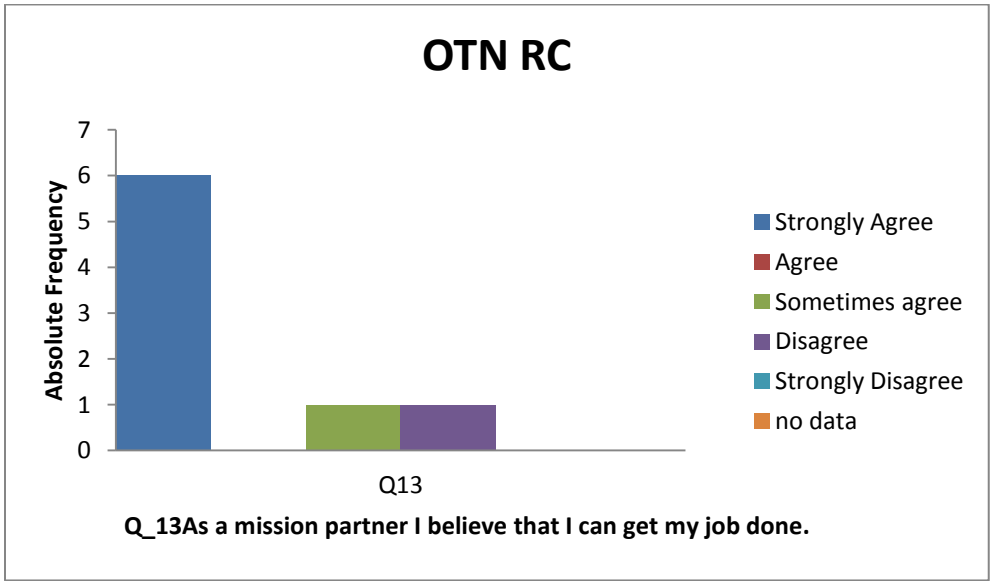

OTN RC
Absolute Frequency
5
4
3
2
1
0
Q12
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q12_As a mission partner I always look for better ways to do a job.

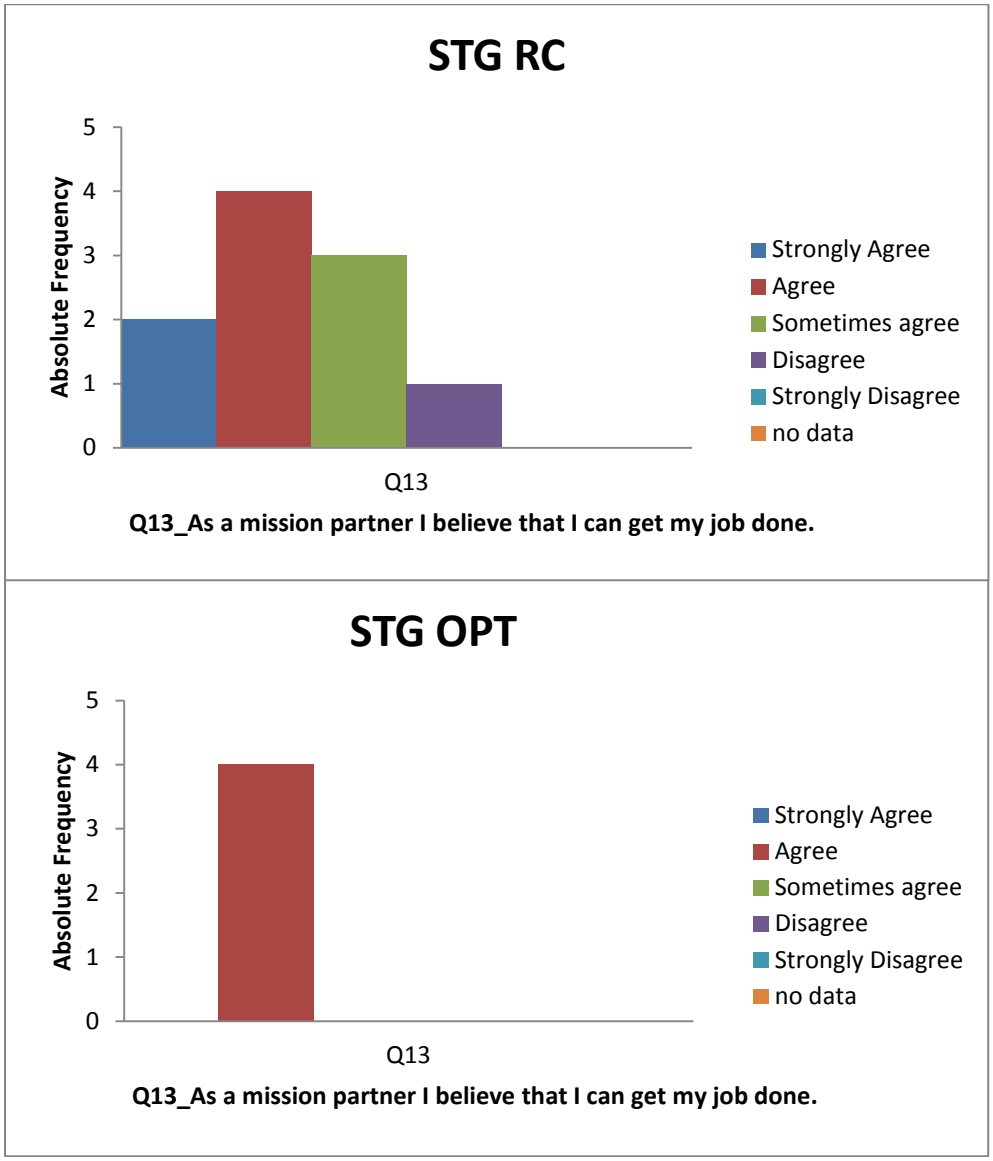


IQ13

"As a mission partner I believe that I can get my job done."

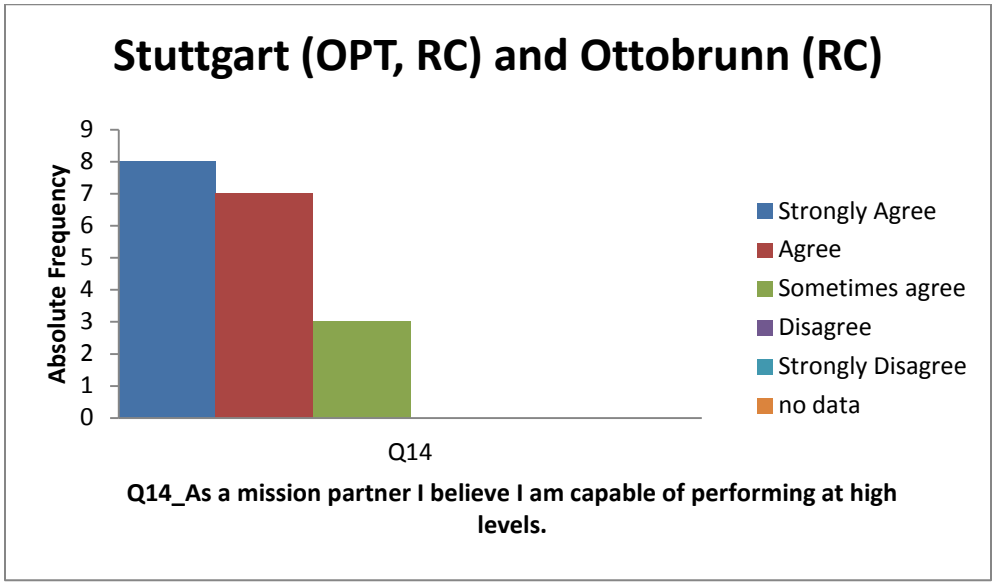

Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
9
8
7
6
5
4
3
2
1
0
Q13
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q13_As a mission partner I believe that I can get my job done.

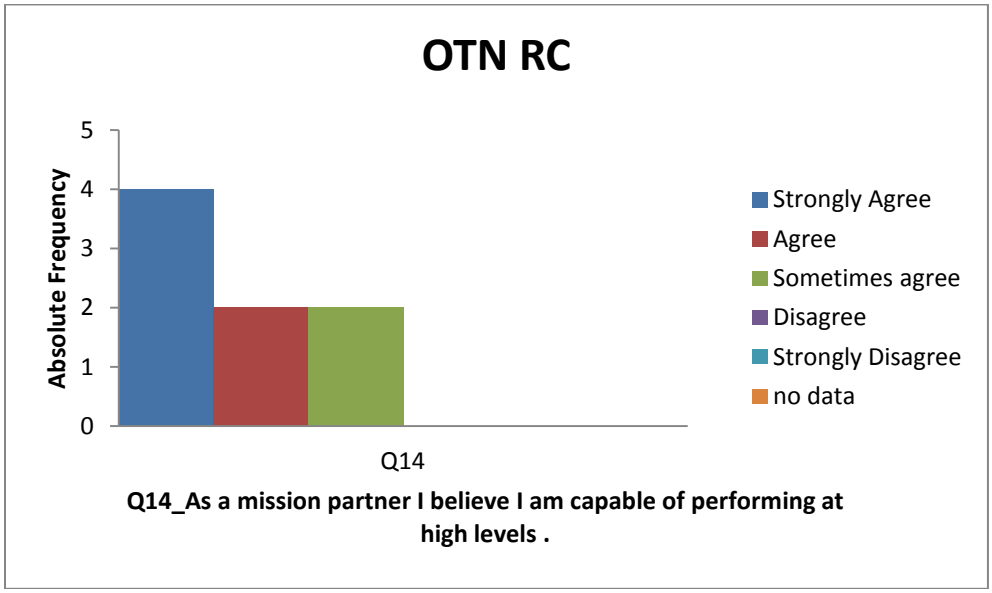

OTN RC
Absolute Frequency
7
6
5
4
3
2
1
0
Q13
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q_13As a mission partner I believe that I can get my job done.

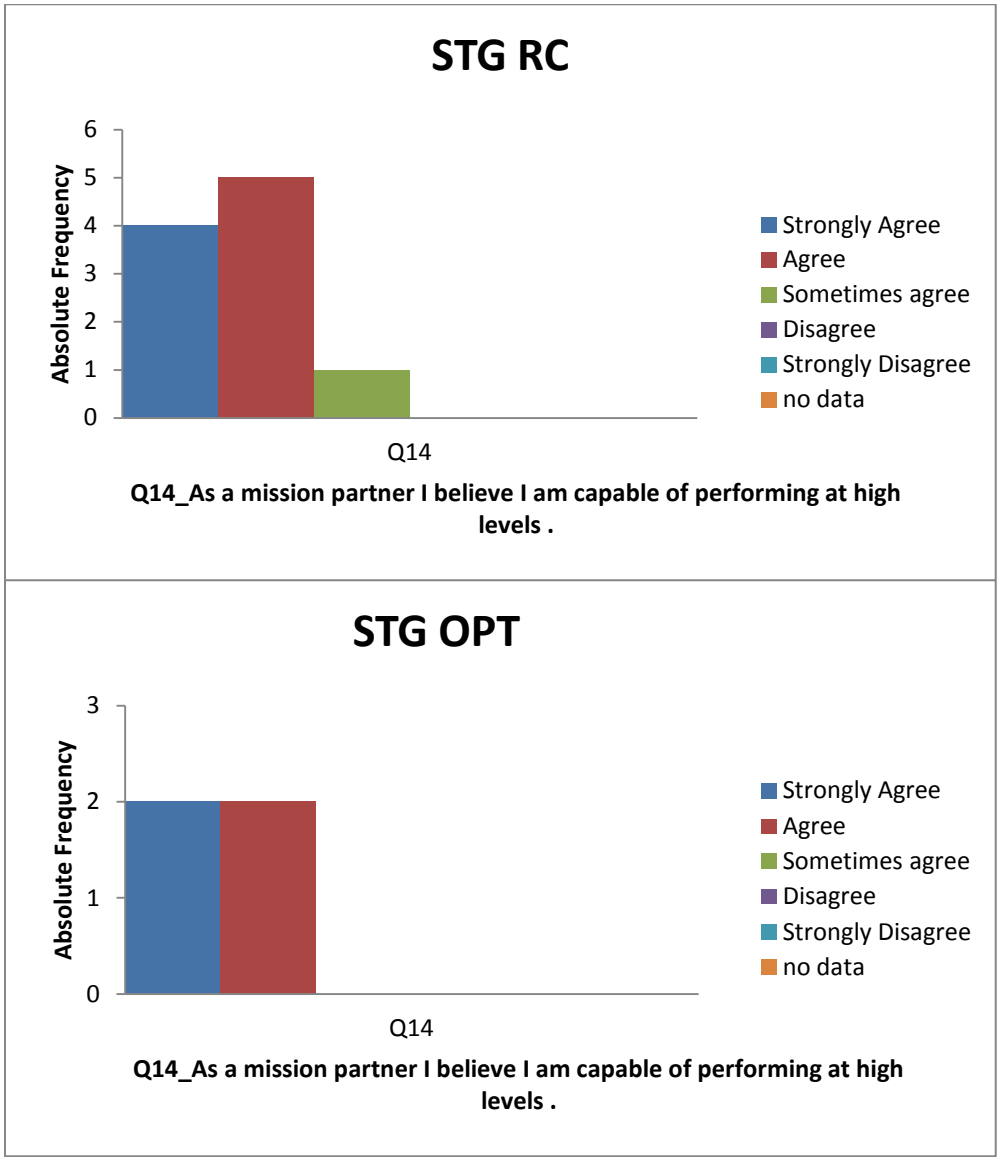


IQ14

"As a mission partner I believe I am capable of performing at high levels."

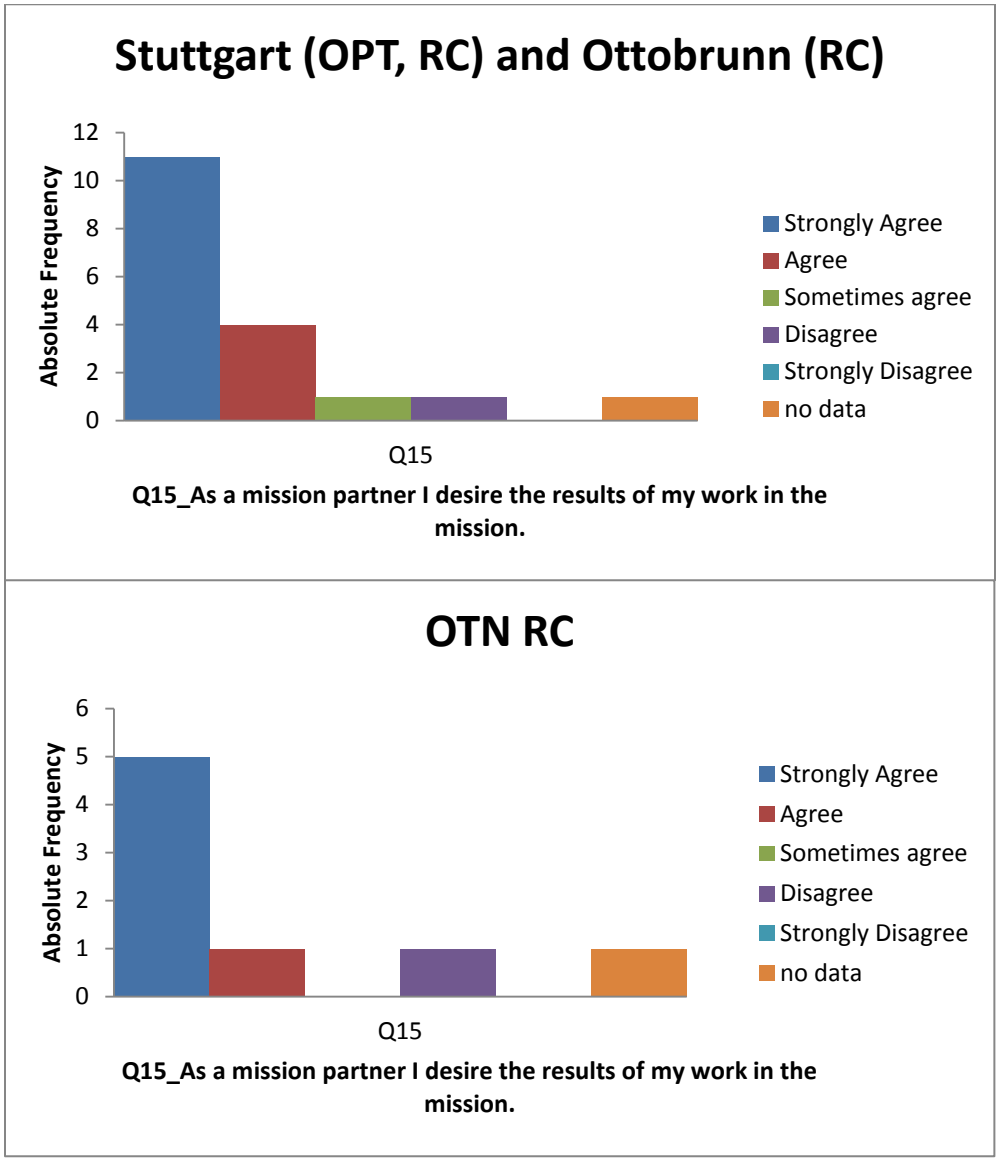

Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
9
8
7
6
5
4
3
2
1
0
Q14
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q14_As a mission partner I believe I am capable of performing at high levels.

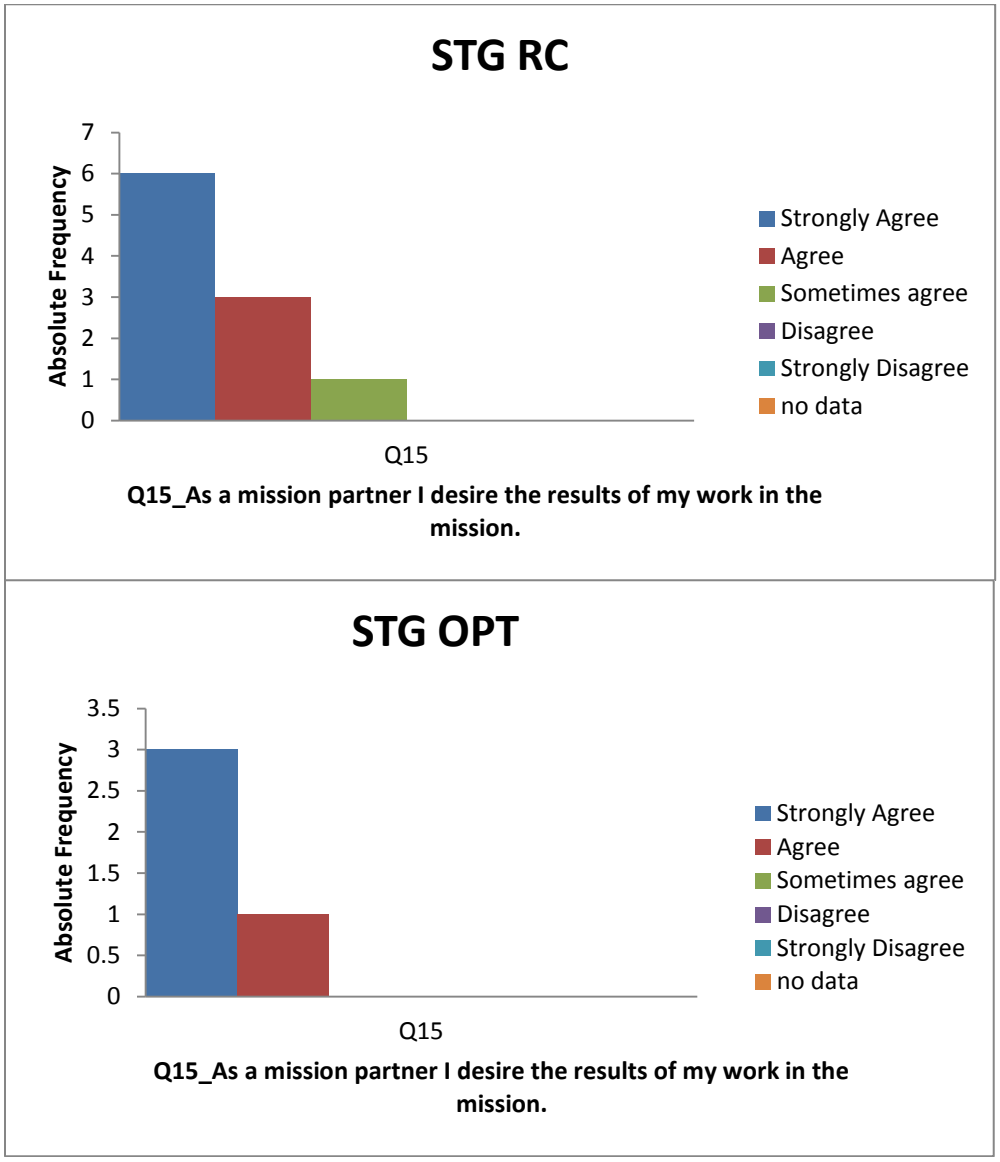

OTN RC
Absolute Frequency
5
4
3
2
1
0
Q14
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q14_As a mission partner I believe I am capable of performing at high levels .



IQ15

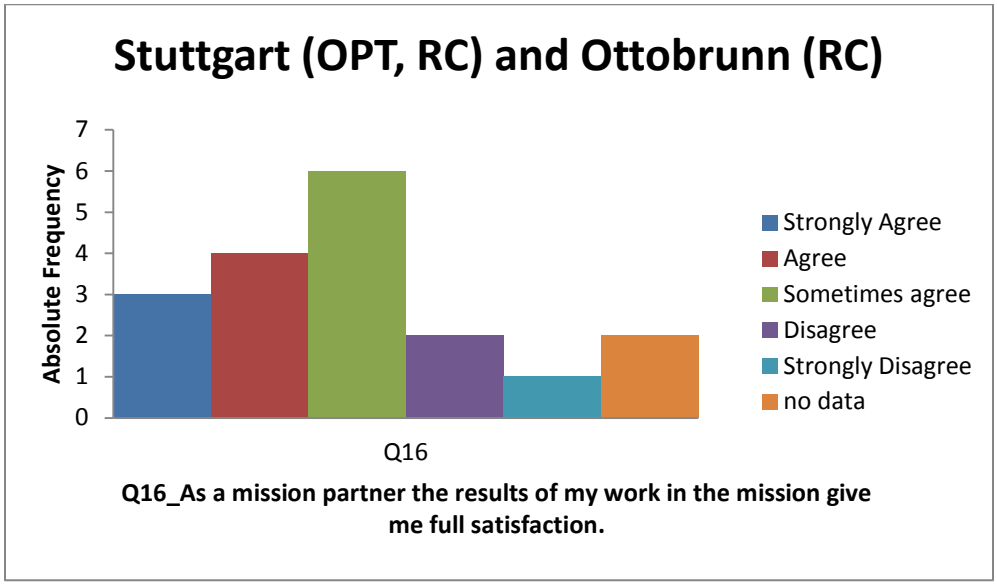
"As a mission partner I desire the results of my work in the mission."

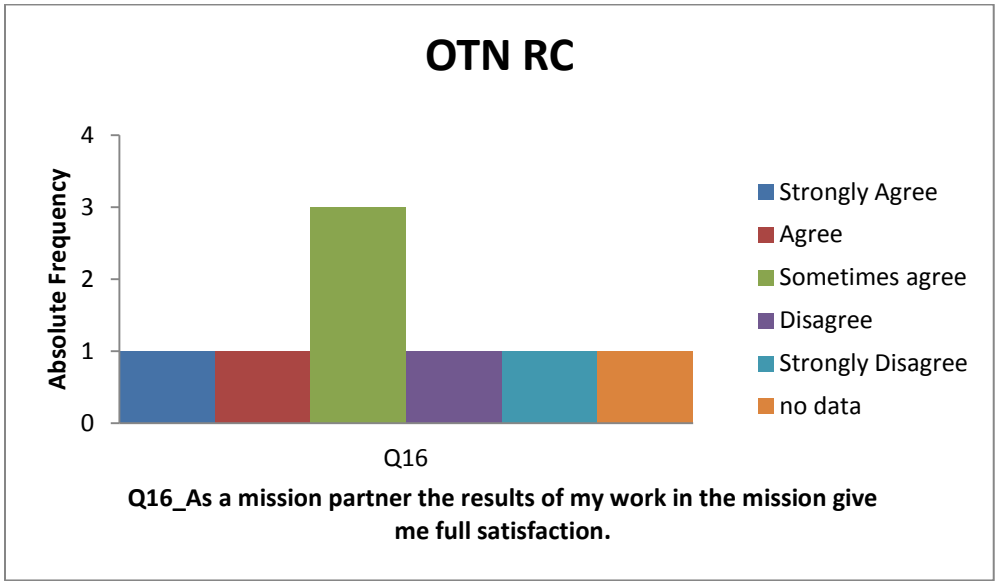

Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
12
10
8
6
4
2
0
Q15
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q15_As a mission partner I desire the results of my work in the mission.
OTN RC
Absolute Frequency
6
5
4
3
2
1
0
Q15
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q15_As a mission partner I desire the results of my work in the mission.

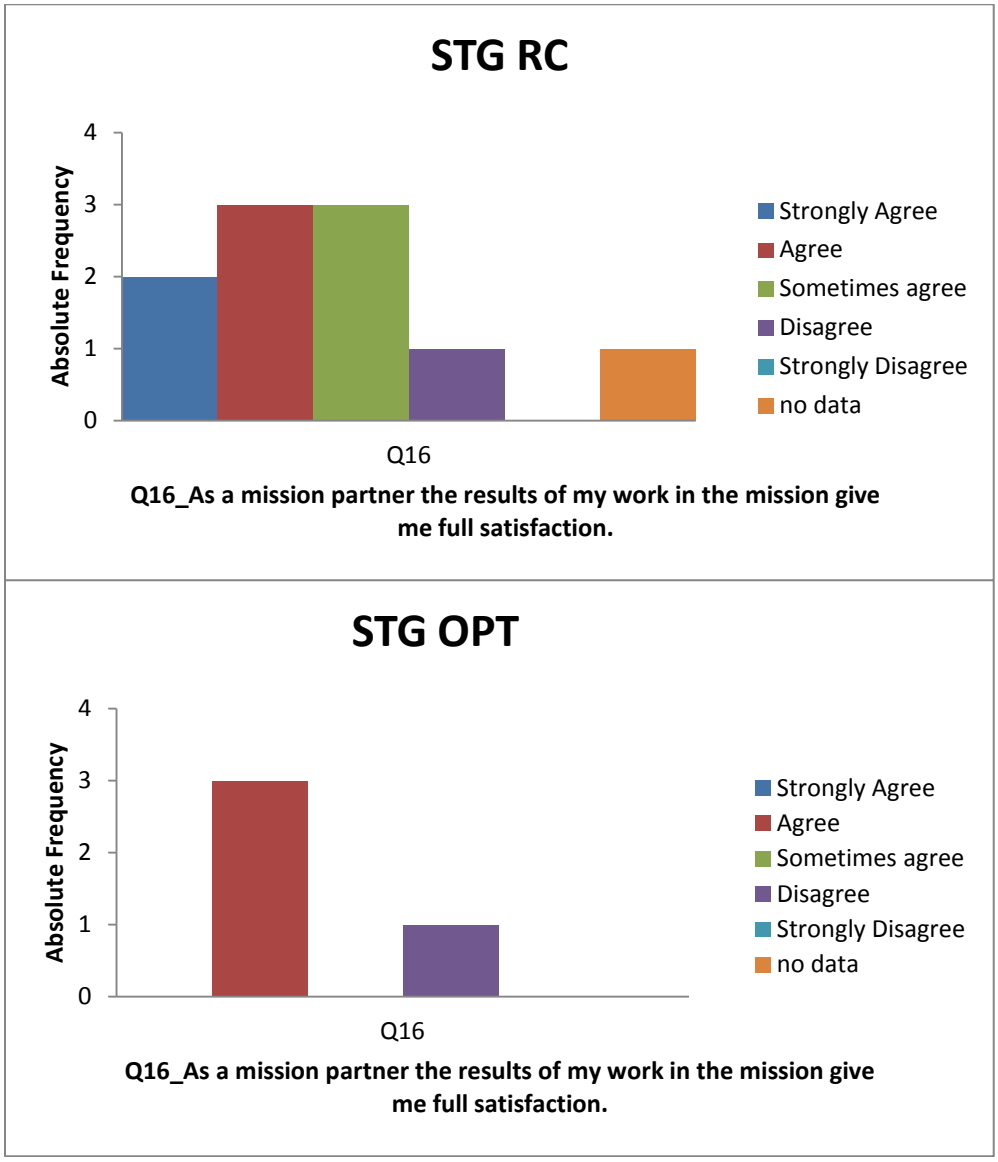


IQ16

"As a mission partner the results of my work in the mission give me full satisfaction."

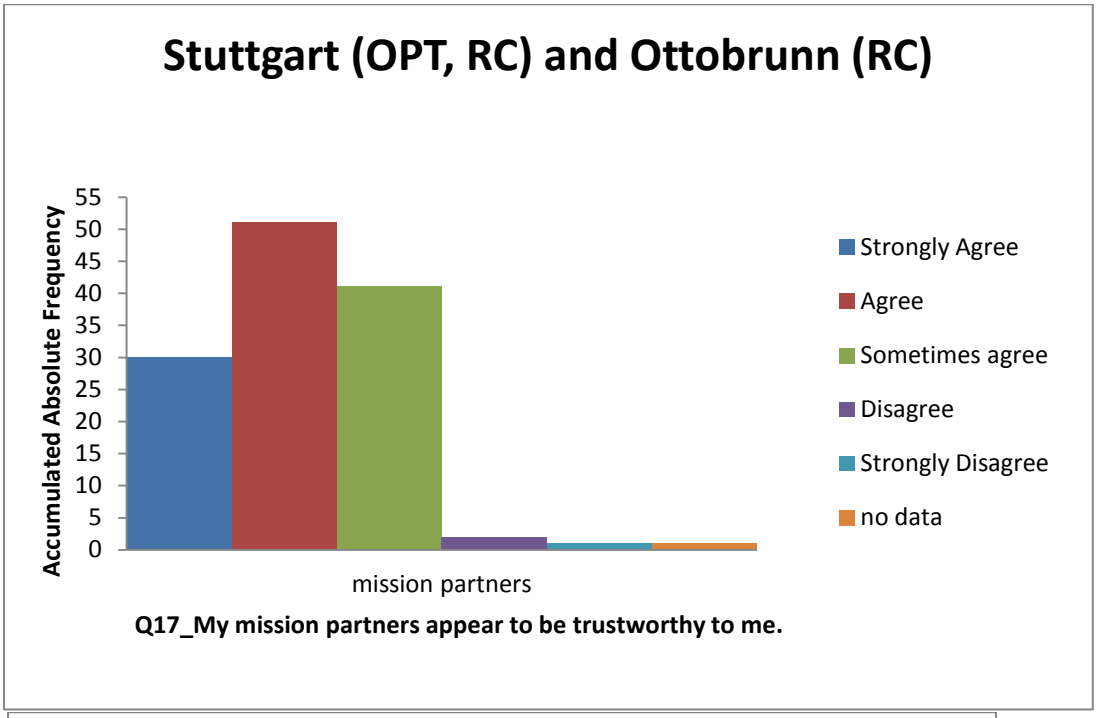

Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
7
6
5
4
3
2
1
0
Q16
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q16_As a mission partner the results of my work in the mission give me full satisfaction.

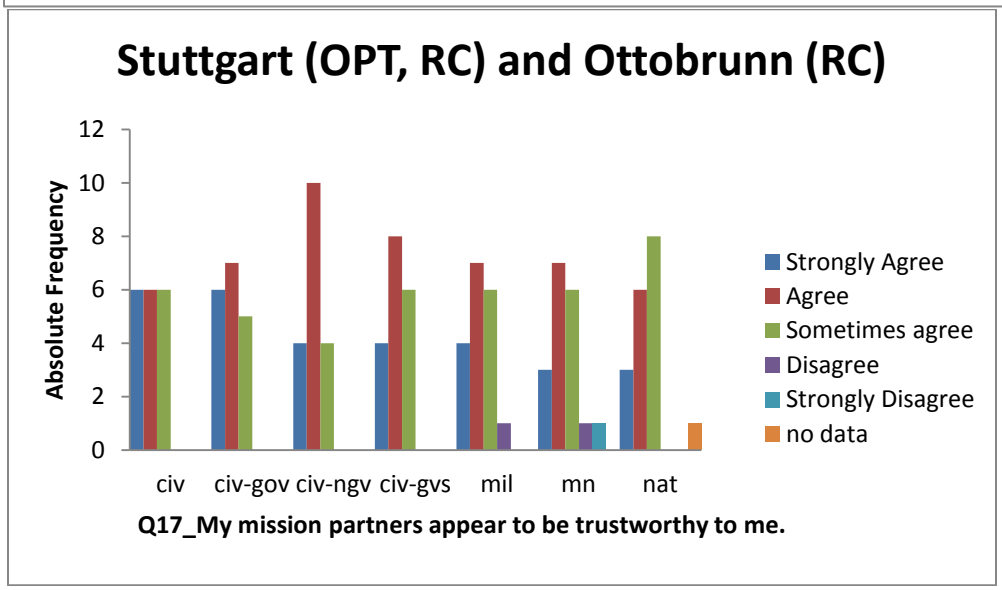

OTN RC
Absolute Frequency
4
3
2
1
0
Q16
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q16_As a mission partner the results of my work in the mission give me full satisfaction.

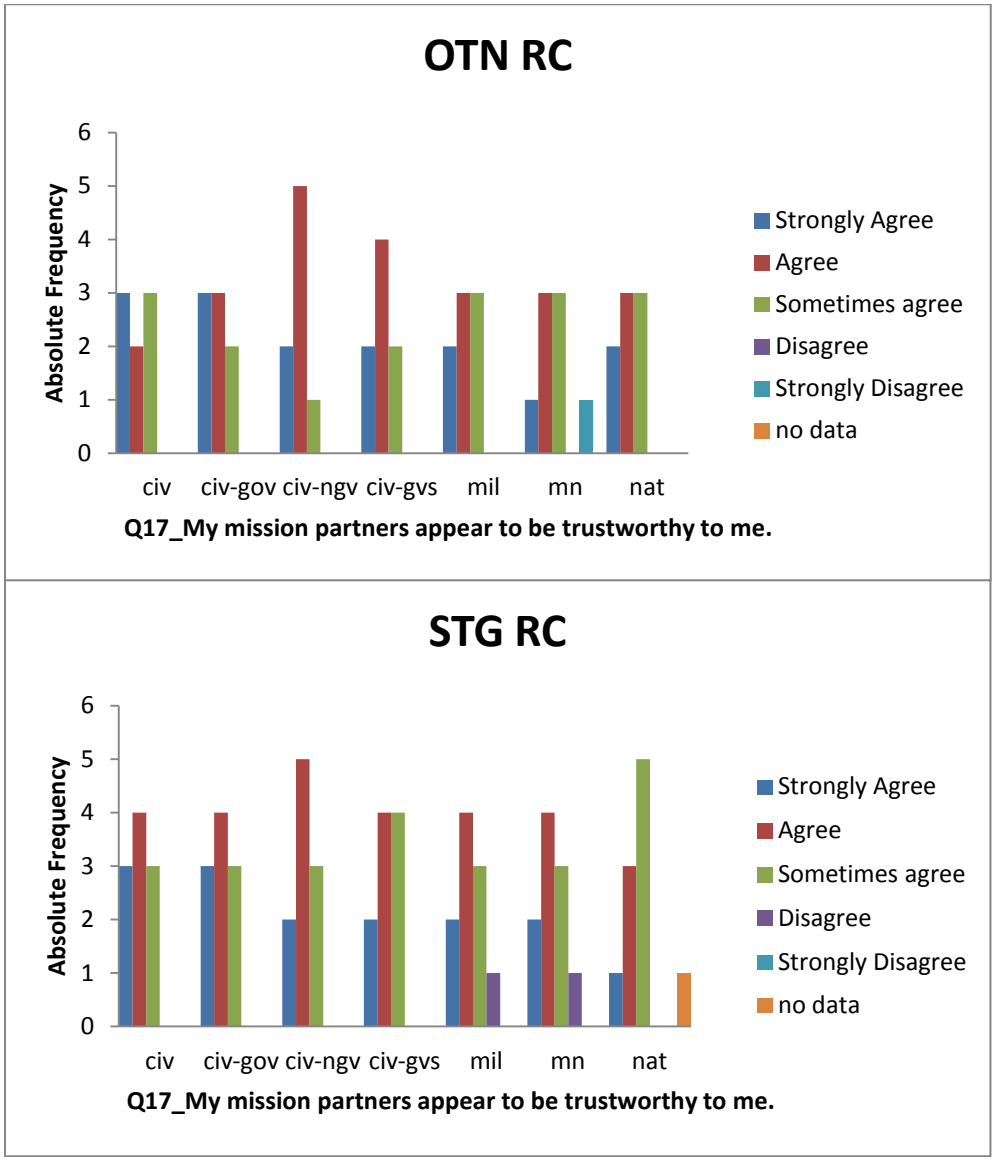


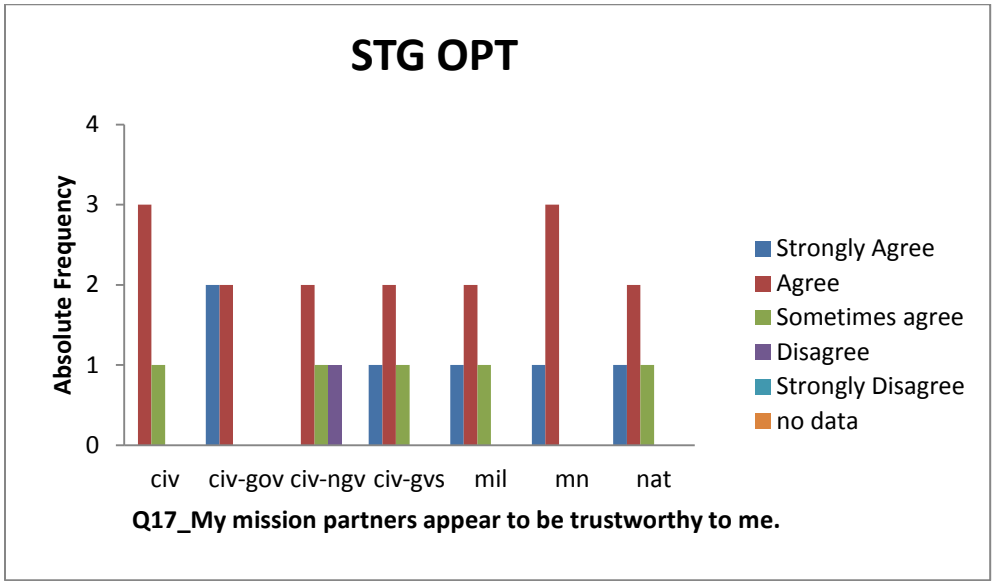
IQ17

"My mission partners appear to be trustworthy to me."


Stuttgart (OPT, RC) and Ottobrunn (RC)
Accumulated Absolute Frequency
55
50
45
40
35
30
25
20
15
10
5
0
mission partners
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q17_My mission partners appear to be trustworthy to me.

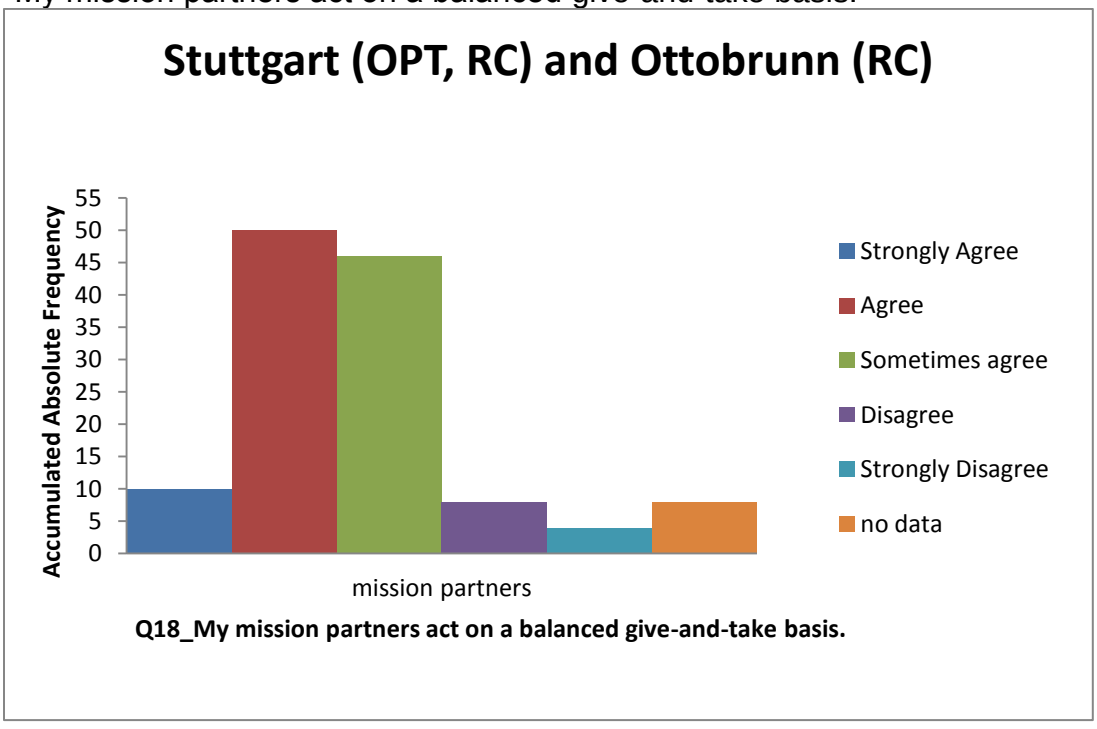

Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
12
10
8
6
4
2
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q17_My mission partners appear to be trustworthy to me.

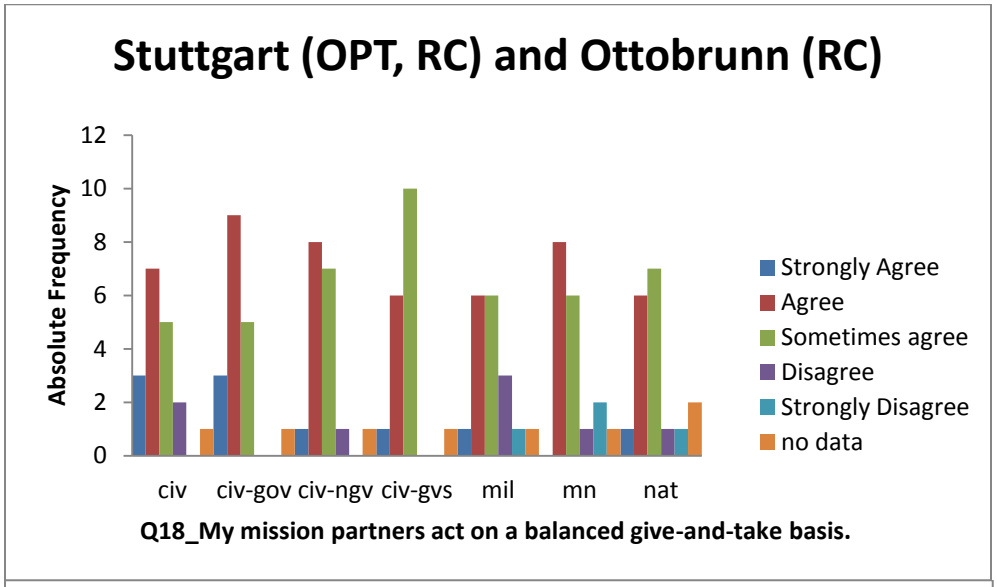

OTN RC
Absolute Frequency
0
1
2
3
4
5
6
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q17_My mission partners appear to be trustworthy to me.
STG RC
Absolute Frequency
0
1
2
3
4
5
6
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q17_My mission partners appear to be trustworthy to me.

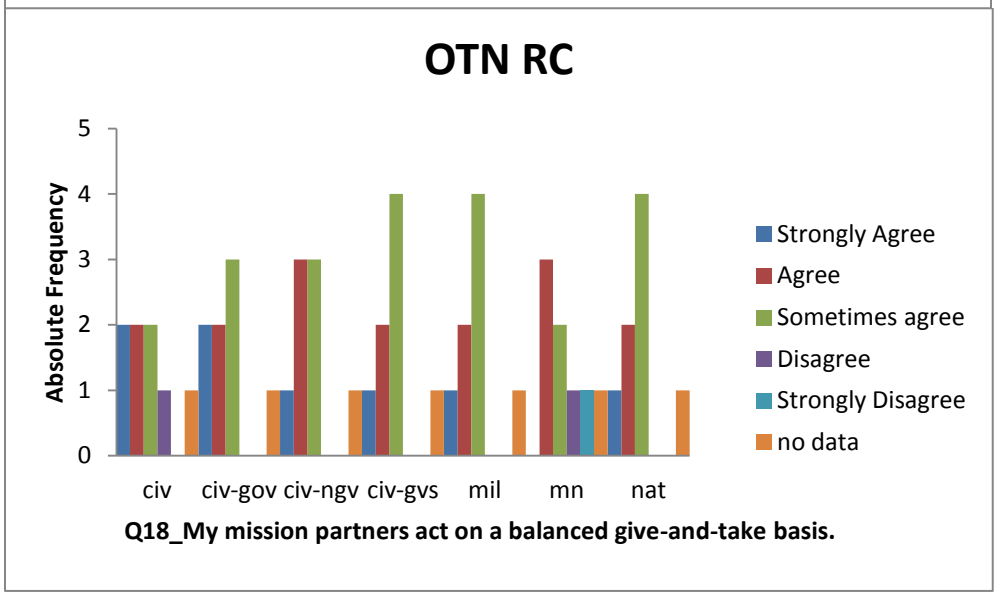


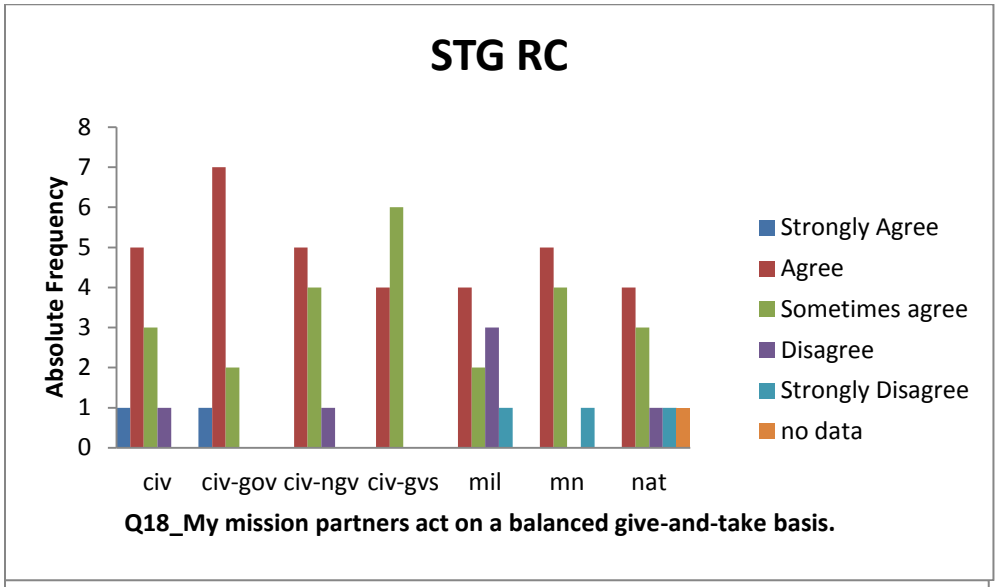
IQ18

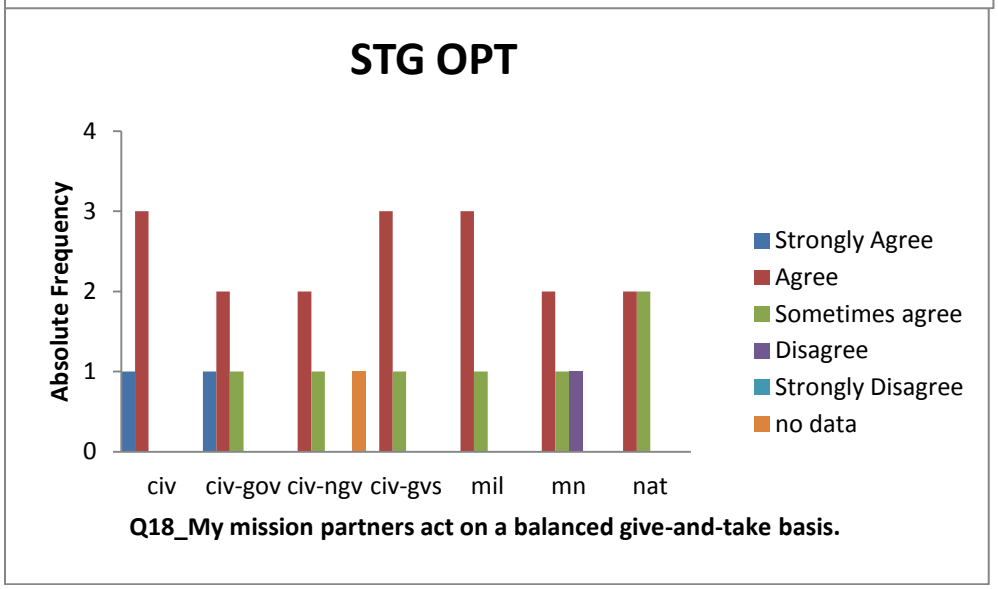
"My mission partners act on a balanced give-and-take basis."




Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
12
10
8
6
4
2
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q18_My mission partners act on a balanced give-and-take basis.

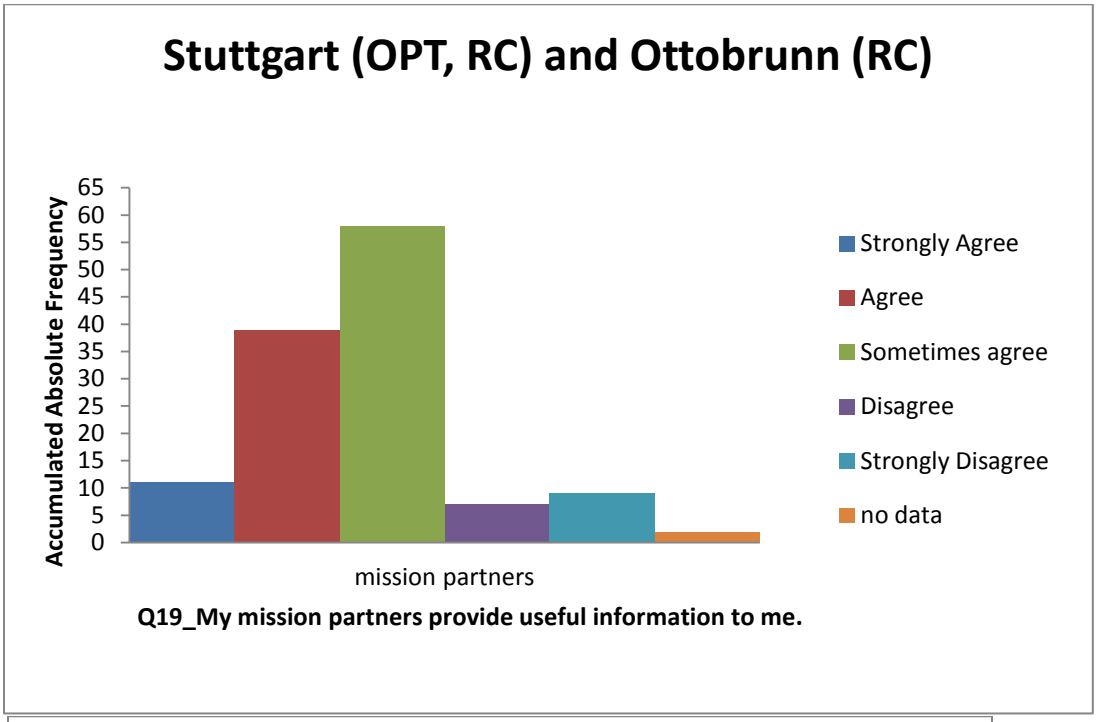

OTN RC
Absolute Frequency
5
4
3
2
1
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q18_My mission partners act on a balanced give-and-take basis.

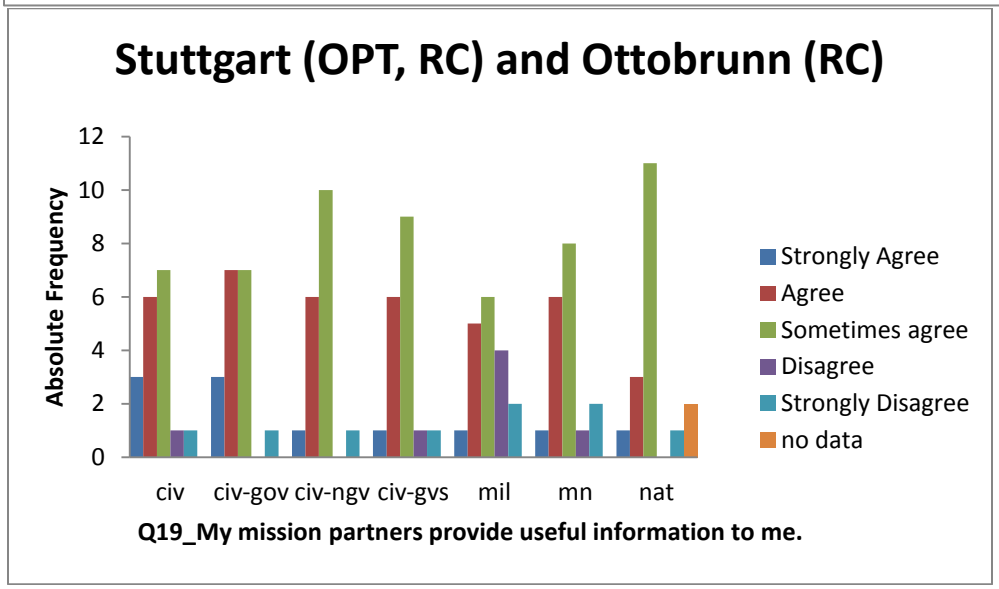


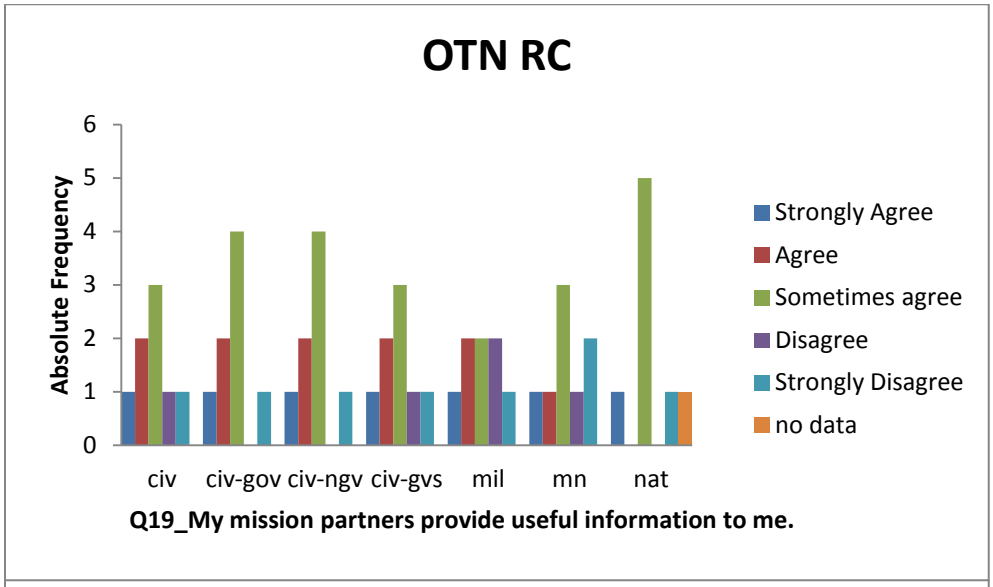


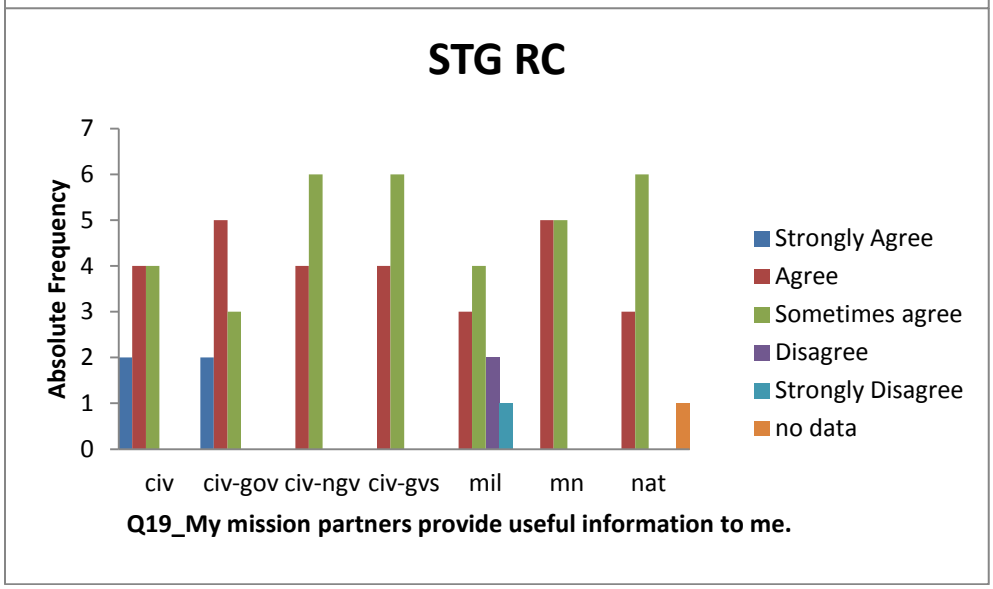
IQ19

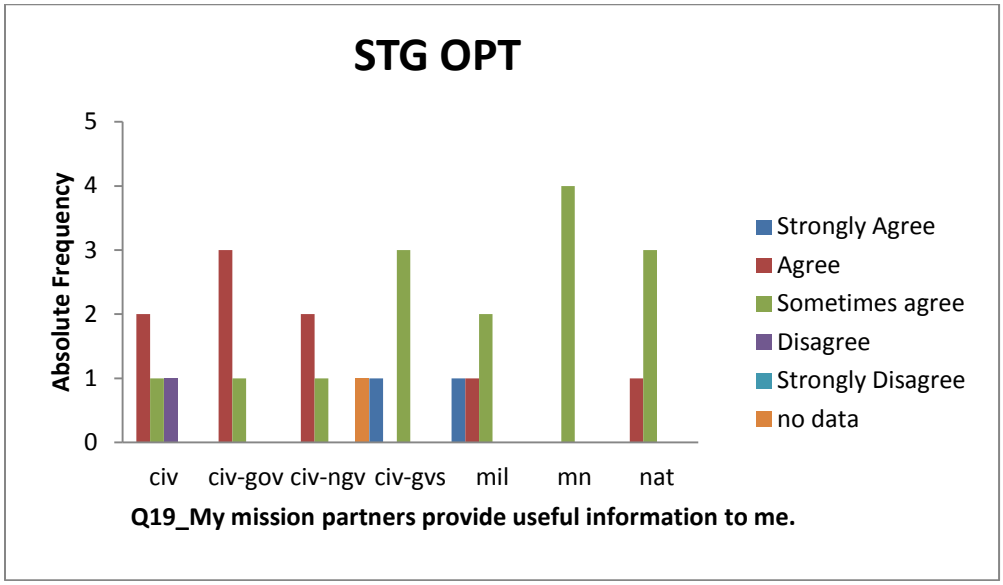
"My mission partners provide useful information to me."


Stuttgart (OPT, RC) and Ottobrunn (RC)
Accumulated Absolute Frequency
65
60
55
50
45
40
35
30
25
20
15
10
5
0
mission partners
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q19_My mission partners provide useful information to me.

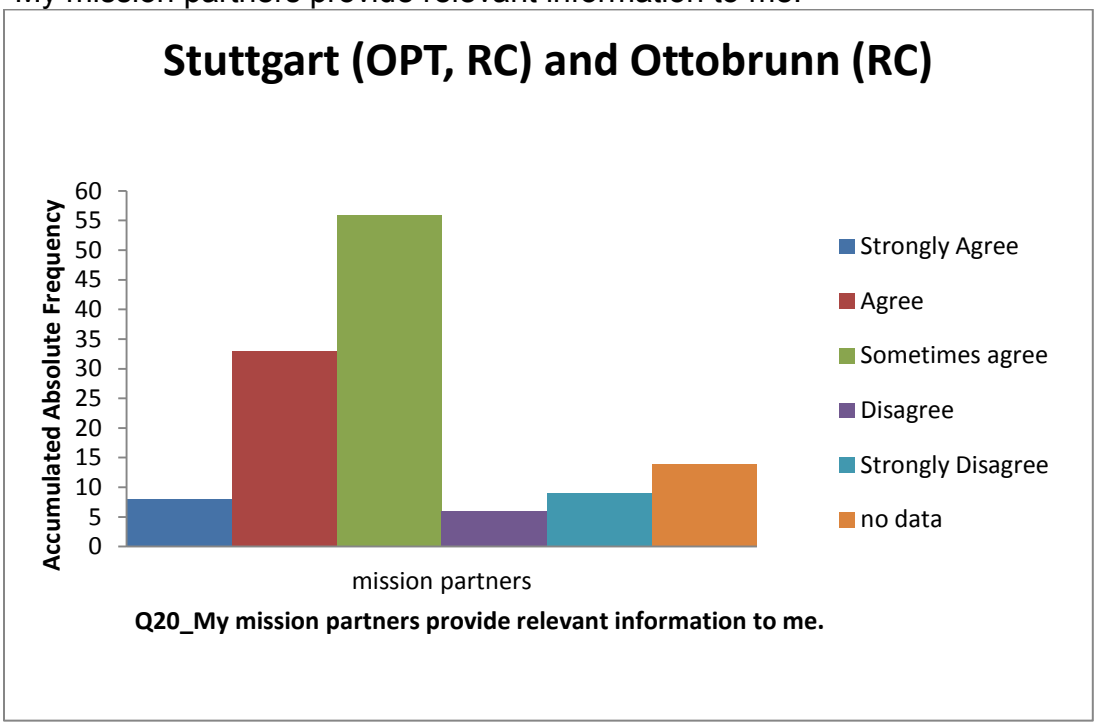

Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
12
10
8
6
4
2
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q19_My mission partners provide useful information to me.

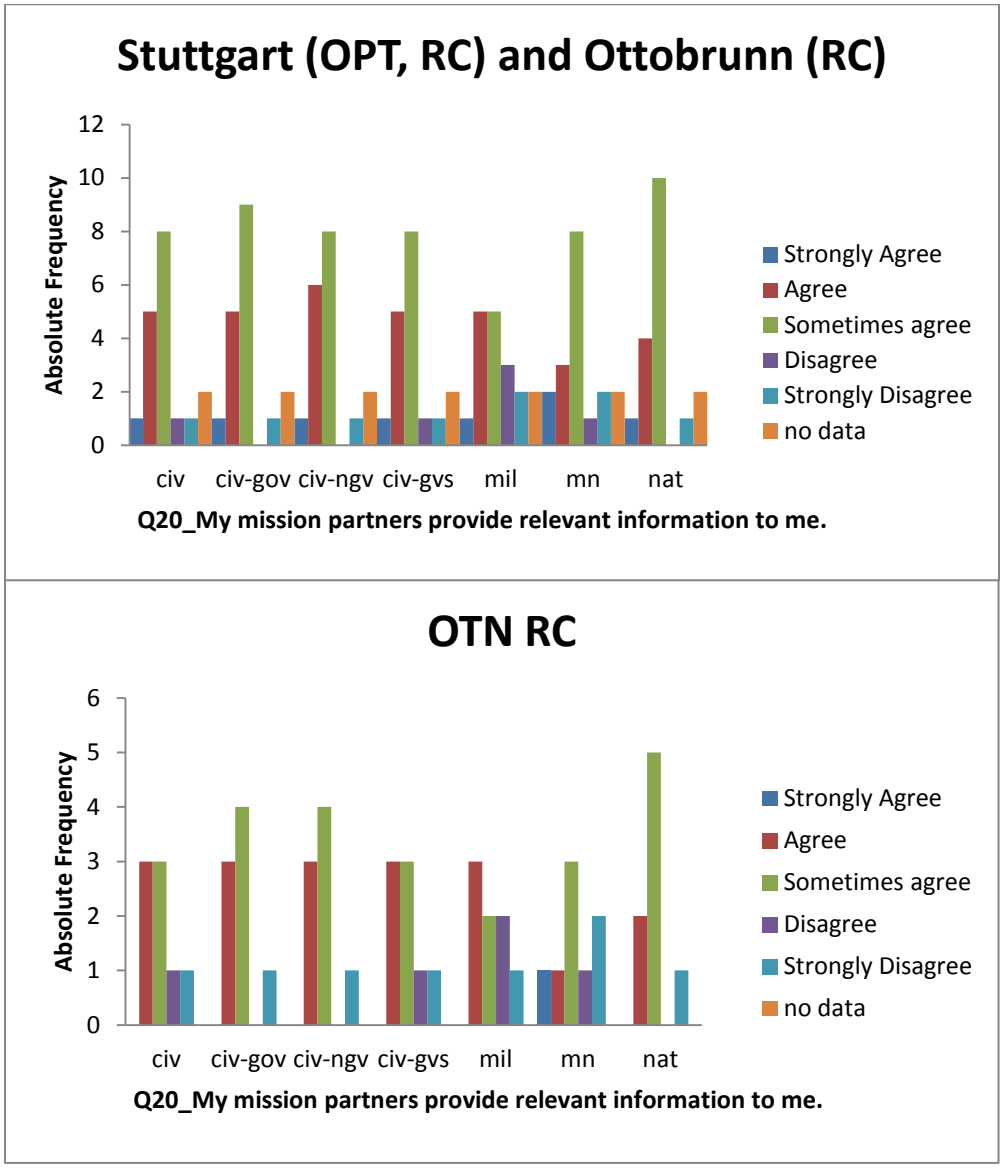

OTN RC
Absolute Frequency
0
1
2
3
4
5
6
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q19_My mission partners provide useful information to me.

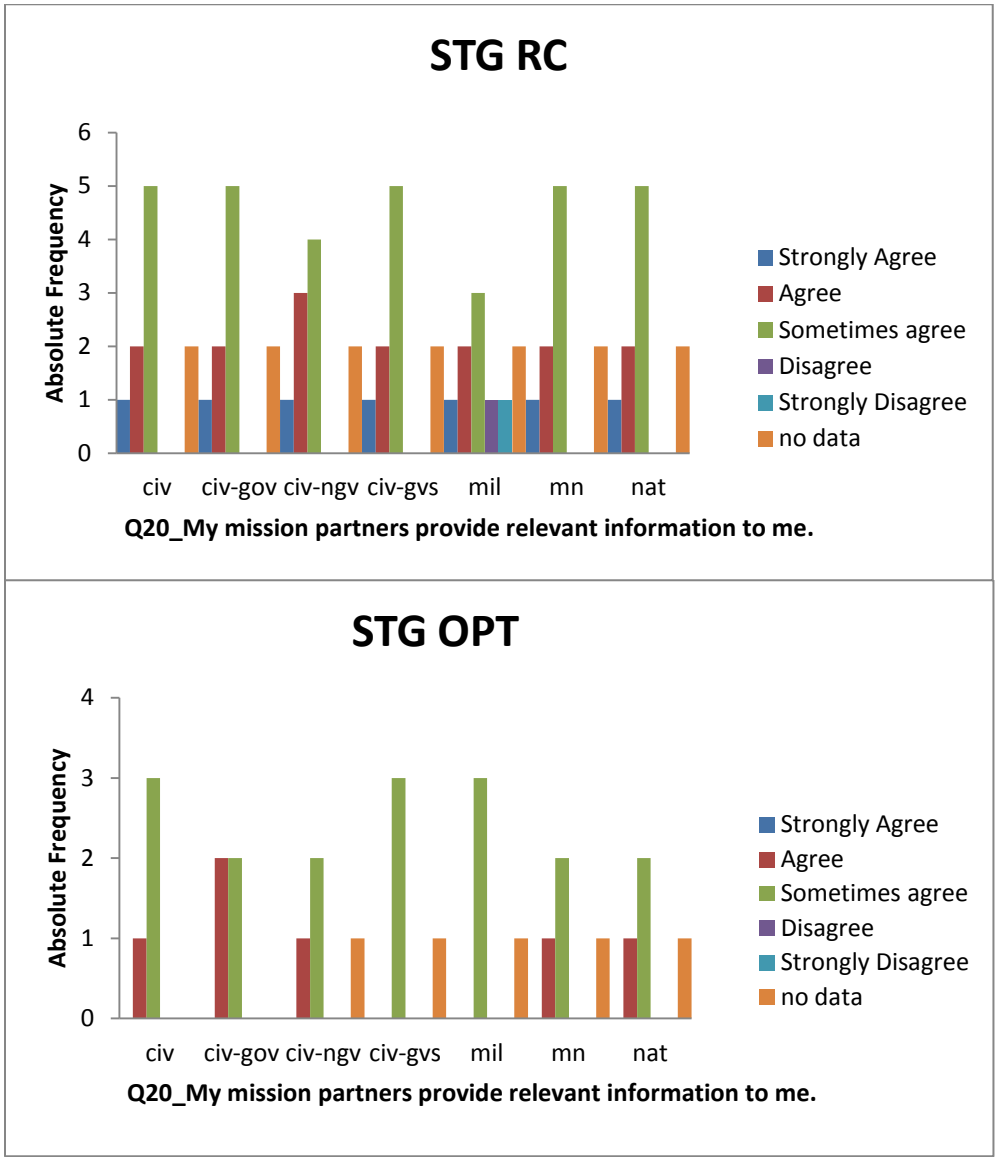

STG RC
Absolute Frequency
0
1
2
3
4
5
6
7
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q19_My mission partners provide useful information to me.



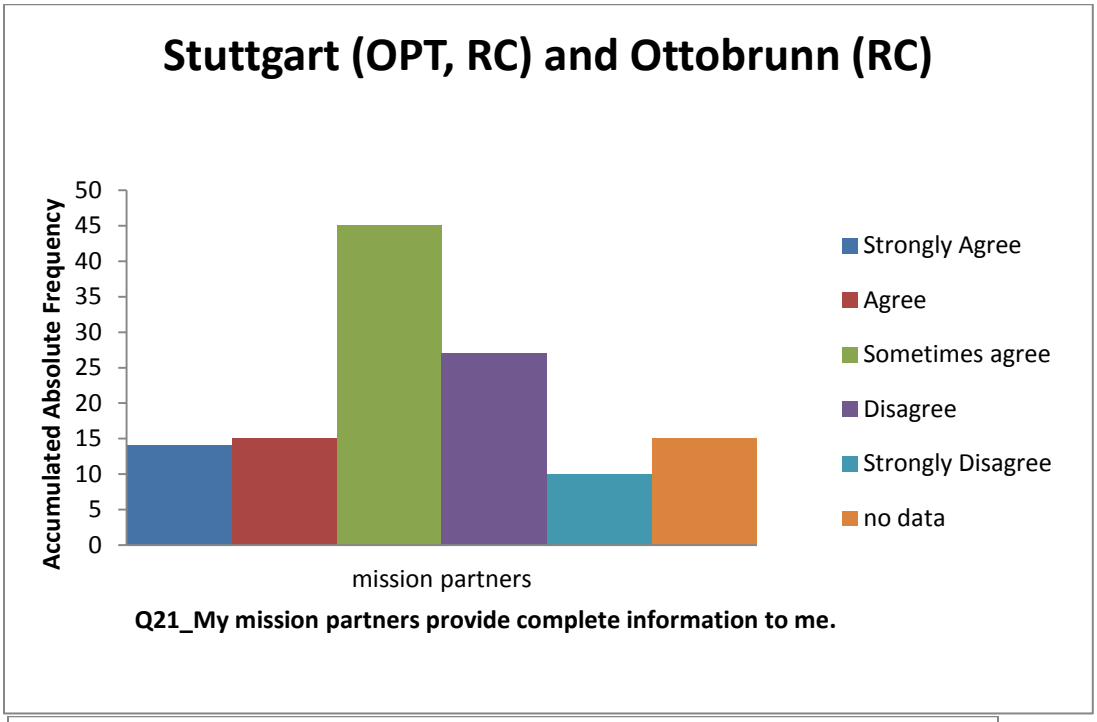
IQ20
"My mission partners provide relevant information to me."

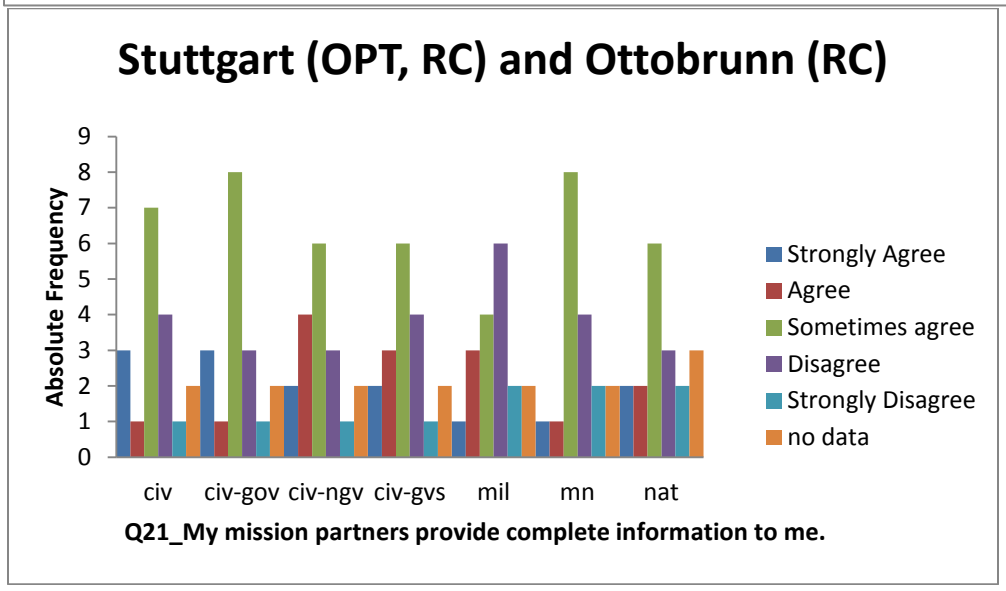


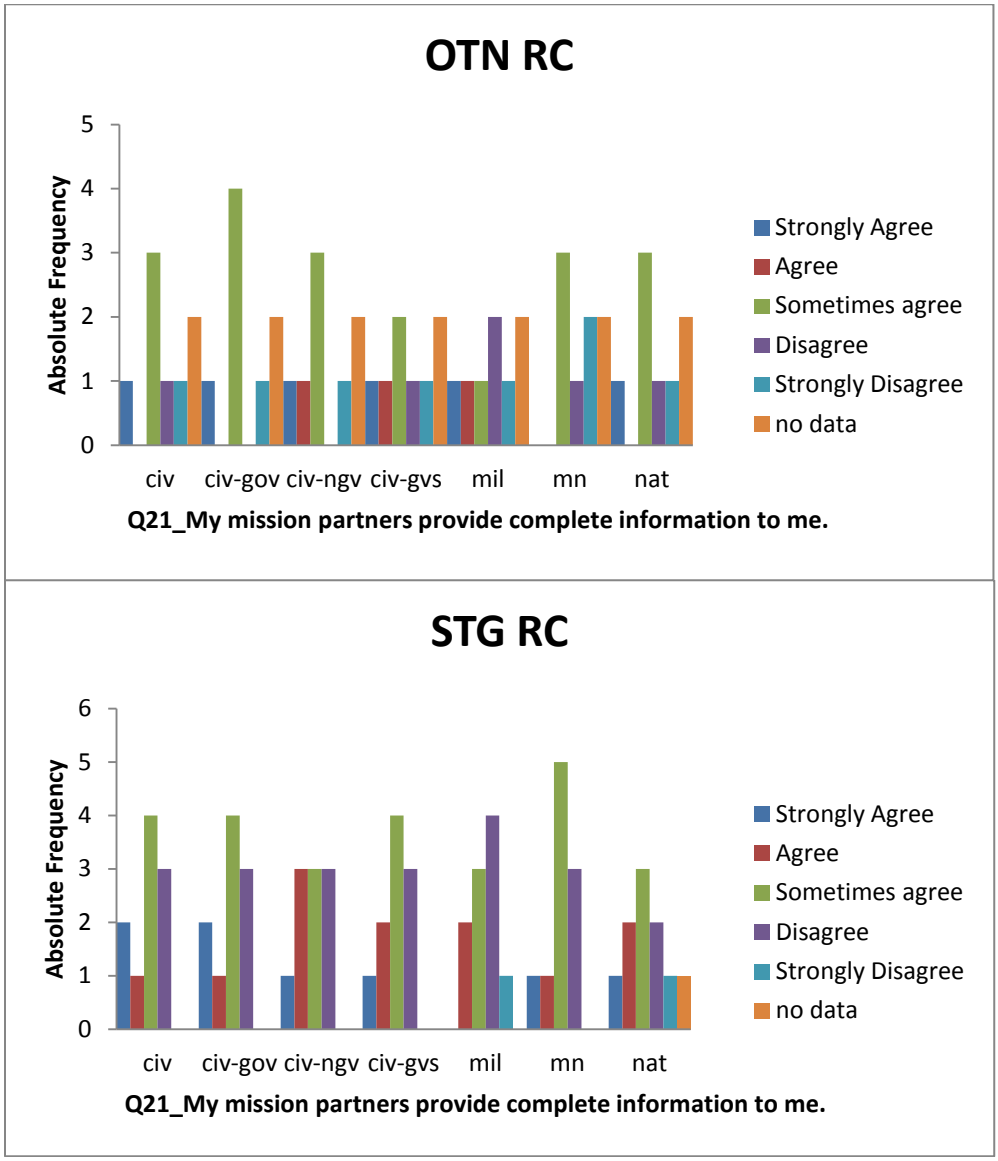

Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
12
10
8
6
4
2
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q20_My mission partners provide relevant information to me.
OTN RC
Absolute Frequency
6
5
4
3
2
1
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q20_My mission partners provide relevant information to me.

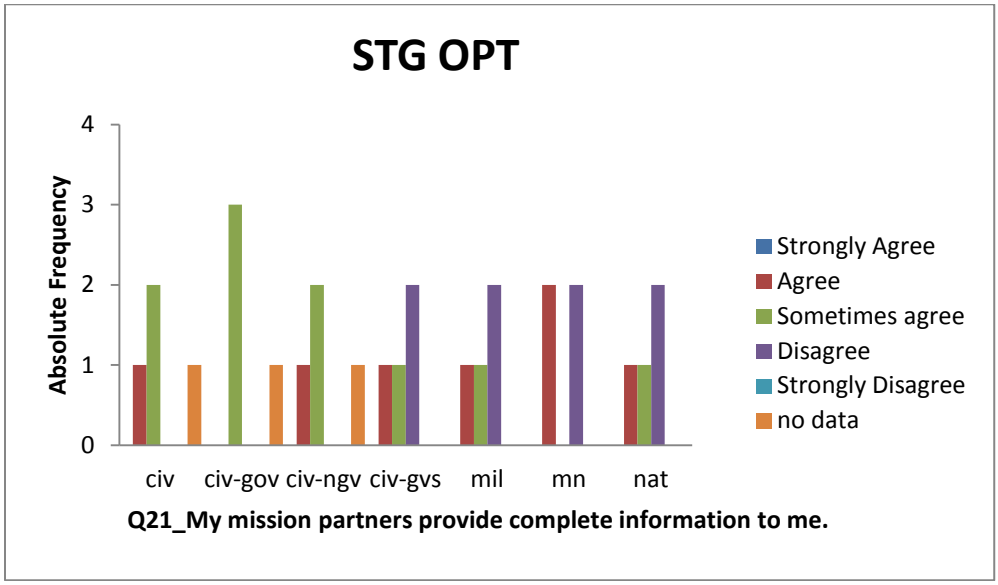


IQ21
"My mission partners provide complete information to me."

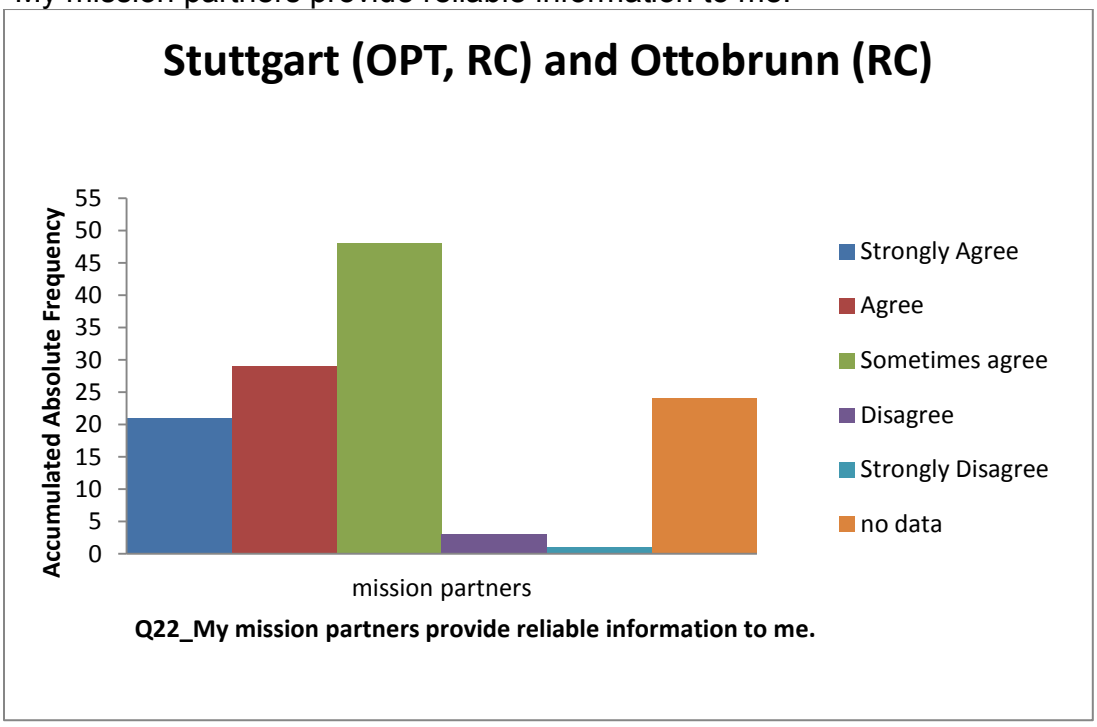

Stuttgart (OPT, RC) and Ottobrunn (RC)
Accumulated Absolute Frequency
50
45
40
35
30
25
20
15
10
5
0
mission partners
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q21_My mission partners provide complete information to me.

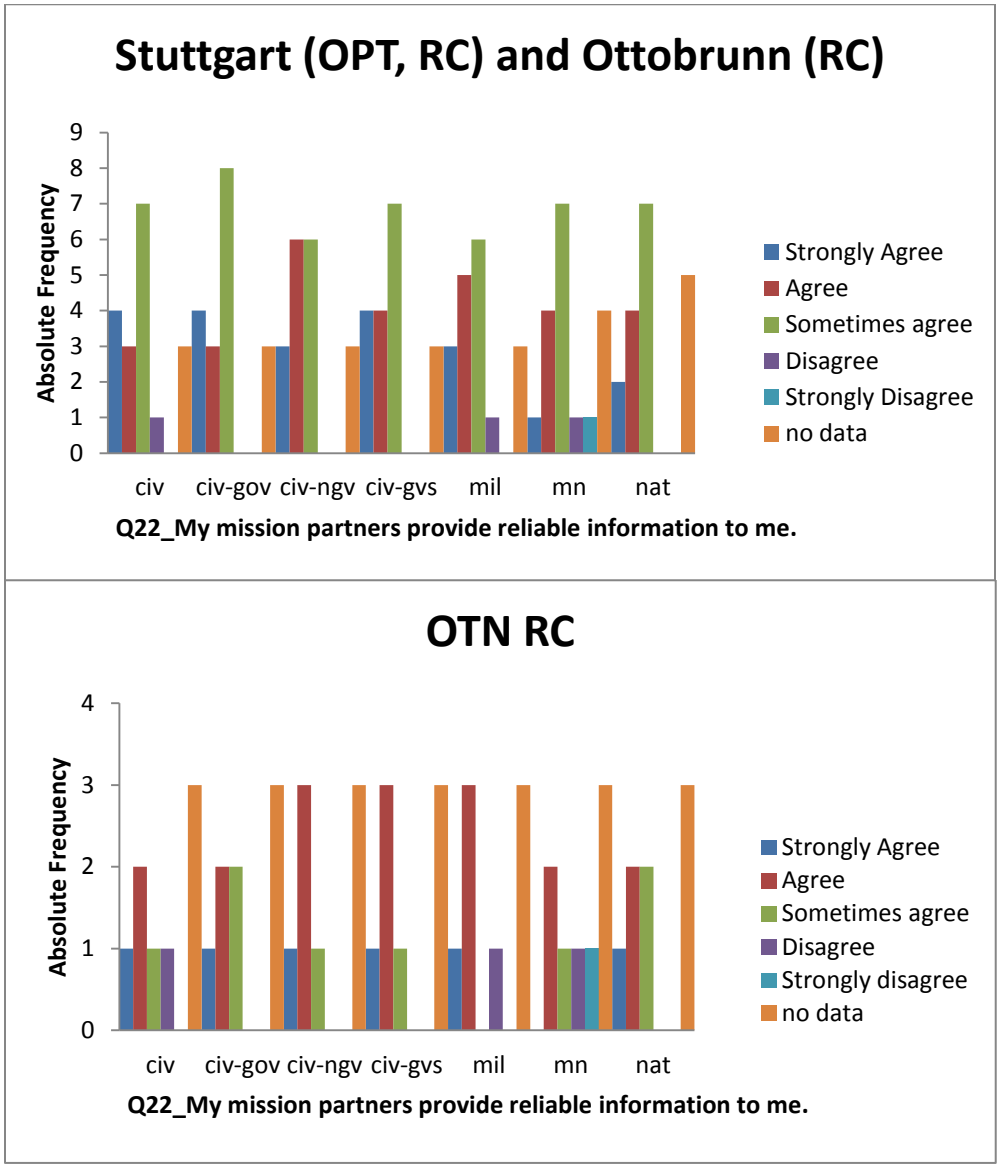

Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
9
8
7
6
5
4
3
2
1
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q21_My mission partners provide complete information to me.

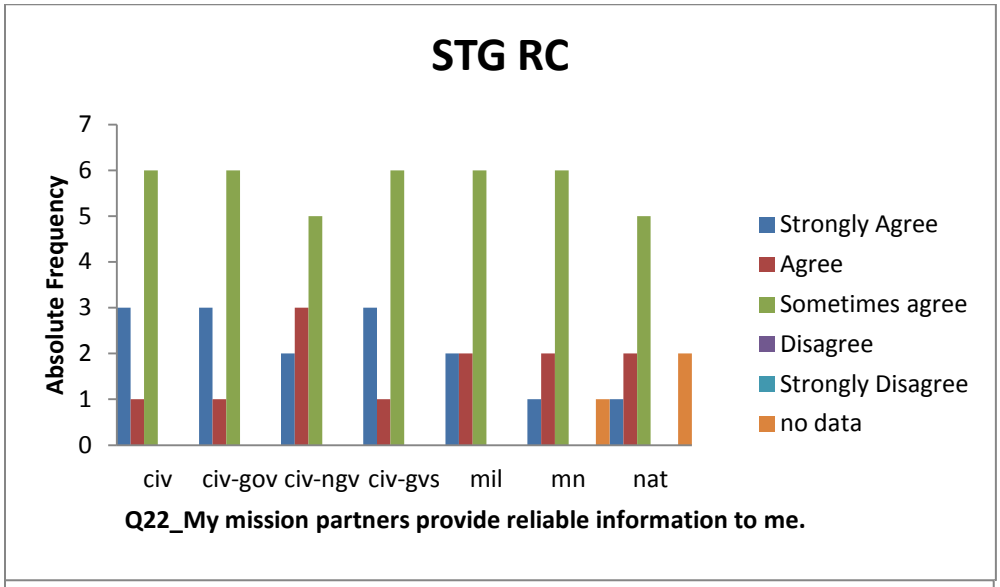

OTN RC
Absolute Frequency
0
1
2
3
4
5
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q21_My mission partners provide complete information to me.
STG RC
Absolute Frequency
0
1
2
3
4
5
6
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q21_My mission partners provide complete information to me.

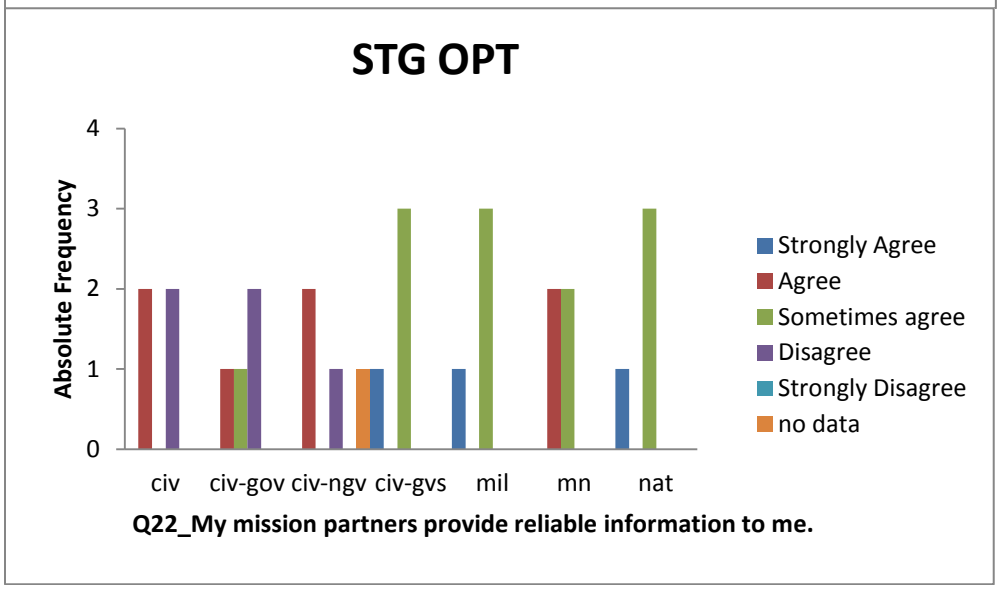


IQ22
"My mission partners provide reliable information to me."

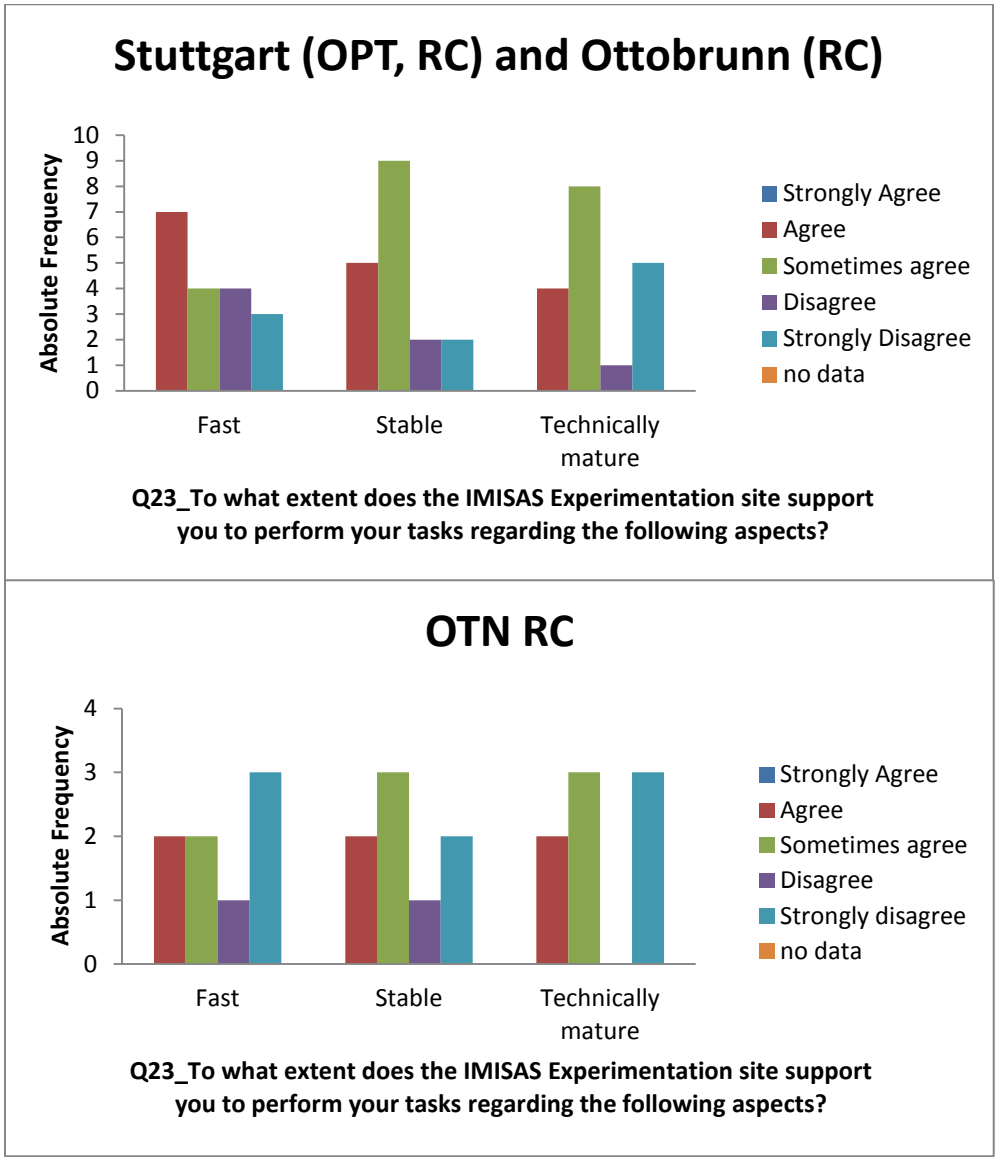


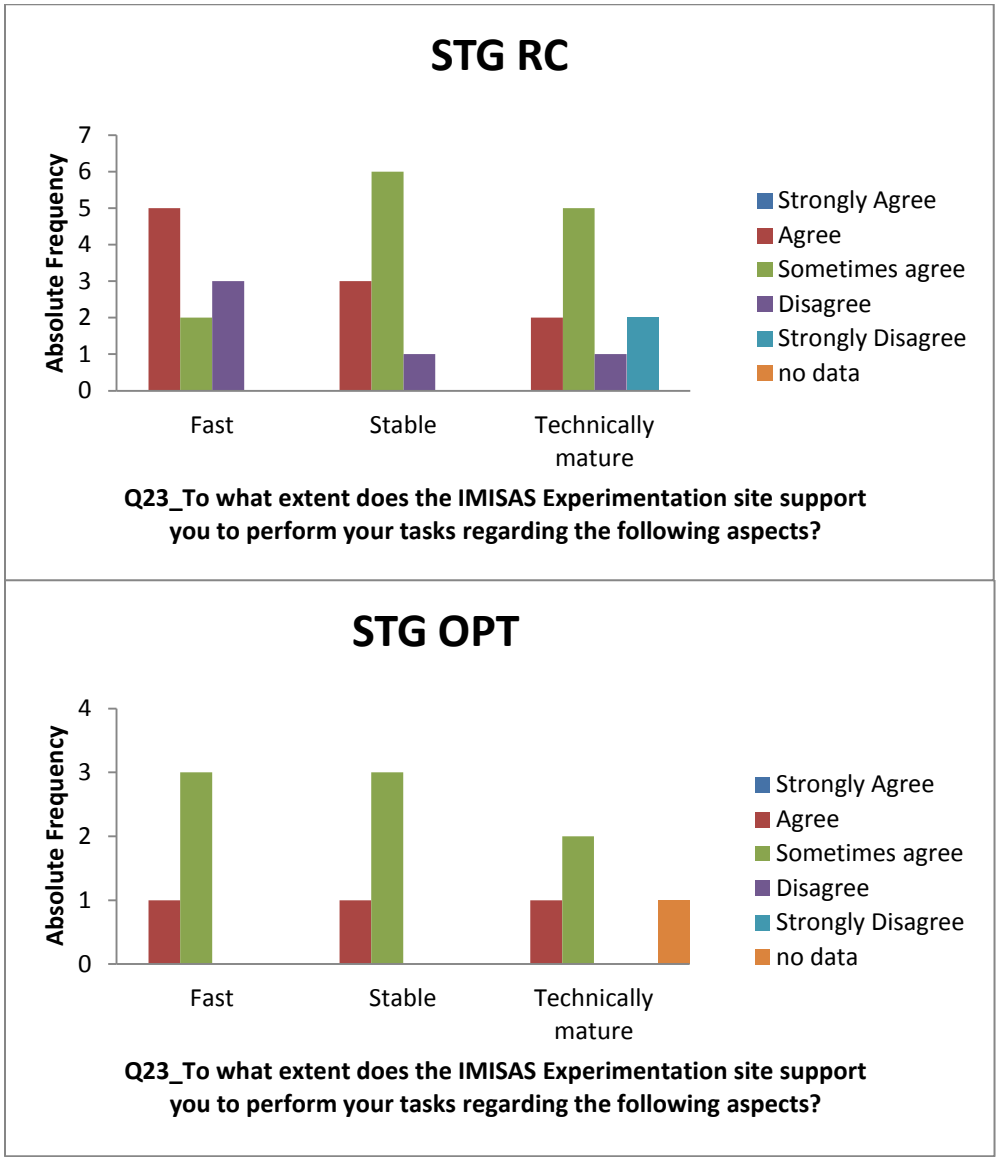

Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
0
1
2
3
4
5
6
7
8
9
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q22_My mission partners provide reliable information to me.
OTN RC
Absolute Frequency
0
1
2
3
4
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly disagree
no data
Q22_My mission partners provide reliable information to me.



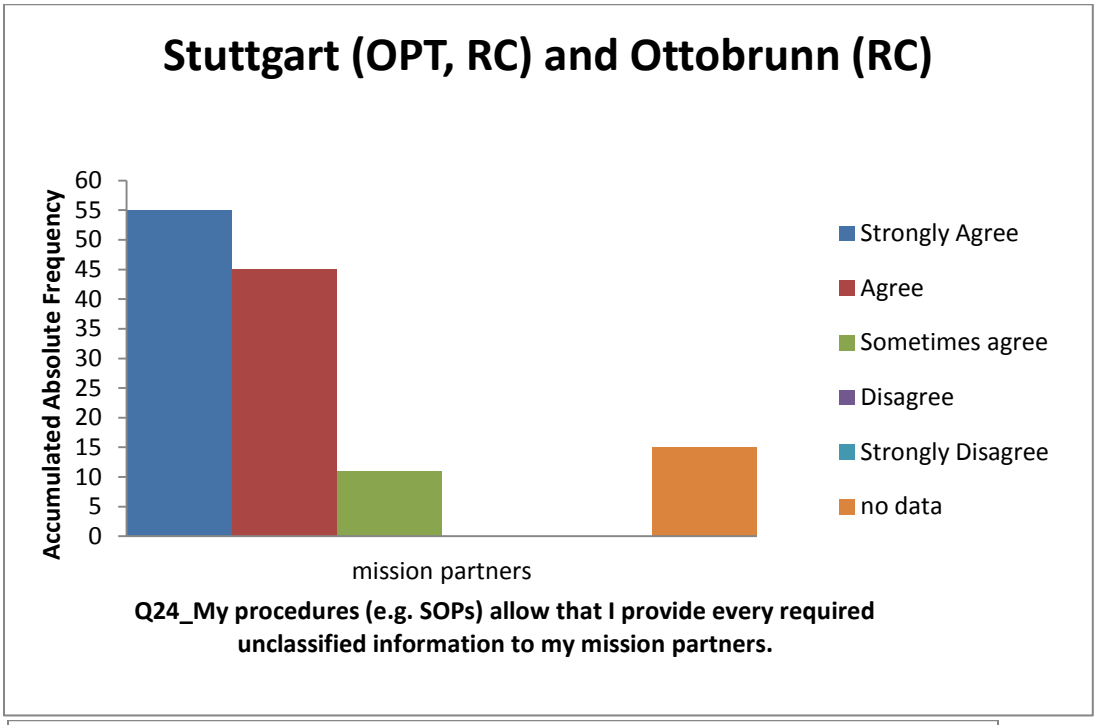


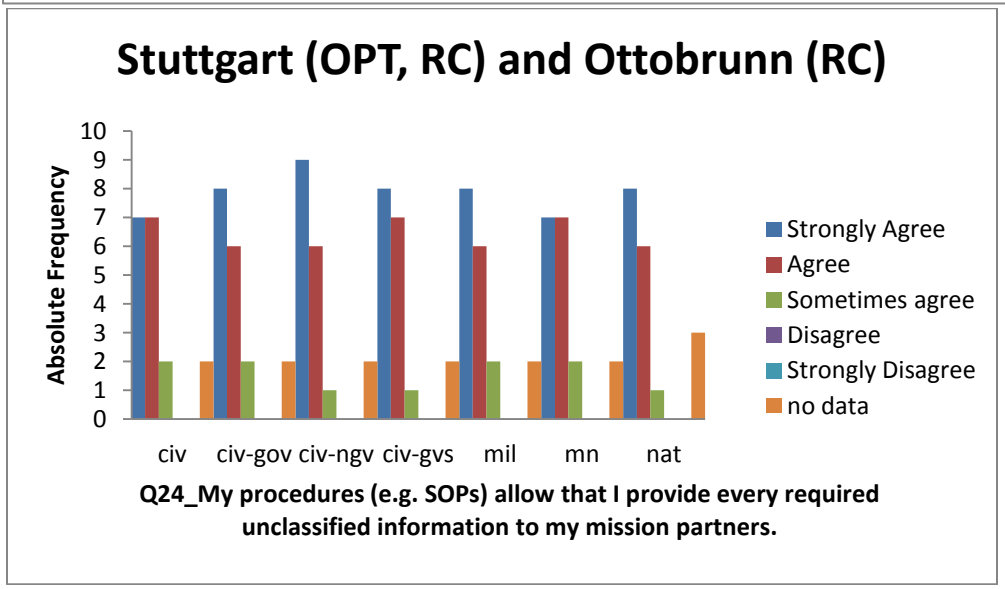
IQ23
"To what extent does the IMISAS Experimentation site support you to perform your tasks regarding the following aspects?"

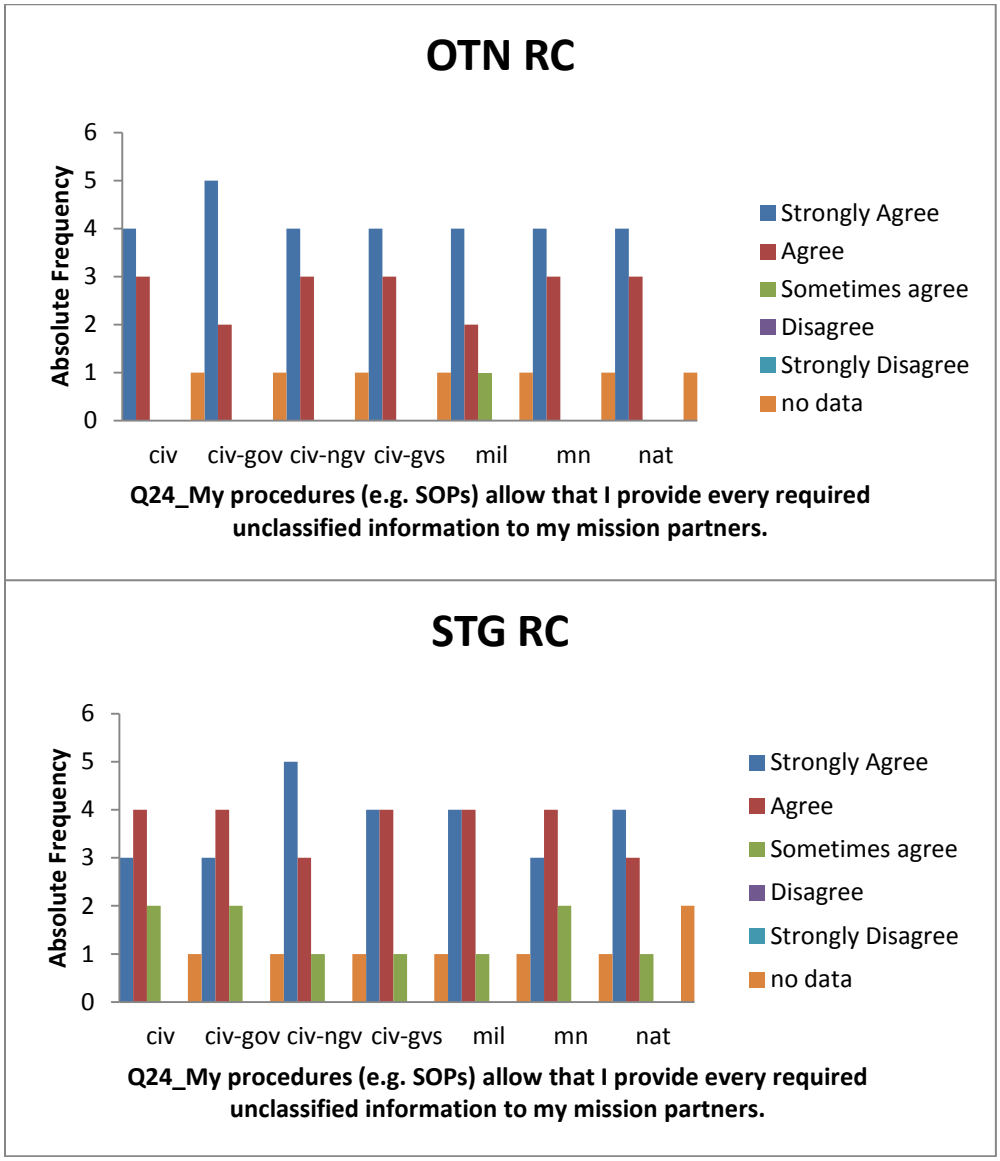

Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
10
9
8
7
6
5
4
3
2
1
0
Fast
Stable
Technically mature
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q23_To what extent does the IMISAS Experimentation site support you to perform your tasks regarding the following aspects?
OTN RC
Absolute Frequency
4
3
2
1
0
Fast
Stable
Technically mature
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly disagree
no data
Q23_To what extent does the IMISAS Experimentation site support you to perform your tasks regarding the following aspects?

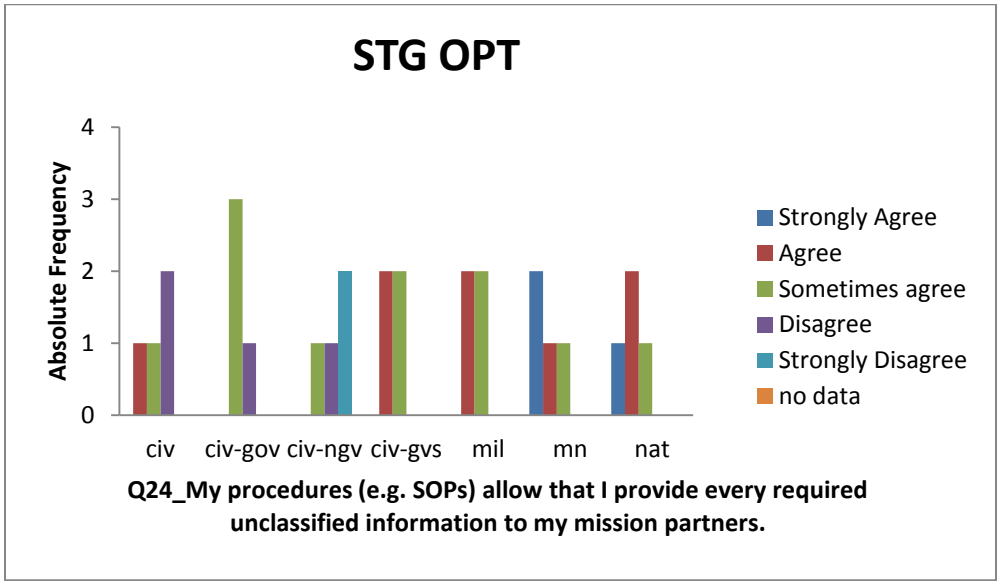


IQ24
"My procedures (e.g., SOPs) allow that I provide every required unclassified information to my mission partners."


Stuttgart (OPT, RC) and Ottobrunn (RC)
Accumulated Absolute Frequency
60
55
50
45
40
35
30
25
20
15
10
5
0
mission partners
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q24_My procedures (e.g. SOPs) allow that I provide every required unclassified information to my mission partners.


Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
10
9
8
7
6
5
4
3
2
1
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q24_My procedures (e.g. SOPs) allow that I provide every required unclassified information to my mission partners.


OTN RC
Absolute Frequency
6
5
4
3
2
1
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q24_My procedures (e.g. SOPs) allow that I provide every required unclassified information to my mission partners.
STG RC
Absolute Frequency
6
5
4
3
2
1
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q24_My procedures (e.g. SOPs) allow that I provide every required unclassified information to my mission partners.



IQ24.8

„Please comment“

OPT Stuttgart

Regardless of whom the partner is - certain aspects of CUI cannot be shared without a specific need to know.
(?) The process is still unclear and not (???) from COCOM to COCOM
Not sure what you mean by required

RC Stuttgart

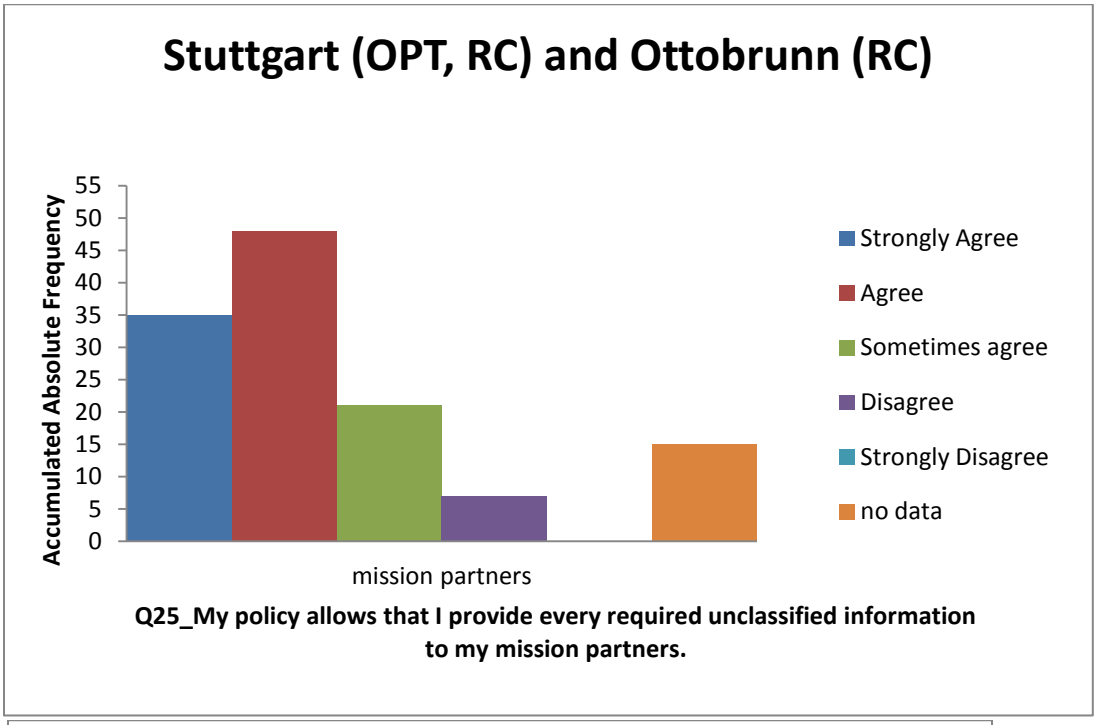
See response below question 25
This question is not clear to me (required information)
no unclassified info within my NGO

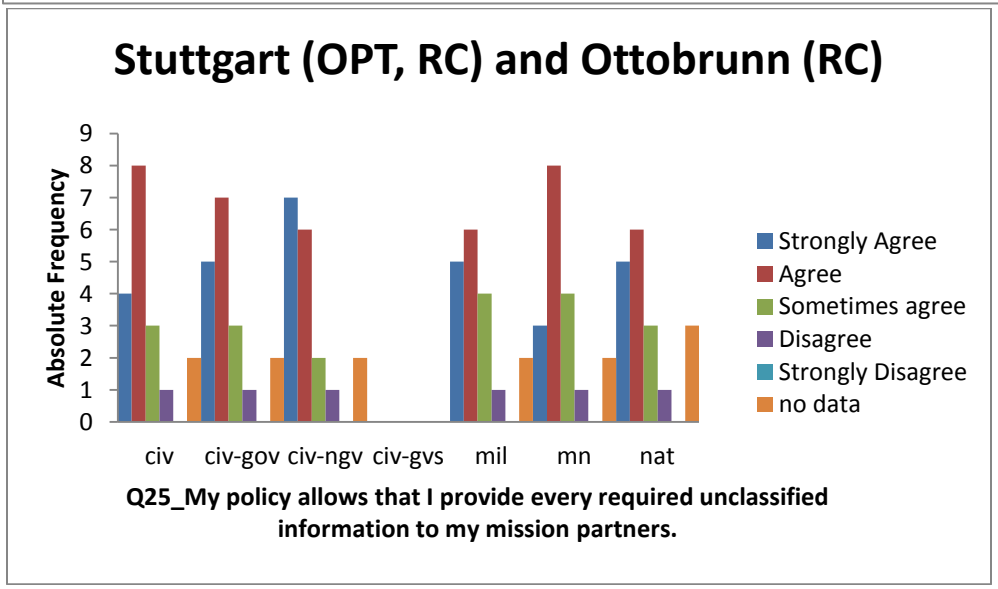
RC Ottobrunn

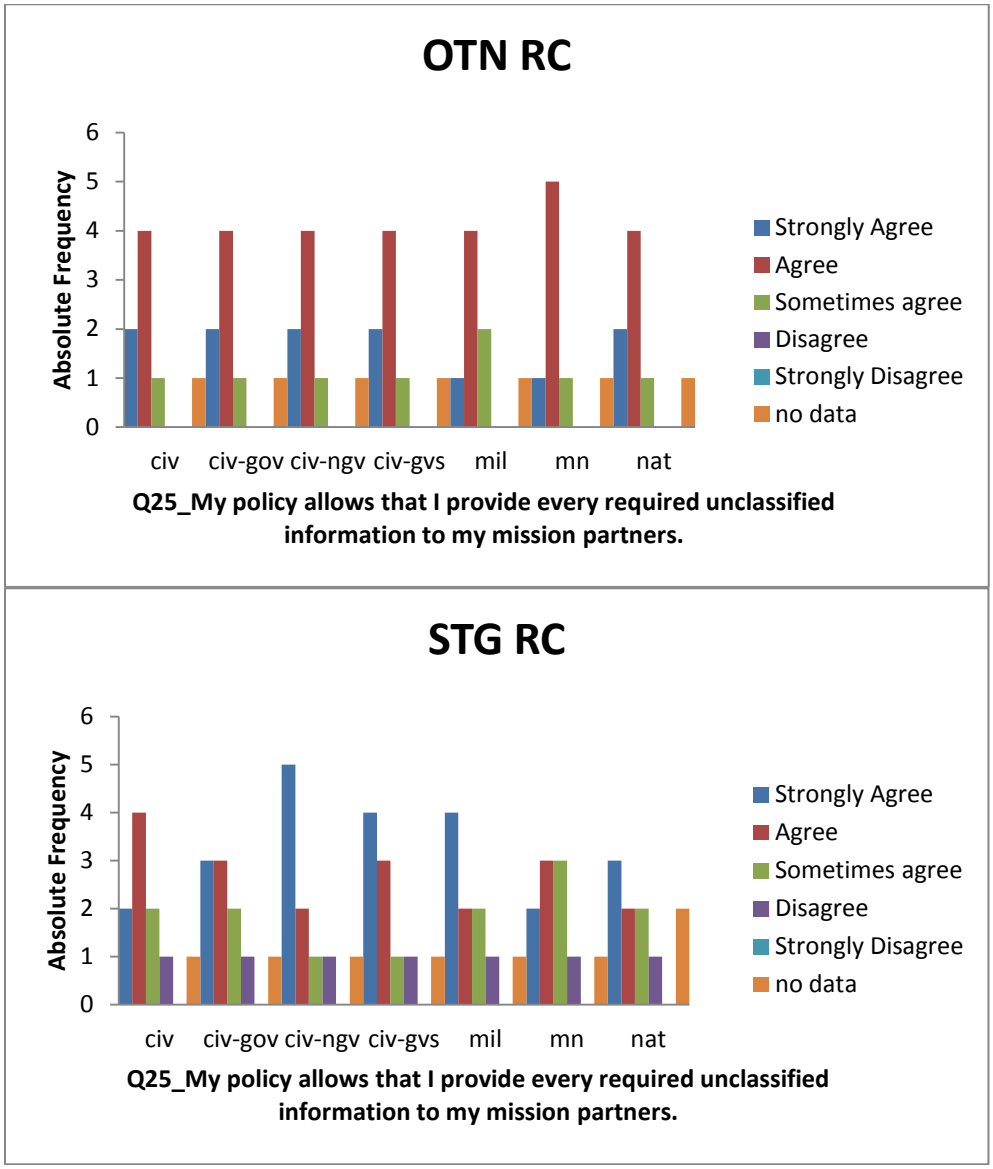
I don't know.
Die Frage stellt sich nicht da generell keine eingestuften Informationen vorlagen.
To be honest, NGOs don't have classification on their infos, they decide case by case.
Working CIMIC is working open source!

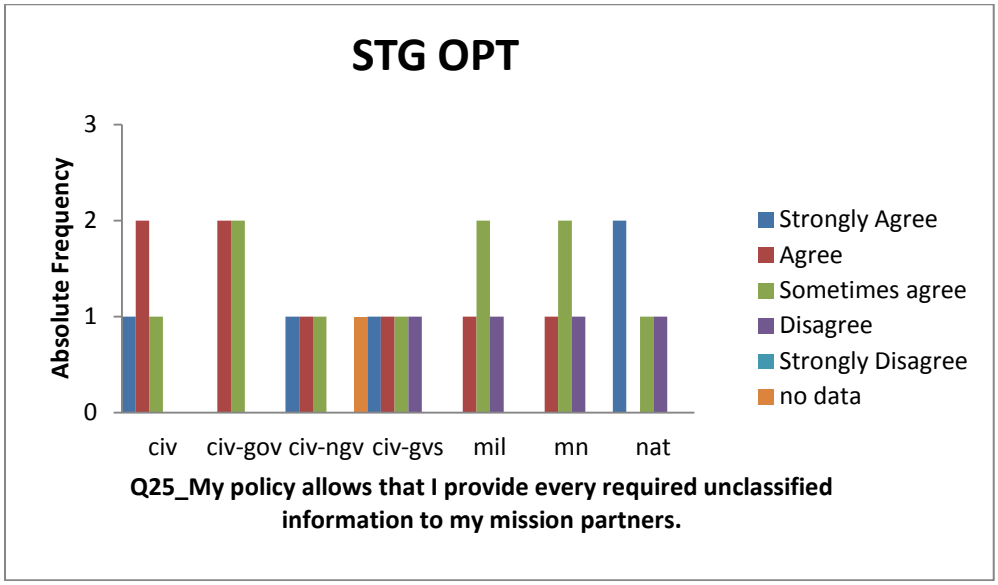
IQ25

“My policy allows that I provide every required unclassified information to my mission partners.”


Stuttgart (OPT, RC) and Ottobrunn (RC)
Accumulated Absolute Frequency
55
50
45
40
35
30
25
20
15
10
5
0
mission partners
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q25_My policy allows that I provide every required unclassified information to my mission partners.


Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
9
8
7
6
5
4
3
2
1
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q25_My policy allows that I provide every required unclassified information to my mission partners.


OTN RC
Absolute Frequency
0
1
2
3
4
5
6
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q25_My policy allows that I provide every required unclassified information to my mission partners.
STG RC
Absolute Frequency
0
1
2
3
4
5
6
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q25_My policy allows that I provide every required unclassified information to my mission partners.



IQ25.8

„Please comment“

OPT Stuttgart

Please refer to comment above
There is no requirement for this at EUCOM

RC Stuttgart

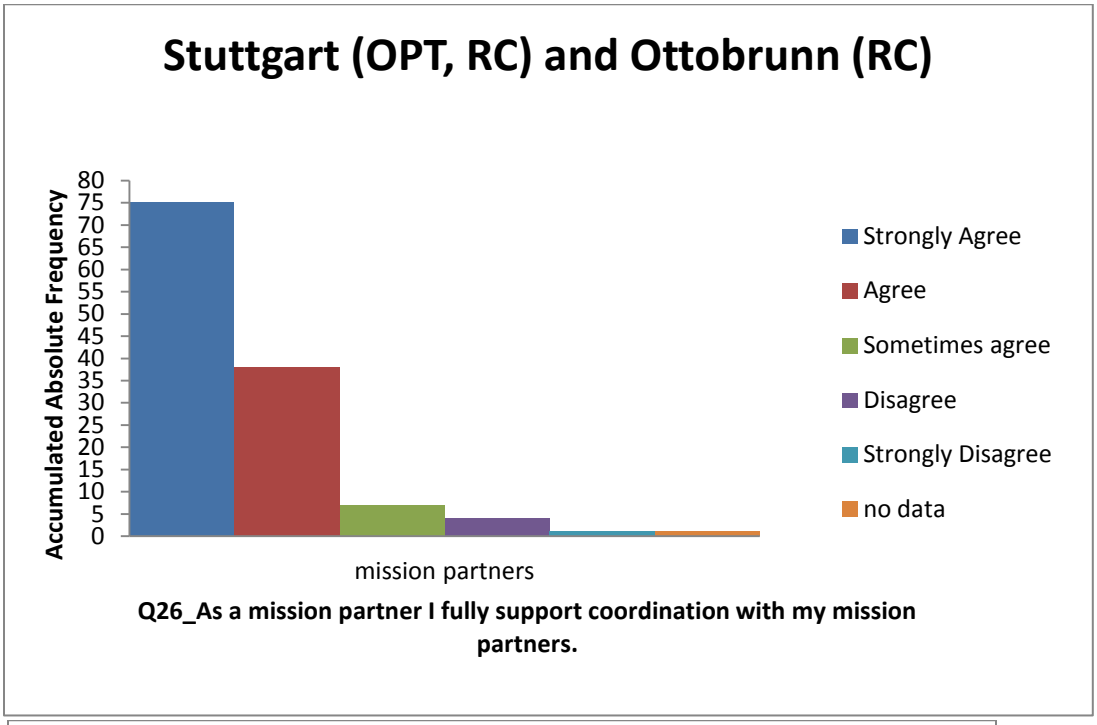
Some sensitive info is not released if they can damage the organization. This would be reviewed by PAO / POLAD prior to release.
same above

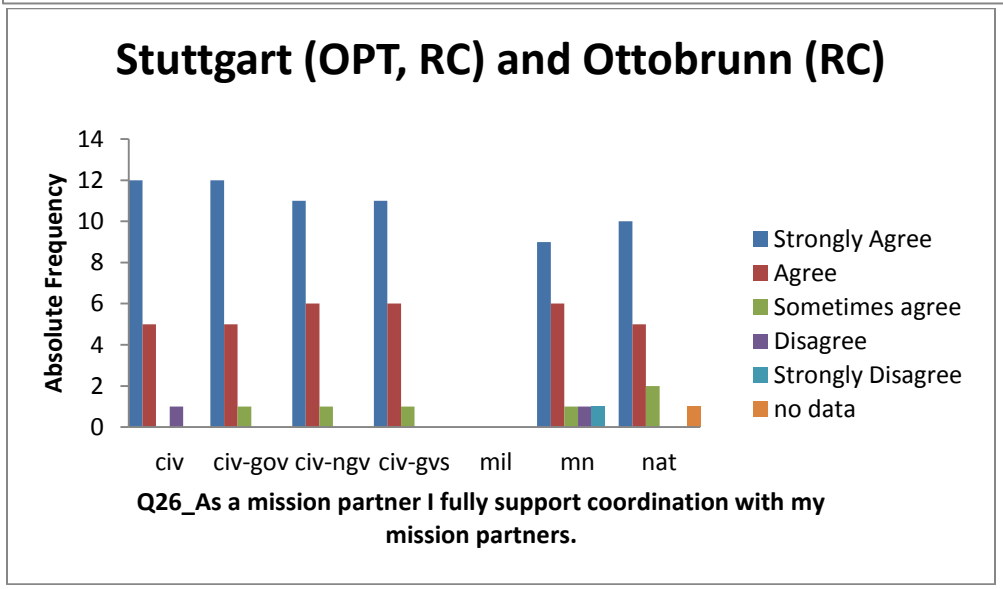
RC Ottobrunn

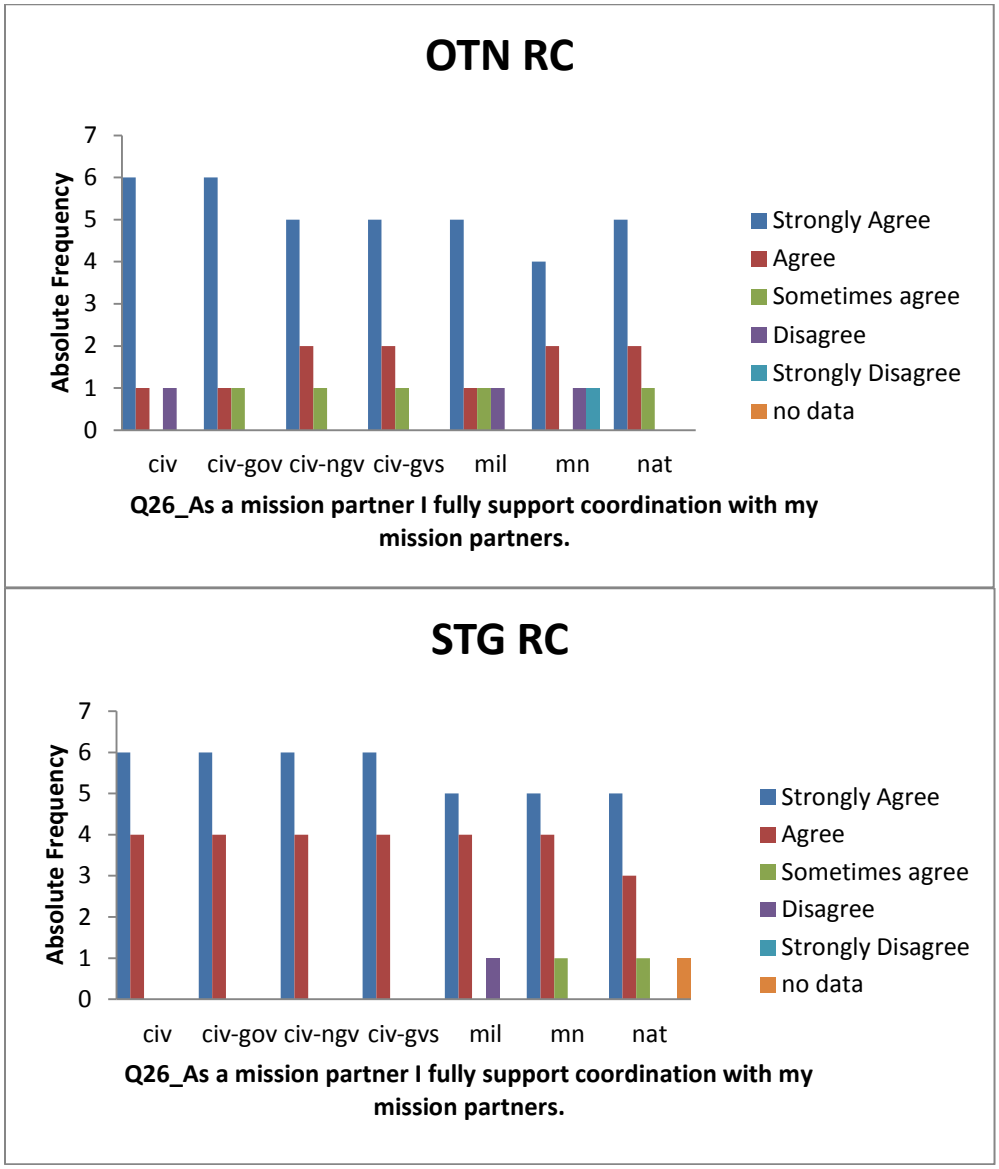
I don't know.
Depends on quality of information.
Die Frage stellt sich nicht da generell keine eingestuften Informationen vorlagen.
see 24

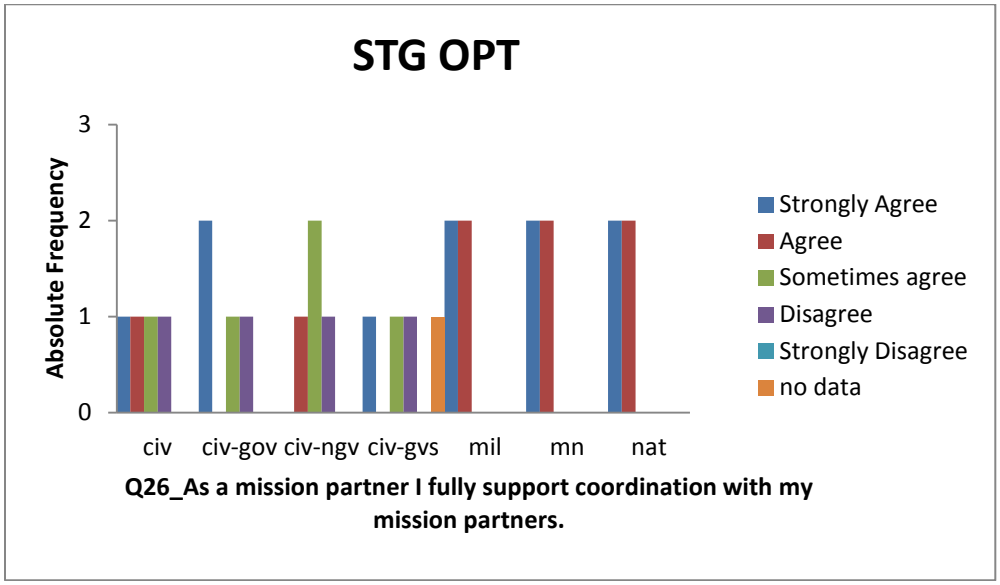
IQ26

“As a mission partner I fully support coordination with my mission partners.”

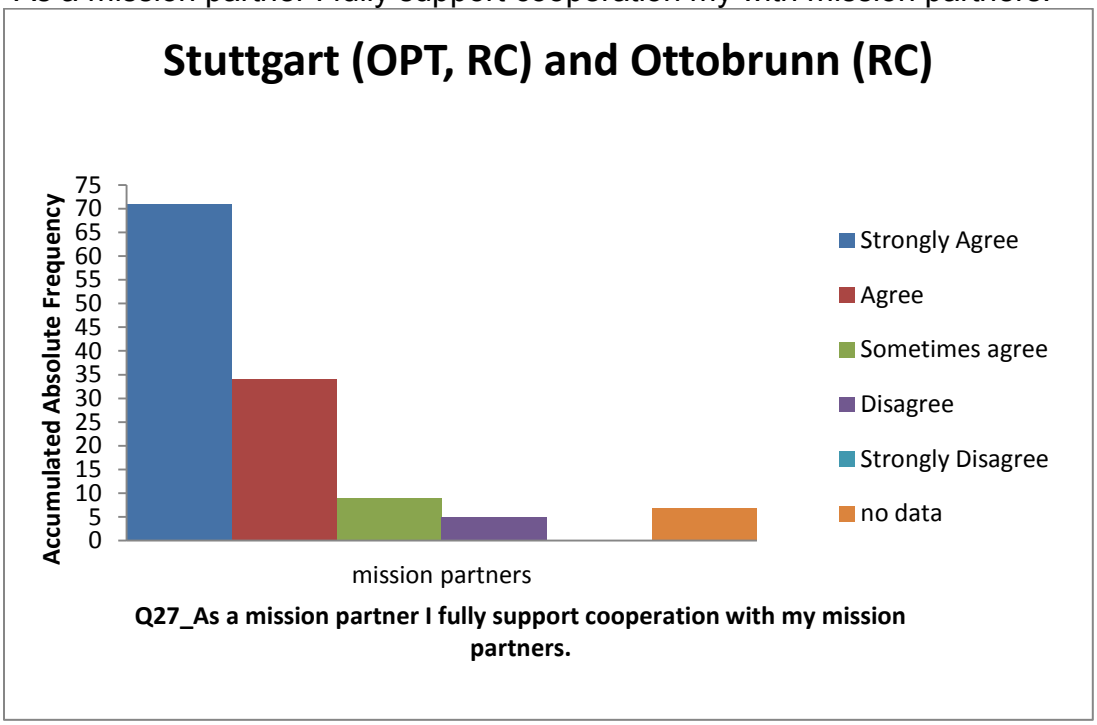

Stuttgart (OPT, RC) and Ottobrunn (RC)
Accumulated Absolute Frequency
80
75
70
65
60
55
50
45
40
35
30
25
20
15
10
5
0
mission partners
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q26_As a mission partner I fully support coordination with my mission partners.

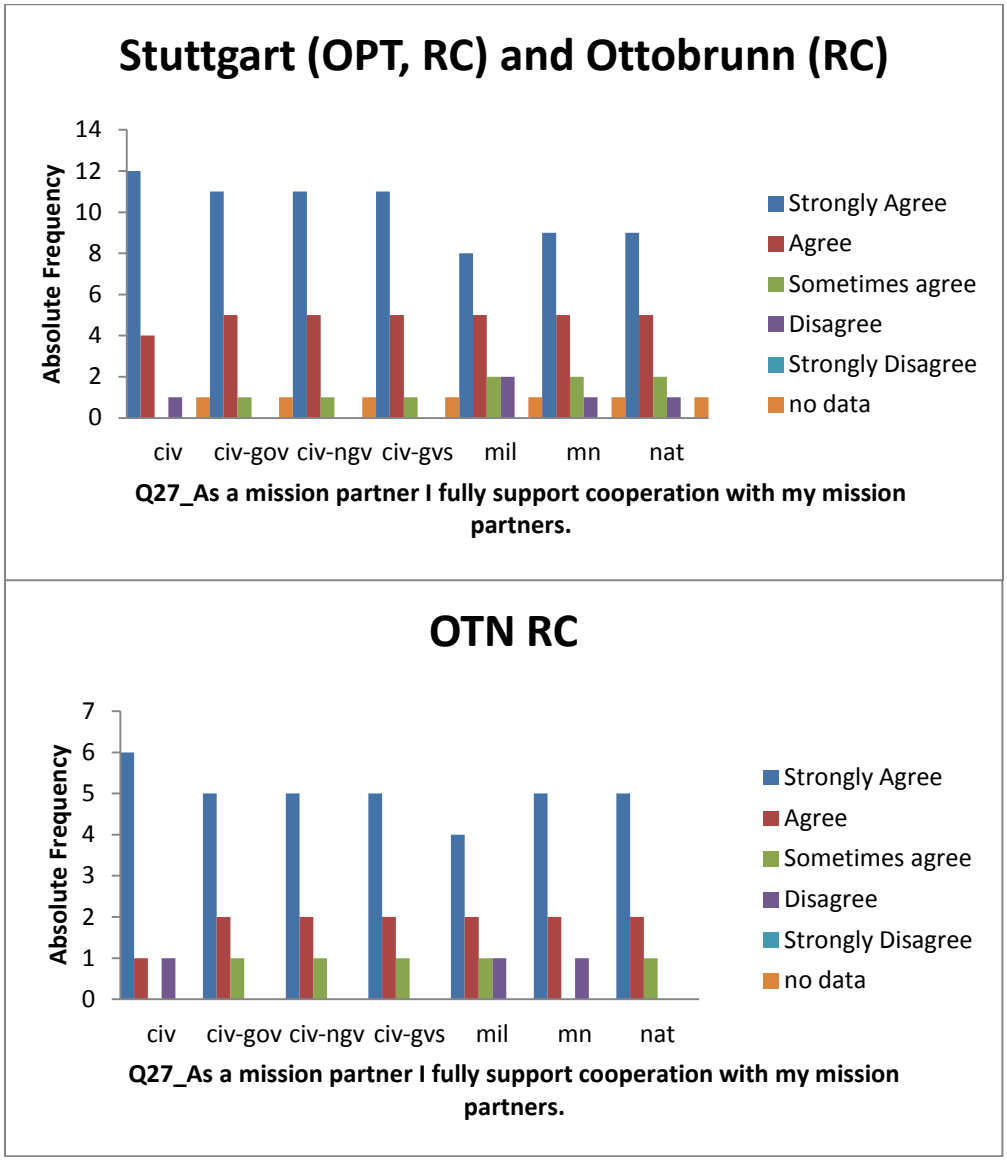

Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
14
12
10
8
6
4
2
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q26_As a mission partner I fully support coordination with my mission partners.

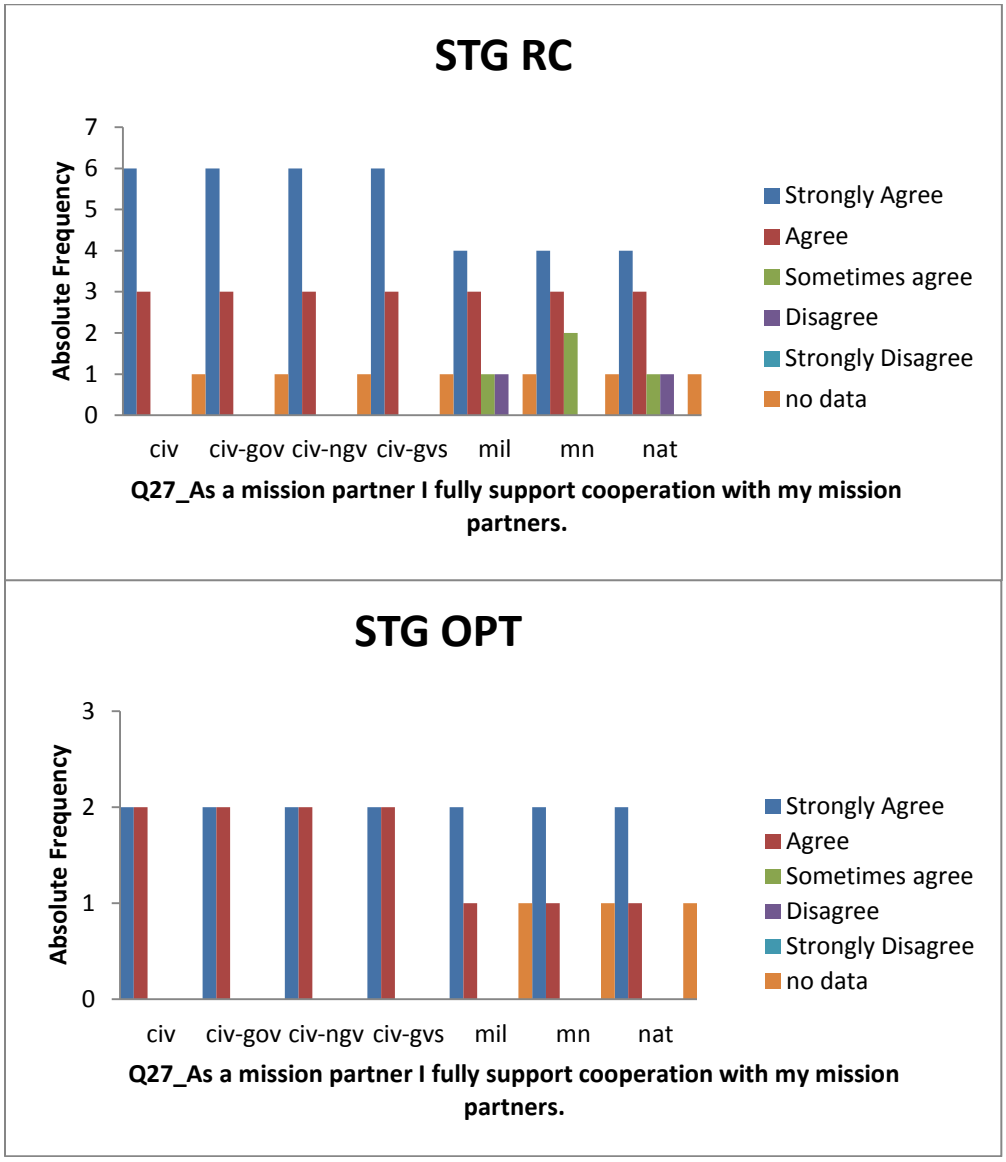

OTN RC
Absolute Frequency
0
1
2
3
4
5
6
7
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q26_As a mission partner I fully support coordination with my mission partners.
STG RC
Absolute Frequency
0
1
2
3
4
5
6
7
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q26_As a mission partner I fully support coordination with my mission partners.



IQ27
"As a mission partner I fully support cooperation my with mission partners."




Stuttgart (OPT, RC) and Ottobrunn (RC)
Absolute Frequency
14
12
10
8
6
4
2
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q27_As a mission partner I fully support cooperation with my mission partners.
OTN RC
Absolute Frequency
7
6
5
4
3
2
1
0
civ
civ-gov
civ-ngv
civ-gvs
mil
mn
nat
Strongly Agree
Agree
Sometimes agree
Disagree
Strongly Disagree
no data
Q27_As a mission partner I fully support cooperation with my mission partners.



IQ28
„If you were your mission partner, what would you propose in order to change your own way of information sharing in order to achieve mission objectives?“
OPT Stuttgart

There is limited applicability on information sharing in public affairs. I think we share info in our lane appropriately.
Improve communication(s) infrastructure that can handle large bandwidths to facilitae sharing speed.
(?) They must realize the military is only there to help as they are and we are prone to make the same mistakes they are
(?) more training on military procedures for conops; work with military individuals who shared some of my concerns and use them as entry ways for my info;

longterm (???) of set up accepted procedures for … info into this military process; a military mentor to help me perhaps

RC Stuttgart

Develop stronger personal and organisational relationships.
k.A.
(?) Exchanging information instead of only "asking" of them; gaining a better understanding of (???) corporate (???) and how to negotiate with them.
k.A.
A more pro-active approach needed; more info-sharing instead of obtaining info from other actors
I would do more training to understand military roles and procedures

RC Ottobrunn

Get more work to do!
If I were the training audience I would answer the requests / I would try to get in contact with other forces / players in theatre.
Immer eine Meldung weitergegeben, dass Anfrage bearbeitet wird und öfter den Gruppenchat nutzen (schnellere Übergabe / Transfer von Informationen).
Nothing.
For the time being, there is no two-way info flow yet.
Force everyone to have a facebook and twitter account.
At that period of time: Nothing

Annex G.1.3: UIS Handbook Questions (HBQ)

Missing data.

Annex G.2: Shared Situational Awareness

Data directly located in section 5.3 above.

Annex H: Discussion of High-Level, Experimental Hypotheses

High-Level, Experimental Hypothesis 1

Hypothesis 1: "If the unclassified information sharing capability (UISC) combines knowledge management methodologies with a minimum-demand user interface and carefully designed software composition including social media interfaces, then accessibility, completeness, responsiveness, and timeliness of information will increase, with attendant increases in relevance to the activity of responders and their situational understanding." [IMISAS ED 2011]

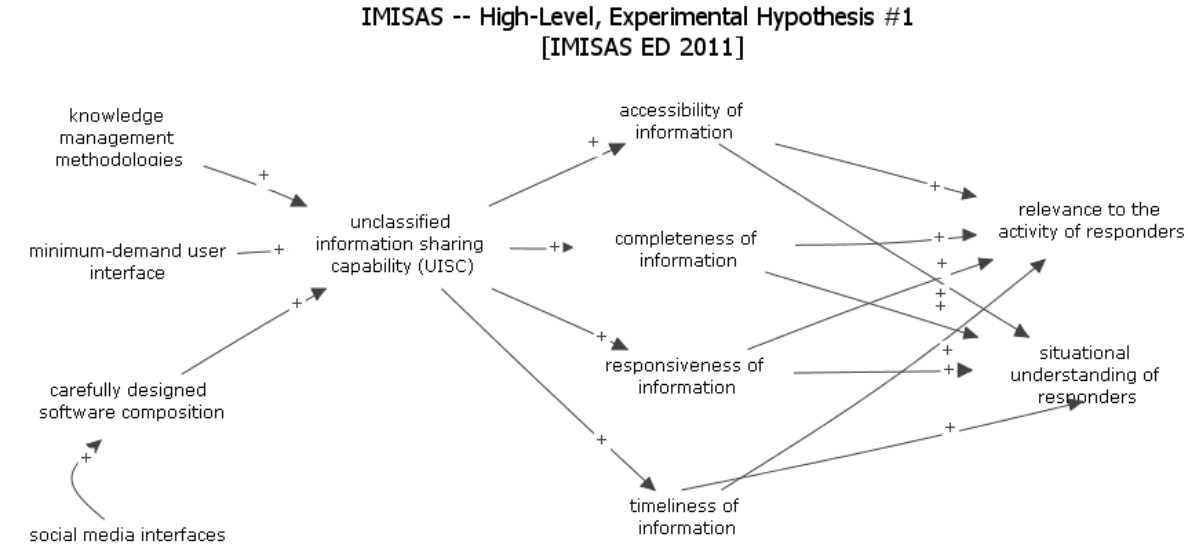


Figure 29: Influence Diagram H1

Interpretation: It is assumed that by (a) provision of KM methodologies, ergonomic prepositions ("minimum demand user interface") in connection with social media (b) the level of unclassified information sharing capability (UISC) will be increased. An increased (b) level of UISC causes (c) an increased level of accessibility, completeness, responsiveness, and timeliness of information. An increased (c) causes (d) increased relevance to the activity and increased situational understanding of responders. The combination of causal statements "if (a) then (b)", "if (b) then (c)", "if (c) then (d)" may suggest derived transitive statements like "if (b) then (d)". On the other hand, "if (b) then (d)" has not to be true in every situation, since (a), (b), (c), and (d) could be dependent of other factors, like motivation and other cognitive capabilities of users. Therefore, each causal statement has to be validated separately. Also, each constituent in such a complex statement has to be terminologically clarified.

High-Level, Experimental Hypothesis 2

Hypothesis 2: "If COCOMs foster coordination with, outreach to, and holistic comprehension of the span of humanitarian assistance and disaster relief (HA / DR) responders, then the coherence, agility, responsiveness, robustness, and speed of combined HA / DR response will increase." [IMISAS ED 2011]

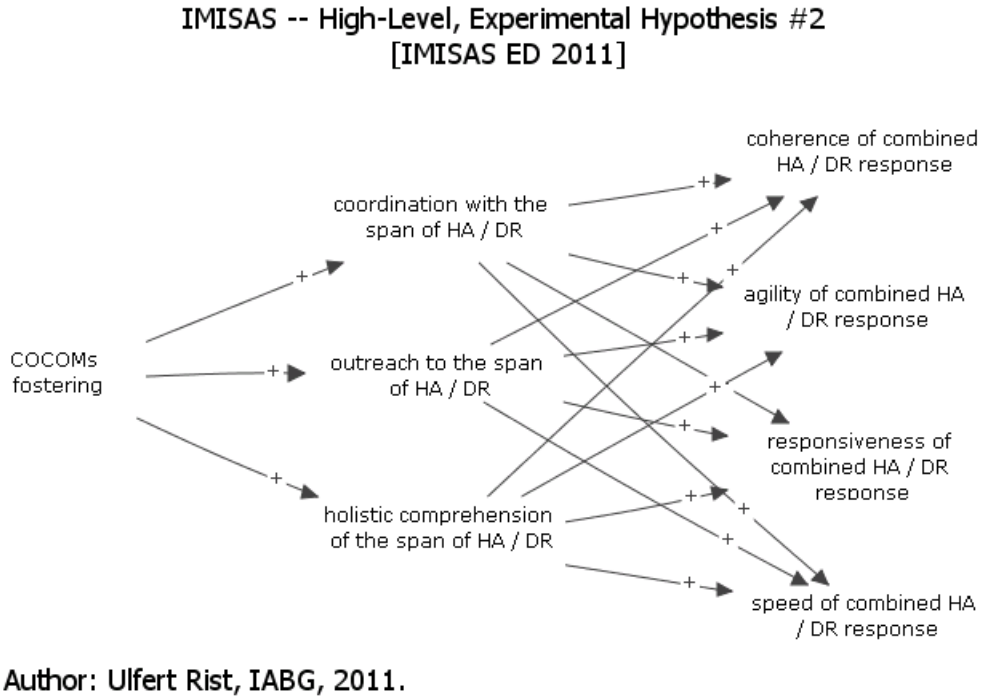


Figure 30: Influence Diagram H2

Interpretation: If (a) combatant command fosters coordination, outreach to, and holistic comprehension of the span of HA / DR, then (b) coherence, agility, responsiveness, and speed of combined HA / DR response will be increased. It appears to be not necessarily the case that (a) has causal influence on (b). This has to be proofed in a single case, e.g., "*If COCOMs foster coordination with the span of humanitarian assistance and disaster relief (HA / DR) responders, then the coherence of combined HA / DR response will increase."*

From a terminological viewpoint, clarification is needed, e.g., the term coordination in the context of civilian and military mission partners. Similar to H1 above, several factors are interrelated to other factors in a complex format. A complex statement like H2 is hard to validate without decomposition of its parts/constituents.

High-Level, Experimental Hypothesis 3

Hypothesis 3: "If a risk-managed approach to information sharing is adopted, to include information release policy, mechanisms for identity establishment and source vetting, and methods for assuring confidentiality and anonymity, then within acceptable limits of information accuracy and security, improvements will

be garnered in information accessibility and the agility, flexibility, responsiveness, speed, and timeliness of an HA / DR response." [IMISAS ED 2011]

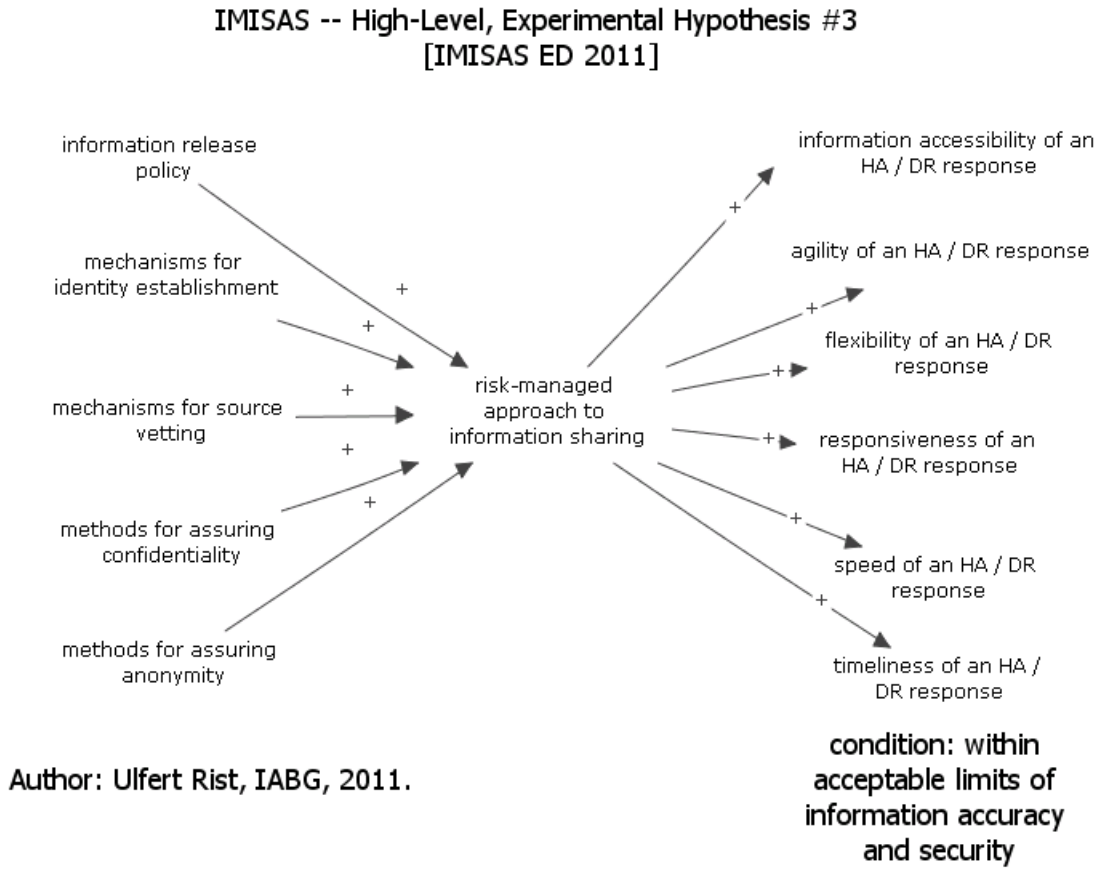


Figure 31: Influence Diagram H3

Interpretation: Similar to H1 and H2 above, several factors are being related in a complex causal manner within a single statement. It appears to be difficult to directly test the related complex references without a maximum break-down of H3.

Analytic Break-Down

From an analytic viewpoint, it appears to be necessary to systematically break down the complex hypotheses H1 to H3 into simple statements like "An increased level of risk-managed approach to information sharing causes an increased speed of HA / DR response."[100] Here, the complex factor "risk-managed approach to information sharing" has to be operationally defined/clarified or further broken down to a simple operational factor. Analytic questions and derived survey/interview questions should reference these simple

[100] Extracted from H3.

statements and contribute to validation. By doing so, high-level hypotheses and selected solutions may serve as answers to the overarching IMISAS problem statement.

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project

Annex F - TRANSITION PLAN

1. Purpose

The purpose of this document is to capture the agreement of all parties required to transition Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) project products and recommendations and carry them forward through the informal pathways as described below.

2. Overview

Unclassified information sharing (UIS) processes and procedures used by the combatant commanders must enable and promote information sharing and collaboration with a wide range of mission partners and stakeholders. Technology must be able to support the requirements of the UIS enterprise, and enhancements and developments should be fully integrated with the processes and procedures through standardized business rules. Through research, on-site visits and leveraging of related initiatives, the IMISAS project examined the best ways to improve information sharing between Department of Defense (DOD) and non-DOD partners. Human factors, cultural, policy and procedural barriers were identified and solutions developed to improve information sharing and collaboration. The solutions included policy, processes, procedures, business rules, and technical recommendations to improve the effectiveness of information sharing and collaboration across organizational and security boundaries. The proposed solutions effectiveness in solving information sharing problems was evaluated during a series of technical spirals and an analytic seminar composed of participants from DOD, United States Government (USG) agencies, coalition military and civilian, international organizations and nongovernmental organizations. At the IMISAS Transition Conference, findings and recommendations from the experimental events were approved by all stakeholders and consensus was reached on transition pathways and responsibilities for implementation.

2.1 Situation

Success in theater cooperation, stabilization, humanitarian assistance and disaster relief missions depends on sustained and habitual information sharing and the ability to collaborate across security domains among actors supporting these missions. Combatant commands (COCOMs) have identified joint shortfalls in the current art and practice of UIS between a diverse community of potential mission partners as well as non-aligned organizations. That community includes enduring and familiar partners such as the Department of State, as well other USG agencies, alliance partners, host nations, inter-governmental organizations, nongovernmental and ad hoc organizations, and individuals. The complexities of operating and sharing information with an evolving and often unfamiliar community of interest places a premium on DOD's ability to understand the nuances of potential partner organizational cultures, needs, strengths and limitations.

2.2 Operational Problem

As described in the warfighter challenge (WFC) submitted by United States European Command (USEUCOM) and United States Africa Command (USAFRICOM), U.S. commanders lack a consistent and coherent framework and capability to share essential information across multiple domains with a broad range of mission partners (government/interagency, multinational, multilateral and private sector). Problem causes include:

- restrictive policies;
- conflicting authorities;
- ad hoc or non-existent procedures and business rules; and
- non-interoperable networks and systems.

3. Transition Management

3.1 Overall Transition Strategy

The primary transition pathway will be using informal processes described in the Manual for Joint Concept Development and Experimentation (CJCSM 3010.02) to effect changes in the areas of doctrine, training, materiel, leadership and education, and policy. The major products of the IMISAS project are: a pre-doctrinal handbook, *Handbook for Unclassified Information Sharing (UIS);*White Paper on UIS; UIS Architecture; and recommendations for changes/additions to training, materiel, leadership and education, and policy.

3.2 Products Transition

3.2.1 Handbook for UIS

3.2.1.1 Transition Product

The handbook provides a pre-doctrinal reference point for use during development of military staff standard operating procedures (SOP), and a basis for continuing research and development regarding the issues of unclassified information sharing with USG civilian agencies, coalition, and other potential mission partners.

The pre-doctrinal handbook was developed by the IMISAS project team and fully coordinated with the UIS community of interest (COI). Following acceptance by the Joint Staff (JS) J7, Joint and Coalition Warfighting (JCW), Solution Evaluation Group, the final draft will be forwarded to the JS J7, JCW, Joint Doctrine Group, for review, approval and distribution. The handbook could be made available to users via various formats: printed document, electronic file (e.g. .pdf) or ebook.

The handbook is of immediate use to USAFRICOM, USEUCOM and United States Pacific Command (USPACOM) to inform development of COCOM SOPs through training and evaluation during fiscal year (FY) 12 command post exercises (CPX) such as Exercise JUDICIOUS RESPONSE 12 sponsored by USAFRICOM, and exercises with Department of State and the United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA) sponsored by USEUCOM.

UIS processes and procedures in the handbook can be used in any operational-level exercise with non-DOD participants. DOD Chief Information Officer (CIO), supported by JS J7, JCW, Solution Evaluation Group, will address other training and evaluation opportunities at the Worldwide Joint Training and Scheduling Conference (WJTSC) 2011-2, 26-30 September 2011.

The pre-doctrinal handbook will be used to socialize UIS processes and concepts for inclusion into joint publication upgrades. Recommended changes to joint doctrine will be made during the regular review cycle for each applicable joint publication. The applicable joint publications include, in order of revision opportunity:

- JP 3-16, Multinational Operations;
- JP 3-57, Civil-Military Operations;
- JP 3-29, Foreign Humanitarian Assistance;
- JP 3-61, Public Affairs;
- JP 3-08, Inter-organizational Coordination During Joint Operations

3.2.1.2 Organizations:

JS J7, JCW, Joint Doctrine

Mr. Marc Halyard, marc.halyard@hr.js.mil, (757) 203-5508

USAFRICOM

Mr. Arthur Reyes, arthur.reyes@africom.mil, DSN: (314) 421-3023

USEUCOM

LtCol Matthew R. Jeppson, jeppsomr@eucom.mil, DSN (314) 430-6398

DOD CIO

Mr. William Barlow, william.barlow@osd.mil, (703) 601-2437

3.2.1.3 Delivery Dates

30 September 2011 – Delivery of *Handbook for Unclassified Information Sharing (UIS)* to JS J7, JCW, Solution Evaluation. Upon acceptance by JS J7, JCW, Solution Evaluation, forward to JS J7, JCW, Joint Doctrine Group, for review, approval and distribution.

3.2.1.4 Agreements

At the IMISAS Transition Conference, USAFRICOM and USEUCOM agreed to integrate unclassified information sharing in their FY 12 training and exercise plan using the products from the IMISAS project. Additionally, the representative from the USPACOM Pacific Warfighting Center expressed a need for the Handbook for UIS for use by the exercise planners at USPACOM.

3.2.1.5 Resources

Handbook publication currently unfunded

3.2.2 White Paper on UIS

3.2.2.1 Transition Product:

The White Paper on UIS describes the near-term (three-to-five years) UIS operating environment in which DOD will be expected to operate. Building on current UIS documents (DOD Information Sharing Implementation Plan and Unclassified Information Sharing Capability (UISC) Concept of Operations), it sets conditions for exploring the unclassified information sharing and collaboration "to-be" environment.

The White Paper on UIS was developed by the IMISAS project team and fully coordinated with the UIS COI. Following acceptance by the JS J7, JCW, Solution Evaluation Group, the White Paper on UIS will be forwarded to USAFRICOM, USEUCOM and other geographic combatant commanders for their use in informing future joint concept development. The White Paper on UIS could serve as a foundational document for the inclusion of UIS into applicable mission area joint operating concepts.

The White Paper on UIS will be made available to DOD CIO and JS J36 to inform updates to the DOD Information Sharing Strategy and the UISC Concept of Operations (CONOPS).

3.2.2.2 Organizations

USAFRICOM

Mr. Arthur Reyes, arthur.reyes@africom.mil, DSN: (314) 421-3023

USEUCOM

LtCol Matthew R. Jeppson, jeppsomr@eucom.mil, DSN (314) 430-6398

DOD CIO

Mr. William Barlow, william.barlow@osd.mil, (703) 601-2437

3.2.2.3 Delivery Dates

30 September 2011 – Delivery of White Paper on UIS to JS J7, JCW, Solution Evaluation. Upon acceptance by JS J7, JCW, Solution Evaluation, forward to USAFRICOM, USEUCOM and other geographic combatant commanders, DOD CIO and JS J36.

3.2.2.4. Agreements

At the IMISAS Transition Conference, USAFRICOM and USEUCOM agreed to consider the White Paper on UIS in the future development of joint operating concepts.

3.2.2.5 Resources

None required

3.2.3 UIS Architecture

3.2.3.1 Transition Product:

Describes (in architectural views and supporting narrative), the organizations, activities and information exchange requirements at the strategic theater-level in a foreign humanitarian assistance/disaster relief context. This effort will contribute to the development of an architecture framework describing a broader UIS enterprise across the spectrum of operations. The UIS architecture was developed as a series of views; each view is DOD Architecture Framework (DoDAF) compliant.

The UIS Architecture was developed by the IMISAS project team. Following acceptance by the JS J7, JCW, Solution Evaluation Group, the UIS Architecture will be posted at the JS J8 repository so that it is available to the COI.

The architecture will be made available to DOD CIO and the Defense Information Systems Agency (DISA) to inform the development of the DOD UIS Enterprise architecture and DISA's role as a service provider.

The architecture will be made available to the DOD Executive Agent (EA) for Maritime Domain Awareness (MDA) to facilitate alignment of UIS users and related capabilities.

The architecture will be made available to JS J8, Deputy Director for C4 (DDC4), Combat Capability Developer Division (CCDD), to inform the UIS requirements for Multinational Information Sharing (MNIS) and the Multinational and Other Mission Partner (MNMP) Information-Sharing Capability Framework and related architecture.

The Architecture will be made available to United States Southern Command (USSOUTHCOM) to inform the development and evaluation of the Regional Domain Awareness (RDA) Joint Capability Technology Demonstration (JCTD).

3.2.3.2 Organizations

DOD CIO

Mr. William Barlow, william.barlow@osd.mil, (703) 601-2437

DISA

Mr. Burhan Adam, burhan.adam@disa.mil, (703) 681-2142

DOD EA for MDA

Ms. Alicia Belmas, alicia.belmas@navy.mil, (703) 695-0332

JS J8, DDC4, CCDD

Ms. Heather Long, heather.long@hr.js.mil, (757) 836-8943

JS J8, DDC4, Force Architectures, Standards, and Analysis Division

Mr. Michael Rapp, michael.rapp@hr.js.mil, (757) 836-7308.

USSOUTHCOM

LTC John Ferrell, john.ferrell@hq.southcom.mil, (305) 437-1460

3.2.3.3 Delivery Dates

30 September 2011 – Delivery of UIS Architecture to JS J7, JCW, Solution Evaluation. Upon acceptance by JS J7, JCW, Solution Evaluation, post to JS J8 repository and make available to DOD CIO, DISA, DOD EA for MDA, JS J8, DDC4, CCDD and USSOUTHCOM.

3.2.3.4 Agreements

At the IMISAS Transition Conference, DOD CIO and DISA agreed to use the UIS Architecture to inform DOD UIS Enterprise development.

3.2.3.5 Resources

None required

3.2.4 Recommendations for changes/additions to training

3.2.4.1 Transition Products

UIS must be included in appropriate individual training courses for staff officers; complementing joint and Service professional military education (PME), and collective training. Supported by the *Handbook for Unclassified Information Sharing (UIS)*, the importance of UIS and the attendant planning considerations should inform Capstone training for senior officers and be included in the following Joint Knowledge Online (JKO) courses for prospective and serving staff officers.

- J3OP-US094, The Interagency Process: Full Spectrum Implementation Presentation
- J3OP-US272, DOD 101-Interagency Course
- J3OP-US298, Department of State 101-Interagency Course
- J3OP-US345, USAID 101-Interagency Course

Additionally, the Handbook for Unclassified Information Sharing (UIS) and the White Paper for UIS should be made available to the NATO centres of excellence (COE) to inform their sponsored training.

Command and Control (C2) COE training seminars and workshops, including:

- NNEC (NATO Network Enabled Capabilities) Education Programme
- The importance of the Human Factor
- Information Management (IM) from Policy to Practice
- Social Media in a Comprehensive Approach

Civil-Military Co-operation (CIMIC) COE (CCOE) training courses including:

- NATO CIMIC Staff Worker Course
- NATO CIMIC Liaison Course
- NATO CIMIC Functional Specialist Course
- NATO CIMIC Higher Command Course

3.2.4.2 Organizations

JS J7, JCW, Joint Training, Individual Training, Joint Knowledge Online

Mr. Michael Barnum, michael.barnum@hr.js.mil, (757) 203-6164

JS J8 DDC4 Interoperability and Integration Division (IID)

Mr. John Martie, john.martie@hr.js.mil, (757) 836-4161

C2COE, Utrecht, The Netherlands

LtCol A. Mueller, Deputy Director, +31(0) 30 2187012

CCOE, Enschede, The Netherlands

Colonel Henny Snellen, Deputy Director, +31 534 80 3400

3.2.4.3 Delivery Dates

30 September 2011 – Delivery of the *Handbook for Unclassified Information Sharing (UIS)* and the White Paper on UIS JS J7, JCW, Solution Evaluation. Upon acceptance by JS J7, JCW, Solution Evaluation, forward to JS J7, Joint Training, USEUCOM J7, USAFRICOM J7, C2 COE and CCOE.

3.2.4.4 Agreements

Coordinated with JS J7, JCW, Joint Training

3.2.4.5 Resources

None

3.2.5 Recommendations for changes/additions to materiel

3.2.5.1 Transition Products

Based on the findings from the series of technical spirals and Analytic Seminar, technical recommendations were developed for the initial DOD Unclassified Information Sharing Capability (UISC). These recommendations address software-related capabilities, system availability, user training and UISC governance. These recommendations were developed by the IMISAS project team, fully coordinated with the UIS COI and are included as part of the IMISAS Final Report and Annex J. DISA will take the Final Report, including technical recommendations, and the UIS architecture for use in responding to Joint Requirements Oversight Council Memorandum (JROCM) tasking and further developing the initial DOD UISC.

3.2.5.2 Organizations

DOD CIO

Mr. William Barlow, william.barlow@osd.mil, (703) 601-2437

DISA

Mr. Burhan Adam, burhan.adam@disa.mil, (703) 681-2142

JS J8, DDC4, CCDD

Mr. John Wellman, john.wellman@hr.js.mil

USPACOM, Pacific Warfighting Center (PWC)

Mr. Timothy Gramp, tim.gramp@apan-info.net

USAFRICOM

Mr. Tony Wilson, tony.wilson@africom.mil, DSN: 314 421-5299

USEUCOM

Mr. Stephen Ewell, stephen.ewell@eucom.mil, DSN: 314 430-7159

3.2.5.3 Delivery Dates

30 September 2011 – Delivery of the IMISAS Final Report to JS J7, JCW, Solution Evaluation. Upon acceptance by JS J7, JCW, Solution Evaluation, forward to DOD CIO, DISA, JS J8 DDC4 CCDD, USPACOM PWC, USAFRICOM, USEUCOM.

3.2.5.4 Agreements

At the IMISAS Transition Conference, DOD CIO, DISA, JS J8 DDC4 CCDD, USPACOM PWC, USAFRICOM and USEUCOM representatives reviewed the experimental findings and agreed to the technical recommendations.

3.2.5.5.Resources

DISA and JS J8 DDC4 CCDD agreed to review the recommendations, incorporate them into the requirements process and develop a prioritized program based on available FY 12 funding.

3.2.6 Recommendations for changes/additions to leadership and education

3.2.6.1 Transition Products

Mid-grade officers must be made aware of the importance of UIS in conducting joint operations with non-DOD partners. Supported by the *Handbook for Unclassified Information Sharing (UIS)* and the White Paper on UIS, unclassified information sharing may be nominated as a special area of emphasis for PME curricula. The submission will be made in accordance with CJCSI 1800.01D, Officer Professional Military Education Policy (OBMEP) for consideration by the FY 12 Joint Faculty Education Conference (JFEC).

3.2.6.2 Organizations

JS J7 Strategy & Policy (S&P), Joint Education and Doctrine Division

Action officer for FY 12 JFEC to be named later.

3.2.6.3 Delivery Dates

30 September 2011 – Delivery of the *Handbook for Unclassified Information Sharing (UIS)* and the White Paper on UIS to JS J7, JCW, Solution Evaluation. Upon acceptance by JS J7, JCW, Solution Evaluation, forward to JS J7 S&P, Joint Education and Doctrine Division.

3.2.6.4 Agreements

Coordinated with JS J7 S&P, Joint Education and Doctrine Division

3.2.6.5 Resources

None required

3.2.7 Recommendations for changes/additions to policy

3.2.7.1 Transition Products

DOD policy for UIS requires clarification with respect to existing DOD policies governing clearance of DOD information for public release, export-controlled information foreign disclosure and use of the internet. Recommendations for UIS policy are contained in the *Handbook for Unclassified Information Sharing (UIS)* and the IMISAS Final Report. DOD CIO will take the Final Report, including all recommendations for use in responding to JROCM tasking and developing the UIS Enterprise policies.

3.2.7.2 Organizations

DOD CIO

Mr. William Barlow, william.barlow@osd.mil, (703) 601-2437

3.2.7.3 Delivery Dates

30 September 2011 – Delivery of the *Handbook for Unclassified Information Sharing (UIS)* and IMISAS Final Report to JS J7, JCW, Solution Evaluation. Upon acceptance by JS J7, JCW, Solution Evaluation, forward to DOD CIO.

3.2.7.4 Agreements

At the IMISAS Transition Conference, DOD CIO agreed to need for clarification of DOD policy with respect to UIS. USAFRICOM and USEUCOM agreed to review local implementing policies for UIS.

3.2.7.5 Resources

None required

4. Project Archiving and Contact Information

4.1 Archiving location:

Contact Ms. Kathryn Smith, JS J7, JCW for current location

4.2 Contact information:

Ms. Kathryn Smith, JS J7, JCW, Solution Evaluation Division, kathryn.smith@hr.js.mil, (757) 203-5322

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project

Annex M – Operational Guide for Unclassified Information Sharing

PREFACE

Scope

This *Operational Guide for Unclassified Information Sharing* provides basic guidance, planning considerations, techniques and procedures for ensuring an effective information sharing environment during military operations in support of a wide variety of civilian and other non-Department of Defense (DOD) partners, regardless of the particular mission. In today's interconnected world, contingency operations routinely involve a wide variety of stakeholders and participating organizations outside the military domain. While the warfighting mission generally compels a need for strict operational security and information protection, experiences over the last several years have underscored that success in many mission areas is best achieved by open information sharing with a range of actors and partners.

Purpose

This Guide is intended to provide a pre-doctrinal reference point for use during development of military staff standard operating procedures, and to provide a basis for continuing research and development regarding the issue of unclassified information sharing with United States Government civilian agencies, coalition, and other potential mission partners.

Background and Context

The information and procedures in this Guide are the result of research and analysis in response to a combined Warfighter Challenge (WFC) submitted by the United States European Command and United States Africa Command. Both commands recognized the significant impact of the free flow of information in ensuring effective support to many mission areas, most evident in the realm of humanitarian assistance and disaster relief (HA/DR).[1] With non-DOD participant organizations routinely managing the vast amount of information flow on open data exchange networks (i.e., the Internet), military commands working almost exclusively on secure data networks (i.e., Secure Internet Protocol Router Network (SIPRNet) and Non-classified (but Sensitive) Internet Protocol Router Network (NIPRNet) to execute timely information exchanges with their civilian and multi-national counterparts.

[1] A similar term in use by many commands is "Foreign Humanitarian Assistance" (FHA), which is a more narrowly defined mission set within the larger HA/DR mission. For consistency, this Guide will use the term HA/DR, understanding that FHA is inclusive.

Development

This Guide is the result of research, analysis, published lessons learned, and extensive interviews with staff officers, interagency field officers, liaison officers and representatives from a range of organizations conducting support operations in the field.

Application

This Guide is not approved joint doctrine, but serves as a non-authoritative supplement to extant doctrine and policy guidance. The information contained will enhance the effectiveness of military operations involving extensive civil-military coordination in a low threat environment. The reader will develop a better understanding of the dynamic nature of the unclassified information environment, and learn to use procedures to share mission essential unclassified information with partners. This is not a prescriptive "How To" manual. Commanders remain responsible for considering the potential benefits and risks of using the procedures recommended in this Guide in actual operations.

Distribution and Contact Information

Distribution of this Guide to United States government agencies and their contractors is authorized. Other requests for this document shall be submitted to Joint Staff J7, Joint and Coalition Warfighting.

Table of Contents

PREFACE ..... M-ii
Scope ..... M-ii
Purpose ..... M-ii
Background and Context ..... M-ii
Development ..... M-iii
Application ..... M-iii
Distribution and Contact Information ..... M-iii
Executive Summary M-1
1. Introduction to Unclassified Information Sharing (UIS) M-2
1.1. Purpose M-2
1.2. Scope and Applicability M-2
1.3. Operational Environment M-3
1.3.1. Cultural Considerations M-5
1.3.2. Local Policy Drivers M-7
2. Guidelines for Civilian Coordination M-8
2.1. Introduction M-8
2.2. Key U.S. Government (USG) Interagency Partners M-9
3. UIS Design and Planning Considerations M-12
3.1. Introduction M-12
3.2. Information Management M-12
3.2.1. Creating Pre-Planned Unclassified Information Release Categories and Authorities M-12
3.2.2. Expediting Cross-Domain Transfer of Unclassified Information M-17
3.2.3. Establishing a UISC Portal Worksite M-18
3.2.4. Sharing Information with Mission Partners via UISC M-19
3.2.5. Access M-21

3.2.6. Contact Information M-21
3.2.7. Foreign Disclosure and Unclassified Information Controls M-23
3.2.8. Social Media Integration M-23
3.2.9. UISC Tool Suite, Interfaces, and Capabilities M-24
4. UIS Way Ahead M-30
4.1. Introduction M-30
4.2. Doctrine M-30
4.3. Training and Education M-30
Sub-Annex A: Guide to Selected Non-DOD Mission Partners M-A-1
A.1 Introduction M-A-1
A.2 Key U.S. Government (USG) Agencies M-A-1
A.3 International Organizations M-A-6
A.4 Selected Non-governmental Organizations (NGO) M-A-10
A.5. Information Sharing Websites & Tools M-A-12
Sub-Annex B: Risk-Managed Methodology for the Evaluation of Releasability of Unclassified Information (Release Matrix) M-B-1
B.1 Introduction M-B-1
B.2 Graduated Criteria Release Matrix M-B-2
B.3 Determination of Release Evaluation Authority and Disposition of Information M-B-5
Sub-Appendix 1 to Sub-Annex B: Freedom of Information Release Exemptions M-B-1
Sub-Annex C: Centralized Cross-Domain Transfer Procedures M-C-1
C.1. Cross Domain Cell (CDC) Configuration M-C-2
C.2. CDC Requests M-C-3
C.3. CDC Work Cycle M-C-4
Sub-Annex D: Expanded IM/KM Best Practices for UIS M-D-1
D.1 Collaboration Tools (General) M-D-2
D.2 Asynchronous Collaboration M-D-3

D.3 Synchronous Collaboration M-D-3
D.4 Standardization and Data Tagging M-D-5
D.5 Archiving M-D-6
D.6 Information Maintenance M-D-6
D.7 Continuity of Operations M-D-7
D.8 Bandwidth and Storage Space Considerations M-D-7
D.9 Information Organization and Presentation M-D-8
D.10 Functional Accounts M-D-9
Sub-Annex E: Sample Template for Establishing UIS Portal M-E-1
E.1 UIS Portal Template M-E-1
E.2 Title Banner M-E-2
E.3 Site Navigation Bar M-E-2
E.4 Quick Launch Links M-E-3
E.5 RSS Links M-E-3
E.6 Purpose Statement M-E-3
E.7 Low Bandwidth Link M-E-3
E.8 Group Activity M-E-4
E.9 Adobe Connect Online (ACO) M-E-4
E.10 Weather M-E-4
E.11 Group Members M-E-5
E.12 Social Media M-E-5
E.13 Situation Report Blog M-E-6
E.14 Questions: Request for Information (RFI) and Request for Assistance (RFA) Forum M-E-6
E.15 Files and Imagery – Media Galleries M-E-7
E.16 Document Collaboration Wiki M-E-7
E.17 Map View User of Defined Operational Picture (UDOP) M-E-7
E.18 Group Chat M-E-8
E.19 Other Business Rules M-E-8

Sub-Annex F: Glossary M-F-1
F.1 Acronyms and Abbreviations M-F-1
F.2 Terms and Definitions M-F-6
Sub-Annex G: Bibliography M-G-1

Executive Summary

Contingency operations routinely involve a wide variety of stakeholders and participating organizations outside the military domain. The *Operational Guide for Unclassified Information Sharing* provides guidance, planning considerations, techniques and procedures for military staffs to ensure an effective information sharing environment during military operations in cooperation with a wide variety of civilian and other non-Department of Defense (DOD) partners, particularly in support of low threat environment, such as a humanitarian assistance and disaster reliefs operations.

While the warfighting mission compels a need for strict operational security and information protection, success in many other mission areas is best achieved by open information sharing with partners and other key actors. Local policy considerations must be developed so that any natural tension between these competing interests can be met with flexibility and effective use of information sharing tools. In many instances, working with non-DOD mission partners requires that staff officers share working documents and unclassified or non-classified data over more commonly accessed information platforms. Part of the imperative of this environment is that military staffs themselves must learn to condition themselves to recognize the operational need to share information, and thus move from a default position of *need to protect* (as evidenced by routine SIPRNet use for unclassified information processing) and shift to a *need to share* paradigm which allows for a more open and resultantly more timely information exchange between military staffs and their non-DOD counterparts.

Potential tools available to aid in this transition include creating expanded authorization for release of unclassified data, expediting cross-domain transfer of unclassified information between SIPRNet and NIPRNet systems, creating pre-established mission portals, and exploiting the promise both of social media and the wide variety of dynamic and effective information sharing tools available in the open internet environment. At the end of this Executive Summary is a short checklist to aid staffs in establishing a viable unclassified information sharing (UIS) environment for themselves and the organizations with whom they will potentially interact.

This Guide's purpose is to provide staffs with a pre-doctrinal reference point for use during development of staff standard operating procedures, and to provide support for continuing policy development regarding the issue of unclassified information sharing with U.S. Government civilian agencies, coalition and other potential non-DOD mission partners.

Unclassified Information Sharing "Planner's Checklist"

1. Understand the operating and information environments, including the organizational and political cultures of potential partners.
2. Clarify information sharing requirements, both within the command and with potential partners. Create and/or validate assumptions on potential partners' information requirements.
3. Understand potential non-DOD partners' technical capabilities and limitations, but remember that communication with partners is, at its core, *a human interaction*, not a technical one.
4. Establish clear information-sharing guidance that is designed for ease of release, including such principles as:
   - "Write for release"
   - Create pre-planned release categories and expanded release authorization
   - Move unclassified information production and storage to outside-accessible web-based platforms
   - Establish simple cross-domain transfer procedures to break potential logjams
5. Establish clear information exchange requirements with potential mission partners.
6. Understand the current policy environment concerning Controlled Unclassified Information and foreign disclosure.
7. Join or build a web-based portal focused on the particular mission.
8. Use "best of the web" tools (wikis, blogs, e-mail, simple syndication, etc.) and social media to enhance communications with a wide variety of potential audiences.

1. Introduction to Unclassified Information Sharing (UIS)

1.1. Purpose

The *Operational Guide for Unclassified Information Sharing* is designed to provide guidance, planning considerations, examples of techniques and best practices, and local policy recommendations in order to ensure effective information sharing among military staffs and the potentially wide-range of non-DOD partners with whom they may be interacting during military and humanitarian operations.

1.2. Scope and Applicability

This Guide is focused on an Operational Planning Team (OPT) involved in crisis action planning (CAP) per Joint Publication (JP) 5-0, *Joint Operation Planning*, but it has applicability in any level of staff circumstances calling for an open exchange of information between a military staff and its civilian counterparts, whether government, non-governmental humanitarian aid organizations, or foreign government agencies. *Although the Guide is written in the general context of the humanitarian assistance and disaster relief (HA/DR) mission, readers should find the principles useful across the full spectrum*[2] *of civilian-military engagement.*

1.3. Operational Environment

Aside from the more controlled daily interaction engendered by routine, partnership-building operations, military commands are faced with a rapidly increasing demand for information sharing when they are tasked to plan for or respond to a natural disaster or other humanitarian catastrophe. Military "first responders" will often find they are preceded to the scene by civilian agencies or organizations, many of whom have had "boots on the ground" prior to the precipitating event, and who will likely remain on the scene after the military forces have departed. Civilians encountering fresh military forces in a disaster area may be relieved, resentful, grateful, distrustful, demanding, or any combination of the above. Reasons for this vary, and are discussed in more detail below.

Assuming a stable security situation, military commanders will most likely find themselves supporting civilian organizations already at work on the ground who will usually work under the coordinating umbrella of a United Nations (UN) "cluster" group (see callout box below). As such, it is incumbent on the commander to quickly ascertain the boundaries of command authorities and capabilities, and to clearly communicate those operational parameters to new civilian partners. Many military staffs operate with embedded civilian agency liaisons or foreign military liaison officers, whose roles may prove crucial, provided they are privy to ongoing staff discussions and available information resources.

UN Clusters: The vast majority of international humanitarian aid events are managed under the auspices of the UN "cluster" system, which are "…*groupings of UN agencies, non-governmental organizations (NGOs) and other international organizations (IOs) around a sector or service provided during a humanitarian crisis. Each of the nine clusters (Protection, Camp Coordination and Management, Water Sanitation and Hygiene, Health, Emergency Shelter,*

[2] Many other joint DOD and civilian interactions demand similar levels of open engagement and unclassified information sharing, including issues that cut across security, humanitarian, law enforcement, judicial, financial & military aid, and international relations lines, among others.

Nutrition, Emergency Telecommunications, Logistics, and Early Recovery) is led by a designated agency. Two additional clusters, Education and Agriculture, were later added."[3] In the context of this Guide, the UN Logistics Cluster would become a primary venue for multi-lateral coordination.

Chief among the capabilities the military brings to an HA/DR mission are a highly developed and responsive logistics (including medical and engineering support) infrastructure, extensive communications, and trained personnel resources.

Civil-Military Planning during Operation UNIFIED RESPONSE: United States Southern Command (USSOUTHCOM) played a significant role in the United States' response to the 2010 earthquake that devastated Haiti. The mission theme assigned to USSOUTHCOM and Joint Task Force (JTF) – Haiti was "… [Work] in support of United States Agency for International Development (USAID) as part of a global relief effort to deliver food, water, medical, and shelter assistance to the Haitian people." USAID's stated priorities on distribution of relief supplies focused on, Health (water, sanitation & hygiene (WASH)), re-establishment of governing authority, and ensuring a functioning banking system.

USSOUTHCOM's derived missions centered on:

- Distribution
- Medical
- Unity of Effort
- Security
- Logistics Balance
- Shelter

JTF-Haiti's missions became:

- Distribution
- Medical Facility Assessment
- Support to Haitian people

[3] Taken from online report: *"United Nations Integrated Mission in Timor-Lest;"* describing the UN's 2005 creation of a predictable structure for humanitarian aid missions. Website reference: http://unmit.unmissions.org/Default.aspx?tabid=760

- Integration with the United Nations Stabilization Mission in Haiti (MINUSTAH)

Among the more innovative accomplishments of the overall United States (U.S.) mission was the air component's engagement in planning and controlling the enormous flow of airlift from around the world into the stricken region. With the Port-au-Prince airport completely overwhelmed, U.S. Air Force personnel began routing planes into other regional airports (i.e., in the Dominican Republic), and created arrival and departure "slots" to smooth out logistics handling once on the ground, in addition to establishing localized aerial distribution procedures. Of interest too, in the context of Unity of Effort, is the political distribution of air logistics sorties: 30% U.S. government (USG), 43% U.S. Commercial, and 26% UN and/or other international aid providers.[4]

As they begin their participation, staffs must be aware that military planning procedures, its scope, its depth and jargon can be virtually impenetrable to their civilian[5] counterparts. Further confounding the flow of information is the propensity for military staffs to conduct virtually all of their actual planning and communications over secure data networks, i.e., either the classified Secure Internet Protocol Router Network (SIPRNet) or Non-classified (but Sensitive) Internet Protocol Router Network (NIPRNet) domains. A crucial component to bridging the gap between military and civilian planners, and their responders on the ground, is the willingness of the military staff to modify their institutional information protection paradigm toward a framework of sharing and receiving unclassified information in an open manner that invites trust in both directions. The White Paper on Unclassified Information Sharing[6] and this Guide are tools to that end.

1.3.1. Cultural Considerations

In today's operating environment, there is a compelling need for operational military commanders to understand the impact of culture, both social and organizational, on mission success. For example: some non-DOD mission partners and other contributors maintain strict charter requirements for impartiality, neutrality, and non-alignment with military or government organizations, especially when confronted by possible reprisal from local actors. Instead of the military norm of structured command relationships, a properly functioning UIS operating

[4] Statics accurate as of late January, 2010. Operational summary derived from USSOUTHCOM *"Mission Update Brief, Operation Unified Response, 24 0600 January 2010"* unclassified PowerPoint briefing.
[5] Ironically, the reverse is also true regarding civilian-speak on DOD members, a point which emphasizes the broad need for cultural sensitivity between agencies themselves.
[6] Joint Staff J7 Joint and Coalition Warfighting *White Paper on Unclassified Information Sharing*, 01 Novemberl 2011.

environment enables and supports a more complex and dynamic context, where relationships among stakeholders tend to be more transactional, 'give and take,' and mediated by 'what can you do for me' self-interest. In many ways, this type of UIS context represents a cultural minefield: it is an environment where our military staffs are not adequately trained and equipped for success. These, and similar concerns need to be addressed in the approach to UIS.

In Afghanistan, the U.S. Mission created organizations and systems to map the host nation's cultural terrain, providing important context for achieving objectives in regional conflicts. In the UIS context, this aspect of understanding the cultural environment holds true as well, where simple misunderstandings or superficial treatment of mission partners' organizational goals, objectives, and approaches to problem solving can rapidly derail the military's best efforts.

Accordingly, rigorous information management, better understanding of group dynamic skill sets, and a focused effort to identify "win-win" spaces among participants would clearly help to overcome many barriers to information sharing. The root of the problem is organizational culture and not technology. Existing technology in the UIS capability (UISC) helps mitigate these problems by providing both mechanisms encouraging openness and, where necessary, measures of anonymity and confidentiality.

One way to consider the solution is in terms of "shared situational awareness" (SSA), in which a conscientious mindset of cooperation sets the conditions for developing effective information sharing relationships, including:

- Development of a common operational picture
- Development of courses of action (COAs) supporting strategic goals
- Establishment of informal alliances or agreements between military and civilian partners
- Focusing operational planning and execution on relevant environments and strategic partners

Situational Awareness (SA): Rapid and accurate information dissemination remains a high priority, particularly when lives are at stake in an HA/DR situation. During the federal response to Hurricane Katrina, false situational assessments distracted emergency providers' responses, their sense of urgency and their priorities. Maintaining a high standard of timely and accurate communications is essential to relief operations, using all available communications tools to understand the situation, demonstrate a presence, and provide calming and assurance to improve an otherwise distorted situation.

1.3.2. Local Policy

Directly related to cultural considerations noted in Paragraph 1.3.1 are the imperatives of an operational security (OPSEC) environment that significantly raised the issue of unclassified information management to near-classified levels by creating a category of "controlled unclassified information" (CUI). Staff officers attempting to navigate the often complex guidance and caveats involved with unclassified information sharing often find it easier and less risky to simply work in the classified domain. The result is a large amount of unclassified material filling information storage sites due to local policy environments that successfully inhibit free-flow of working-level information. Another less than desirable result is the production highly sanitized documents that are labeled "cleared for public release," a situation that complicates, rather than enhances, the information sharing environment under which many staffs work.

Importantly, and in contrast to the above, published DOD policy guidance offers an important caveat to the multi-layered proscriptions of CUI: *"The volume of classified national security information and CUI, in whatever format or media, shall be reduced to the minimum necessary to meet operational requirements."*[7] Accordingly, local policy guidance must be structured to not jeopardize mission objectives over CUI policy. Operational needs should take precedence over all such administrative requirements.

[7] Department of Defense Instruction 5200.1 *DoD Information Security Program and Protection of Sensitive Compartmented Information;* Washington, DC, October 9, 2008; page 2, paragraph 4.d.

2. Guidelines for Civilian Coordination

2.1. Introduction

This chapter introduces considerations regarding establishment of core civilian partnerships. JP 3-08[8] provides extensive detail on the overarching policy and procedures guiding the interaction of a civilian-military relationship. This section provides a basic introduction to key civilian organizations with whom the UISC will aid in establishing and maintaining effective unclassified communications. Appendix 1 of this Guide is intended to provide further introductory and contact information regarding the most commonly accessed organizations.

Communications links with mission partners should not be limited by potential single points of failure within a system, or by artificial barriers within the UISC set up in response to existing security concerns and practices. Further, staff officers must not limit their information sharing to DOD systems, but must actively engage on the information sharing systems used by non-DOD mission partners, to include other nations, IGOs and NGOs.

Joint Doctrine: JP 3-08 covers in extensive detail the rationale and basic procedures for creating effective coordination and collaboration between military forces and the larger non-DOD community. Chapter III of Volume 1 highlights the following important principles:

- Recognize all USG agencies, departments, inter-governmental organizations (IGOs), and NGOs that are or should be involved in the operation.
- Define the objectives of the response.
- Define COAs for the assigned military tasks, while striving for operational compatibility with other USG agencies.
- Cooperate with each agency, department, or organization and obtain a clear definition of the role that each plays.
- Identify potential obstacles arising from conflicting departmental or agency priorities.
- Determine which agencies, departments, or organizations are committed to provide these resources in order to reduce duplication, increase coherence in the collective effort, and identify what additional resources are needed.

[8] Joint Publication 3-08: *Interagency, Inter-governmental Organization, and Nongovernmental Organization Coordination during Joint Operations, Volumes 1 & 2*; Joint Staff, Washington, DC, 17 March 2006.

- Define the desired military end states, plan for transition from military to civil authority, and recommend exit criteria.
- Maximize the joint force assets to support long-term goals.
- Coordinate the establishment of interagency assessment teams.
- Implement Crisis Action Planning (CAP).

2.2. Key U.S. Government (USG) Interagency Partners

In the opening stages of an HA/DR or other operation requiring civil-military interaction, planners need to ensure they are fully engaged with key USG civilian counterparts who are working the same issues through their own agencies. Chief among them will be:

2.2.1 Department of State (DOS)

The Department of State establishes the USG's diplomatic goals and advances U.S. interests overseas. It manages that process on site through the American Embassy (AMEMB) in a host nation capital, and consulates located in major host nation cities where there is significant U.S. interest. DOS also provides Ambassadorial level Foreign Policy Advisor (POLAD) to Combatant Command commanders to ensure the military leadership is fully cognizant of diplomatic nuances and potential "redlines" in the conduct of day-to-day military operations.

It is important to understand that the POLAD functions as personal advisor to the commander, not as a DOS representative to the military planning staff. For that purpose, COCOMs are staffed with a Foreign Service Officer who provides first point of contact and liaison functions with key DOS offices, including:

- American Embassy in Host Nation. Embassies function as sovereign U.S. territory overseas, and serve as the primary conduit for interaction between the host nation and the United States government. During crisis response, staffs work with the affected embassy on the basis of already-established relationships between COCOM leadership and the American Ambassador or Charge d'Affaires, the Deputy Chief of Mission (DCM) and other key consular and functional officers based out of the embassy.

- Bureau of Political-Military Affairs (PM). PM's mission is specifically designed to provide a bridging mechanism between diplomatic efforts and DOD. It should be prominent as part of planning any collaborative operations

- Country and/or regional Desk Officers (for host nation). Regional desks at Main State maintain the most comprehensive understanding of issues relating to specific host nations and regions where a JTF may operate.

- Humanitarian Information Unit (HIU). The HIU maintains a detailed database of humanitarian, demographic, resource and infrastructure information for use with a variety of mapping and other geo-referenced products.

- Bureau of Population, Refugees, and Migration (PRM). The mission of PRM is to provide protection, ease suffering, and assist persecuted and uprooted people around the world by providing life-sustaining assistance and ensuring that humanitarian principles are thoroughly integrated into U.S. foreign and national security policy.

2.2.2 United States Agency for International Development (USAID)

USAID is an independent federal government agency that receives overall foreign policy guidance from the Secretary of State. Its work supports long-term and equitable economic growth and advances U.S. foreign policy objectives by supporting:

- Economic growth, agriculture and trade;
- Global health; and,
- Democracy, conflict prevention and humanitarian assistance.

Military planning staffs engaged in HA/DR mission support will have significant interaction with USAID representatives both in the embassy and in the field. Additionally they will be in contact with other key bureaus within the USIAD headquarters, including:

- Office of Foreign Disaster Assistance (OFDA) is the designated lead USG office to provide and coordinate official U.S. humanitarian assistance in response to international emergencies and disasters. OFDA monitors and manages U.S. aid in a number of specific sectors related to humanitarian assistance and disaster recovery.

- Office of Military Affairs (OMA) functions as USAID's primary point of contact with the Department of Defense (DOD). Representing the spectrum of USAID functions, OMA addresses USAID-DOD areas of common interest in humanitarian assistance, terrorism prevention, strategic communications, conflict prevention and mitigation, counter-insurgency, post-conflict reconstruction and stabilization, and operational implementation.

2.2.3 The United Nations (UN)

The United Nations is an international organization committed to maintaining international peace and security, developing friendly relations among nations and promoting social progress, better living standards and human rights. The UN plays an important role in providing assistance in response to major humanitarian emergencies, as well as in promoting disaster reduction as part of the development plans of countries. Key UN agencies with whom a military staff may operate will likely include:

- United Nations Office for the Coordination of Humanitarian Affairs (UNOCHA). UNOCHA coordinates the UN System's response to major humanitarian emergencies,

both natural and man-made, and promotes action to improve disaster prevention and preparedness.

- United Nations World Food Programme (WFP). The WFP furnishes large amounts of foodstuffs in support of economic and social development projects in developing countries. In addition, it has substantial resources with which to meet emergency food needs, some of which can be furnished from project food stocks already in a disaster-stricken country.

- United Nations High Commissioner for Refugees (UNHCR). UNHCR safeguards the rights and well-being of refugees. Their mandate is to lead and coordinate international action to protect refugees and resolve refugee problems worldwide.

- United Nations World Health Organization (WHO). WHO is the directing and coordinating authority for health within the UN. They are responsible for providing leadership on global health matters, setting norms and standards, providing technical support to countries and monitoring and assessing health trends. The group is also responsible for assessing, tracking, and reviewing organizational performance and health outcomes in response to crises.

- United Nations Global Cluster Leads. The UN designates cluster leads for nine sectors[9] or areas of activity that in the past either lacked predictable leadership in situations of humanitarian emergency, or where there was considered to be a need to strengthen leadership and partnership with other humanitarian actors.

[9] See callout box, page 2 of this Guide.

3. UIS Design and Planning Considerations

3.1. Introduction

This chapter outlines key planning and design considerations for establishing a viable unclassified information sharing environment. In order to ensure timely information exchange with non-DOD partners, the following sections describes the tension between information security and release, foreign disclosure, controlled unclassified information (CUI) management and risk mitigation strategies, integration of social media, and the basic characteristics of a technical tool suite - a "UISC platform" facilitating the desired information sharing end state.

3.2. Information Management

While there are legitimate security concerns for maintaining controls on certain unclassified documents and information, there are also compelling reasons for transparency during operations with non-DOD agencies and organizations. *This requires a substantial change in information management policy from "need to protect" to "need to share,"*[10] particularly during operations in support of HA/DR missions, when timeliness is of the essence. The core issue is whether the staff can clear information fast enough to correctly respond to the operational community of interest (COI).[11]

An important factor aiding the expeditious release of unclassified information is to *"write for release"* when initially drafting a document; i.e., do not include the kind of information that routinely creates confusion or concern regarding document releasability. Writing for release also includes such techniques as careful portion[12] marking, the use of "tear-lines" to segregate text, and pre-sanitizing sensitive text on the initial draft. When considering the need for expedited release of unclassified information, which may include CUI, the solutions outlined below may be useful.

3.2.1. Creating Pre-Planned Unclassified Information Release Categories and Authorities

[10] General James Cartwright, USMC, Vice-Chairman, Joint Chiefs of Staff; cited in Intellipedia discussion of "Web 2.0" capabilities. Website - http://www.intelink.sgov.gov/wiki/User:john.l.schirrippa2/Web2.0Brief.
[11] An important caveat: This issue does not refer to the well-established and understood process of declassification; it concerns the process of sharing unclassified information.
[12] Portion marking: i.e., classification labeling of individual paragraphs.

Planners can anticipate the requirement for extensive information sharing with non-military partners during HA/DR operations. As part of the pre-crisis or steady-state planning environments, the commander's release guidance can define categories of unrestricted information access without further deliberation. The tone of the commander's guidance will provide a framework for a Designated Release Authority (whose function can be executed by the Foreign Disclosure Officer (FDO), Public Affairs Officer (PAO), or other officer) to develop additional pre-planned release cases. Appendix 2 provides additional detail on the process by which documents can be efficiently evaluated for releasability using this construct, including recommendations for dynamically updating release cases and applying risk mitigation techniques.

Expanding Unclassified Release Authorization. During the joint planning process, a clear statement of the commander's release guidance (see callout box below), truncated as necessary to fit in as part of Paragraph 5 of the Operational Order (OPORD) and as part of the Base Plan, can set the foundation for the staff's handling of unclassified information, including Public Affairs Officer (PAO) and Foreign Disclosure Officer (FDO) considerations. For example, "For *this operation* everything that is produced by this staff with regard to [some specific aspect] is automatically categorized as unclassified, and is expected to be made available to any designated partner organizations with whom we will engage." The guiding mindset in this regard is *overt transparency*, a communications condition between partners that is generally considered critical for establishing and maintaining legitimacy. For example, common sense subject matter that is easily deduced from the outside but often remains unnecessarily protected may include (but not be limited to):

- Flight information available on the international flight plans (i.e., create a releasable HA/DR "callout box" as part of the Air Tasking Order (ATO)
- Quantity and type of relief supplies en-route
- Expected arrivals and availability at surface and air terminal facilities
- Identification and contact information for units engaged in the operation
- Identification and location of ships clearly operating in view of the host nation
- Assessment of operational risk

Graduated Criteria Release Matrix. Based upon the commander's release guidance, situational analysis, operational phasing, potential risk[13] factors, and the guidance contained in

[13] NOTE: Commander's risk versus benefit determinations should be guided by both physical security and legitimate OPSEC requirements, while still ensuring mission accomplishment.

Annex 3 of DoD 5200.1-R (Information Security Program), the Designated Release Authority can develop categories of information defined by the potential of adverse consequences to unrestricted release. This partitioning of information categories by risk level is codified in a Graduated Criteria Release Matrix. Given a document with potential release sensitivities, the OPT can quickly refer to the matrix to determine whether the information can be made available without deliberation to an unrestricted audience, or whether its releasability requires further evaluation. For the latter case, the matrix indicates whether this evaluation must be made by the Designated Release Authority, or whether it can be delegated to the OPT Chief or other designated trustee(s).

NOTE: the devolution of releasing authority runs contrary to the experience and instinct of many, if not most, staff officers. The Commander must take the lead and insist on opening the "mental aperture" of the staff to accommodate this new thinking. The sample Commander's Guidance shown at the end of this section provides some thoughts to reinforce this new kind of thinking. During risk versus release deliberations, it is particularly important to think through and define the potential negative consequences of inappropriately released data, and to pre-script mitigating procedures that can respond to an actual negative outcome.

Formalized Trust. Maximize the use of "Unless Otherwise Directed" (UNODIR) authorities, and/or command by negation,[14] or create specific release "surge authorities" as part of the overall blanket authorization discussed above. All of these actions represent an intentional move from *risk aversion* to *risk mitigation*.

The callout box below offers a sample of unambiguous language a commander can release to the command to ensure an open, unclassified information sharing environment is not compromised by excessive bureaucracy.

Sample Commander's Release Guidance for Unclassified Information Sharing (Full Version)

The purpose of this directive is to promulgate my command guidance for the release and sharing of unclassified information with our non-DOD partners. Our mission in *this operation*[15] is to

[14] Refers to a general principle along the lines of: *"You may do what you need to do unless I tell you otherwise; keep me informed; under these sets of circumstances, you do not need explicit permission to operate."*

[15] Although this example is written in the context of HA/DR, the principles are applicable for the full range of civilian-military mission sets.

provide humanitarian and disaster relief support to the nations within the crisis region. Our mission partners include our U.S. civilian interagency partners, their counterparts in other supporting nations, the various IOs, IGOs, NGOs involved in this effort, as well as coalition and host nation military forces. We cannot accomplish our mission without them; we are not in charge – we are in support of them. To successfully accomplish our mission, we must openly share information with our non-DOD mission partners and support the establishment of an open information-sharing environment among the group. We keep secrets only from the enemy; our enemy in this operation is human suffering.

I expect my staff and subordinate organizations to immediately reach out in an open manner to our mission partners to determine their assessment of the situation, their capabilities, their needs, and their ideas for how we can best work together. While our partners in the Department of State (DOS) and USAID have the lead for the U.S. effort, we cannot overburden them with our own needs, and must assume that they will do all the required information sharing and coordination with our non-DOD partners.

I expect the members of this command to keep the classification levels of information for this operation, and restrictions to the release of unclassified information, to an absolute minimum. If a document does not absolutely require classification, do not classify it. We will use unclassified and open communication and planning means whenever possible. I have trust and confidence in my staff and subordinate commanders to execute a transparent and logical process, to make the right call and to encourage the delegation of release authority for unclassified information to the lowest-level possible. You are authorized to explore innovative solutions. So that there is no misunderstanding or confusion of my command intent, let me reiterate – I expect everyone in this command to proactively share unclassified information directly with all our mission partners to the maximum extent possible. I am willing to accept risk in order to keep our partners and ourselves fully informed.

Truncated Version for OPORD (paragraph 5 and Base Plan)

For *this operation*, everything that is produced by this staff with regard to [a specific aspect or aspects of the operation] is automatically categorized as unclassified, and is expected to be made available to any designated partner organizations with whom we will engage. I expect my staff and subordinate organizations to immediately reach out in an open manner to our mission partners to determine their assessment of the situation, their capabilities, their needs, and their ideas to see how we can best work together. The staff will build and use a pre-planned release matrix or mission–specific security classification guide to clarify ambiguities in designated unclassified handling procedures.

Designing Unclassified Information Storage for Ease of Release and Re-use. Local security policies can be modified to encourage staffs toward pre-populating open UISC portals with current unclassified materials that are created or resident on controlled networks. Migration standards should be based on the risk matrix outlined above, and conducted per the enhanced cross-domain procedures outlined in Appendix 3. During steady-state or non-crisis periods, staff officers should create and save their unclassified work on NIPRNet or Internet domains,[16] using SIPRNet for unclassified work by exception only. The goal is to migrate virtually all pertinent unclassified documents and databases onto unclassified platforms. Staff operating procedures can be structured around the following points for document owners:

- Create and store all documents subject to the expedited release noted above on the UIS domain in a mission-specific file area. Protection of working documents may be limited to simple password access, with consideration given to creating some level of graduated access permissions consistent with differentiating between draft working documents and workspace, and those that are generally releasable to the larger COI.

- Use a standardized naming convention and maintain visibility of what is available on particular domains.

- For ease of search, include in filing criteria a pre-derived set of content data tags and timing and/or age data for the document.

Business rules for creating and using standardized content tagging are included in Appendix 4.

To the maximum extent possible, the public-facing (i.e., non-password protected) pages of the UIS domain mission portal should provide direct access to core documents, links, and contact information. The portal's homepage should make clear that it is a working space that does not represent the official position of a particular command. At the very least, it should provide clear direction on how a potential user can gain access to available information, using simple identification and verification procedures.

In order to enhance civilian and non-native English speakers' understanding of planning documents, military staffs are reminded to use plain English syntax and avoid use of unusual idioms or un-defined or obscure acronyms.

[16] NOTE: This Guide recognizes that many useful web-based portals (i.e., APAN) may have very limited long-term document storage capacity.

Staff Knowledge Management (KM) maintains responsibility for day-to-day system monitoring and maintenance of the UISC, with particular emphasis on its usability in supporting mission success.

Knowledge managers should actively guide the larger staff in establishing a logical setup of contents, including standardized filing conventions, file types (i.e., Microsoft Word (.doc and .docx) versus Adobe Acrobat Portable Document Format (.pdf) considerations),17 imagery and video "drop boxes," category link-ups, ease of navigation, and in the case of a mission portal, the functionality of the user interface.

Knowledge management plans should factor in at least a preliminary requirement for 24/7 active moderation of the mission workspace for enforcement of content tagging, etc., with a conditions-based branch plan to reduce the need for an active moderator.

3.2.2. Expediting Cross-Domain Transfer of Unclassified Information

The cross domain methodology acknowledges that procedures and technical systems exist to varying degrees among the COCOMs for migrating data[18] across controlled network boundaries. Rather than supplanting these existing systems and procedures, this solution proposes that under high tempo operations such as an OPT humanitarian response, efficiencies of scale and uniformity of procedural compliance should result from the creation of a centralized service for implementing such transfers, whether via manual "air gaps" or high assurance guards. Specifically assigning a small group of personnel[19] to execute the mechanical aspects of file transfer reduces variation in procedural familiarity and compliance for the specific tools. Providing thorough training to this group ensures familiarity and a high degree of compliance. Likewise, the centralization of file transfer activity under high operational tempo, and the centralization of the tools to effect that transfer, should reduce the amount of total integrated time for personnel to become familiar with the procedure and locating or transiting to the physical interfaces for the file transfer. The latter time requirement could be significant for an average user depending on location relative to the approved interfaces; for a member of the Cross Domain Cell, this time requirement would be zero.

---

[17] Operational experience with non-DOD partners indicates a desire to simply extract data that can be directly integrated with theirs. Practitioners need to weigh the relative strengths and weaknesses of PDF and Word formats in light of partners' requirements.

[18] Reiterating the note from earlier in the section, this issue does not refer to the well-established and understood process of declassification; it concerns the process of sharing unclassified information. In the context of this section, this refers to moving unclassified info off of the SIPRNet (or other classified systems) and onto unclassified systems.

[19] Perhaps to be stood up as part of the establishment of a JTF staff.

This procedure does not address the production of unclassified information or retention of unclassified information on classified networks. Rather, for those cases where unclassified information must reasonably reside for some time on classified networks, the procedure provides a means of rapidly transferring that information to an unclassified network with a high degree of procedural compliance and efficiency under significant operational load. The following are the specific recommendations to the staff, with a detailed breakdown of a suggested centralized cross domain procedure contained in Appendix 3:

Establish staff procedures to create a central cross domain process. The process should implement:

- A method of file transfer to a cross domain "drop box" on the source network and a cross domain "pickup box" on the destination network
- A means of communicating the transfer request along with an explicit statement that the requester has verified the file to be transferred to be free of classified information
- An independent check for classified material by another person knowledgeable in the subject matter along with his/her communication of those results to the Cross Domain Cell
- A means of unambiguously associating the identities of the requester and independent checker with their respective communications
- A DoD approved method and equipment for effecting the physical transfer
- Maintenance of a log containing information pertinent to the transfers.

As part of day-to-day operations, pertinent unclassified information and data currently produced and stored on SIPRNet should be pre-migrated to an appropriately protected location within the UIS.

Documents produced in Adobe® portable document format (.pdf) normally provide for faster domain transfer, as they do not contain as many exploitable embedded layers as are available in Microsoft™ Word® document (.doc and .docx) files. Depending on local command policy or the limitations of the cross domain capabilities available, only certain types of files may be transferred, and some file types must be converted to "flatter" types during the transfer. For example, USAFRICOM's air gap procedure requires Microsoft™ Word®, Excel®, and PowerPoint® files to be converted to ASCII text, delimited text, or Joint Photographic Experts Group (JPEG) files, respectively, prior to transfer to the destination domain.

Of note, once the transition begins to create regular work on the NIPRNet and the UISC as the prime information platforms, the need for cross-domain transfers should decrease.

3.2.3. Establishing a UISC Portal Worksite

A primary goal in creating a functional UISC portal is to design it as a repeatable process: a blueprint into which one only needs to insert the mission name and purpose to get started, and whose format is completely recognizable to returning users. To the maximum extent possible, staffs should work within a shared unclassified environment for their day-to-day operations.

Appendix 5 provides an illustrative example of key capabilities for a COCOM-established UISC portal to support an HA/DR operation.

- At the start of the planning process, the OPT should have available a pre-established portal template specific to the JTF mission from which to plan and conduct the operation.

- Portal availability and associated linkages should be made available to all potential actors via a conventional internet connection and structured to be federated[20] with other related sites and portals.
- During the operation, the portal's publically accessible open functionality includes as much relevant information as practical. Information demanding some level of discretion may be made available behind nominal firewalls, to be managed per the risk matrix noted above in section 3.2.1 and Appendix 2.
- Worksite management: per the Commander's enhanced release guidance, all unclassified staff work relevant to the operation shifts to the operation's site for the duration of the event.
- Where possible, staffs should consider using already-established websites and portals created and used by non-DOD mission partners. Direct links should be made available for these sites to minimize duplication of efforts.
- The pre-established HA/DR portal presentation should be structured to be intuitive to non-military personnel and non-native English speakers.

3.2.4. Sharing Information with Mission Partners via UISC

The concept of "whole of government" and multilateral response implies a need for extensive coordination. Staff officers must be able to communicate quickly and efficiently with other mission actors and partners. The UISC includes not only conventional internet web portals, but also wikis, blogs, forums, tweets, Voice-Over Internet Protocol (VOIP), Skype, conventional telephonic transmission, text messaging, e-mail, and geo-visualization tools like Google Earth. Conceptual emphasis is for UISC users to remain agile and free to use the "best of the web" when establishing and maintaining communications linkages, regardless of their circumstances.

Non-DOD access to an operational mission portal can be set up to accommodate varying levels of trust between the portal managers and potential external users. Additionally, UISC must be configured for active two-way connectivity under varying levels of degradation, both procedural, i.e., unfamiliarity with certain capabilities, and physical.

[20] "Federated" in this sense means interoperable, such that appropriate interfaces have been implemented among the work sites to facilitate the transfer of information. See Glossary for more detailed definition.

The methods mentioned above represent the technical side of the information sharing equation, but none of these technical tools are fully effective without staff officers establishing and nurturing professional and mutually supportive relationships with partners outside the confines of their own staff. *This is a human interaction*, enhanced by the capabilities of the UISC. The interactive relationship itself exists to solve mutual problems. Accordingly, the staff officer's measure of success is not the technical means by which communication is established, but by the communication itself. The following points can assist in opening lines of communication:

Liaison Officers. In HA/DR operations, first contact should be with the civilian agency and foreign military liaison officers (LNO) assigned to the military staff. Their insights will not only prove critical when they are included in every phase of staff planning deliberations, but also their own organizational contact lists, and contacts within their particular spheres of influence can help guide the staff's interaction with civilian and non U.S. military partners. LNOs provide the quickest and most accurate access to their home agencies. They provide information regarding those agencies, and should be familiar with their agency's primary information sharing tools, in order to assist in creating the correct operational links to that capability (to include knowledge of SIPRNet capability at the home agency). Staff officers must initiate operational contact on the basis of a two-way exchange of information with LNOs. Additionally, staffs that have an interagency "fusion cell" structure should not bypass it in favor of personality-driven collaboration.

Embedded Foreign and Civilian Staff Officers. Many commands carry on their personnel rolls both civilian and coalition military officers as embedded members of the staff itself. The distinction between embeds and liaisons centers on to whom they report: liaison officers work for their home agency, whereas embeds work directly for the commander. It is a "distinction with a difference" that may bind the parameters of the kind of home agency interaction one might normally expect, but embeds should be capable of pointing to initial points of contact and unique agency procedures.

Country Desk Officers. State Department and USAID country desk officers should be integral to the staff's regular external contact list. They are the best single source for understanding the conditions in the region of interest, and like the LNOs, enable broader situational understanding via their own contact lists. Initial approach and contact should be through agency LNOs; if feasible, follow-on arrangements should also be made for continuing contact via the UISC.

Non-Governmental Organizations (NGO). For initial planning, military staffs should establish and maintain contact with NGOs through the auspices of USAID, and as the operation develops, the UN Cluster system. As noted in Chapter One, many NGOs are committed to specific charter requirements for impartiality, neutrality, and non-alignment with military or government

organizations. Understanding this, staffs need to accommodate this sensitivity by being careful to work with the NGO community on the basis of community[21] and partnership, not exploitation. In a low security risk HA/DR scenario, NGOs will be particularly interested in how they might benefit from the command's logistics infrastructure. From the staff's perspective, understanding the NGO's end-user distribution capabilities can aid in determining practical flow rates of relief supplies into the affected area. NGOs generally work in a highly flexible collaborative information environment that allows for the most straightforward means to move information between players; it may be as simple as daily face-to-face meetings in a tent, or as complex as a database exchange hosted on an internet portal. Staffs should work to keep themselves as adaptable and flexible as the NGOs with whom they will deal.

3.2.5. Access

LNOs and other regular non-DOD contacts should have full access to all portions of the operational portal. As noted earlier, a data filing system compatible with standard UN data tags enhances and encourages non-DOD partners' searches for useful information on the UISC.

3.2.6. Contact Information

Staff officer contact list information should be migrated to a top-level section of the UISC platform as part of the initial stand-up of a dedicated site. Where available, identification of agency networks, systems (and systems limitations i.e. "disadvantaged users"), and introductory access procedures would be helpful. Avoid creating a comprehensive "laundry list" of contacts, but retain enough backup depth to accommodate contingencies. Any public contact list must be designed around usefulness and accuracy.

Contact Lists carry the potential to run afoul of laws regarding release of Personally Identifiable Information (PII). Planners should carefully think through the minimum attributes necessary to support the operation, and then bounce those attributes against a known and strict PII standard (perhaps from the European Community, which is very strict). If possible, HN cultural sensitivities should be consulted in order to get a workable solution in place ahead of time.

Information Exchange Requirements (IER)

[21] Understanding the "community" idea may allow a staff to effectively, if indirectly, communicate with an NGO who might otherwise be inaccessible. It can be expected that some level of staff-to-NGO information exchange will be rereleased as community-wide knowledge, thus creating some essence of 3rd party communications.

After establishing contact, a crucial, early, administrative task is establishing a predictable set of information requirements between the parties. Such a list[22] may include, but is not limited to:

- Personnel contact information
- Meeting Schedules
- Country advisories and updates, including imagery
- Partners' needs assessment approach and methods
- Partners' priorities for administering assistance
- Partners' strategies for addressing common issues, such as access
- Scope and magnitude of the event
- Mission Disaster Relief Plan of the AMEMB Emergency Action Plan
- Disaster Alert Cable
- Disaster Assistance Request
- Significant Event Log and Numbered Situation Report cables
- Disaster relief guidance
- Status of approaching natural disaster
- Anticipated disruption of services
- Potential suspension of USAID and Peace Corps operations
- Anticipated decrease in commercial flights out
- Imagery products and assessment
- Status updates
- Aircraft support requests
- Victims' needs assessment
- DART Situation Reports

[22] NOTE: An expanded version of this list is available as an *Operational Resource Flow Matrix (OV-3)*, which includes Information Exchange Requirements (IER), provides a description of the resources exchanged and the relevant attributes of the exchanges; capturing information-related requirements in a coherent manner and in a way that really reflects the user collaboration needs. Resource flows provide further detail of the interoperability requirements associated with the operational capability of interest, focusing on those that cross the capability boundary.

- Airfields Suitability Reports
- Seaport Suitability Reports
- Road Network Analysis
- JTF Situation Reports

These IERs are known and should be included in Operational Plan (OPLAN) and/or Contingency Plan (CONPLAN) development. Release policy and IER request procedures should also be resident in these plans in order to facilitate quick implementation of any operational changes to local policies and procedures for UIS.

3.2.7. Foreign Disclosure and Unclassified Information Controls

While acknowledging the complexities of foreign disclosure, this Guide recognizes that non-U.S. actors in many operations have legitimate needs for the same information used by, or in the possession of, U.S. forces. Disclosure of classified information to foreign partners is closely regulated by law and policy,[23] and except for the comments directly below, are not addressed further by this Guide. The following guidance is germane:

Foreign Disclosure Officer. In most commands, the Foreign Disclosure Officer (FDO) is responsible only for the release of classified information, although the office may also have a stake in release of CUI to foreign entities. [Editorial NOTE: as of this writing, no DOD instruction specifically addressing the release of unclassified information to foreign entities has been located.]

Controlled Unclassified Information. Issues regarding the release of Controlled unclassified information (CUI), (which includes For Official Use Only (FOUO), Sensitive But Unclassified (SBU), etc.), are often complicated by incorrect application of published procedures in marking the material; for example, as with doing unclassified work on the SIPRNet, many staff officers simply assign an FOUO label on a paper, even if it doesn't meet the criteria outlined in germane security classification guidelines. Working under the assumption that for the mission, some CUI may need to be released to a civilian and multi-national audience, the procedures outlined in Section 3.2.1 and Appendix 2 provide a viable risk versus benefit analysis to guide the release decision. Under current DOD guidance, it is incumbent on the release decision-maker to understand what exactly is "controlled" in the CUI document and sanitize it accordingly.

3.2.8. Social Media Integration

[23] DOD Directive 5230.11; *Disclosure of Classified Military Information to Foreign Governments and International Organizations*. Washington, DC (June 16, 1992).

The ubiquity of contemporary social media provides opportunities for a dramatic improvement in the speed and proliferation of relevant information, not only to already-known mission partners but also to other interested or unaffiliated audiences who may have a stake in the outcome of the operation. Social media integration into UISC platforms also presents real challenges to interpreting the viability of incoming data, discerning a level of trust regarding the source of the data, and developing a means to sift through potentially huge volumes of data to find useful information. This section introduces several ideas regarding the usage and management of social media.

The widespread availability of social media can provide the command with an active and easily accessible venue for presenting its strategic communication message to a broader audience. It can also be used as the introductory venue for a command's operational mission portal.

Viability of social media information is enhanced by the use of content tagging and development of easily developed user trust ratings ("Star" ratings, Telligent "Points" system, etc., that document confidence ratings, content reliability and user credibility). NOTE: verification of information and veracity will remain difficult to conclusively ascertain. Users must be aware that during previous experiences (i.e., Haiti earthquake response), many false requests for assistance arrived via social media, wasting both time and resources. Trust ratings work best only if they are made on the basis of repeat requests or information provisions.

3.2.9. UISC Tool Suite, Interfaces, and Capabilities

This section contains a description of the UISC environment in terms of the tools required and the capabilities needed to share with the mission's community of interest. The UISC environment and the information sharing community are depicted below in Figure M-1 and described below.

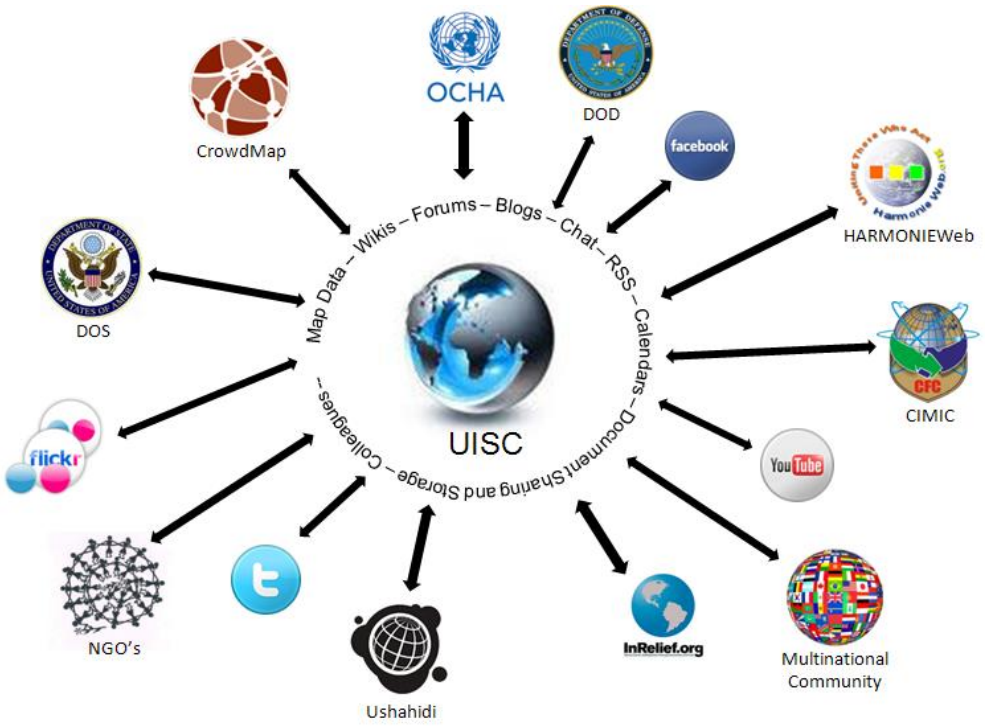


Figure M-1 – UISC Tool Suite and Interfaces

UISC Tools and Interfaces

Chat - The UISC should have an Extensible Messaging and Presence Protocol (XMPP) chat tool. XMPP has been adopted as the mandatory standard for chat by the DOD IT Standards Registry. The tool allows any XMPP client (including web based chat) to be used. Both group chat and peer-to-peer chat is enabled. The user is able to create group chat rooms on the fly, change conversation topics, and manage the users that can access the chat rooms, if needed. Chat room history is available for users to review at a later date and the user are able to export conversations to text documents. Chat rooms should have the ability to be undocked (i.e., not linked to a specific open web page) so they can remain open as other tools are used.

E-mail and Distribution - The UISC does not need an embedded e-mail capability but must have the ability to send out e-mail alerts to users who subscribe to a UISC feed. The UISC should limit the use of e-mail to enforce the need to post information to locations that are searchable and available to the larger community.

NOTE: UISC planners must also be mindful that for many users, e-mail will remain a primary communications tool. Accordingly, e-mail functions need to be compatible with and able to cross domains between various agencies (i.e., into government (.gov) or military (.mil) accounts.) Users may need to deploy and create separate HN e-mail accounts. International cross-domain capability may also become an important criterion to ensure assess with all mission partners.

Wiki - A wiki is a web site developed collaboratively by a community of users, allowing any user to add and edit content. The UISC must have a Wiki tool. The tool will allow for editing and moderation of content, as well as multiple user collaboration. The user will have access to the version history and the ability to compare prior versions for any possible roll-back or reversion of edited content, and if possible, provide a history of who made the updates. Wiki's should contain both a table of contents and content tagging to aid in the location of desired information. The inclusion of images can enrich content. Users should have the option to subscribe to any future content changes and/or be alerted when content is changed.

Blog - A blog is a web site on which an individual or group of users record opinions, information, etc. on a regular basis. The UISC should have a Blog tool allowing for posting of content by individual group members topically and time relevant to the site. The user should have access to content, user rankings, and date and time stamps to self-determine the relevancy and accuracy of any content posted.

Blogs should enable site owners or administrators to have the option to moderate content. Users should also have the option to provide comments to any posted content and to subscribe to any future content changes and/or be alerted when content is changed.

Calendar - The UISC should have a calendar tool. The tool allows for posting important events, meetings, etc. that are topically relevant to the group. The user will have access to the calendar and have the ability to post and update content. Calendars should have the capability to send meeting and/or appointment reminders as well as having the ability to be integrated with popular Simple Mail Transfer Protocol (SMTP) clients such as Microsoft™ Outlook®. Users should have the option to subscribe to any future content changes and/or be alerted when content has changed.

Forum - A forum is an online exchange of information between users about a particular topic. It provides a venue for questions and answers and may be monitored to keep the content appropriate. The UISC should have a forum tool allowing for discussion and questioning of any content that is topically and time relevant to the site. The user will have access to content and user rankings, and date-time stamps to determine the relevancy and accuracy of any content posted. Also, the user should have the ability to reply, comment, suggest an answer, and confirm an answer to any posted content.

Forums should have the ability to allow site owners and administrators to moderate content and capture that content to a wiki to provide permanence to relevant information. Users should have the option to subscribe to any future content changes.

File Access and Management - The UISC should have a file access and management tool. The tool will provide the means to upload documents, images, slides, spreadsheets, videos, etc. to a location that is easy to sort, search and retrieve. Files should only be posted in one location so that the document owners only have to update the single file. Links to the document from other places in the UISC or other community sites are used so that the most current version is always

available. Naming conventions (UISC site name, date) and standard tags are used to ensure the files are easy to locate.

Situational Awareness and Geographical Information Systems Based Mapping - The UISC should have a tool to provide situational awareness (SA) via a geographical information system (GIS) based mapping tool. The GIS tool will provide the user with further insight to the latest topically relevant information affecting the situation in a graphical format. The tool should allow for the control and customization of relevant content layers with the capability to sequence that content in time. The user should be enabled to activate and deactivate layers, change base maps, and modify zoom levels to create their own User Defined Operational Picture (UDOP). GIS tools should accommodate various files types such as KML, KMZ, RSS, GeoRSS, Shape and comma delimited files. Site owners and administrators should have the capability to build, update, and post maps for use by all.

Web Based Meeting and Communication - The UISC will provide a web based meeting and communication venue. It will provide the user with an area to present content using voice, chat, video, and static content such as slide presentations and documents.

The site owner or administrator will monitor and manage the session by using Robert's Rules of Order. The capability will possess such features as the hand raise function, agree and disagree, and various other voting features. Site owners or administrators should have the option to manage entry into the session. Users, site owners, and administrators should have access to a recorded transcript of the session.

Search - The UISC should have a search tool that is able to search titles, tags and content. The search should be as broad or as narrow as needed to be able to search all of the UISC or selected portions of the UISC, to include specific sites and tools.

Really Simple Syndication (RSS) Feeds – RSS is a family of web feed formats used to publish frequently updated works—such as blog entries, news headlines, audio, and video—in a standardized format. An RSS document (which is called a "feed", "web feed", or "channel") includes full or summarized text, plus metadata such as publishing dates and authorship. The UISC needs the ability to provide RSS feeds to other users and have the ability to receive these feeds from other sites.

Disadvantaged User/Cell Phone/Laptop/Mobile Device/Low Bandwidth - The UISC should have a full content site for users accessing the site from a network connected computer. It will also be a limited rich content site enabling content to reach users across a range of mobile devices, including netbooks, tablets, smart phones or other users in low bandwidth environments virtually anywhere. These users must have the ability to post to the UISC and view and respond to UISC content – including imagery.

Short Message Service (SMS) and Multimedia Messaging (MMS) Tracking Tools - SMS is the text communication service component of phone, web, or mobile communication systems, using standardized communication protocols allowing the exchange of short text messages

between fixed line or mobile phone devices. MMS is a standard way to send messages that include multimedia content to and from mobile devices. The UISC must have the ability to receive SMS and MMS content and display it. This enables the information exchange between UISC and disconnected, intermittent, or low-bandwidth (DIL) users.

UISC Capabilities

Request for Information (RFI) - The UISC should have an RFI capability. The RFI capability provides the user with a venue to create a request for information that is topically relevant to the site. The capability allows for the creation of a question and answer type venue enabling the user to accept or approve an answer from the community. A forum tool provides that environment. Approved and answered RFIs should be considered closed. Likewise, the user is able to recommend and organize the questions in an orderly fashion.

The RFI capability must enable site owners and administrators to moderate content. The user should have access to content and user rankings, and date and time stamps to self-determine the relevancy and accuracy of any content posted. Users should also have the ability to track RFIs by having the option to subscribe to any future content changes.

Situation Reports (SITREPs) - The UISC will have a capability to provide situation reports (SITREPs). It will provide the user insight to the latest topically relevant information affecting the situation. It will allow for the creation of reports that enable the user to access content and user ranking, and date-time stamps to self-determine the relevancy and accuracy of any posted content.

The SITREP capability should follow a standardized naming convention and enable the site owners and administrator to moderate content. Also, SITREPs should provide links to supporting, informing, and assistive organizations to allow for further self awareness and the awareness of the greater COI. The user should also have the option to subscribe to any future content changes and/or be alerted when content is changed.

Validity and Rating of Information Posted on UIS Sites - The UISC must have the capability to enable the user to rate the validity and accuracy of content posted on UIS sites. A validity and ration system provides the user a method of communication to provide an opinion of content to the sites COI. The UISC must also have the capability to use rule sets to automate the validity of information. For example, if the information is from a known credible source, it can be automatically validated. (NOTE: Users should be careful to distinguish between *source* validity and i*nformation* validity; in many disasters, otherwise reliable sources often provide unreliable information, particularly in the early stages, where rumor and high emotion interfere with accurate assessments).

The validity and rating capability must provide an easily recognizable graphic interface to alert users of the contents ranking – such as number of stars, ribbons, etc. This ranking should display the median rating of all scores.

Document Collaboration - The UISC should have the capability for multiple users to simultaneously edit and collaborate on a single file at the same time. Document collaboration provides the user an interface to compose files using a rich text editor with spell-check. The capability should also inform users if any editing conflicts occur with other users.

The document collaboration capability must contain file version control with the ability to compare versions and revert to a previous version if needed. The site owners and administrators should have the capability to moderate content. Users should also have the option to subscribe to any future content changes and/or be alerted when the content has changed.

Access, Permissions and Graduated Access - The UISC must have the capability to control site access and enable graduated permissions to provide users an easy entry point to access all content within the site without having to provide credentials. If the user chooses to participate within the site, the user must have a UISC user account and the appropriate permissions to post and edit content within the site. Likewise, enhanced permissions should be granted to those users with special requirements to prevent public view.

The site owners or administrators must verify and approve individuals for participation within the site. Verification is accomplished using several methods such as e-mail, biography, user ranking, and proxy. Another straightforward means of verification is based on the word of a documented "authoritative source" who speaks for the organization, and whose say-so is deemed sufficient to grant access. Given that most organizations know who they've sent into HA/DR types of situations, they can also be asked to post their deployed roster somewhere in the UIS system, which may also provide a quick check for granting more granular access.

Cross-Domain - Manual cross-domain transfer is discussed in section 3.2.2 and Appendix 3. There are technical solutions allowing for the automation of either all or only parts of the cross-domain transfer. The UISC is enhanced by using some of these automated capabilities, particularly as cross-domain services become part of the larger enterprise of available services.

UIS Links and Interfaces - The UISC must provide an interface to any community of users that need to collaborate on the open internet. Most access will be over Hypertext Transfer Protocol (HTTP) (port 80) or HTTPS (port 443). XMPP chat uses standard XMPP ports (5222 or 5223 (secure)). Online conferencing and communication also has port requirements, depending on the service the UISC provides. The UISC should also allow community users to search for content and subscribe to content as well as provide the ability to push content to other sites to populate that site with information. Lastly, UISC links and interfaces must be capable of integrating authoritative data from external sources.

4. UIS Way Ahead

4.1. Introduction

Capabilities outlined in the *Unclassified Information Sharing Capability (UISC) Concept of Operations*[24] and the *Department of Defense Information Sharing Implementation Plan*[25] describes an initial operating capability for a common suite of UIS tools. The way ahead blends aspects of technology, policy, and organizational cultures in order to achieve collective mission objectives in a better way. Accordingly, this Guide supports development of an affordable, scalable, sustainable, and interoperable suite of capabilities providing information sharing and collaboration among: combatant commands; their joint task force and Service commands, and their global partners; real and virtual communities; broader private and public sector communities; and interested, relevant individuals, all performed without traditional boundaries.[26]

4.2. Doctrine

This pre-doctrinal Guide will be used to socialize UIS procedures and insert them and other key principles into appropriate joint publications. Currently, the potential joint publications impacted include (in order of revision opportunity):

- JP 3-16, Multinational Operations
- JP 3-57, Civil-Military Operations
- JP 3-29, Foreign Humanitarian Assistance
- JP 3-61, Public Affairs
- JP 3-08, Inter-organizational Coordination During Joint Operations
- JP 3-0, Joint Operations
- JP 5-0, Joint Planning

4.3. Training and Education

[24] United States Joint Chiefs of Staff, J-3, *Unclassified Information Sharing Capability (UISC) Concept of Operations*, 10 November 2010.
[25] OASD/NII, *Department of Defense Information Sharing Implementation Plan*, April 2009.
[26] Brigadier General Michael J. Carey, USAF, Deputy Director, Joint Staff (J-36); *Unclassified Information Sharing Capability (UISC) Concept of Operations*. Washington, DC (15 Nov 2010).

In the near-term, exercise planners should consider inclusion of UIS as an important training objective. Mission rehearsal exercises (MRXs) for units employing UIS (e.g., JTF HOA), as well as other COCOM-level exercises with significant non-DOD participants (VIKING, JUDICIOUS RESPONSE), would provide immediate lessons learned and identify best practices. In the longer-term, UIS practices should be incorporated in appropriate schoolhouse and online training, as well as professional military education.

With the understanding that the only technical commonality between potential information sharing partners may be access to the Internet, training and education should focus on expansion of UISC usage beyond the conventional HA/DR mission set, into a more comprehensive basket of interests, including:

- Partnership building and enhancement
- World Health issues
- Environmental concerns and events
- Weapons of mass destruction proliferation
- Illicit trafficking (persons, drugs, etc.)
- Support to combat operations
- Diplomatic support
- Event security (Olympics, World Cup, etc.)
- Geospatial visualization tools
- Cyber attack[27]

Training can focus on not only the capabilities of the UISC tool suite itself, but also its intangible factors and indicators, such as:

- Temporal availability of information
- Perceived and real value of information exchanged
- Accuracy and reliability of information
- Increased shared awareness by all mission partners and decision makers at all levels
- Levels of trust, reputation and reliability among mission partners

[27] Ibid. (page 7)

- Improvement in creating unity of effort, mission coordination and response across groups or communities
- Crowd sourcing[28]

Training and education goals should be designed to maximize recognition of the opportunity for increased collaboration, enabled by UISC's information sharing component, and the content created within a group or community. Techniques and procedures, such as "broadcasting" or "forums" or any of the ubiquitous Social Media applications should be understood for both their capabilities and their limitations. Training and education curricula should also emphasize that the core value of unclassified information sharing is not the technical parts and processes, but rather it is the human interaction - the actual communication between people-- that creates value in the operational environment.

[28] Ibid. (page 8)

Sub-Annex A: Guide to Selected Non-DOD Mission Partners

A.1 Introduction

This Annex provides staff officers with a quick reference guide to the roles, responsibilities of selected key potential non-DOD partners during many types of operations. A much more comprehensive discussion of the USG interagency community and other non-DOD groups can be found in Joint Publication 3-08, Volume II.

A.2 Key U.S. Government (USG) Agencies

In the opening stages of an HA/DR or other operation requiring civil-military interaction, planners will need to ensure they are fully engaged with key USG civilian counterparts who will be working the same issues through their own agencies. Chief among them will be:

A.2.1 Department of State (DOS)

The Department of State (http://www.state.gov/) establishes the USG's diplomatic goals and advances U.S. interests overseas. It manages that process on site through the American Embassy (AMEMB) in host nation capitals, and consulates located in major host nation cities where there is significant U.S. interest. DOS also provides Ambassadorial level diplomatic advisors (POLAD) to Combatant Command commanders to ensure the military leadership is fully cognizant of diplomatic nuances and potential "redlines" in the conduct of day-to-day military operations.

It is important to understand that the POLAD functions as personal advisor to the commander, not as a DOS representative to the military planning staff. For that purpose, COCOMs should be staffed with a Foreign Service Officer who will provide first point of contact and liaison functions with key DOS offices, including:

Operations Center. The Operations Center (S/ES-O) is the Secretary's and the Department's communications and crisis management center. Working 24 hours a day, the Operations Center monitors world events, prepares briefings for the Secretary and other Department principals, and facilitates communication between the Department and the rest of the world. The

Operations Center also coordinates the Department's response to crises and supports task forces, monitoring groups, and other crisis-related activities.
Main Switchboard: (202) 647-4000

Bureau of Political-Military Affairs (PM). PM's mission is specifically designed to provide a bridging mechanism between diplomatic efforts and DOD. It should be prominent as part of planning any collaborative operations. PM focuses on six primary aspects:

- Providing the Secretary with a global perspective on political-military issues;
- Supporting the U.S. Department of Defense by negotiating basing agreements, reviewing military exercises, facilitating overseas operations, and by providing embedded Foreign Policy Advisors to military service branch chiefs and combatant commands worldwide;
- Promoting regional stability by building partnership capacity and strengthening friends and allies through security assistance programs;
- Reducing threats from conventional weapons through humanitarian demining and small arms destruction programs, setting the stage for post-conflict recovery in more than 50 nations around the world;
- Contributing to Defense and Political-Military Policy and Planning; and
- Regulating arms transfers and U.S. defense trade.

PM Contact Information:

Bureau Front Office
202-647-9022/3

Office of International Security Operations
202-647-3136

Office of Plans, Policy, and Analysis
202-647-7775

Country and/or regional Desk Officers (for host nation). Regional desks at Main State maintain the most comprehensive understanding of issues relating to specific host nations and regions in which a JTF may operate. They are guided by overarching national guidance and can provide advice with solid long-term considerations.

Humanitarian Information Unit (HIU). The HIU maintains a detailed database of humanitarian, demographic, resource and infrastructure information for use with a variety of mapping and other geo-referenced products. The mission of HIU is to serve as a U.S. Government interagency center to identify, collect, analyze, and disseminate all-source information critical to U.S. Government decision-makers and partners in preparation for and response to humanitarian emergencies worldwide, and to promote innovative technologies and best practices for humanitarian information management.

- To accomplish this mission, the HIU performs the following tasks:
- Identifies key sources of geospatial and geo-referenced data best suited to meet the information requirements of their consumers;
- Collects timely, verifiable, and relevant data utilizing an extensive network of information partnerships;
- Analyzes data using multi-agency expertise and applying proven technologies to determine significant trends and relationships; and
- Disseminates information of value to all levels of consumers, from national-level policymakers to operational field managers.
- The HIU is part of the Bureau of Intelligence and Research, U.S. Department of State. Its staff is composed of personnel from the U.S. Department of State (DoS), U.S. Agency for International Development (USAID), the Department of Defense (DoD), the National Geospatial-Intelligence Agency (NGA), and other technical and specialist personnel.

HIU Contact Information:

Director, Humanitarian Information Unit
Department of State
2025 E St., NW, Suite NE5-037
Washington, DC 20522
Telephone: (202) 634-0341
Fax: (202) 634-0380
E-mail: hiu_info@state.gov
Website: http://hiu.state.gov (Note: Some areas of the site are accessible to or meant for internal users only.)

Bureau of Population, Refugees, and Migration (PRM). The mission of PRM is to provide protection, ease suffering, and resolve the plight of persecuted and uprooted people around the world on behalf of the American people by providing life-sustaining assistance, working through multilateral systems to build global partnerships, promoting best practices in humanitarian response, and ensuring that humanitarian principles are thoroughly integrated into U.S. foreign and national security policy.

PRM provides humanitarian protection and assistance through U.S. government diplomatic efforts and by working with the United Nations (UN), other international organizations, and non-governmental organization. PRM is responsible for U.S. government's institutional with UNCR, IOM and ICRC. PRM website: http://www.state.gov/g/prm/

A.2.2 US Agency for International Development (USAID)

USAID (http://www.usaid.gov/) USAID is an independent federal government agency that receives overall foreign policy guidance from the Secretary of State. Its work supports long-term and equitable economic growth and advances U.S. foreign policy objectives by supporting:

- Economic growth, agriculture and trade
- Global health
- Democracy, conflict prevention and humanitarian assistance

USAID provides assistance in five regions of the world:

- Sub-Saharan Africa
- Asia
- Latin America and the Caribbean
- Europe and Eurasia
- The Middle East

With headquarters in Washington, D.C., USAID's maintains field offices around the world. They work in close partnership with private voluntary organizations, indigenous organizations, universities, American businesses, international agencies, other governments, and other U.S. government agencies. USAID has

working relationships with more than 3,500 American companies and over 300 U.S.-based private voluntary organizations.

USAID's Office of Foreign Disaster Assistance (OFDA) is designated as the lead USG office to provide and coordinate official U.S. humanitarian assistance in response to international emergencies and disasters. OFDA monitors and manages U.S. aid in a number of specific sectors related to humanitarian assistance and disaster recovery, including:

- Agriculture and Food Security
- Economic Recovery and Market Systems
- Health
- Humanitarian Coordination and Information Management
- Humanitarian Studies, Analysis, or Applications
- Logistics and Relief Commodities
- Nutrition
- Protection
- Risk Reduction
- Shelter and Settlements
- Water, Sanitation and Hygiene

USAID also maintains an Office of Military Affairs (OMA) which functions as USIAD's primary point of contact with the Department of Defense (DoD). Representing the spectrum of USAID functions, OMA addresses USAID-DoD areas of common interest in humanitarian assistance, countering violent extremism, strategic communications, conflict prevention and mitigation, counter-insurgency, illicit power structures, post-conflict reconstruction and stabilization, and operational implementation.

OMA manages and facilitates USAID's day-to-day interface with DoD and coordinates joint planning, training, conferences, exercises, and communications.

Combatant command (COCOM) liaison officers (LNOs) assigned to OMA-from both regional and functional commands- ensure access to all levels of DoD. OMA has links with USAID's regional and central bureaus, and coordinates with State Department's Office of the Coordinator for Reconstruction and Stabilization (S/CRS) on planning and implementation of activities.

OMA operations are organized around three focus areas: plans and policy, operations, and training. OMA produces training materials for use in joint training (e.g., conflict assessment frameworks, Provincial Reconstruction Team (PRT) pre-deployment orientation, after-action reports, lessons learned) and coordinates USAID participation in civilian-military exercises.

A.3 International Organizations

A.3.1 United Nations (UN)

The United Nations (http://www.un.org) is an international organization founded in 1945 after the Second World War by 51 countries committed to maintaining international peace and security, developing friendly relations among nations and promoting social progress, better living standards and human rights. Due to its unique international character, and the powers vested in its founding Charter, the Organization can take action on a wide range of issues. It provides a forum for its 192 Member States to express their views, through the General Assembly, the Security Council, the Economic and Social Council and other bodies and committees. Some specific UN offices that may be of interest include:

United Nations Office for the Coordination of Humanitarian Affairs (UNOCHA). The UN plays an important role in providing assistance in response to major humanitarian emergencies, as well as in promoting disaster reduction as part of the development plans of countries. The UN Office for the Coordination of Humanitarian Affairs (UNOCHA) coordinates the UN System's response to major humanitarian emergencies, both natural and man-made, and promotes action to improve disaster prevention and preparedness. UNOCHA's responsibilities after disaster are, at the request of the disaster-stricken country, to assess needs, issue inter-agency appeals for funding humanitarian assistance, organize donor meetings and follow-up arrangements, monitor the status of contributions in response to appeals, and issue reports regarding developments. The Resident Representative of the UN Development Program (UNDP) in individual countries reports to UNOCHA, and provides a channel for requests from governments to the international community. In addition, the UN disaster management teams, country-level representatives of the UN agencies have been established in many countries and can make arrangements to coordinate relief activities in anticipation of an emergency. To permit rapid

response to emergencies, UNOCHA has established a UN Disaster Assessment and Coordination (UNDAC) Team, which can be deployed immediately to an affected country to help local and national authorities determine relief requirements and carry out coordination. (http://ochaonline.un.org/)

United Nations World Food Programme (WFP). WFP furnishes large amounts of foodstuffs in support of economic and social development projects in developing countries. In addition, it has substantial resources with which to meet emergency food needs, some of which can be furnished from project food stocks already in a disaster-stricken country. The WFP purchases and ships food needed in emergencies on behalf of donors, and cooperates closely with the WHO in the nutritional monitoring of emergencies. The WFP is the lead for the Logistics Cluster and the co-lead for the Emergency Telecommunications Cluster. (http://www.wfp.org)

United Nations Children's Fund (UNICEF). UNICEF is mandated to advocate for the protection of children's rights, to help meet their basic needs, and to expand their opportunities to reach their full potential. They respond in emergencies to protect the rights of children. In coordination with UN partners and humanitarian agencies, UNICEF makes its unique facilities for rapid response available to its partners to relieve the suffering of children and those who provide their care. They use materials from emergency stockpiles in the UNICEF warehouses in Copenhagen to meet emergency requirements. They can also procure relief supplies on behalf of other UN agencies and relief organizations. UNICEF is the driving force that helps build a world where the rights of every child are realized. UNICEF is the lead for three clusters: Education, Water Sanitation Hygiene, and Nutrition Clusters. (http://www.unicef.org)

United Nations Department of Humanitarian Affairs (UNDHA). DHA mobilizes and coordinates collective efforts of the international community, in particular those of the UN system, to meet in a coherent and timely manner the needs of those exposed to human suffering and material destruction in disasters and emergencies. (http://www.un.org/Depts/dha/)

United Nations Development Programme (UNDP). UNDP is the UN's global development network. Following disasters and armed conflict, UNDP assists national governments and communities to lay the foundation for sustainable development. Early recovery focuses on restoring the capacity of national institutions and communities after a crisis. Early recovery encompasses a wide

range of areas such as governance, livelihoods, shelter, environment, and social dimensions, including the reintegration of displaced populations. UNDP leads the Early Recovery Cluster. (http://undp.org)

United Nations Food and Agriculture Organization (FAO). FAO leads international efforts to defeat hunger. Serving both developed and developing countries, FAO acts as a neutral forum where all nations meet as equals to negotiate agreements and debate policy. In responding to an emergency, FAO collaborates with many partners, including governments, other UN organizations, and humanitarian groups. During these crises, assistance is required to restore local food production and reduce dependency on food aid, an essential part of the recovery process. FAO designs a relief and rehabilitation program and mobilizes funds for its implementation. In response to emergencies, FAO distributes material assets, such as seed and fertilizer, fishing equipment, livestock, and farm tools. FAO leads the Agriculture Cluster. (http://www.fao.org)

United Nations High Commissioner for Refugees (UNHCR). UNHCR safeguards the rights and well-being of refugees. Their mandate is to lead and coordinate international action to protect refugees and resolve refugee problems worldwide. UNHCR's primary purpose is to safeguard the rights and well-being of refugees. They strive to ensure that everyone can exercise the right to seek asylum and find safe refuge in another State, and to return home voluntarily. As a humanitarian, nonpolitical organization, UNHCR has two basic and closely related aims – to protect refugees and to seek ways to help them restart their lives in a normal environment. UNHCR leads the Protection Cluster. (http://www.unhcr.org/cgi-bin/texis/vtx/home)

United Nations World Health Organization (WHO). WHO is the directing and coordinating authority for health within the UN. They are responsible for providing leadership on global health matters, shaping the health research agenda, setting norms and standards, articulating evidence-based policy options, providing technical support to countries and monitoring and assessing health trends. The group is also responsible for assessing, tracking, and reviewing organizational performance and health outcomes in response to crises. They will empower the UN organizations in the affected country to better address the health aspects of crises. WHO leads the Health Cluster. (http://www.who.int/en/)

United Nations Global Cluster Leads. In December 2005, the IASC Principals designated global cluster leads for nine sectors or areas of activity which in the past either lacked predictable leadership in situations of humanitarian emergency, or where there was considered to be a need to strengthen leadership and partnership with other humanitarian actors. This complements those sectors and categories of population where leadership and accountability are already clear, e.g., agriculture (led by FAO), logistics (led by WFP), refugees (led by UNHCR) and education, led by UNICEF.

United Nations Economic Commission for Africa (ECA). One of the UN's five regional commissions, mandated to promote the economic and social development of its member States, foster intra-regional integration, and promote international cooperation for Africa's development. ECA's dual role as a regional arm of the UN, and a part of the regional institutional landscape in Africa, positions it well to make unique contributions to member States' efforts to address their development challenges. Its strength derives from its role as the only UN agency mandated to operate at the regional and sub-regional levels to harness resources and bring them to bear on Africa's priorities. (http://www.uneca.org/)

United Nations Office of the Special Adviser on Africa (OSAA). OSAA's mission is to enhance international support for Africa's development and security through its advocacy and analytical work, assist the UN Secretary General in improving coherence and coordination of the UN system support to Africa, and facilitate inter-governmental deliberations on Africa at the global level, in particular relating to the New Partnership for Africa's Development (NEPAD). OSAA convenes an inter-departmental Task Force on African Affairs to improve coherence in United Nations support to Africa. (http://www.un.org/africa/osaa/)

A.3.2 International Committee of the Red Cross (ICRC)

ICRC is a private, Swiss, and strictly neutral humanitarian organization based in Geneva. It works to protect and assist victims of armed conflict or disturbances. If a natural disaster should befall war refugees, ICRC can provide aid in kind and services, particularly nutritional and medical assistance. (http://www.icrc.org/)

A.3.3 International Federation of Red Cross and Red Crescent Societies (IFRC)

The IFRC is an international humanitarian organization, composed of, and representing 175 separate national societies. It coordinates humanitarian assistance internationally and operates within an affected country through the member national society or its own staff if no local society exists. The IFRC obtains cash donations and specific emergency items through international appeals, and donates them through the national society. Assistance provided by IFRC consists of food, shelter, water and sanitation, medical supplies, telecommunications, volunteer workers, and in some cases, self-supporting field hospitals and medical teams. (http://www.ifrc.org)

A.3.4 International Red Cross and Red Crescent Movement

The International Red Cross and Red Crescent Movement is the world's largest humanitarian network, with a presence and activities in almost every country. (http://www.redcross.int/en/default.asp)

A.4 Selected Non-governmental Organizations (NGO)

A.4.1 American Council for Voluntary International Action (InterAction)

InterAction is a coalition of over 150 NGOs involved in global disaster relief and humanitarian assistance, and as such provides Web access (in the form of an alphabetized list of links) to these organizations. While the site covers all types of disaster situations, it places an emphasis on complex emergencies. The website operates as an information clearinghouse, and contains links to most of the key players (both NGOs and others such as the World Bank) in this area of disaster relief. (http://www.interaction.org)

A.4.2 Catholic Relief Services (CRS)

CRS responds rapidly to emergencies by providing food, clothing, medical supplies, and shelter. Assistance is coordinated with the national CARITAS organization and the local Catholic clergy. CRS employs health professionals such as public health advisers and nutritionists who work closely with national health authorities. (http://www.catholicrelief.org)

A.4.3 Cooperative for Assistance and Relief Everywhere (CARE)

CARE International is a confederation of 10 national members in North America, Europe, Japan, and Australia. It manages more than 340 relief and development projects in 62 countries in Africa, Asia, Latin America, and Eastern Europe. CARE provides emergency relief in the form of food, hand tools, and similar goods to disaster affected communities. Its post disaster projects include rehabilitation of water supply systems, rebuilding houses, and provision of basic sanitation or health facilities. (http://www.care.org/)

A.4.4 Médecins Sans Frontiéres (MSF) (Doctors Without Borders)

The MSF is a humanitarian aid organization that provides emergency medical assistance to vulnerable populations in more than 80 countries. In countries where health structures are insufficient or even non-existent, MSF collaborates with national health authorities, working in rehabilitation of hospitals and pharmacies, vaccination programs, and water and sanitation projects. In addition to providing medical teams, MSF transports and distributes emergency supplies. (http://www.msf.org)

A.4.5 Oxford Committee for Famine Relief (Oxfam)

Oxfam International is a network of 11 humanitarian organizations who address issues of poverty, providing financial, technical, and networking assistance to grassroots groups undertaking community development. During disasters, Oxfam provides funding and technical support for immediate and long-term assistance. It has developed considerable expertise in managing refugee camps, nutritional relief, and housing projects.
(http://www.oxfamamerica.org)

A.4.6 Directory of African NGOs

The organizations are arranged by country, and under each country are listed alphabetically according to their official name within the country. Each description gives general information, including the name of the organization, the year of creation, the type of organization, the contact person and address. It also includes the NGO's purpose, its major activities, an illustration of the organization's work, the international and local languages used in its work, financial sources and the list of networks, umbrella organizations or federations with which the NGO is affiliated.
(http://www.un.org/africa/osaa/ngodirectory/index.htm)

A.5. Information Sharing Websites & Tools

A.5.1 AlertNet

Reuters AlertNet is a humanitarian news network based around a popular website. It aims to keep relief professionals and the wider public up-to-date on humanitarian crises around the globe. AlertNet attracts upwards of ten million users a year, has a network of 400 contributing humanitarian organizations and its weekly e-mail digest is received by more than 26,000 readers. AlertNet focuses its resources on covering fast-moving humanitarian emergencies and on the early warning of future emergencies. In so doing it provides relatively little on economic development which is a closely related subject and makes up the majority of the work of AlertNet member NGOs. (http://www.alertnet.org/)

A.5.2 All Partners Access Network (APAN)

APAN is a DoD sponsored community of communities website that combines the benefits of unstructured collaboration (wikis, blogs, forums) and structured collaboration (file sharing, calendar) with the personalization of social networking to facilitate UIS with multinational partners, non-governmental organizations, and among various federal and state agencies.
(https://community.apan.org/)

A.5.3 Humanitarian Information Centers (HIC) and Partners

HIC supports the coordination of humanitarian assistance through the provision of information products and services. The HIC supports the decision-making process at headquarters and field level by contributing to the creation of a common framework for information management within the humanitarian community to improve the planning and delivery of humanitarian assistance. HIC is a focal point for data collection, analysis and dissemination in support of the provision of humanitarian assistance, developing and supporting data standards. (http://www.humanitarianinfo.org/)

A.5.4 Integrated Regional Information Networks (IRIN)

IRIN is an award-winning humanitarian news and analysis service that delivers unique reporting from the front lines of humanitarian action to over a million online readers. IRIN is the premier online humanitarian news source. IRIN's head office is in Nairobi, Kenya, with regional desks in Nairobi, Johannesburg, Dakar, Dubai and Bangkok, covering some 70 countries.
(http://www.irinnews.org/)

A.5.5 National Earthquake Information Center (NEIC)

The NEIC is an agency within the U.S. Geological Survey that harbors extensive national and global data on earthquakes. The site provides information on earthquakes over history, by country, by state; a glossary of terminology; earthquake lists, facts, and statistics; resources and mitigation; and information on tsunamis (tidal waves caused by earthquakes). On the home page is a quasi-GIS map of the world with all recent earthquakes delineated by magnitude. Click on the earthquake icon to get detailed information. In addition, the site provides access to a database that can be searched by location/date range, date, magnitude, depth, and intensity.
(http://earthquake.usgs.gov/regional/neic/)

A.5.6 National Geophysical Data Center (NGDC)

NGDC is a division of the National Oceanographic and Atmospheric Administration (NOAA) provides the Worldwide Volcano Database that contains 4,300+ records. Searchable fields include volcano name, eruption year, map

coordinates, geographic region, and magnitude. (http://www.ngdc.noaa.gov/hazard/volcano.shtml)

This site also hosts the Worldwide Earthquake Database. (http://www.ngdc.noaa.gov/hazard/earthqk.shtml and the Tsunami Event Database http://www.ngdc.noaa.gov/hazard/tsu.shtml)

A.5.7 ReliefWeb

ReliefWeb is an online gateway to information on humanitarian emergencies and disasters which scans the websites of international and non-governmental organizations, governments, research institutions and the media for news, reports, press releases, appeals, policy documents, analysis and maps related to humanitarian emergencies worldwide. In addition, ReliefWeb produces maps and infographics to illustrate and explain humanitarian crises. (http://www.reliefweb.int/)

A.5.8 World Factbook

The World Factbook provides information on the history, people, government, economy, geography, communications, transportation, military, and transnational issues for 267 countries, territories, and other entities. The reference tab links to maps of the major world regions, as well as flags of the world, a physical map of the world, a political map of the world, standard time zones of the world, political systems, tribes, sensitive issues, local laws, languages, etc. (https://www.cia.gov/library/publications/the-world-factbook/)

Sub-Annex B: Risk-Managed Methodology for the Evaluation of Releasability of Unclassified Information (Release Matrix)

B.1 Introduction

This Annex provides staff officers with sample processes and procedures to expedite the evaluation of releasability of potentially sensitive unclassified information in support of a crisis response situation. The applicability of the annex is limited to those cases of unclassified information which permit some latitude in judgment in establishing their eligibility for unrestricted release. This judgment is based upon the guidance of Appendix 3 of DoD 5200.1-R, which addresses the various categories of CUI. An example of such latitude is exemption #2 of the Freedom of Information Act (FOIA), which permits withholding of unclassified information from public release if such release would "allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission", or if the information is of no public interest and an administrative burden to process for release. The nine FOIA exemptions are provided for reference in Appendix 1 to this annex.

NOTE: The focus of any IER-related unrestricted release request should be addressed from the perspective of: *"Is non-release of DoD generated CUI worth the risk of mission failure?*

The procedure acknowledges the native risk in exercising such judgment, and follows a methodology developed by the University of Virginia's Center for Risk Management of Engineering Systems,[29] a process used by the President's Commission on Critical Infrastructure Protection (PCCIP) and other governmental agencies dealing with risk in large, complex systems. The procedure does not presume to relax general responsibility for cognizance of the rules contained in DoD 5200.1-R, and indeed encourages the widest familiarity with this document, as the exercise of collective judgment is always less risky than the exercise of isolated judgment.

[29] (Haimes, Kaplan, & and Lambert, 2002).

B.2 Graduated Criteria Release Matrix

The Graduated Criteria Release Matrix is intended to accelerate the release of unclassified information to an unrestricted forum or storage space by expediting the process of evaluating that information for releasability through the establishment of pre-evaluated release cases and authorities. The matrix is developed by a Designated Release Authority based on the Commander's guidance for disclosure and/or release, the potential for adverse consequences of release given the prevailing operations security (OPSEC) condition, and the guidance contained within Appendix 3 of DoD 5200.1-R. The function of the Designated Release Authority may be carried out by the FDO, PAO, or other assigned officer having firm familiarity with the rules for the identification, marking, and handling of CUI.

In generating the Graduated Criteria Release Matrix, the Designated Release Authority will consider the totality of unclassified information expected to be of interest to the COCOM's external partners during a crisis response event, and identify classes of documents having identical potential release sensitivities relative to Appendix 3 of DoD 5200.1-R. Categories of information that permit no discretion in the determination of releasability, such as personal medical information, are excluded from consideration for the matrix. For all remaining categories, the Designated Release Authority will evaluate the risk level associated with the release of the respective information type. A standard industry tool to assist in that determination is provided in Figure M-B-1. This table, adapted from MIL-STD-882C (DOD Standard Practice for System Safety)[30], associates a level of risk to various combinations of likelihood and consequence of an adverse reaction to an event. In this context, an event is the release of an unclassified document with potential sensitivities to a publicly accessible space. An adverse reaction to that event could take many forms, many of which are explicitly anticipated in DoD 5200.1-R.

[30] (Headquarters, 2000).

Risk (High, Medium, or Low) of Adverse Reaction to an Event as a Function of Likelihood and Consequence		Consequence of Adverse Reaction		
		Severe	Moderate	Negligible
Likelihood of Adverse Reaction	High Probability	High	High	Medium
	Significant Probability	High	Medium	Low
	Improbable	Medium	Low	Low

Figure M-B-1 – Risk Evaluation Table

A systematic approach to determining the potential consequences to each document category is to compile a list of "what can go wrong" and taking the most severe of the potential outcomes as the consequence level. A (non-exhaustive) list of attributes potentially affecting the severity of outcomes (Haimes, Kaplan, & and Lambert, 2002)[31] is given below. These attributes are taken from a general systems perspective; the "system" in the present context is the interaction of the COCOM with its external partners.

- The absence of modes by which the events of a scenario can be discovered before harm occurs.
- The absence of control modes that makes it possible to take action or make adjustments to prevent harm.
- Multiple and potentially unknown ways for the events of a scenario to harm the system.
- Inability to restore the system to its initial pre-event condition.
- Duration of adverse consequences.
- The potential for effects unanticipated from current knowledge of the operational situation.

Classes of documents explicitly identified by the commander as being unconditionally releasable for the given operation are automatically classified as low risk.

Risk level is annotated in column 2 of the Graduated Criteria Release Matrix for each category of information identified. Where risk mitigating measures can affordably be implemented relative to a specific category of information, those measures should be annotated in column 3. If the mitigation plan is

[31] (Headquarters, 2000).

lengthy, a reference to the plan can be annotated in column 3. A notional example of a completed Graduated Criteria Release Matrix is provided in M-B-2.

Information Type	Risk Level	Mitigation
Weather reports	Low	
Sanitized low level perishable spot reports/threat assessments	Low	
Time sensitive imminent danger threats	Low	
Daily Message Traffic requiring coordination/synchronization of assets	Medium	Plan A
Sanitized releasable Situation Reports (SITREPS)	Medium	Plan B
UNCLASSIFIED Common Operating Picture (COP)/Order of Battle (OB)	Medium	
Sanitized Air Tasking Order (ATO)	Medium	Plan C
Law Enforcement Agency Sensitive (LEAS), FBI, DEA info, except when authorized by appropriate agency	High	Plan D
CUI provided by any third country, unless prior approval obtained	High	PlanE
Restrictive markings/special handling instructions	High	Plan A
Internal government actions of participating nations	High	
U.S. capabilities, vulnerabilities or limitations	High	
National imagery	High	PlanF
Info potentially embarrassing to the USG	High	PlanB
Friends on Friends	High	

Figure M-B-2 – Graduated Criteria Release Matrix (Notional)

The OPT shall refer to the Graduated Criteria Release Matrix whenever there is the need to evaluate an article of unclassified information for release to an unrestricted forum or storage space. The Graduated Criteria Release Matrix should be viewed as a dynamic document, evaluated on a continuous basis and updated as necessary in response to changes in the operational environment. Such changes may be indicated by updates to the commander's release guidance, the Designated Release Authority's own review, or recommendations by the OPT Chief. Where the risk associated with certain information categories can be mitigated affordably, the OPT Chief should

implement those changes, annotate the Graduated Criteria Release Matrix accordingly, and make appropriate recommendations to the Designated Release Authority on the adjustment of risk levels. Changes to the matrix may take either of the following forms:

- Changes to risk levels of specific categories
- Merging of document categories
- Creation of new document categories
- Changes to the wording of specific categories
- Addition, deletion, or change to risk mitigation measures

B.3 Determination of Release Evaluation Authority and Disposition of Information

With the Graduated Criteria Release Matrix provided by the Designated Release Authority, the OPT has a tool for quickly determining the level of review necessary for any given unclassified document it handles. Any such document is compared to column 1 of the matrix to determine the category in which it belongs. If the category assignment is unclear, or there are clearly no applicable categories, the OPT Chief shall recommend to the Designated Release Authority an appropriate change to the matrix.

Given the risk level identified in column 2 for the category to which a given document belongs, the OPT shall take one of the following three courses of action:

1. High Risk Documents: Evaluation for releasability shall be elevated to the Designated Release Authority. If the document is determined to require exemption from public release under DoD 5200.1-R, the document shall be marked, handled, and protected accordingly. Otherwise it shall be considered unconditionally releasable to the public, subject to any additional review required by the PAO if the document represents an official command position.
2. Medium Risk Documents: Evaluation for releasability shall be assumed by the OPT Chief (or other trustee(s) designated by the Designated Release Authority). The same disposition rules apply as above.
3. Low Risk Documents. These documents are authorized to be made unconditionally accessible without further deliberation. If the document in

question represents an official command position, a PAO review may additionally be required.

The above process is depicted graphically in M-B-3 below.

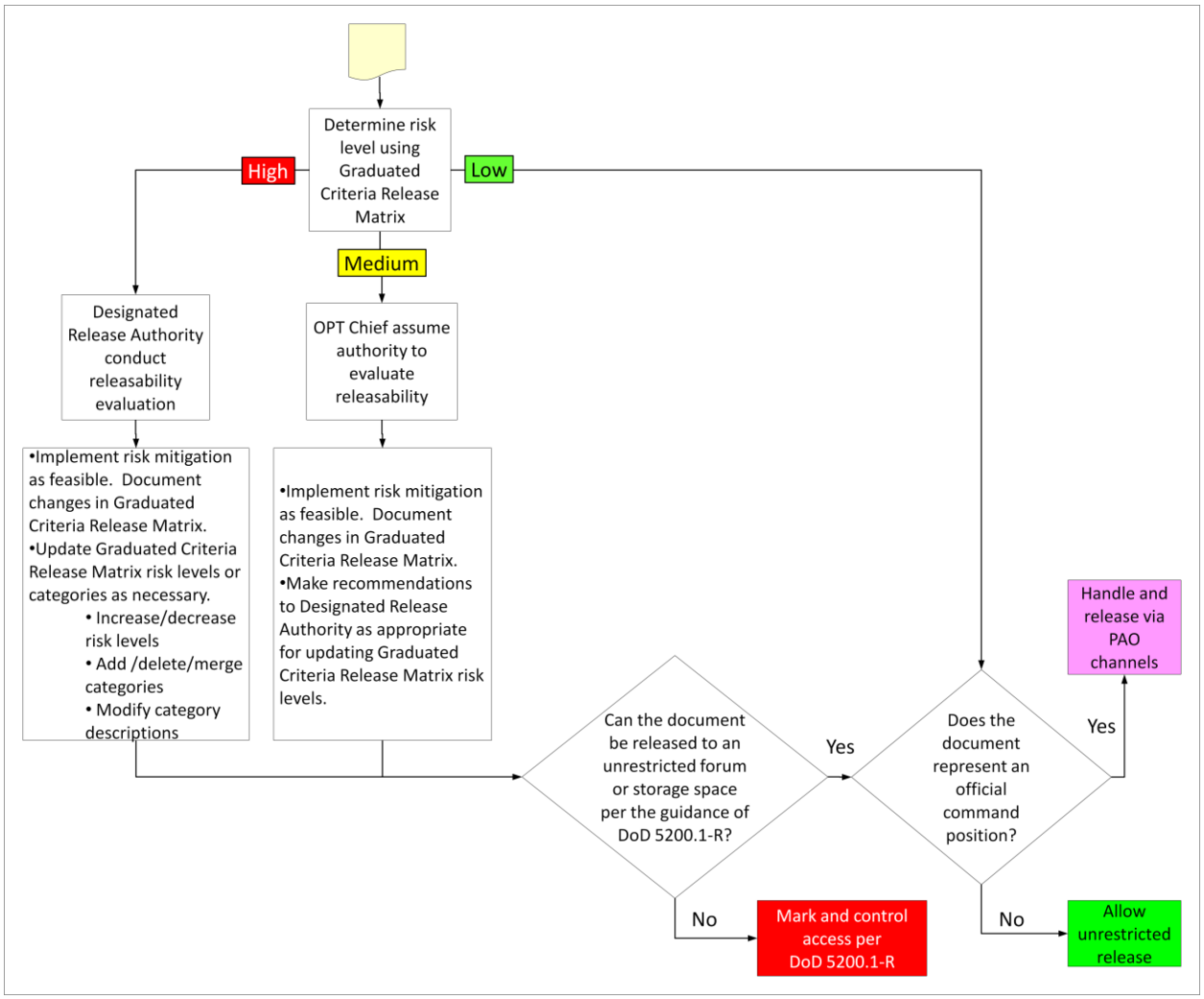


Figure M-B-3 – Document Releasability Evaluation Process

Sub-Appendix 1 to Sub-Annex B: Freedom of Information Release Exemptions

DoD Regulation 5200.1-R, Appendix 1 to Annex C, describes the nine FOIA exemptions as written below. The wording reflects the history of court decisions interpreting the Freedom of Information Act (FOIA) and, therefore, differs from the language of the act itself. To be exempt from mandatory release, information must fit into one of the following categories and there must be a legitimate government purpose served by withholding it.

- Information which is currently and properly classified.
- Information that pertains solely to the internal rules and practices of the agency.

(This exemption has two profiles, "high" and "low." The "high" profile permits withholding of a document that, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The "low" profile permits withholding if there is no public interest in the document, and it would be an administrative burden to process the request).

- Information specifically exempted by statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.
- Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future or to protect the government's interest in compliance with program effectiveness.
- Inter-agency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions and recommendations.

- Information the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
- Records or information compiled for law enforcement purposes that (a) could reasonably be expected to interfere with law enforcement proceedings; (b) would deprive a person of a right to a fair trial or impartial adjudication; (c) could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others, (d) disclose the identity of a confidential source; (e) disclose investigative techniques or procedures; or (f) could reasonably be expected to endanger the life or physical safety of any individual.
- Certain records of agencies responsible for supervision of financial institutions.
- Geological and geophysical information concerning wells.

Sub-Annex C: Centralized Cross-Domain Transfer Procedures

This procedure is intended to illustrate a general centralized process for transfers of information from classified to unclassified networks. The principles extend to any kind of operation involving the need to handle both classified and unclassified information. The procedure's anticipated impact is particularly to operations having a high operational tempo, although low-tempo operations would also be expected to derive benefit.

This solution hypothesizes that cross-domain flows will be accelerated by the centralization of the mechanical portions of the cross-domain process within a dedicated Cross Domain Cell (CDC). This cell manages "drop boxes" and "pick up" boxes in both SIPRNet and NIPRNet networking spaces, and executes the physical transfer of documents across domains. Compared to transfers conducted on a decentralized basis, this procedure is expected to achieve more efficient throughput, accountability, and security by channeling all cross-domain traffic through a specifically assigned body of personnel who are highly proficient with the process, knowledgeable about the procedures, and resourced with all necessary equipment and software (with the ultimate responsibility for the releasability of a document to the destination network residing solely with the person requesting the transfer). Accountability for this responsibility is established and maintained through the submission and archiving of a formal request to the CDC.

The transfer mechanism used in this procedure is a manual air gap. While approved high assurance guards exist to transfer files between networks of different classifications, this procedure is universally applicable in that it can be implemented regardless of the state of accreditation or availability of such guards. Furthermore, a manual air gap levies no requirement to register into a guard. It simply requires simply the ability to burn files to CD/DVDs, an Exclusive Use Stand Alone (EUSA) computer with approved and current DoD antivirus signatures, and common DoD utilities (SecureCopy and Buster) to ensure positive erasure of residual data and the flagging of keywords indicating possible classified data. There is no loss of generality in assuming a manual air gap for the transfer mechanism, as the solution's focus is not on the specific transfer means, but rather the centralizing of the associated tools and activities. The actual air gap procedure that follows is that used by

USAFRICOM, modified as necessary to demonstrate centralization. This procedure will only address transfers from SIPRNet to NIPRNet, although it can be applied equally in the other direction; in this case a check for embedded classified information is not required.

C.1. Cross Domain Cell (CDC) Configuration

The CDC may be manned by one or multiple personnel (CDC watch standers). The CDC requires use of three computers:

1. A computer connected to the NIPRNet. Over this terminal, the CDC watch stander will monitor requests (via the UISC) for cross domain transfers, receive files on CD/DVD for uploading into the "Cross Domain Pickup Box" folder on the NIPRNet, maintain a transfer log, and send notification of completed transfers to the personnel who requested them.

2. An Exclusive Use Stand Alone (EUSA) computer. This is a computer whose sole purpose is to scan, in a non-networked environment, files to be transferred between networks. This computer must be compliant with US Cyber Command's requirements for EUSA computers. After burning the files to be transferred to a write-once CD/DVD on the CDC SIPRNet terminal, the CDC watch will insert the CD/DVD into the EUSA computer's disc drive and scan the disc for malicious code. Once the CDC watch stander determines the files to be free of malicious code, he/she will insert the disc into the CDC NIPRNet terminal's CD/DVD drive and transfer the files to the "CDC Pickup Box" on the NIPRNet.

3. A computer connected to the SIPRNet. This terminal is the source of files to be transferred to the NIPRNet. The CDC will monitor the "Cross Domain Drop Box" folder on SIPRNet in response to transfer requests received over the Cross Domain Cell APAN e-mail account, scan files for transfer using Buster and Secure Copy, convert the files as necessary to the allowable text or PDF formats, and load the files into the copy buffer of the CD/DVD burning utility. The watch will burn the files to disc at a frequency appropriate to the priority of requests and operational tempo, and transfer them to the EUSA computer for virus scanning and ultimate delivery to the NIPRNet. The cross-domain transfer process recognizes two priorities of transfer: high and normal. The priority of a file determines the response

time for transfer, with high priority transfers taking precedence over all other activity and resources.

C.2. CDC Requests

To request the transfer of an unclassified document from SIPRNet to NIPRNet:

1) The requesting participant (referred to as the "Requester") shall review the document(s) to be transferred to ensure no classified information is contained.
2) The Requester shall upload the document into the "Cross Domain Drop Box" on SIPRNet.
3) The Requester shall send an e-mail to the Cross Domain Cell listing the name of the file(s) to be transferred, their priority (high or normal), and the following verbatim statements:

I HAVE REVIEWED THE INDICATED DOCUMENT(S) AND CONFIRM THAT NO CLASSIFIED DATA IS CONTAINED THEREIN.

I UNDERSTAND THAT ONLY TEXT AND PDF FILES ARE ALLOWED TO BE TRANSFERRED TO NIPRNET AND THAT CONSEQUENTLY MY ORIGINAL FILES MAY LOSE FUNCTIONALITY IN THE TRANSFER. IN PARTICULAR, I UNDERSTAND THAT MICROSOFT WORD, EXCEL, AND POWERPOINT FILES WILL BE CONVERTED TO ASCII TEXT, DELIMITED TEXT, AND JPG FORMAT, RESPECTIVELY.

Note: The priority of a file determines the response time for transfer, with high priority transfers taking precedence over all other activity and resources. This designation should be used judiciously, as overuse can be disrupting and counterproductive.

The requester shall include as an e-mail addressee a Second Checker who is knowledgeable of the subject matter of the file to be transferred.

4) The Second Checker, using his/her own account, shall navigate to the document(s) delivered to the Cross Domain Drop Box, and review them for the presence of classified data. If no classified data is found, he/she shall reply to the requester's original e-mail, copying crossdomain@apanmail.org on the reply, with the following verbatim statement:

I HAVE CONDUCTED AN INDEPENDENT REVIEW OF THE INDICATED DOCUMENT(S) AND CONFIRM THAT NO CLASSIFIED DATA IS CONTAINED THEREIN.

C.3. CDC Work Cycle

C.3.1 High Priority Requests

For any documents deposited in the "Cross Domain Drop Box" with corresponding e-mail indicating high priority, the CDC shall, without delay or interruption, perform the following:

1) Scan the file(s) using anti-virus software, Buster, and Secure Copy.
2) Convert file(s) as necessary to .txt or .pdf format.
3) Load the file(s) into the buffer of the CD/DVD burning utility.
4) Label a new write-once CD/DVD with a unique local identification number.
5) Burn the file(s) to a write-once CD/DVD along with any other files in the buffer.
6) Transfer the CD/DVD to the EUSA computer and run the virus scan software on the disc's contents
7) Transfer the CD/DVD to the CDC NIPRNet terminal's CD/DVD drive and upload the file(s) to the "Cross Domain Pickup Box" on NIPRNet.
8) E-mail the Requester to alert him/her of completion of the transfer.
9) Log the transfer of the file in the CDC transfer log, with the following annotations:
    a. Time of transfer
    b. Name of Requester
    c. Name of Second Checker
    d. Name of file(s) transferred
    e. Local identification number of the CD/DVD used for the transfer
10) Delete the original file(s) from the "Cross Domain Transfer Box" on SIPRNet.

NOTE: If at any time during this procedure classified data or malicious code is detected in the files to be transferred, the procedure shall be halted, and no further action taken with regard to the transfer until the classification issues have been resolved and appropriate local procedures executed in response to malicious code.

C.3.2 Normal Priority Requests

Documents deposited in the "Cross Domain Drop Box" with corresponding e-mail indicating normal priority shall be transferred, using the same steps indicated above, after any pending high priority requests have been liquidated. The transfer operation shall be executed on the half hour, with additional hard media used as necessary to meet demand. The CDC lead shall adjust cycle periodicity as appropriate to the pace of operations while maintaining effective review.

Sub-Annex D: Expanded IM/KM Best Practices for UIS

This annex provides examples of a number of best practices regarding UIS. They were derived from various sources. They are not intended to conflict with existing command IM/KM guidance, but are offered as supplementary measures to be implemented where they may offer utility. “Collaboration” in this annex refers to the act of communicating between partners for the purposes of reaching some kind of common understanding of an issue.

A key consideration in establishing collaboration among a broad range of partners is that each may have its own preferences, policies, or limitations that limit the span of tools and venues it uses. Communications infrastructure may also be lacking depending on the location, nature, or stage of the contingency, further constraining a partner's options for collaboration.

Partner engagement is facilitated by preparedness to support multiple means of collaboration, and to meet those partners on their respective "home fields." For military members accustomed to a familiar and accredited system of systems, this may necessitate rapidly establishing proficiency with less familiar and possibly cutting-edge collaboration means. Accommodating partners' preferred means of collaboration (which may change dynamically) is a challenging task. It involves first identifying the physical means that are available; these can be precluded by disparate authentication requirements, information security restrictions, bandwidth limitations, communications infrastructure shortfalls, software availability and compatibility, licensing, and a host of other issues. The collaboration tool survey located at http://en.wikipedia.org/wiki/List_of_collaborative_software is an excellent starting point for becoming familiar with the capabilities, limitations, and requirements of a host of collaboration tools. Users need to identify the best and alternate options based upon the needs of the partners and the "learning curve" levied upon all parties. The discussion below provides basic considerations for achieving a viable collaboration plan for among a range of partners.

As a starting point, the definition of *asynchronous* is collaboration where the participants’ input is not sequenced and cued in real time, does not convey the non-verbal subtleties of synchronous exchanges, nor permits the rapid, iterative problem solving enabled by synchronous exchanges such as face-to-

face conversations, video teleconferencing or live chat. However, it allows participants to provide input based on their availability, and to conduct deliberation in depth that would hinder the progress of a synchronous meeting. Both methods are examined in more detail below.

D.1 Collaboration Tools (General)

Collaborative tool suites provide the capability for web-based file storage, and thus serve as a centrally accessible repository for information. The same concerns for file and folder management apply just as they do for share drive storage.

Use the most effective collaborative tool for the intended communication, consistent with others' ability to correspond over that medium. For example, Chat may be a better solution than a repetitive chain of e-mails.

Generally, avoid capital letters in collaboration, as they have the psychological effect of a raised voice.

Users of collaboration systems (asynchronous or synchronous) should identify themselves unambiguously and according to the host's naming convention for user names, which may include fields defining the organization, position, rank, etc.

Plan for and consider the needs and constraints (i.e., bandwidth, access credentials, network and application availability, and licenses) of all expected participants when selecting the collaboration format. Keep in mind that the user base may evolve over time.

Individuals need to continuously evaluate the balance of work done collaboratively and in isolation. Both are necessary in varying degrees; however, if there is no compelling reason not to collaborate on the work, then it benefits the UIS environment to do so in a forum that supports collaboration, as opposed to working at one's desktop (virtual or real) where it cannot be seen or accessed by others.

Information needs change dynamically. Information sharing structures such as portals that can flexibly accommodate a change will remain more relevant than those that cannot evolve with demand.

D.2 Asynchronous Collaboration

Weblogs (blogs) and wikis are excellent vehicles for the dynamic editing of documents by multiple personnel. They are uniquely suited to collaboration situations where timeliness of information has primacy over polish or where an 80 percent solution can suffice to capture perishable opportunities.

One significant challenge to asynchronous collaboration is the need to ensure that information is adequately received and, as necessary, acted on by relevant actors. Users need to guard against the 'staff action posted or sent is a staff action completed' syndrome.

E-mail is an asynchronous collaboration tool with which most are familiar, and about which lessons learned abound on the Internet. A few key points not mentioned elsewhere in this section are:

- Use meaningful subject lines in e-mails. Make your most important point in the first sentence or paragraph, and be as concise and precise as possible.
- Most e-mail systems provide the capability to automatically generate text blocks. These can be tailored to provide additional contact information, organizational disclaimers or policy statements.
- E-mail should only be used when communicating to particular people or specific, narrowly constructed groups. For "shotgun" notifications, information should be posted in the UISC with appropriate naming and tagging to facilitate the search. E-mail notification in this case would simply be a link to the pertinent section of the UISC.
- Per the note directly above, e-mail does not lend itself well to searches by others who might benefit from the information in them.

D.3 Synchronous Collaboration

During group teleconferences or collaborative web-based sessions, care should be taken to log off of the collaborative tools and/or adjust one's status icons so that others do not unnecessarily await responses from you.

Be aware of and adhere to user naming conventions and rules of protocol for the collaborative tool of interest. Meetings are frequently led by a facilitator who sequences the voice traffic and other activity in the session.

Avoid the use of jargon which is not known by all participants. Humor and sarcasm do not translate well across different cultures and languages. Use a common lexicon for abbreviations.

Keep statements short and relevant.

When statements are being interpreted into other languages, divide dialog into manageable, thematically related clusters to facilitate translation. In any case, speak slowly and articulately enough that the entire audience can keep up with you, as many may not be native English speakers.

Explicitly state when you are changing the subject, and when you are finished with your communication. For example, saying "over" when you are done speaking or "break" to change the subject.

Restrict the ability to control shared presentations so that slides are only controlled by the presenter.

Many collaborative tool suites have a microphone lock. Normally, this should not be used, and should be verified to be off at the start of a collaborative session.

Although the web-based collaborative environment emulates normal conversation, it does not provide the subtle cues that control the flow of traffic in conversations. The following options, alone or in combination, should prevent inadvertently "talking over" other users:

- Invoke moderator control of microphones.
- Use "raised hand" or "question" icons, where provided, to alert the moderator of your need to speak; allow the moderator to cue your traffic. Alternately, use Chat to request the use of the microphone.
- Be sensitive to the delay between the keying of one's microphone and the actual enablement of their audio. This delay can be substantial. Some collaborative tool suites such as ACO have a visual sound level meter that indicates when the channel is ready to carry a transmission.

When sidebar discussions are necessary during collaborative sessions, they should be short and carried over a private audio or chat channel. Excessive use of private channels defeats the purpose of the session and should be avoided.

Many collaborative tools provide a capability for maintaining meeting minutes. This is an excellent way to capture, display, save, and transfer to other media any key issues from a session.

Some collaborative tool suites provide the capability to record sessions and provide hyper-links to those recordings. This is a helpful resource, but all participants should give their consent to being recorded.

White boards are provided by many collaborative tool suites for small groups; these tools provide a dynamic graphical environment for participants to mark up and compose a wide-range of files with their personal marking tools. Facilitation is still recommended to sequence editing within the workspace. Because whiteboard is a higher-bandwidth capability, consideration should be given to the abilities of the most bandwidth-challenged participants.

Online chat is a low-bandwidth tool with a wide familiarity base. It may well be possible to send information over a chat connection when all other methods are bandwidth-precluded. The basic informality of the chat venue may be unproductive for particular missions or partners, and users must be wary of inducing a lapse into overly casual discourse and the use of unofficial acronyms. The Air-Land-Sea Application organization has published a useful tract detailing how to avoid unproductive mannerisms and get the most productivity out of chat. The TTP is located at: https://jdeis.js.mil/jdeis/index.jsp?pindex=66&pubId=473&parId=32649&SearchString=chat

At the end of a collaboration session, facilitators should specify the portal location for posting meeting notes/minutes, displayed documents, and recordings if executed.

D.4 Standardization and Data Tagging

Standardization of web page formats across an organization facilitates assigning information locations by category, criticality, and format, ensuring that members always know where to find what they're looking for, regardless of its ownership within the command structure.

The site KM will establish file naming and data tagging standards. Standard data tags should be developed to make it easy for mission partners to locate information that may be in a different file structure than what they are using. For example: when working with the UN, tags should include the UN Clusters;

files can also be tagged where they might best support one cluster or multiple clusters. Personnel from the UN can search the site based on the name of the document that will include an indication of the operation and then on the cluster of interest and only get back those documents that are applicable to their need. This will greatly reduce the numbers of files they would need to review.

Briefing slides should adhere to a standard format with respect to font, size, and spacing of text; placement of classification markings; and content layout.

Maintenance of hyper-link functionality requires continuous effort and care on the part of designated managers. Changing the file name or folder location of a document after it has been published in official areas of the portal, for example, will break the link for users that may have bookmarked the document hyper-link or posted the link to other portals.

D.5 Archiving

All workforce members should periodically (e.g., quarterly, etc. (but more frequently during disasters)) review all documents that they have posted for accuracy, relevancy, redundancy and currency. Once reviewed, a decision should be made for each document to either retain it at the present location, move the document to the designated "archive" folder, or on rare occasions, delete the file.

Users should be familiar with DOD archiving rules established under 36 CFR 1230. In a multi-national operation, United Nations or European Union archiving policies may also apply

D.6 Information Maintenance

Organizational web page updating should be a team effort, thus ensuring the correctness, timeliness, and relevance of posted information.

The maintainer of each information store (folder, web page, blog, etc.) should be unambiguously identified on that information product or container with contact information provided. A useful practice for share drive or web-based folders is to include a help file in the root folder whose only purpose is to provide information about the folder’s contents, including responsibility for maintenance of the information itself and its accessibility, timeliness, etc.

File and folder naming standards facilitate both machine and visual searches, and the use of scripts to restructure directories and move files. Combined with a well-composed folder permissions structure, they prevent unorganized and uncontrolled growth of the folder space. Finally, they ensure that the authoritative version of documents having revision histories can be quickly and unambiguously identified (note that some portal systems such as SharePoint may automatically append version numbers, dates, and other metadata to documents). File names should contain dashes in place of spaces, as underscores are obscured by hyperlink underlining. Other special characters should be avoided, to facilitate hyper-linking across Microsoft applications. Using Arabic numerals rather than Roman numerals facilitates automatic alpha-numeric sorting.

D.7 Continuity of Operations

Communications may suffer a continuum of degradation. The staff should have a plan for exchanging information based on the priority of that information and the supportability of circuits and applications under a variety of conditions such as loss of landline service or partial network shutdown for intrusion response. A well-maintained Information Exchange Requirement (IER) matrix helps in this regard. An IER matrix identifies all required information exchanges for the command. It identifies sender, receiver, priority, circuit, timeliness requirement, classification, and other attributes. The DOD Architectural Framework (DODAF)[32] Operational View 3 (OV-3) provides additional information regarding IER matrices. Individual collaboration sessions should have a backup plan to facilitate a rapid shift to another medium should the original capability fail.

Hard drives on individual computers are susceptible to failure and difficult to recover from crashes. Information should be stored sparingly on local hard drives, and users should be in the habit of backing up data remotely.

D.8 Bandwidth and Storage Space Considerations

[32] DoD Architecture Framework Version 2.0, 28 May 2009

Many file types allow saving to less memory-intensive formats. This should be done as a matter of course when the capability lost in the transformation is irrelevant to the recipient. For example, PowerPoint files can be saved as .pdf files if there is no necessity for the recipient to manipulate the objects on individual slides and the format is otherwise acceptable.

If the capability is provided by the collaborative tool suite, disable high-bandwidth tools, such as those that are not needed, e.g., web camera.

Use discretion in forwarding e-mails, especially those with attachments, as these can consume significant space in the inboxes of all addressees. Only reply to e-mail that absolutely requires a response and minimize the use of the "Reply to All" function. You should end any e-mail text sections with "no reply needed" to discourage responses. Per the note in Section B.2 of this annex, regular use of UISC postings will minimize users' e-mail bandwidth requirements.

D.9 Information Organization and Presentation

The attractiveness of an information source involves a combination of human factors and the value and uniqueness of information hosted at that source. The vast amount of unclassified information that must be processed by a COCOM places a premium on speed of discovery. Evolving commercial technology has invested heavily in human factors engineering and user feedback, with the result of most users having zero tolerance for "clunky" interfaces. A user who encounters one will dismiss it immediately with a mouse click and go elsewhere to find the desired information, even if that subsequent search is fruitless and the user is ultimately compelled to come back to the first source. Therefore, every opportunity to reduce the number of mechanical or mental steps a consumer must execute to locate needed information should be seized. With regard to web-based collaboration, simple metrics include the number of mouse clicks or the amount of scrolling a user has to make in navigation, download speed, neatness of layout, or intuitiveness of the connections between information containers or streams. Not all information can have equal ease of access (only so much information can be presented on the front page of a web site, for example); however, the structure of the information store should be such that ease of accessibility should track with the importance of the information. Keep in mind that cultural differences impact the perception of information importance in terms of its placement.

Western users associate higher importance with information presented to the left and top of a graphical field, for example[33].

Simple formats are generally better than complex formats in terms of memory and bandwidth requirements, span of utility, comprehensibility, and speed of file scans. No repetitive logos, symbols, or lines should be used in slides or other media. Graphics should only be used where they add something unique and useful to the message being conveyed. In terms of space for memory, the most lightweight graphical formats should be used that are consistent with the resolution requirement. Many available software packages effect substantial reductions in memory consumption by compressing and "cleaning up" graphical compositions; PowerPoint itself has a native picture compression option.

Color schemes in presentations and documents should be as simple as possible, keeping in mind that some colors do not render well when displayed by some projection equipment and that some users cannot distinguish between certain pairs of colors (or have no color discrimination at all).

Unnecessary duplication of files should be avoided, as it presents the risk of outdated or non-authoritative versions being acted upon. Hyper-linking to a single authoritative source is preferable to creating copies that are not updated with revisions to the master.

If presenting "Left-Right" dual-language slides, ensure the presenting software can support both language character sets.

Pages should be designed to render similarly on different web browsers (Microsoft Internet Explorer, Firefox, Chrome, etc.)

It may be desirable to distinguish "information current as of" and "reviewed on" dates for slide presentations and documents.

D.10 Functional Accounts

[33] Edward Tufte (http://www.edwardtufte.com/tufte/) is a long-standing authority on the effective presentation of information, and has published works speaking directly to these issues.

Functional accounts, or e-mail lists such as “J3_Civil Affairs” can be physically established on e-mail servers or collaborative tool suites. They are oriented to specific functions or offices so that multiple people may use it. These accounts are difficult to trace for accountability purposes; to meet information assurance requirements on DOD networks, it may be necessary to establish mitigating measures such as a watch bill that ensures accountability of activity to specific personnel. The command’s Information Assurance office can provide additional information.

Sub-Annex E: Sample Template for Establishing UIS Portal

This annex provides details of a template UIS portal site that is described in Chapter 3. It is presented here only as a set of individual capabilities within the larger UIS environment. It is intended to be a starting point for developing a JTF mission-specific UIS portal that can be used to share information with partners outside the DOD. It is not meant to be prescriptive but demonstrates a collection of current best practices available in the HA/DR community.

In developing the template, other portals and reference documents were reviewed. The list below details some of those sources. The template was also reviewed by APAN knowledge managers.

- USEUCOM OPT site
- Japan Earthquake APAN site
- https://community.apan.org/hadr/japan_earthquake/p/dependents.aspx
- Libya Crisis APAN site
- https://community.apan.org/apcn/lhac/
- Haiti APAN site and lessons learned
- Other lessons learned documents
- Department of State Humanitarian Information Unit (HIU) experience
- EUCOM Exercise “X24”
- United Nations Office for the Coordination of Humanitarian Affairs (UNOCHA)
- Intellipedia/Intellink

When required, this template should be used to coordinate between the OPT chief and the KM manager as the basis for organizing and sharing unclassified information. Modifications to the template can be made as required for the specific sharing environment. The Information Manager (IM) shall produce and conduct informal staff training on the use of the portal.

E.1 UIS Portal Template

The homepage of the template site should create a visual snapshot of everything that is available on the site. It should be visually appealing, and offer users straightforward access to its primary links via “buttons” or informative short sentences. This annex will outline many of the tools that can be incorporated into a basic portal template.

Each section of the template is discussed below.

E.2 Title Banner

Purpose – The title banner should provide a descriptive icon, title and short description of purpose of the Site.

Business Rule(s) – Icon, title, and description should capture the intent of operation and information sharing environment. Remember: this is the first thing a visitor will learn about this site; make it clear and understandable.

E.3 Site Navigation Bar

Figure M-E-1 depicts a sample site navigation bar.

Figure M-E-4 – Site Navigation Bar

Purpose – The Site Navigation Bar provides a simple visual aid in user navigation. It uses the familiar iPhone style buttons, with both text and graphical icons to direct the user to site’s major capabilities. The selected capability should be surrounded with a black border and have black text. The other buttons will have no border and grayed out text.

Business Rule(s) – Click on the capability button to navigate to each capability.

E.4 Quick Launch Links

Purpose – The quick launch links aid new and existing users to easily navigate to the most frequently visited areas of the site by task type, written out in a simple sentence or statement. Users do not need to know which larger capability area that the task is under. The link will take them directly to the capability that supports the task they are trying to perform. It may also include links to outside resources and support areas.

Business Rule(s) – Simply click on the task that needs to be performed.

E.5 RSS Links

Purpose –RSS feeds ("Real Simple Syndication") allow the user to have access to the latest news and content to help provide for situational awareness. RSS feeds may be modified to reflect current topical needs (i.e., feed from a local newspaper). Links can include a direct connection to the contents of the originating site for further information.

Business Rule(s) – The user can select the RSS feeds of interest that are being pulled into the site. The user can also push information to social media sites or another organizations portal via an approved RSS.

E.6 Purpose Statement

Purpose – The purpose statement provides a clear, written description of the identity for your site that will show potential members what your group is about. It will also help to remind your current group members and site visitors of the focus of the information sharing effort. The prose can be modified to any topical need.

Business Rule(s) – Always include a prominently positioned purpose statement that identifies your site's focus.

E.7 Low Bandwidth Link

Purpose – A low bandwidth link can direct low bandwidth (DIL) users to a limited rich content site. It can be used by both mobile and disadvantaged PC users.

Business Rule(s) – Use low the bandwidth site when the data rate of a full-featured site is not feasible. Planners will need to coordinate to make an intentional decision on the types and volume of information available in a DIL environment. Such information may include refugee SITREPs, other official SITREPs, postings from other partners, etc. Subject matter availability should be tailored to the specific operation.

E.8 Group Activity

Purpose – A group activity section is an ongoing listing of group actions within the site that is constantly updated by new entries from the designated range of users. It provides users with awareness of what others are doing on the website. Group activity will include the posting of documents, entries or commentary on blogs, wikis, or forums. It also includes and introduces the group to new members.

Business Rule(s) – Users can use the group activity to monitor the latest action found on the site. Links in the group activity list can be used to connect directly to the location of the activity listed.

E.9 Adobe Connect Online (ACO)

Purpose – an ACO link enables the group to host topically-based virtual meetings using voice, chat, video, white board, and slide presentations. It provides the user a direct connection to the available Adobe Connect Online capabilities. Other similar links can be included, as appropriate.

Business Rule(s) – Use the Adobe Connect links to access group or to hold topically-based virtual meetings.

E.10 Weather

Figure M-E-2 depicts a basic link to local weather.

Figure M-E-2 – Weather

Purpose – A weather box can be configured by the site owner to provide the latest regionally based weather based on need. It will provide the user with local weather awareness and can be modified to any locality. The temperature can be displayed in both Celsius and Fahrenheit.

Business Rule(s) – Display weather for areas of interest for your operation on the home page. Include, if available, an hour-to-hour forecast and 5-day forecast (as a link if needed, to save space on the homepage).

E.11 Group Members

Purpose – The group members section provides the user with a quick sampling of fellow group members. By clicking "More" the user can search for other users by first or last name, or by role, in order to find users to become colleagues, and gain group member awareness.

Business Rule(s) – The group members section should be easily accessible to other group members to facilitate social networking. Users will use the group members section to search for colleagues and fellow users to facilitate chat.

E.12 Social Media

M-E-3 depicts the link for social media and RSS feeds.

Figure M-E-3 – Social Media

Purpose – The social media area provides links to Facebook, Twitter, and RSS sites.

E.13 Situation Report Blog

Purpose – The situation report icon in the header provides a link to official status reports from the COI.

Business Rule(s) – Users should always rate the information that you have reviewed to inform other users of its relevance, accuracy, and reliability. Users will respond with comments that are topic relevant. Use tag clouds to help focus on area of interest. Users will visit the situation report area frequently to maintain SA.

E.14 Questions: Request for Information (RFI) and Request for Assistance (RFA) Forum

Purpose – The questions capability allows the user to ask topic related questions and pass on your information, knowledge or lessons learned to other partners in the community.

Business Rule(s) – Users should always rate the information that you have reviewed either questions or answers. They should respond to discussions with topic relevant replies and answer questions to assist other users. Users should tag all posts using the standard tags when possible. Users and site managers should frequently follow-up and check the status of discussions and questions that they have posted and verify that the posts have been answered. Users can both moderate and provide constructive comments to posts to keep on topic.

E.15 Files and Imagery – Media Galleries

Purpose – A "Files and Imagery" capability allows the user to post topically relevant files and images.

Business Rule(s) – The user must ensure that files that are posted are unclassified and approved for public release. Use site naming standards set forth by the managing KM. A basic standard would include site name, date, and a short descriptive title. Users should tag all posts using standard tags when possible. Complete all information requested by the upload utility, such as secondary file names and file descriptions.

E.16 Document Collaboration Wiki

Purpose – The document collaboration provides a place for multiple people to collaborate on a document.

Business Rule(s) – There should be a moderator that is monitoring all collaboration on a particular document to avoid people working on the same document and overwriting other peoples' changes. Users should coordinate the portions of a document on which they are working. Documents should be broken into logical, manageable sections so that multiple people can work on different sections at the same time.

E.17 Map View User of Defined Operational Picture (UDOP)

M-E-4 depicts the link for the map view UDOP.

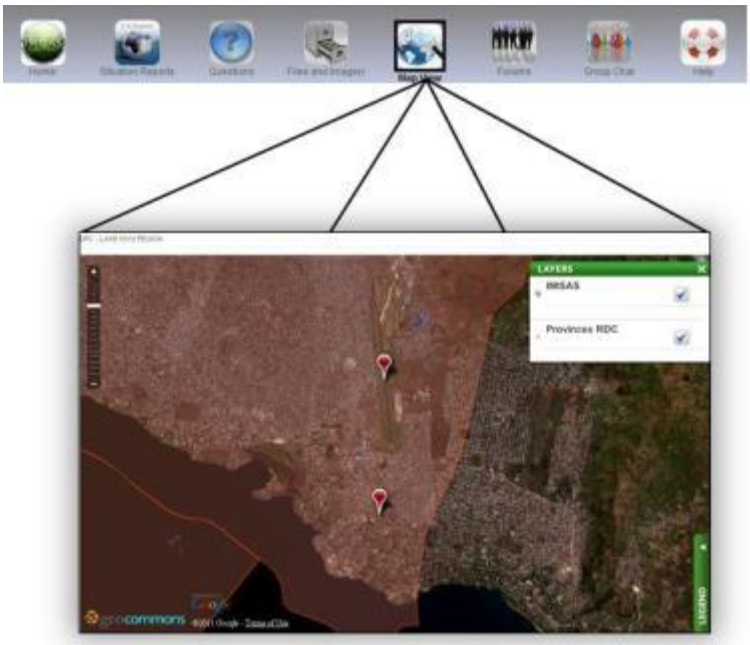


Figure M-E-4 – Map View of User Defined Operational Picture (UDOP)

Purpose – The map view provides the venue to view information on a map. Any geospatial data can be viewed on as icons on the map in order to provide graphical situational awareness.

E.18 Group Chat

Purpose – The group chat feature provides the capability to communicate with fellow group members in a common meeting place. Conversations are exportable by any group member. Be aware that conversations are not anonymous.

Business Rule(s) – Limit conversations to topically based discussions. The moderator should change topic headings, as required. Export the chat contents on a regular basis to ensure that the chat window remains current.

E.19 Other Business Rules

E.19.1 Daily Recommended Business Rules

1) Read the latest status – usually found front and center on the home page.

2) Visit content posts of interest.

3) Review the latest situation reports (SITREPS) and available geospatial information (UDOP) to increase SA. Use tag clouds to help focus on areas of interest.

4) Open the group chat capability to review and join discussions within the COI.

5) Review the latest questions and reply to those relating to your expertise. Post questions as applicable.

E.19.2 Graduated User Accounts

If necessary, a website portal can be structured to provide for varying levels of site access, dependent on confirmation of identity, trust ratings, or other values. A basic breakdown of varying access levels could be:

1) Anyone can find and view all content on the site.

2) Only registered users who are members of the group can add posts and respond to questions.

3) A restricted unclassified site is available, if needed, for information that is not being shared with everyone.

Sub-Annex F: Glossary

F.1 Acronyms and Abbreviations

ACO	Adobe Connect Online
AFSOUTH	United States Southern Command Air Component
APAN	All Partners Access Network
ATO	air tasking order
AU	African Union
AWN	Aid Workers Network
CAP	crisis action planning
CARE	Cooperative for Assistance and Relief Everywhere
CDC	cross-domain cell
CDHAM	Center for Disaster and Humanitarian Assistance Medicine
CMCS	Civil-Military Coordination Section
COA	course of action
COCOM	combatant command
COI	community of interest
COMESA	Common Market for Eastern and Southern Africa
CRS	Catholic Relief Services
CUI	controlled unclassified information
DAA	designated accreditation authority
DART	Disaster Assistance Response Team
DDR	disarmament, demobilization and reintegration
DEC	Disasters Emergency Committee
DIL	disconnected intermittent low-bandwidth
DODAF	DOD architectural framework

DOS	Department of State
DRC	Democratic Republic of Congo
EAC	African Economic Community
ECA	Economic Commission for Africa
ECCAS	Economic Community of Central African States
ECHO	European Community Humanitarian Office
ECOWAS	Economic Community of West African States
EU	European Union
FAO	Food and Agriculture Organization
FDO	foreign disclosure officer
FOIA	Freedom of Information Act
FOUO	for official use only
GIS	geographical information system
HA/DR	humanitarian assistance and disaster relief
HDPT	Humanitarian and Development Partnership Team
HEWSweb	Humanitarian Early Warning Service
HIC	humanitarian information centers
HIU	humanitarian information unit
HLA	Humanitarian Logistics Association
HN	host nation
HPN	humanitarian practice network
HTTP	hypertext transfer protocol
ICRC	International Committee of the Red Cross
ICVA	International Council of Voluntary Agencies
IER	information exchange requirements
IFRC	International Federation of Red Cross and Red Crescent Societies

IGAD	inter-governmental authority on development
IGOs	inter-governmental organizations
IM	information manager
IMC	International Medical Corps
InterAction	American Council for Voluntary International Action
IOs	international organizations
IRIN	integrated regional information networks
JP	joint publication
JTF	joint task force
KM	knowledge management
LNO	liaison officers
MINUSTAH	United Nations Stabilization Mission in Haiti
MMS	multi-media messaging
MRXs	mission rehearsal exercises
MSF	Médecins Sans Frontiéres
NEIC	National Earthquake Information Center
NEPAD	New Partnership for Africa's Development
NEPARC	New Partnership for African Red Cross and Red Crescent Societies
NGDC	National Geophysical Data Center
NGOs	non-governmental organizations
NIPRNet	Non-classified but Sensitive Internet Protocol Router Network
NOAA	National Oceanographic and Atmospheric Administration
OCHA	Office for the Coordination of Humanitarian Affairs
OFDA	Office of Foreign Disaster Assistance
OMA	Office of Military Affairs

OPORD	operational order
OPSEC	operational security
OPT	Operational Planning Team
OSAA	Office of the Special Adviser on Africa
OSCE	Organization for Security and Co-operation in Europe
OSOCC	On-Site Operations Coordination Centre
OV-3	operational view 3
Oxfam	Oxford Committee for Famine Relief
PAO	public affairs officer
PCCIP	President's Commission on Critical Infrastructure Protection
.pdf	portable document format
PRM	population, resources and migration
RFA	request for assistance
RFI	request for information
RSS	really simple syndication
SA	situational awareness
SADC	Southern African Development Community
SBU	sensitive but unclassified
SIPRNet	Secure Internet Protocol Router Network
SITREPs	situation reports
SMS	short message service
SMTP	simple mail transfer protocol
UDOP	user defined operational picture
UIS	unclassified information sharing
UISC	UIS capability
UK	United Kingdom

UN	United Nations
UNDAC	UN Disaster Assessment and Coordination
UNDHA	UN Department of Humanitarian Affairs
UNDP	UN Development Program
UNDP	UN Development Programme
UNHCR	UN High Commissioner for Refugees
UNICEF	UN Children's Fund
UNOCHA	UN Office for the Coordination of Humanitarian Affairs
UNODIR	unless otherwise directed
USAID	United States Agency for International Development
USG	U.S. Government
USSOUTHCOM	United States Southern Command
USUHS	Uniformed Services University of the Health Sciences
VOICE	Voluntary Organizations in Cooperation in Emergencies
VOIP	voice-over internet protocol
WCC	World Council of Churches
WFP	World Food Programme
WHO	World Health Organization
XMPP	extensible messaging and presence protocol

F.2 Terms and Definitions

Combatant Command. A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (JP 5-0)

Combatant Commander. A commander of one of the unified or specified combatant commands established by the President. (JP 3-0)

Federated. Interoperable, such that appropriate interfaces have been implemented among the work sites to facilitate the transfer of information. These interfaces could be effected at the application level through the use of compatible software or the use/establishment of translation tables or ontology's. At the networking level, this could be effected through protocol translation.

Web references:

PC Magazine definition: "Connected and treated as one. See federated database and federated directories." (http://www.pcmag.com/encyclopedia_term/0,2542,t=federated&i=43082,00.asp)

Federated Database. A collection of databases that are treated as one entity and viewed through a single user interface."

Webopedia Definition (http://www.webopedia.com/TERM/F/federation.html): "In instant messaging, federated IM networks are those that allow communications across different IM clients and platforms, similar to the way e-mail allows people to communicate regardless of which e-mail client they choose to use. Federated IM networks are those which maintain an open directory that allows other IM networks to message their users.

Many federated IM networks communicate using an open standard, such as Jabber/XMPP. IM Networks using XMPP provide open communications with other XMPP-based networks. Some federated networks work on the basis of interoperability where the software from two or more vendors share data between the different proprietary platforms."

Foreign Disaster Relief. Prompt aid that can be used to alleviate the suffering of foreign disaster victims. Normally it includes humanitarian services and transportation; the provision of food, clothing, medicine, beds, and bedding; temporary shelter and housing; the furnishing of medical materiel, and medical and technical personnel; and making repairs to essential services. (JP 3-29)

Foreign Humanitarian Assistance. Department of Defense activities, normally in support of the United States Agency for International Development or Department of State, conducted outside the United States, its territories, and possessions to relieve or reduce human suffering, disease, hunger, or privation. (JP 3-29)

Humanitarian Assistance. Programs conducted to relieve or reduce the results of natural or manmade disasters or other endemic conditions such as human pain, disease, hunger, or privation that might present a serious threat to life or that can result in great damage to or loss of property. Humanitarian assistance provided by U.S. forces is limited in scope and duration. The assistance provided is designed to supplement or complement the efforts of the host nation civil authorities or agencies that may have the primary responsibility for providing humanitarian assistance. (JP 3-57)

Humanitarian and Civic Assistance. Assistance to the local populace provided by predominantly U.S. forces in conjunction with military operations and exercises. This assistance is specifically authorized by title 10, United States Code, section 401, and funded under separate authorities. Assistance provided under these provisions is limited to (1) medical, dental, and veterinary care provided in rural areas of a country; (2) construction of rudimentary surface transportation systems; (3) well drilling and construction of basic sanitation facilities; and (4) rudimentary construction and repair of public facilities. Assistance must fulfill unit training requirements that incidentally create humanitarian benefit to the local populace. (JP 3-29)

Information Sharing. Making information available to participants (people, processes, or systems). Information sharing includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant. (DOD ISIP)

Inter-governmental Organization. An organization created by a formal agreement (e.g., a treaty) between two or more governments. It may be established on a global, regional, or functional basis for wide-ranging or

narrowly defined purposes. Formed to protect and promote national interests shared by member states. Examples include the United Nations, North Atlantic Treaty Organization, and the African Union. (JP 3-08)

Joint Task Force. A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a sub-unified commander, or an existing joint task force commander. (JP 1)

Mission Partner. External partners as defined in the DOD Information Sharing Strategy: Federal, State, local, tribal, coalition partners, foreign governments and security forces, IOs, NGOs, and the private sector. (DOD ISIP)

Multi-national. Between two or more forces or agencies of two or more nations or coalition partners. (JP 5-0)

Non-governmental Organization (NGO). A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging the establishment of democratic institutions and civil society. (JP 3-08)

Sub-Annex G: Bibliography

Assistant Secretary of Defense for Command, Control, Communications and Intelligence: Department of Defense REGULATION 5200.1-R; *Information Security Program*; Washington, DC (January 14, 1997)

Department of Defense DIRECTIVE 5230.09; *Clearance of DOD Information for Public Release*. Washington, DC (August 22, 2008)

Department of Defense DIRECTIVE 5230.11; *Disclosure of Classified Military Information to Foreign Governments and International Organizations*. Washington, DC (June 16, 1992)

Department of Defense INSTRUCTION 5200.01, incorporating Change 1: *DOD Information Security Program and Protection of Sensitive Compartmented Information*. Washington, DC (June 13, 2011)

Department of Defense INSTRUCTION 5230.29; *Security and Policy Review of DOD Information for Public Release*. Washington, DC (January 8, 2009)

Deputy Director, Joint Staff J-36: *Unclassified Information Sharing Capability (UISC) Concept of Operations*. Washington, DC (15 November 2010)

Haimes, Yacov Y; Kaplan, Stan; and Lambert, James H.: *Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling*. Society for Risk Analysis; McLean, Virginia. Risk Analysis, Volume 22, No. 2, (2002)

United States Agency for International Development; *Economic Growth, Agriculture & Trade (EGAT); Bureau Primer*. Washington, DC (2007)

Lake, Anthony; Whitman, Christine Todd; et al: *More than Humanitarianism; A strategic U.S. Approach Toward Africa.* Council on Foreign Relations, Independent Task Force Report No. 56. New York (2006)

Aall, Pamela: Miltenberger, Lt. Col. Daniel; Weiss, Thomas G: *Guide to IGOs, NGOs and the Military in Peace and Relief Operations*. United States Institute for Peace, Washington, DC. (2000)

Center for Law and Military Operations; *U.S. Government Interagency Complex Contingency Operations Organizational and Legal Handbook*. The Judge Advocat General's Legal Center and School, United States Army. Charlottesville, Virginia (24 February 2004)

Perito, Robert M. (Ed.); *Guide for Participants in Peace, Stability and Relief Operations.* United States Institute for Peace, Washington, DC (2007)

Joint Publication 3-08: *Interagency, Inter-governmental Organization, and Nongovernmental Organization Coordination during Joint Operations, Volumes 1 & 2*; Joint Staff, Washington, DC, 17 March 2006.

Case Study; *USSOUTHCOM and JTF-Haiti; Some Challenges and Considerations in Forming a Joint Task Force*. US Joint Forces Command Joint Center for Operational Analysis. Suffolk, VA (24 June 2010)

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project

Annex N1 - Unclassified Information Sharing (UIS) Overview and Summary Information All Viewpoint (AV) – 1

Table of Contents

1. ARCHITECTURE DESCRIPTION IDENTIFICATION N-1

1.1 Introduction N-1
1.2 Task N-1
1.3 General Information N-1
1.4 Background N-2
1.5 Status N-3
1.6 Facts, Assumptions, and Constraints N-3
1.7 Level of Effort N-4

2. SCOPE N-5

2.1 Architecture Deliverables N-5
2.2 Other Deliverables N-6
2.3 Time Frame N-7
2.4 Organizations Involved N-7

3. PURPOSE AND VIEWPOINT N-7

3.1 Purpose N-7
3.2 Viewpoint N-8
3.3 Architecture Time Frame N-8
3.4 Organization N-8

4. CONTEXT N-9

4.1 Operational Concept "As-Is" N-9
4.2 Vision N-11
4.3 Operational Capabilities N-12
4.4 Joint Capability Area N-13
4.5 Mission Area Analysis N-13
4.6 UIS Architecture Construct N-14
4.7 Approach N-14
4.8 Linkages to Other Architectures N-14

5. TOOLS AND FILE FORMATS N-14

5.1 Tools N-14
5.2 File Formats N-15
5.3 Repository NN-15

6. FINDINGS N-15

List of Figures

Figure N1-1 – Model for Coordination Between Stakeholders Organizations for Foreign Support N1-9
Figure N1-2 – "As-Is" OV-1 High-Level Operational Concept Graphic N1-10
Figure N1-3 – "To-Be" OV-1 High-Level Operational Concept Graphic N1-11

List of Tables

Table N1-1 – General Architecture Information N1-2
Table N1-2 – Architecture Deliverables N1-5

1. Architecture description identification

1.1 Introduction

This overview and summary of the Unclassified Information Sharing (UIS) architecture identifies the architecture task and provides general information on the effort. It describes the scope, purpose and perspective while providing the context for the architecture. It also identifies the tools and file formats used for the architecture description and includes a high-level discussion of findings and a way ahead. Additional findings with analysis are provided following the completion of the architecture description.

1.2 Task

The task is to design and develop a UIS architecture describing both "as-is" and "to-be" conditions. The context for the "as-is" architecture is that combatant commanders (CCDRs) "lack a coherent capability to share information and collaborate across multiple domains with a broad range of mission partners (government/interagency, multi-national, multi-lateral and private sector) due primarily to restrictive policies, conflicting authorities, ineffective procedures and non-interoperable networks and systems."[1] The "to-be" architecture describes essential multi-level information sharing capabilities in a federated system to include the business rules, processes, procedures, roles and responsibilities to operate in the UIS environment. The "to-be" architecture will reflect capabilities outlined in the *Unclassified Information Sharing Capability (UISC) Concept of Operations*,[2] and logically derived or experimentally validated solutions derived from mature focus areas of the *Department of Defense Information Sharing Implementation Plan*[3] that are expected to be implemented in the near-term (less than 5 years).

The UIS architecture is scoped to be "fit-for-purpose" (i.e., responsive to the goals and objectives of the process owner, useful in the decision-making process, and responsive to internal and external stakeholder concerns) and, in accordance with guidance for architecture federation, does not duplicate or replace any related Department of Defense (DOD) architectures.[4]

1.3 General Information

[1] Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) experimentation project problem statement.
[2] United States Joint Chiefs of Staff, J-3, *Unclassified Information Sharing Capability (UISC) Concept of Operations*, 10 November 2010.
[3] OASD/NII, *Department of Defense Information Sharing Implementation Plan*, April 2009.
[4] DOD-CIO, *The Department of Defense Architecture Framework (DODAF) Version 2.0, Vol. 1: Introduction, Overview, and Concepts*, 28 May 2009.

Table N1-1 – General Architecture Information

Name	Information
Short Name	UIS Architecture
Organization Developing the Architecture Products	Joint Staff J7, JCW, IMISAS Project Team
Completion Date	September 2011
Approval Authority	Deputy Director, Joint Staff, J7
Chief Architect	Ms. Kathryn Smith, IMISAS Project Lead
Point of Contact	Ms. Kathryn Smith, IMISAS Project Lead (757-203-5322, DSN 668-5322) kathryn.smith@hr.js.mil
Architecture Classification and Handling Caveats	Unclassified

1.4 Background

In order to perform the range of military operations most effectively, there is a critical need for interaction and cooperation between the U.S. Government (USG), foreign government agencies and militaries, intergovernmental organizations (IGOs), regional organizations, nongovernmental organizations (NGOs) and the public and private sectors. In the current operational environment, the conduct of mission operations requires that CCDRs engage a dynamic set of extended partners and stakeholder participant organizations, in person, via e-mails or dispatches and more frequently, via the Internet. Responding to mission challenges requires effective situational awareness, communication, coordination, and virtual collaboration among the myriad of participants. These organizations must identify information exchange requirements to obtain relevant information to answer these, as well as when and how to share the information routinely to plan and execute operations for mission success. The UISC is an initial DOD capability to serve as a key information sharing enabler in support of enhanced unity of effort in planning and

execution of missions, and is envisioned to be available for use by other USG lead federal agencies for collaborative efforts.[5]

Combatant commands (COCOMs) require the capability to share essential information with interagency partners, coalition and alliance partners, emerging partner nations in bi-lateral or multinational efforts, nongovernmental organizations and members of the public and private sector that may be active in a related mission or geographical area. The following factors have been identified as preventing the achievement of full capability:

- restrictive network access and information sharing policies
- restrictive and cumbersome accreditation procedures for coalition networks and systems
- lack of a coherent strategy for a whole of government approach to an information sharing, collaborative environment
- lack of resourcing to support a UIS environment and its associated network enterprise services[6]

1.5 Status

The UIS Architecture is projected to be developed in steps, "as-is" followed by the "to-be", with final deliverables projected in the September 2011 timeframe. All deliverables and viewpoints are based on information from official documents supplemented with interviews with subject matter experts.

- **Step 1 -** Develop UIS all viewpoint-1 (AV-1) and high-level operational concept graphic (OV-1) on the present "as-is" unclassified information sharing concept. Develop an initial draft "To-Be" OV-1.

- **Step 2 -** Develop viewpoints for the "to-be" unclassified information sharing based on logically derived or experimentally validated solutions developed in coordination with combatant commander stakeholders.

1.6 Facts, Assumptions, and Constraints

Primary overarching assumptions and constraints are provided here. Additional assumptions and constraints relevant to specific architecture products and analyses are included in those deliverables.

[5] United States Joint Chiefs of Staff, J-3, *Unclassified Information Sharing Capability (UISC) Concept of Operations*, 10 November 2010, p. 3.
[6] USAFRICOM/USEUCOM Warfighter Challenge 2010.

- Fact - Success in theater security cooperation, stabilization and humanitarian assistance/disaster relief (HA/DR) missions depends on sustained and habitual information sharing and the ability to collaborate across domains and among actors supporting these missions. COCOMs lack a coherent framework and capability to share information and collaborate across multiple domains with a broad range of mission partners and stakeholder participants in the international community (government/interagency, multinational, and private sector) due primarily to restrictive policies, conflicting authorities, ad hoc/non-existent procedures, and non-interoperable networks/systems. Without the ability to share information that would enable collaboration, critical opportunities are lost due to the inability to harmonize collective efforts.
- Assumption - The development of ad hoc solutions during a crisis response compounds the problem. These situation based solutions do not foster the development of habitual relations that build trust and enable enduring information sharing and collaboration. Non-interoperable networks fail to consider the needs of disconnected, interrupted, and low-bandwidth (DIL) users and a proliferation of specialized systems have atomized, rather than integrated, information sharing, thus hampering habitual coordination and collaboration.
- Assumption - Standard processes, and associated policies and procedures, are critical to effective information sharing and collaboration across organizational and domain boundaries.
- Constraint - Effective UIS solutions should reflect a consensus of USG, multinational, multilateral, academic and private sector organizations in addressing the impact of human, cultural, policy, process and procedural factors on information sharing and collaboration among actors operating in a broad range of mission settings.
- Constraint - Any UISC should leverage related efforts and fully support information sharing, cooperation, coordination and collaboration between DOD and non-military mission partners.

1.7 Level of Effort

The UIS Architecture is being developed as a series of products. Each product is DOD Architecture Framework (DODAF) compliant and adds detail to previous versions as information becomes available. Upon completion, this architecture will transition to the Joint Staff, J8.

2. Scope

The scope of the UIS Architecture is to capture processes and procedures (activities) with their associated resources and information (produced and consumed) to achieve mission effectiveness during a HA/DR effort.

2.1 Architecture Deliverables[7]

The AV, OV, and Systems Viewpoint (SV) models and views[8] are described in Table N1-2. This list of architecture models and views ensures accurate depiction of the UISC and related processes and procedures. Final delivery of the architecture views are projected to be delivered in September 2011.

Table N1-2 – Architecture Deliverables

Models	Short Name	File Format/Description
Overview and Summary Information	AV-1	Word Document The overarching document guiding the architecture effort. It defines tasking, status, assumptions, scope, purpose, context, tools, findings and analysis.
Integrated Dictionary	AV-2	Excel Workbook Definition of activities, organizational performers (nodes)[9], information exchanges, and systems information.

[7] This section reflects new terminology provided in DODAF V 2.0. The description of the models in Table N1-2 reflects the tailoring of the standard DODAF V 2.0 models so that the resulting views meet project objectives for the UIS Architecture.

[8] Per DODAF V 2.0, a model is a template for collecting data and a view is a representation of specific data in either a defined DODAF model or any other understandable format.

[9] DODAF 2.0 no longer uses the term "node" and instead uses the term "performer" as the "who" in the architecture description. DODAF 2.0 defines performer as "Any entity - human, automated, or any aggregation of human and/or automated - that performs an activity and provides a capability." [DODAF 2.0 , Vol 1, p. 76] The term "node" continues to be used within the UISC Architecture deliverables since this architecture's customers are familiar with the term and understand its use in the context of the architecture. The use of "Nodes" also supports federation efforts.

Models	Short Name	File Format/Description
High-Level Operational Concept Graphic	"As-Is" & "To-Be" OV-1	Word Document High-level graphical/textual description of the operational concept.
Operational Resource Flow Description	OV-2 (Traditional)	PowerPoint Graphics Description of the operational resource flows (needlines) exchanged between organizational performers (nodes).
Operational Resource Flow Matrix	OV-3	Excel Spreadsheet Resource exchanged and the relevant attributes of that exchange.
Organizational Relationships Chart	OV-4	Word Document Organizational context, role, or other relationships among organizations.
Operational Activity Decomposition List	OV-5a (modified)	Excel Spreadsheet The operational activities organized in a hierarchal list that provides a quick reference for the activities used in the OV-5b.
Operational Activity Model	OV-5b	System Architect ABM Model and Adobe Acrobat Activities, the relationships among activities, and information inputs and outputs.

2.2 Other Deliverables

None.

2.3 Time Frame

The UIS Architecture viewpoints are intended to depict near-term operations.

2.4 Organizations Involved

- USAFRICOM
- USEUCOM
- U.S. Pacific Command (USPACOM) / All Partners Access Network (APAN)
- DISA
- Joint Staff, J7
- Joint Staff, J8
- Bundeswehr Transformation Centre (Germany)
- Office of the Assistant Secretary of Defense (OASD)/ Networks and Information Integration (NII)/Chief Information Officer (CIO)
- U.S. Department of State (DOS) Humanitarian Information Unit (HIU)

3. Purpose and Viewpoint

3.1 Purpose

The DOD Architecture Framework (DODAF) v2.0 states in part:

Because architecture can be applied at myriad levels of an enterprise, the purpose or use of architecture at each level will be different in content, structure, and level of detail. In order to ensure that architecture meets program and mission objectives, the approach to architecture development must be tailored to address a specific, well-articulated, and understood purpose.

Architectures are created for a number of reasons. From a compliance perspective, DOD development of architectures is compelled by law and policy (i.e., Clinger-Cohen Act, Office of Management, and Budget (OMB) Circular A-130). From a practical perspective, the management of large organizations employing sophisticated systems, technologies, and services in pursuit of often complex joint missions demands a structured, repeatable method for evaluating investments and investment alternatives, as well as the ability to implement organizational change effectively, create new systems, deploy new technologies, and offer services which add value to management decisions and practices.

The purpose of the UIS Architecture is to:

- Support development of process, policy and procedural recommendations to encourage effective information sharing and collaboration across organizational and domain boundaries. The processes, policies and procedures will be validated through experimentation by USAFRICOM, USEUCOM, and non-DOD mission partners.
- Support "fit-for-purpose" architecture builds, use for multiple process-owners and analyses, and "fit-for-federation" architecture governance.

3.2 Viewpoint

The perspective is that of a combatant commander conducting HA/DR operations.

3.3 Architecture Time Frame

The UIS Architecture will include a set of products generated to depict "to-be" operational capabilities that will be implemented in the near-term (less than 5 years).

3.4 Organization

For the UIS architecture, the organization is based on the model contained in *Interorganizational Coordination During Joint Operations*, JP 3-08 (Figure N1-1).

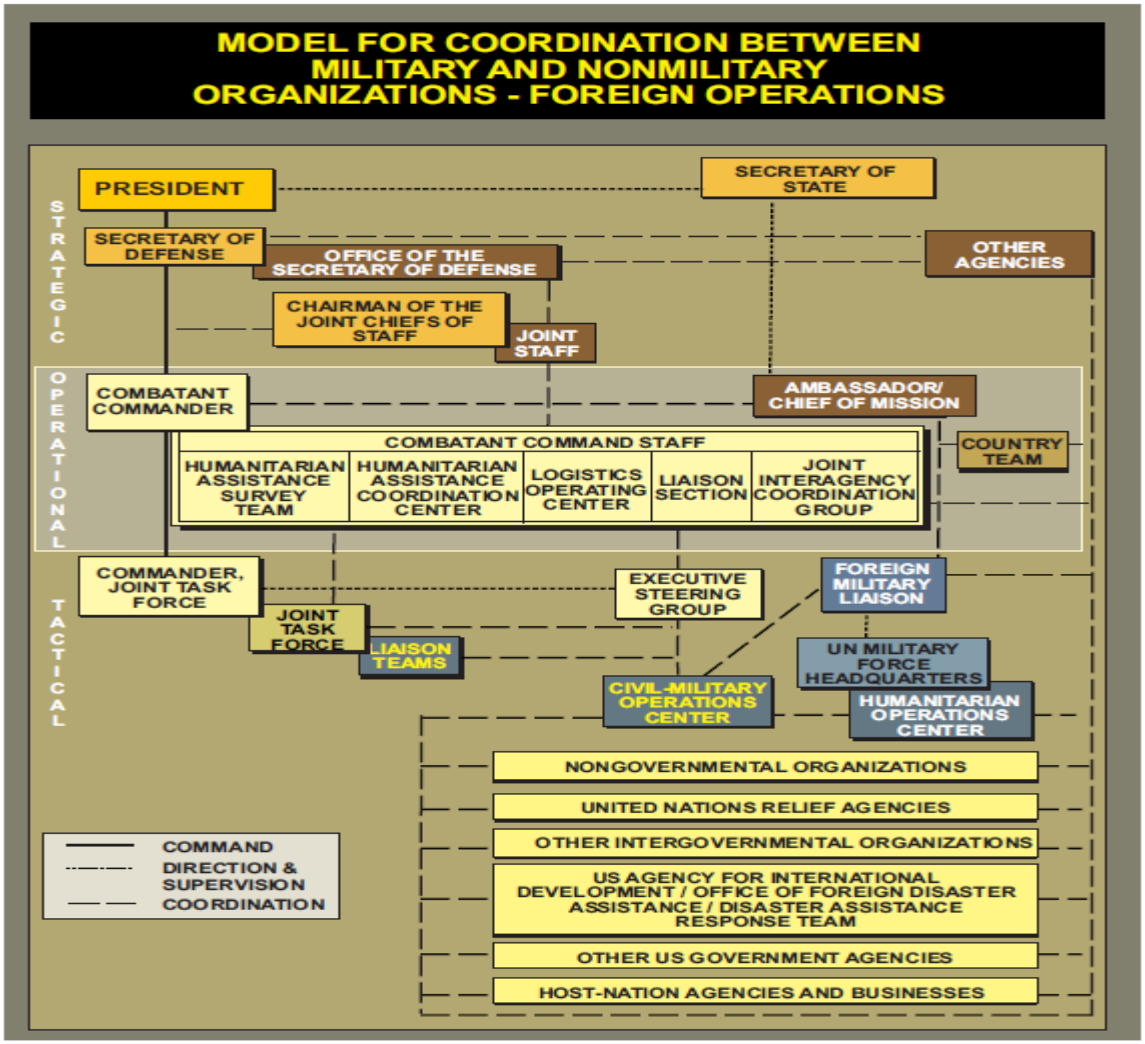


Figure N1-1 – Model for Coordination Between Stakeholders Organizations for Foreign Support[10]

4. CONTEXT

4.1 Operational Concept "As-Is"

Currently, UIS mission partners and stakeholder participant organizations face rapid and accelerating advances in information technology. Coupled with the rapid and accelerating growth of human knowledge, this proliferation of capabilities and technology choices contributes to an overwhelming UIS information overload. Policy, processes and procedures issues, such as the lack of compatible procedures and a general consensus on business rules, complicate and

[10] JP 3-08, *Interorganizational Coordination During Joint Operations*, 24 Jun 2011, Figure III-1.

inhibit effective cooperation. Strong organizational cultures, while naturally building unit, homogenous worldviews among members, tend to inhibit efforts to build trust and create a shared understanding with other organizations.

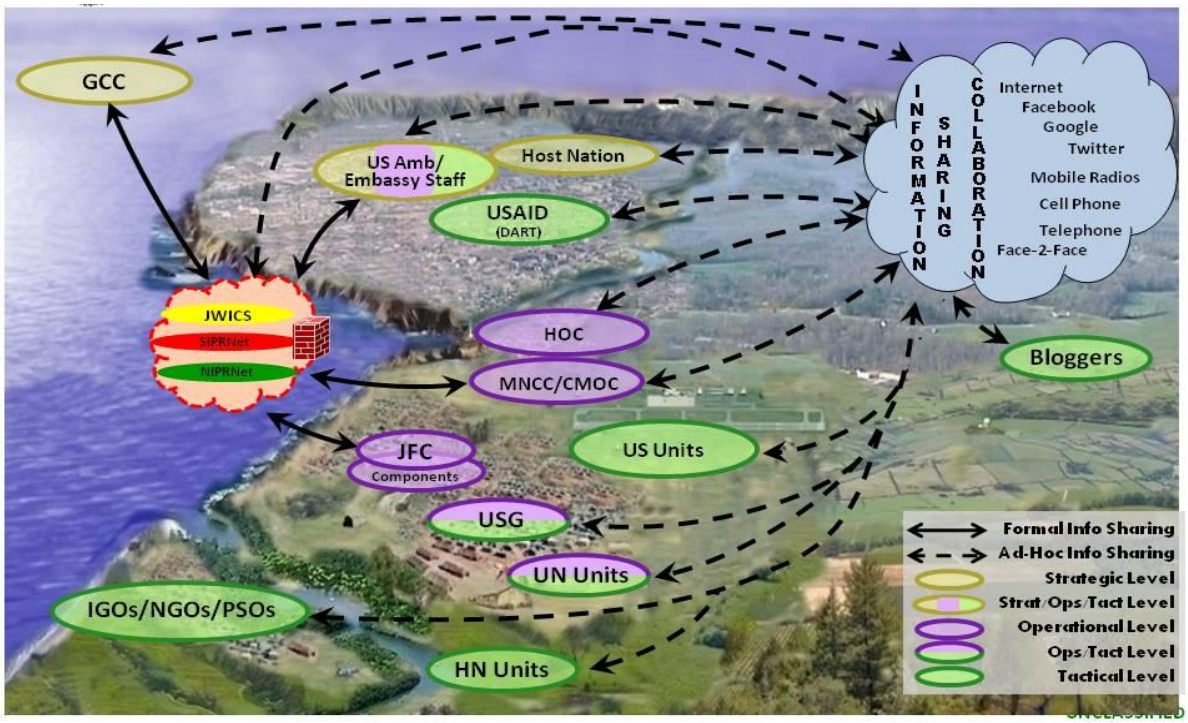


Figure N1-2 – "As-Is" OV-1 High-Level Operational Concept Graphic

The complexities of operating and sharing information with an evolving and often unfamiliar community of interest (COI) place a premium on DOD's ability to understand the nuances of potential partner and stakeholder participant organizational cultures, needs, strengths and limitations. For this architecture, the context of UIS is focused on COCOMs and their mission partners. This includes use of the UISC to facilitate information sharing and collaboration with non-DOD users. These mission partners include, but are not limited to, USG agencies, foreign governments and their militaries, IGOs, NGOs, and members of the public and private sectors involved with the same COI or mission. UIS activities will be employed at the strategic, operational, and tactical levels with the spectrum of use focused primarily on non-combat operations. These operations include HA/DR, homeland defense/defense support of civil authorities (HD/DSCA), stability, security, transition and reconstruction (SSTR), and theater security cooperation (TSC). The high level operational concept "as-is" OV-1' identifies unclassified information sharing during HA/DR operations (Figure N1-2).

Information sharing in support of HA/DR operations is not without difficulties. The challenges are formidable and involve dimensions of organizational culture, policies, processes, procedures, and technology. Information sharing is sometimes impeded by sensitivities associated with the neutrality and independent policies and processes of IGOs and NGOs, lack of cultural and social

situation awareness, the political will of participants and organizations, differences in communication and authority structures across the span of HA/DR responders, and the need to build trust and a shared understanding of expectations. Further complicating information sharing are conflicts and shortfalls in policy, doctrine, tactics, techniques and procedures. These include differing interpretation and application of security and information release policy, information management and assurance requirements, and organizational authority and resources for network management. Technical challenges include the necessity of integrating *ad hoc* and stove-piped capabilities, lack of a unifying architecture and concept of operations, large and complex problems in data management, the need to accommodate the disadvantaged user, and the need to address the problems of linguistic differences over a potentially vast set of languages and dialects.

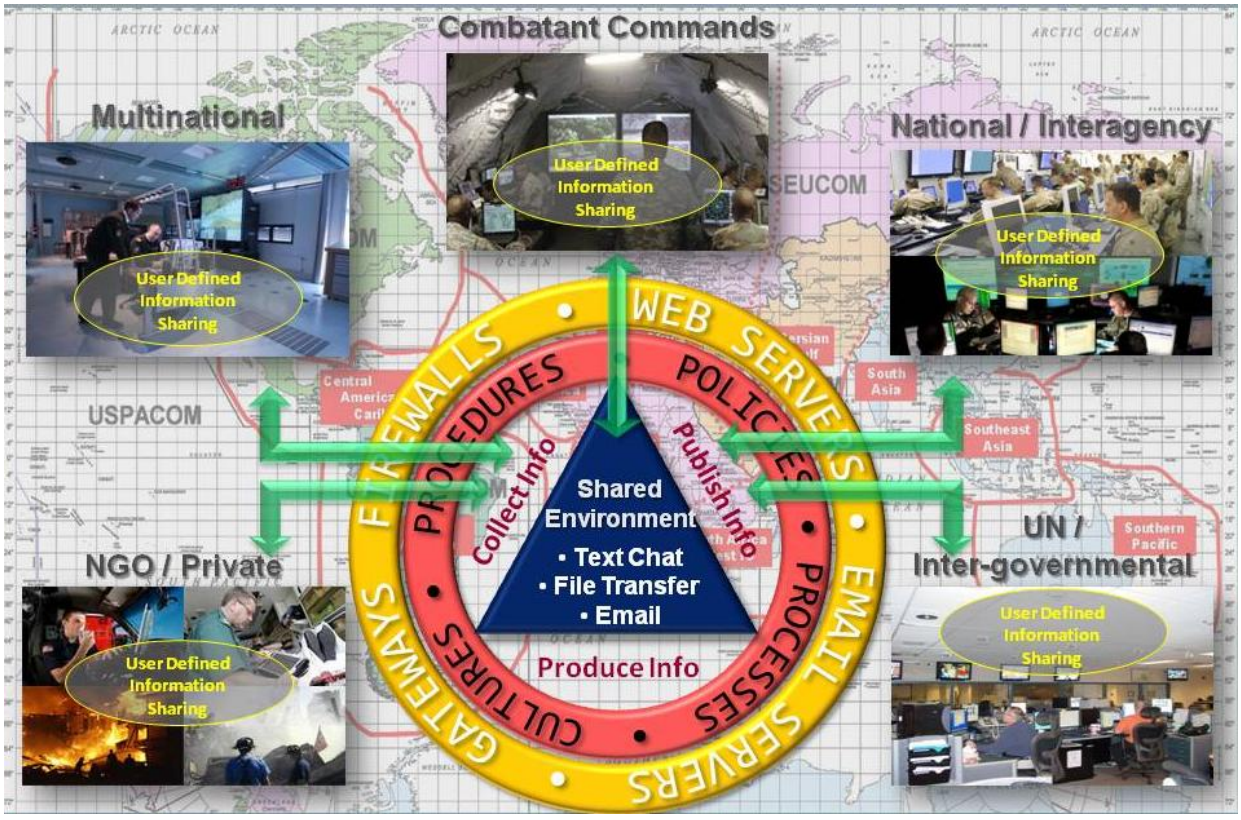


Figure N1-3 – "To-Be" OV-1 High-Level Operational Concept Graphic

4.2 Vision

Consistent with the DOD Information Sharing Implementation Plan, this architecture envisions a UIS "to-be" capability (Figure N1-3) in which "transparent, open, agile, timely, and relevant information sharing occurs to promote freedom of maneuverability across a trusted information environment."[11] Procedural recommendations for implementation of information handling and

[11] Appendix A, OASD/NII, Department of Defense Information Sharing Implementation Plan, April 2009

sharing policies mitigate obstacles caused by DOD's organizational culture, and enable a wide-ranging COI to achieve shared objectives. The establishment of an initial, enterprise level UISC supports effective sharing of unclassified information between the DOD and its various mission partners and other stakeholder participants. The "to-be" capability leverages, incorporate, and apply recent innovations and advances found in various social network sites to meet and improve mission success and effectiveness among combatant commands and their respective real and virtual communities. The "to-be" UISC is a shared enterprise service useable by all members of the DOD to facilitate information sharing with mission partners not having or wanting access to DOD networks.

4.3 Operational Capabilities

COCOMs and their mission partners and stakeholder participant organizations require an interoperable, web-based capability supporting unclassified, multi-media information sharing and collaboration to better achieve mission success. Complementing the UISC are a set of policy-based procedures and business rules enabling the COCOMs to share information, cooperate and coordinate, and collaborate with interagency, multinational, intergovernmental, nongovernmental, and broader private and public sector partners.

UIS procedures are required to govern the COCOMs' handling, storage and potential exchange of unclassified information with mission partners. These procedures mitigate culturally or infrastructure related impediments such as development and storage of unclassified information on classified networks. Business rules address the establishment and management of UISC worksites in support of information sharing and collaboration, as well as, maximizing the use of UISC tools.

The UISC is not a military-centric environment, but a DOD capability to enable relevant exchange among a wide range of mission partners and stakeholder participant organizations (Figure N1-3). This capability supports both enduring and *ad hoc* communities for a range of missions such as HA/DR, HD/DSCA and SSTR.

Technical protocols and standards follow common U.S. national, international, and industry standards to provide interoperability with existing capabilities. The UISC collaborative environment is compatible with commonly used operating systems, and the client connections are accessible through commonly used web browsers. During development, disconnected, interrupted, and low-bandwidth (DIL) considerations will be addressed. Users will be able to collaborate by employing a number of useful collaborative capabilities. At a minimum, authorized users are expected to be able to read and contribute to the COI they join.

Finally, the COCOMs need processes for engaging mission partners that are fully integrated with the standard procedures, business rules and supporting UISC. These processes should reflect the characteristics of enduring partners (e.g., U.S. agencies, IGOs) and be sufficiently flexible to accommodate ad hoc relationships with public and private partners.

4.4 Joint Capability Area

All Tier I Joint Capability Areas will be potentially affected through the operational utility of UIS.

- Force Support
- Battlespace Awareness
- Force Application
- Logistics
- Command and Control
- Net-Centric
- Protection
- Building Partnerships
- Corporate Management and Support

4.5 Mission Area Analysis

The UIS architecture focuses on the COCOM conducting HA/DR operations, but the processes and procedures are broadly applicable to other mission and general interest areas including:

- Partnership building and enhancement
- World Health issues
- Environmental Concerns/Events
- Political dynamics and instability
- Support to civil authorities/law enforcement
- Weather Events and Natural Disasters
- Conflict resolution
- Lines of Communication
- Conflict deterrence/avoidance
- WMD Proliferation
- Illicit trafficking
- Support to combat operations
- Diplomatic support
- Security (e.g., Olympics, World Cup Soccer, etc.)
- Force Protection
- Ethnic, cultural, and religious events
- Exercise/Training/Rehearsal support
- Geospatial visualization tools
- Cyber Attack
- U.S. Critical Infrastructure Attack

4.6 UIS Architecture Construct

To support the phasing of UIS Architecture development, the data collection and development of architecture deliverables is conducted in steps. Step 1 provides an "as-is" OV-1 that provides a baseline to analyze the "to-be" operational capabilities during field experimentation with United States Africa Command (USAFRICOM), United States European Command (USEUCOM), and non-DOD mission partners. The Step 2 deliverables are developed from that initial data, with concurrent data collection follow-up and development of the Step 2 "to-be" deliverables.

4.7 Approach

The UIS architecture includes current technical solutions (e.g., All Partners Access Network (APAN), HarmonieWeb) to this operational problem vice new technologies. APAN was used as a proxy during experimentation events to determine the requirements for the initial UIS capability. The approach is to leverage the initial DOD technical capability and apply appropriate procedures and business rules to elevate its usage to the enterprise level by making that capability available to all potential users. The UIS architecture concentrates on identifying processes and procedures to enhance UIS at the COCOM level but is informed by required interactions with the joint task force headquarters (JTF HQ) staff. While the UIS architecture is intended to develop processes and procedures (OV-5a/b) that apply to UIS across the spectrum of operations, an HA/DR scenario was used for experimentation and development of the "to-be" architecture.

4.8 Linkages to Other Architectures

- JTF HQ Architecture date 2007

5. Tools and File Formats

5.1 Tools

The following tools were used in the data collection, management, description, and development of the UIS "as-is" and "to-be" architectures:

- IBM®/Telelogic System Architect™ Version 11.1, Activity Based Model
- Microsoft® Office™ (Word™, PowerPoint™, Excel™)
- Microsoft® Visio™
- Adobe® Acrobat™

5.2 File Formats

File formats used by the tools listed in paragraph 5.1 comprise the minimum acceptable set of formats for collecting and exchanging information among subject matter experts and architects.

5.3 Repository

The final UIS Architecture Version 1.0 will be posted on the JS J8 repository.

6. Findings

The operational activities comprising "Provide Unclassified Information Sharing" are conducted by DOD/DISA and were not described in depth. Initially, 76 operational activities were identified to "Provide Unclassified Information Sharing" to the operational activities UIS 3.3.1 Community of Interest Environment and UIS 3.3.2 "Provide Information Sharing Services" and their sub-activities within the HA/DR scenario. Future updates of "Provide Unclassified Information Sharing" should focus on DOD/DISA operational activities.

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project

Annex N2 - Unclassified Information Sharing (UIS) Integrated Dictionary All Viewpoint (AV) – 2

Table of Contents

1. OPERATIONAL NODES (OPSNODES)..... N2-1

2. OPERATIONAL ACTIVITIES (OPSACT) N2-4

3. INFORMATION EXCHANGES (IES) N2-19

1. Operational Nodes (OpsNodes)

Name	Description	Full Name	Ref1
DISA	DOD agency tasked to develop security technical configuration and implementation validation requirements and associated expected results for IT products and services and provide automated validation capabilities to the DOD Components.	Defense Information Systems Agency	DODI 8510.01
DOD		Department of Defense	
GCC - UIS	For this architecture, opnode created to provide visibility specifically assign ops activities relating to UIS activities.	Geographic Combatant Commander - Unclassified Information Sharing	
GCCs	A commander in chief of one of the unified or specified combatant commands established by the President.	Geographic Combatant Commanders	JP 1-02
HN Units	Host Nation units (operational/tactical) assigned/tasked to support their country's HA/DR mission.	Host Nation Units	
HOC	An international and interagency body that coordinates the overall relief strategy and unity of effort among all participants in a large foreign humanitarian assistance operation. It normally is established under the direction of the government of the affected country or the United Nations, or a US Government agency during a US unilateral operation. Because the humanitarian operations center operates at the national level, it will normally consist of senior representatives from the affected country, assisting countries, the United Nations, nongovernmental organizations, intergovernmental organizations, and other major organizations involved in the operation.	Host Nation Ops Center	JP 3-29
Host Nation	A nation which permits, either by written agreement or official invitation, government representatives and/or agencies of another nation to operate, under specified conditions, within its borders.		JP 2-01.2
IGOs / NGOs / PSOs	IGO - An organization created by a formal agreement (e.g., a treaty) between two or more governments. It may be established on a global, regional, or functional basis for wide-ranging or narrowly defined purposes. Formed to protect and promote national interests shared by member	Intergovernmental Organization/Non-governmental Organization/Private Sector Organization	JP 3-08

	states. Examples include the United Nations, North Atlantic Treaty Organization, and the African Union. NGO - A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging the establishment of democratic institutions and civil society.		
JFC - UIS	For this architecture, opnode created to provide visibility specifically assign ops activities relating to UIS activities.	Joint Force Commander	JP 1
MNCC/CMOC	MNCC - A multinational coordination center that facilitates coordination and cooperation of foreign military forces with the affected nation to support humanitarian assistance and disaster relief (HA/DR) missions. CMOC - An organization normally comprised of civil affairs, established to plan and facilitate coordination of activities of the Armed Forces of the United States with indigenous populations and institutions, the private sector, intergovernmental organizations, nongovernmental organizations, multinational forces, and other governmental agencies in support of the joint force commander. An ad hoc organization, normally established by the geographic combatant commander or subordinate joint force commander, to assist in the coordination of activities of engaged military forces, and other United States Government agencies, nongovernmental organizations, private voluntary organizations, and regional and international organizations. There is no established structure, and its size and composition are situation dependent.	Multi-National Command Center/Civilian-Military Ops Center	Multinational Force (MNF) SOP; JP 3-57; JP 1-02
UN Units	UN units (operational/tactical) assigned/tasked to support a HA/DR mission.	United Nations Units	
UNOCHA	UNOCHA is a coordinating body that pulls together the efforts of numerous humanitarian/relief organizations and is the vehicle through which official requests for military assistance are normally made.	UN Office for the Coordination of Humanitarian Affairs	JP 3-08
US Amb/Embassy Staff/COM	The ambassador is the personal representative of the President to the government of the foreign country or to the IGO to which he or she is accredited and, as such, is the Chief of Mission (COM), responsible for recommending and	US Ambassador/Embassy Staff/Chief of Mission	JP 3-08

	implementing national policy regarding the foreign country or IGO and for overseeing the activities of USG employees in the mission. The ambassador has extraordinary decision making authority as the senior USG official on the ground during crises. COM - Has authority over all USG personnel in country, except for those assigned to a combatant command, a USG multilateral mission, or an IGO. The COM provides recommendations and considerations for crisis action planning directly to the geographic combatant commander (GCC) and commander of a JTF (Joint Force Commander (JFC)). While forces in the field under a geographic combatant commander are exempt from the COM's statutory authority, the COM confers with the combatant commander regularly to coordinate US military activities with the foreign policy direction being taken by the USG toward the host country. The COM's political role is important to the success of military operations involving the Armed Forces of the United States. Each COM as a formal agreement with the geographic combatant commander as to which DOD personnel fall under the force protection responsibility of each. The Mission Disaster Relief Officer (MDRO) is appointed by the COM and is the focal point at post for disaster-related information, planning, and activities affecting the host country. The MDRO should be a regular member of the post's Emergency Action Committee (EAC) and is responsible for preparing and maintaining Annex J of the Emergency Action Plan (EAP), entitled Assistance to Host Country in a Major Accident or Disaster. The MDRO serves as the incident commander for Annex J and ensures that post personnel are familiar with its contents. This section of the EAP is also referred to as the Mission Disaster Relief Plan.		
USAID	The USG agency that maintains the most direct relationship with NGOs, many of which receive USAID funding to carry out programs.	US Agency for International Development	JP 3-08
USG		US Government	

2. Operational Activities (OpsAct)

Name	Description	Ref1	Ref2	Ped1	Ped1 Detail
UIS 1.0 Provide for UIS	This activity includes acquiring, managing, and sustaining UIS assets and their associated needs in support of providing UIS capabilities. This enables consumers to use the services and agencies to manage them. This activity includes the full range of support throughout an UIS Asset lifecycle.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.0 Perform UIS Mgmt	This activity consists of the planning, organizing, coordinating, and controlling the establishment, maintenance, and dissolution of all the capabilities of and services provided by the UIS environment. It comprises the development of the environment's capabilities, the management of its system and network configurations, as well as the conduct of its administration, monitoring, and response activities. It also consists of performance of all UIS activities necessary to manage and protect the flow of information within the information environment. These activities are performed by UIS Personnel. It takes functional and operational performance requirements as inputs and produces operational capabilities within the information environment. This activity is controlled by the operational environment; plans; policies; guidance; laws and regulations; tactics, techniques, and procedures; standards; and funding.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09

UIS 2.1 Perform Command and Control	To perform Command and Control (C2) of network and system Operations, to include control and management oversight of all operations and security aspects for the network. C2 over system and network Management is the set of activities required to provide direction and reporting over fault, configuration, accounting, performance, and security & system management activities within the network.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.1.1 Manage Systems and Networks	System and Network Management is the set of activities required to provide fault, configuration, accounting, performance, and security management within the network.	" GIG NetOps v3.0, para B.2.7"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.1.2 Manage Information Dissemination	Dissemination Management is the set of activities required to dynamically manage competing subscriber requirements and to automatically allocate infostructure resources to service those demands. This activity focuses on the regulation of content placement activities (e.g., publish and subscribe, content mirroring, content migration). The activity provides the capability to establish, select, and manage both general and specific information dissemination channels. The activity provides regulatory measures for governing repositories, directories, catalogs, and dissemination-related metadata. It has the primary control over publish and subscribe mechanisms. Information dissemination relies on commonly-understood metadata "tags" to distribute information products from the Producer to the Consumers.	"Scott A. Renner, PhD, A Community of Interest Approach to Data Interoperability,"	"NCOW A33236 - Regulate Information Dissemination "	"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09

UIS 2.1.3 Perform Operational Control	Activities essential to maintaining control and management of a resilient operational infrastructure, such as establishing and maintaining appropriate network operations situational awareness, planning and executing operational actions, and evaluating, selecting and executing operational courses of action.	"Global Information Grid Net-Centric Implementation Document: Network Management"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.2 Perform UIS Implementation Planning & Engineering	The aim of this planning and engineering activity is to design the UIS services and infrastructure required to support the mission and its needs. This requires a process of identifying the customers with shared interests, determining the technical capability required to support the UIS services demanded, designing the appropriate architectures and selecting the UIS components to form the 'provided' capability. After strategy is defined, implementation and engineering planning must be accomplished. An implementation plan must be created to describe the implementation in more detail and add additional information that enables the project organization to execute implementation in a proper way. The implementation plan should contain at least the following information: - Overview of the parties involved; - Description of the solution to be implemented; - Implementation strategy; - Migration strategy; - Back-out scenarios and procedures; - Risks and Risk Management; - Decision tree; - Necessary changes managed by Change Management; - Migration plan; - Overview of necessary resources; - Implementation schedule; - Site surveys; - Provision for feedback of early implementation experience			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.2.1 Analyze System and Network Requirements	Analyze requirements documents to develop an engineering solution.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09

UIS 2.2.2 Engineer Systems and Networks	Develop Systems and Networks from established and approved requirements.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.2.3 Manage System and Network Resources	Management of finances, people, and equipment.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.3 Deploy and Manage UIS Assets	Deploy and provide management over the people, money, and equipment needed to operate, and maintain systems, networks, and services.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.3.1 Procure Asset	In order to procure assets, there must be a valid need for the assets, there must be finances available to support the procurement, and there must be a procurement vehicle for the acquisition of the asset. Examples of assets include hardware, software, applications, and web services.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.3.2 Deploy New Asset	This activity deploys newly acquired assets into the Constellation Net in accordance with current policies.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.3.3 Identify Asset	In order to properly manage an IT asset, the asset manager must know if its existence, must know the attributes which make it unique, and must know its planned lifecycle.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.3.4 Report Asset Information / Metrics	The AFKS / GCSS-AF systems are used to report on assets within the enterprise and to maintain metrics on their use.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.3.5 Manage Asset Configuration	The process of identifying and defining Configuration Items in a system, recording and reporting the status of Configuration Items, and verifying the completeness and correctness of Configuration Items. Applies to existing systems as well as assets acquired from the Procure Asset activity. Provides a logical model of the infrastructure or a service by identifying, controlling, maintaining and verifying the versions of Configuration Items (CIs) in existence.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09

UIS 2.3.6 Manage Service Desk	The Service desk/support center extends the range of services and offers a more global-focused approach, allowing business processes to be integrated into the Service Management infrastructure. It not only handles incidents, problems and questions, but also provides an interface for other activities such as customer change requests, maintenance contracts, software licenses, Service Level Management, Configuration Management, Availability Management, Financial Management for IT Services, and IT Service Continuity Management.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.3.6.1 Manage Service Desk Procedures	When designing your processes and procedures, and taking the broad view, you will need to: review their validity on a regular basis, and update as required, involve all relevant parties, allocate sufficient time and resources, consider alternatives (e.g. information being computerized rather than in printed form) and provide new reference materials based on incident and problem trend analyses. Includes collecting and managing customer information.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.3.6.2 Provide Help Desk Services				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.3.6.3 Manage Escalations	Even in the best-supported operations, services breaches will occur. What is then important is to successfully manage the service breach, by recording the breach details and escalating to the Problem Management team, where appropriate.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.3.7 Remove Existing Asset	As assets reach the end of their established lifecycles, they must be removed from the enterprise in accordance with established policies.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09

UIS 2.4 Manage UIS Services	Initiates a set of services/activities that manage UIS Information Technology Services available to the Subscriber. Includes activities needed to negotiate Quality of Service (QoS) and cost agreements, and to bind the Subscriber and the Provider once an agreement has been reached. The end result of this negotiation is the Service Level Management (SLM), which is essential in any organization so that the level of UIS Service needed to support the business can be determined, and monitoring can be initiated to identify whether the required service levels are being achieved			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.4.1 Manage Domain Name Services (DNS)	Provides enterprise wide hostname and IP address resolution for CII Enterprise services, C2 nodes, and mission applications. Manage Domain Name Services - ensure domain name services and active directory structures are configured properly to facilitate IP address to host name resolution. Area of focus of this activity is TCP/IP and active directory services domain name structure.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09

UIS 2.4.2 Manage Enterprise Directory Services	Directory Services are used to manage system-network resources (including access control lists and user privileges). Directory Services differs from a directory in that it is both the directory information source and the services making the information available and usable to the user's applications. A meta-data service offers the ability to synchronize authoritative data between disparate but connected directories. Includes support for: Entity (ID) Directory; Authentication and Authorization Directory; Network Directory; Meta-directories and Connectors; Information Assurance Services; Domain, Tree and Forest Management; Print Services; Routing and remote access; Group policy and policies for sites, domains, users, and computers; Message Queuing Services; Quality of Service (QoS); Distributed File System; Network Management; Electronic Mail; Backup and Restore Services; Directory Management; and Exchange Migration	"Directory Services Profile"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.4.3 Set Network Time	Activities required establishing and distributing network time.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.5 Evaluate Service Delivery	This activity identifies and documents the service level management processes which are needed to assess, evaluate and sustain an adequate service level for all customers in accordance with the SLM defined in "Manage UIS Services". This is a cyclical process, where previous service level agreements and targets are re-evaluated periodically to see where improvements can be made.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09

UIS 2.5.1 Evaluate UIS Capabilities	This activity ensures that all capabilities required to support IT services function correctly, reliably, and according to standards as set by Baseline Services and above-baseline SLA contained within the C4IM Service Catalog.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 2.5.2 Evaluate UIS Services	Evaluate the C4IM and underpinning UIS Services necessary to conduct COCOM Operations and Business activities. Activity should result in an overarching Service Improvement Plan (SIP) and underpinning infrastructure, staffing, and training plans focused upon specific UIS capabilities.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.0 Provide UIS Services	This activity provides capabilities that enable users to dynamically interact, share, and use information to operate in a net-centric manner. These services consist of core services, COI services, and environment control services. Note: these services have also been referred to as GIG Enterprise Services (GES).	"NCOW RM Activity, Provide Enterprise Information Environment Services"	"http://www.army.mil/escc/ma/eie/index.htm"	"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.1 Provide Subscriber Interface Services	A set of services provided at the Subscriber interface that provide presentation services to the Subscriber (Input/Output), and translate the Subscriber's requests for Net-Centric services into the proper form/format for communication with Network Service Providers.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.2 Protect the UIS Information Environment	This set of activities depicts the capability required to Protect the UIS Information Environment and associated services from internal and external threats.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09

UIS 3.2.1 Provide Assured Information Sharing and Management Services	This activity provides the ability to securely and dynamically share information. It provides an authorized user timely exchange of information without special technical training or special security clearances to obtain the right information, at the right time, at the right place, and displayed in the right format during normal, degraded, and disconnected conditions, while denying adversaries and unauthorized users access to that same information or service. It enables exchanging information within and between security domains and Communities of Interest (COIs), at multiple levels of sensitivities, and, between authorized users within the DOD, other US Government departments and agencies, law enforcement agencies, selected non-government and private sector entities, allied nations and coalition partners, as appropriate, under normal, degraded, and disconnected conditions. Assured Information Sharing enables the timely, automated, and flexible creation and management of COIs. It also provides for dynamic, trusted and authenticated user access, as well as enabling the sharing of user identity and access rights throughout the enterprise.	"GIG IA Component of the GIG Integrated Architecture"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.2.2 Provide Information Environment Protection Services	This activity provides the ability to monitor, search for, detect, track, and respond to attacks by adversaries within the net-centric environment. Involves integrating a security management infrastructure with the overall management and operation of the environment and deployed to provide net-centric IA services. To manage IA effectively within a security management infrastructure needs to be integrated with the overall management and operation of the environment and deployed to provide net-centric IA services. Any circumstance or event with the	"CJCSI 6510.01E, IA Computer Network Defense"	"CJCSI 6510.01E, IA Computer Network Defense"	"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09

	potential to adversely impact an IA through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.				
UIS 3.2.3 Provide Information Protection Services	This activity delivers Assured Resource (Systems and Networks) Availability and Assured Information Protection. Actions include recognition of attacks as they are initiated or are progressing, efficient and effective response actions to counter the attack and safely and securely recover from such attacks, and reconstituting new capabilities from reserve or reallocated assets when original capabilities are destroyed. Information Protection Services are focused on Assured Resource (Systems and Networks) Availability and on Assured Information Protection. The objectives of this focus are achieved by instituting agile capabilities to resist adversarial attacks, through recognition of such attacks as they are initiated or are progressing, through efficient and effective response actions to counter the attack and safely and securely recover from such attacks; and by reconstituting new capabilities from reserve or reallocated assets when original capabilities are destroyed.	"AFI 33-115, Network Operations (NETOPS)"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.2.4 Provide Network Protection Services	Delivers mechanisms that provide network protection to include network encryption, physical isolation, high assurance guards, and firewalls. Mechanisms are used to create a collection of system high networks and enclaves. Enclave protection mechanisms are also used to provide security within specific security domains. In general, enclave protection mechanisms are installed as part of an Intranet used to connect networks that have similar security requirements and have a common security domain. A site may have multiple security domains with	"CJCSI 6510.01E, IA Computer Network Defense"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09

	protection mechanisms tailored to the security requirements of specific customers.				
UIS 3.3 Provide Core UIS Services	This activity enables warfighters/operators to exercise control over enterprise information and services through a loosely coupled, distributed infrastructure that leverages service modularity, multimedia connectivity, metadata, and collaboration to provide an environment that promotes unifying actions among all UIS participants.	"DOD Net-Centric Services Strategy"	"NCOW A3 -- Provide Net-Centric Services"	"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.3.1 Provide Community of Interest Environment	This activity provides functions developed by a COI for its specific missions or, for the common use of other COIs. A function that is initially specific to a COI can satisfy the requirements of other COIs and become a common function. Furthermore, any COI function can become a core application/function. Communities of Interest: Collaborative groups of users, who must exchange information in pursuit of their shared goals, interests, missions, or business processes, and who, therefore must have a shared vocabulary for the information they exchange. DOD Directive: Data Sharing in a Net-Centric Department of Defense A Community of Interest is the collection of people that are concerned with the exchange of information in some subject area. The community is made up of the users/operators that actually participate in the exchange; the system builders ...., and the functional proponents that define the requirements and acquire the systems on the behalf of the Users. The subject area is the COI domain - whatever the people in the COI need to communicate about.	"Source: Scott A. Renner, PhD. A Community of Interest Approach to Data Interoperability"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09

UIS 3.3.1.1 Create Shared Information Space	Activities required to establish a shared information space for COI members. The "information space" is used to aggregate, integrate, fuse, and disseminate information to users.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.3.1.2 Create Common Workspace	Activities required to establish a shared workspace for COI members.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.3.1.3 Provide COI Management Resources	Activities required for COI Managers to establish COI member roles, membership lists, profiles, access controls, and policy-based network instructions.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.3.1.4 Enable Determination of Resource Availability	Activities required to allow COI members to determine the availability (presence and status) of COI resources (information objects, members, storage services, communications resources, etc.).			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.3.2 Provide Information Sharing Services	Information Management Services include those activities that provide life-cycle management of Subscriber data without regard to data content or meaning. Information Management: The creation, use, sharing, and disposition of information as a resource critical to the effective and efficient operation of functional activities. The structuring of functional processes to produce and control the use of data and information within functional activities, information systems, and computing and communications infrastructure.	"GIG CRD 30 Aug 01"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09

UIS 3.3.2.1 Provide UIS Directory Services	A directory is an information resource used to store information about objects. A directory service can make those objects and their content available to user applications. The data in the directory may come from a number of authoritative data sources. Provides the directory management organization and processes required to create a scalable, secure, and manageable infrastructure for deploying and maintaining directory services. Directory Services Profile V1.9, 13 Jan 03 COIs will establish their own set of one or more directories. The COI will be responsible for configuring and maintaining the configuration of the directories.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.3.2.2 Provide Discovery Services	This set of services enables the formulation of search activities within shared space repositories (e.g., catalogs, directories, registries). It provides the means to articulate the required service argument, provide search service capabilities, locate repositories to search and return search results or, if necessary, initiates a tasking to the system to obtain the requested information.	"NCOW A311 - Perform Discovery Services"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.3.2.3 Provide Collaboration Services	This activity provides and controls the shared resources, capabilities, and communications that allow real-time collaborative interactions among participating group members. This environment provides synchronous collaboration capabilities; asynchronous collaboration can occur through other net-centric services and applications that are provided within the information environment.	"NCOW A312 -- Provide Collaboration Services"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09

UIS 3.3.2.4 Provide Messaging Services	Messaging Services are all formal (organizational) messaging services, to include e-mail, Defense Message Service (DMS), and instant messaging services. Provides services to support asynchronous and synchronous information exchange. This activity consists of all activities needed to support formal (organizational and/or structured) and informal (email and/or unstructured) messaging services. It includes support for tactical requirements. It supports the composition and validation of outgoing messages (message preparation). It supports the processing of incoming messages, including subsequent distribution to intended recipients as users of the information environment. The activity establishes and conducts message (bulletin) board services. It also supports official message traffic.	"NCOW A533 - Manage Messaging Resources"	"NCOW A313 - Provide Messaging Services"	"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.3.2.5 Provide Information Mediation Services	This activity enables transformation processing (translation, aggregation, and integration), situational awareness support (correlation and fusion), negotiation (brokering, trading and auctioning services) and publishing.	"NCOW - A314 Perform Information Mediation Services:"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.3.2.6 Provide Negotiation Services	This set of services applies protocols to establish the most appropriate service capabilities in response to service invocations. The request for data or services may be brokered to provide specific objects and/or object methods. The request for data or services may be supported by trader services that exchange information among brokers. The request for data or services may also be negotiated based upon the attributes of the persona of the requesting principal or upon the service that best matches the request.	"NCOW A3143 - Provide Negotiation Services"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09

UIS 3.3.2.7 Provide Information Management Support Services	Activities required to support the use of Information Objects during business, combat support, or warfighting activities.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.3.2.8 Provide Information Integrity	1) This activity provides protection against unauthorized modification or destruction of information. This protection supports information in storage, in transit and when processing. This capability maintains the quality of information, reflecting the logical correctness and reliability of the data. It ensures the logical completeness of the hardware and software implementing the data protection mechanisms and the consistency of the related data store structures. 2) Activities required to protect Information Objects and meta-data resident in a database or data warehouses (e.g., file encryption, records locking, and access controls).	"Derived from NSA IA Integrated Encyclopedia, 30 Jun 04;"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.4 Provide Computing Infrastructure	Computing Infrastructure includes those activities that provide a secure, robust, and cost effective computing environment to host core, network, and mission/community of interest (COI) application software; capabilities that enable information storage/retrieval and continuity of operations/disaster recover (COOP/DR); and common resources that enable user input and information processing, output, and display.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09
UIS 3.5 Provide Communications Services	Communications Services provide the Subscriber with a full range of information transport services for voice, data, video, imagery, etc. Communications Services provide an integrated network that is managed and configured to provide an information transfer utility for Infostructure Subscribers.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09

3. Information Exchanges (IEs)

Name	Purpose	Ref1	Ref1 Detail	Ref2	Ped1	Ped1 Detail	Format	Transfer Mechanism
Acceptance of Aircraft Support Request	Acceptance of request for relief supplies to be lifted by U.S. military aircraft.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data and voice	Email; phone; face to face
Acceptance of aircraft support request	Acceptance of request for relief supplies to be lifted by U.S. military aircraft.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data and voice	Email; phone; face to face
Advice to HOC Staff	Information on humanitarian support to the relief community.						Data and voice	Email; phone; face to face
Advice to CMOC Staff	Information on military support to the relief community.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data and voice	Email; phone; face to face
Advice to CMOC staff	Information on military support to the relief community.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data and voice	Email; phone; face to face

Advice to HOC Staff	Information on humanitarian support to the relief community.						Data and voice	Email; phone; face to face
Aircraft Support Request	Request for relief supplies to be lifted by U.S. military aircraft.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data and voice	Email; phone; face to face
Aircraft Support Request	Request for relief supplies to be lifted by U.S. military aircraft.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data and voice	Email; phone; face to face
Annex J of the US Emb. EAP	Template provided at http://arpsdir.a.state.gov/fam/12fah01/12fah010000anJ.html	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data	Written document
Annex J of the US Emb. EAP	Template provided at http://arpsdir.a.state.gov/fam/12fah01/12fah010000anJ.html	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response -				Data	Written document

			FY 2011					
Approved Operational Changes	Approved changes to the operational infostructure.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Identification Information	Identifying information for managed objects on the network.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Information	Identification and operational information on assets.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Information Collection Policy	Policy regarding the detail and extent of information to be collected on assets.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Lifecycle Policy	Plans for lifecycle replacement of IT assets.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Metrics	Measurable information regarding the status and performance of assets.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Audit Controls	A set of instructions to network equipment to implement the Audit Services request. Audit trail records from all available sources are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with DOD information system IA	"GIG IA"	"GIG IA Component of the GIG Integrated Architecture"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

	procedures							
Availability Discovery Request	Request to Discovery Services to search for persons or resources needed to conduct collaboration.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Brokered COI Services Request	Request establishment of a Community of Interest (COI) with definition of information requirements, membership, subscriber profiles, catalog and services administration. Includes requests by the COI policy manager to actively create/negotiate policy parameters for a given service/service set and specified information/objects.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Brokered Information Object	Information Objects that have been brokered or prioritized for service delivery.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Brokered Service Request	The Brokered Service Request is produced after the Subscriber's Service Request is compared to other pending service requests, the Subscriber's Profile, and the Commander's Information Policy. It is a response to a Subscribers Service Request. Applies Commander's information policy and network resource status. The Brokered Service Request is the allocation of infostructure resources in support of the Information Network.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Catalog Creation Request					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Catalog Management Requests	Request for services to create, update, and maintain catalog information. Bundle includes: - Catalog Creation Request - Request for publication - Publication Maintenance Request				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Change Request	Request to change any portion of the infrastructure, whether a physical change, a software change, a configuration change, or any other.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Catalog	Catalog of Services or Information Objects available to COI members.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Controlling Authority Guidance	Guidance provided by the Controlling Authority of the Community of Interest.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Information Subscription	COI Member's request to subscribe to Information Objects. Subscribers may choose to receive update notifications only or may choose to receive the updated Information Objects.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Membership List	Community Of Interest (COI) Membership List represents user support provided by COI Services for a COI. Includes membership, user role, catalog, subscription administration, and Roles Based Access Control (RBAC) support.	"NCOW"			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Policy-Enforcement Mechanisms	A set of policy-based controls to COI resources to enforce COI policies and is performed through various policy-enforcement mechanisms distributed throughout the information environment.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

COI Profile	The Subscriber's Profile updated to include information about his/her role and associated rights and privileges within the COI. Community of Interest (COI) Profiles represent a user/entity request to establish a COI identity. The request includes all pertinent information required to initiate the COI profile and accesses authorization. This includes all user profiles associated with the COI upon authentication. Operate and manage the dynamic and automatic feedback mechanisms that enable the profile to "learn" and "anticipate" the user's needs based on his usage patterns and patterns of similarly profiled users. Implement a combination of human and automated means to review, verify, and validate both the user and provider-specified portions of the dynamic profile.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Role Permissions	Permissions assigned to a COI Role To Information Assurances to establish Permissions				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

COI Roles	Roles and Responsibilities within a Community of Interest.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Services Management Information	Data concerning the configuration, performance, use, status, and security of Community of Interest (COI) Services. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Tables	Tables (directories, indexes, registries, metadata repositories, etc.) required to manage COI resources and Information Objects.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Collaboration Configuration Request	A request to UIS Configuration Management to change the configuration of network equipment to allocate or de-allocate resources required for collaboration.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Collaboration Information	Audio, video, multimedia, or data information objects from one or more collaboration participants.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Collaboration Management Data	Data concerning the configuration, performance, use, status, and security of collaborative resources. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Collaboration Results	Information objects that are produced during collaboration. Examples include: audio, video, multimedia files and associated records.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Collaboration Services Request	Request for the creation and use of a collaborative work environment. The users may be members of a persistent Community of Interest (COI) or an ad hoc group needing collaboration services. The work environment be persistent or temporary (needed only for the duration of the collaboration).				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Commander's Information Policy	Consists of operational authorities' policy on use of infostructure and rules governing the classification, releasability and priority of the information presented to the infostructure. Instructions, directions or policy specific to a unit, organization or operation that has local implications for guidance in security and Information Assurance conditions.	"ICD GIG ES dated 03/22/2004"	ICD GIG ES dated 03/22/2004		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Configuration Change Instructions	Change Configuration Instructions are sent to Infostructure components to initiate a change in their configuration. These can include commands to update software				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

	components, change routing tables, activate spare equipment, etc.							
Configuration Instructions	Instructions to configure infostructure equipment. Network Configuration Instructions are the policy based instructions from the network manager. These would include instructions to improve the availability, security, reliability, integrity, and performance of the network. Instructions or policy created by systems administrators, policy analyst, and CND analyst that propose guides and updates for any instructions on the proper procedures for configuration, changes, or updates for Information Assurance process that include IDS, COMSEC, EMSEC, and KMI., VPN management and other IA processes. Information generated from managed IA activity include raw audit data configuration information, request for access, request to perform transactions and credentials.	"GIG NetOps"	"GIG NetOps, Ver 3.0"	"GIG IA IFTR"	"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Coordinated Requirements	Requirements for infostructure services that have been processed, prioritized, coordinated, and a decision has been made to either act on, table, or deny the requirement.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Coordination - Aircraft Support	Information about commodities and delivery requirements.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data and voice	Email; phone; face to face
Coordination - Aircraft Support	Information about commodities and delivery requirements.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data and voice	Email; phone; face to face
Data Management Services Request					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Deploy Disaster Assistance Response Team	Team composition, capabilities, support needs	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data and Voice	MSG

Deploy Disaster Assistance Response Team (DART)	Team composition, capabilities, support needs	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data and Voice	MSG
Design Requirements	System design requirements. - Performance and Quality - Security - Capacity/Size				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Directory Service Request	A request to: - modify the structure of the directory, - manipulate (create, read, update, delete) the directory entry for an information object.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Directory Services Management Data	Data concerning the configuration, performance, use, status, and security of Directory Services. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Directory Services Search Results	Results returned from search in Directory Services.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Disaster Alert Cable	Background, current situation, anticipated course of action.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data	Cable (Message)(DoS equivalent to DMS)
Disaster Alert Cable	Background, current situation, anticipated course of action.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data	Cable (Message)(DoS equivalent to DMS)
Disaster Assistance Request	Request for up to $50,000 USD. Designates specific humanitarian and disaster relief organization to receive.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data	Cable (Message); email; fax

Disaster Assistance Request	Request for up to $50,000 USD. Designates specific humanitarian and disaster relief organization to receive.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data	Cable (Message); email; fax
Disaster Declaration Cable	1. The disaster is of such a magnitude that it is beyond the host country's ability to respond adequately; the host country has requested or will accept USG assistance, and it is in the interest of the USG to provide assistance. 2. The extent to which the host country needs assistance; 3. The intended use of requested resources, including recommended organizations through which funds will be channeled. 4. Estimated number of killed, injured, affected, displaced and homeless; immediate humanitarian needs; background info i.e. geo location, infrastructure, crops, livestock; other donor efforts; info from available assessment reports.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data	Cable (Message) (DoS equivalent to DMS); email; FAX

Disaster Declaration Cable	1. The disaster is of such a magnitude that it is beyond the host country's ability to respond adequately; the host country has requested or will accept USG assistance, and it is in the interest of the USG to provide assistance. 2. The extent to which the host country needs assistance; 3. The intended use of requested resources, including recommended organizations through which funds will be channeled. 4. Estimated number of killed, injured, affected, displaced and homeless; immediate humanitarian needs; background info i.e. geo location, infrastructure, crops, livestock; other donor efforts; info from available assessment reports.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data	Cable (Message) (DoS equivalent to DMS); email; FAX
Disaster Relief Guidance	Resources and agencies available	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data and Voice	MSG

Disaster Relief Guidance	Resources and agencies available	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data and Voice	MSG
Discovery Management Data	Data concerning the configuration, performance, use, status, and security of Discovery Services. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Discovery Results	Location of requested data or service. Once the location of the requested Service or Information is known, the Subscriber, and Application, or another Service can request the Information or invoke the Service.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Discovery Search Controls	Controls used to search repositories for the requested information, service, or metadata. Bundle includes: Service Search Controls Information Search Controls				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

	Person Search Controls Metadata Search Controls							
Discovery Services Request	Subscriber Request to search the network for information and/or services. Includes Availability Discovery Request.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
DNS Response	DNS information response to DNS Query				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Encrypted Information Object	Information Objects that have been encrypted to provide Confidentiality of data-in-transit over backbone networks must be maintained using appropriate encryption measures as per the classification or sensitivity level of the data.	"CJCSI 6510.01E"	"CJCSI 6510.01E, IA Computer Network Defense"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Escalations Incident Report	Report of escalations incidents which operate in a planned and measurable fashion.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Establish/Change COI Subscription	Subscriber's request to establish or change the subscription to a Community of Interest (COI).				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Global Information Grid Status	Status of the GIG infostructure				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Help Desk Information	Assistance and problem resolution information provided to the Requester.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Help Request	A Subscriber's request for UIS assistance. Help requests may be received via e-mail, or web interface.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
HHQ UIS Policy & Guidance	DOD and other Policy and Guidance that regulates Information Technology activities. UIS Policy & Guidance implements all mandatory and discretionary protection policies relevant to the GIG enterprise level. It also implements discretionary protection policies within any given domain. Implementation activities include setting parameters in mechanisms used for protection policy enforcement, deployment and configuration of protection devices, and re-configuration activities to meet changes in threat posture, changes in performance capabilities, and/or changes in protection policy (e.g., INFOCON Directives).				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

IM Services Management Data	Data concerning the configuration, performance, use, status, and security of Information Management Services. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel. Bundle includes: Discovery Management Data Collaboration Management Data Messaging Services Management Data Mediation Services Management Data Negotiation Services Management Data Information Protection Management Data				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Imagery Products	Geo-rectified products	"USSOUTHCOM and JTF-Haiti… Some Challenges and Considerations in Forming a Joint"	US Joint Forces Command Joint, Center for Operational Analysis				Data	Posted on ReliefWeb; Webpage; Email with attachment
Imagery Products Request (Multi-Spectral Imagery)								

Imagery Products Request (Satellite Imagery)	Satellite Imagery	"Joint Lessons Learned: Keys to Successful International Humanitarian Assistance"	Joint Center for Operational Analysis, US Joint Forces Command, Norfolk, Virginia				Data and voice	Email; phone; face to face
Imagery Products Request (Satellite)		"USSOUTHCOM and JTF-Haiti… Some Challenges and Considerations in Forming a Joint"	US Joint Forces Command Joint, Center for Operational Analysis				Data	Posted on ReliefWeb; Webpage; Email with attachment
Incident Escalation Policy	Plans for when/how to escalate incidents to higher levels of support.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Advertisement					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Creation Controls	Controls the development and release of new information objects into the shared information space.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Management Controls	A set of instructions to network equipment to implement the policy-based Information Management request.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Management Services Controls	A set of instructions to network equipment to implement the policy-based Information Management request.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Information Management Services Invocation	Information Management Services Invocation is the approved and brokered Subscriber's request for NCES information management services like Discovery, Collaboration, Messaging, or Mediation. Bundle includes: - Discovery Services Request - Collaboration Services Request - Message Services Request - Mediation Services Request - Data Management Services Request - Web Services Request				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Management Support Objects	Information Objects that have been created of modified during the Information Management Support activities.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Management Support Services Request	A Subscriber's request for Records Mgt, Workflow Mgt, or Data Administration services.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Information Management Transactions	Output from Information Management activities. Bundle includes: Discovery Services Search Results Collaboration Information Objects Messages Mediation Products Records Documents Workflow Products Table Updates				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Object	An Information Object includes audio, video, data, or sensor information and their meta data tags. This ICOM may also be used in a plural context				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Objects	Information Objects include audio, video, data, or sensor information and their meta data tags.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Information Protection Controls	A set of instructions to network equipment to implement the policy-based Information Protection Services.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Protection Management Data	Data concerning the configuration, performance, use, status, and security of Information Protection Services resources. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Storage Services Request	Request to Enterprise Storage Management Services to store, retrieve, or move information. Bundle includes: Modified Tables Updated Metadata Replicated Directory Updated Authoritative Source Data				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Tags	Information Tags are metadata (data about data) All data, that will be exchanged or has the potential to be exchanged, will be tagged IAW the current JTA standard for	"IDM CRD"	22 Jan 2001, pg 38		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

	tagged data items (XML).							
Infostructure Events	Occurrences within the ConstellationNet Infostructure. This includes both normal and anomalous events.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Infostructure Status	Infostructure Status focuses on the reporting requirements at various levels of NetOps management to ensure NetOps Personnel can maintain GIG situational awareness. Situational-awareness requirements, policy, guidance, monitoring capabilities, and standard NetOps operating procedures control this activity. NetOps personnel perform this activity. Infostructure Status is the standardized NetOps status derived from situational awareness capabilities, following reporting procedures, an established reporting hierarchy, and identified authorities for overseeing and controlling NetOps. Bundle includes: • Net-Centric Services Management Data • SSPI Status • Network Status • NCES Status • Storage Management Data				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Infrostructure Status	Infostructure Status focuses on the reporting requirements at various levels of NetOps management to ensure NetOps Personnel can maintain GIG situational awareness. Situational-awareness requirements, policy, guidance, monitoring capabilities, and standard NetOps operating procedures control this activity. NetOps personnel perform this activity. Infostructure Status is the standardized NetOps status derived from situational awareness capabilities, following reporting procedures, an established reporting hierarchy, and identified authorities for overseeing and controlling NetOps. Bundle includes: • Net-Centric Services Management Data • SSPI Status • Network Status • NCES Status • Storage Management Data				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

JFC UIS Policy & Guidance	JFC Policy and Guidance that regulates UIS activities. JFC Policy & Guidance implements all mandatory and discretionary protection policies relevant to the UIS. It also implements discretionary protection policies within any given domain. Implementation activities include setting parameters in mechanisms used for protection policy enforcement, deployment and configuration of protection devices, and re-configuration activities to meet changes in threat posture, changes in performance capabilities, and/or changes in protection policy (e.g., INFOCON Directives).				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Joint Infrastructure Tasking Order	A Joint order, typically from JTF-GNO, that directs configuration, implementation, or other types of action to be taken with regards to information, information protection, and other infrastructure issues				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Managed Service Desk Procedures	Service desk operations and procedures handled in a planned and controlled fashion.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Mediation Products	Information objects that have been produced or altered through the use of Mediation Services.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Mediation Services Management Data	Data concerning the configuration, performance, use, status, and security of Mediation Services resources. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Mediation Services Request	Request to provide mediation services.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Message Service Request	Request to provide support for asynchronous and synchronous information exchange.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Messages	Synchronous or asynchronous messages for distribution.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Messaging Services Management Data	Data concerning the configuration, performance, use, status, and security of Messaging Services resources. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Need to Create/Change Subscriber Profile	(Boundary Input), represents a Subscriber's requirement to create or change a Subscriber Profile.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Negotiation Services Management Data	Data concerning the configuration, performance, use, status, and security of Negotiation Services resources. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Network Time	Updated standard time for the network.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
OPORD	Detailed instructions for executing the Humanitarian Assistance/Disaster Relief operation.	"USSOUTHCOM and JTF-Haiti… Some Challenges and Considerations in Forming a Joint"	US Joint Forces Command Joint, Center for Operational Analysis				Data	Posted on ReliefWeb; Webpage; Email with attachment
OPORD	Detailed instructions for executing the Humanitarian Assistance/Disaster Relief operation.	"USSOUTHCOM and JTF-Haiti… Some Challenges and Considerations in Forming a Joint"	US Joint Forces Command Joint, Center for Operational Analysis				Data	Posted on ReliefWeb; Webpage; Email with attachment

Permissions	Permissions determine the data and applications that may be accessed for each role that is assigned the set of permissions that are necessary for the user to perform his required tasks. Is the act of allowing and authorizing use of specific resources for use in accessing networks? These resources can be identified and allowed for use in many ways that may include file, directory and object access. Normally the access controls that are required and placed on a resource are the permissions granted for access to that resource or a particular object. It focuses on capabilities for enabling and/or disabling entity permissions, rights, or privileges associated with locally or remotely entering host systems. Permission restrictions may be based on time-of-day, user location, device identity, port identity, etc. Authorization Restriction Parameters may be static or dynamic. UIS Security Administrators construct this type of authorization based on local and enterprise-wide policy, and deconflicts this type of authorization with other types of authorization being employed. This activity is controlled by	"NIST/ITL Bulletin"	"NIST/ITL Bulletin, An Introduction to Role-Based Access Control"		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

	access and usage policies that respond to evaluated threats.							
PPBD Information	Planning, Programming, & Budgeting Decision information is used to govern fiscal expenditures supporting the EIE				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Precedence	An information flow precedence tag (e.g., routine, priority, emergency)				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Producer's Information Catalog	Catalog/index of information Producers products and product updates.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Publication Maintenance Request					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Relief Effort Coordination	Information about the plans and execution of DART's relief efforts.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data and voice	Email; phone; face to face
Relief Effort Coordination	Information about the plans and execution of DART's relief efforts.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data and voice	Email; phone; face to face
Request DOD Assistance In Transporting Emergency Relief Commodities	Type, amount, location, destination, Required Delivery Date (RDD), capacity limitations at reception area	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data and Voice	MSG

Request DOD Assistance in Transporting Emergency Relief Commodities	Type, amount, location, destination, Required Delivery Date (RDD), capacity limitations at reception area	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data and Voice	MSG
Request for Information Controls	Request to establish new information/objects either by information collection means or as a result of exploiting, interpreting, assessing, or analyzing existing data to provide additional insights.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Request for Publication					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Request Streaming Video Service	A Request from streaming video services				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Request to Establish a COI	(Boundary Input), represents a requirement to establish a Community of Interest (COI). Gartner defines Community of Interest as "Also known as a community of practice, this group of people associated and linked in a network of communication or knowledge network because of their shared interest or shared responsibility for a subject area. ... Communities continually emerge and dissolve, and their membership, processes and knowledge continually change and evolve. Source: Gartner's Glossary of Terms Used for the Knowledge Workplace: 2004 Update. Bundle includes: COI Membership List COI Member Designation COI Role Descriptions COI Policies	"NCOW: Need to Operate as a COI: (Boundary Input) "	Represents a user requirement to initiate and operate as a COI typically based on missions, tasks, or objectives.		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Request USAID/OFDA Relief Commodities	Material available from USAID/OFDA stockpiles	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data and Voice	MSG
Request USAID/OFDA Relief Commodities	Material available from USAID/OFDA stockpiles	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data and Voice	MSG
Requested Dissemination Service	The Requested Dissemination Services are provided once the Subscriber's Credentials have been authenticated, the appropriate policies have been reviewed, and the required permissions have been granted. Bundle includes: - Smart Push Data - Search Results				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

	- IDM Catalog Data							
Requirements	Requirements Documents received from Subscribers, COI Managers, Systems Program Officers (SPOs), Program Management Offices (PMOs) and others.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Scope and Magnitude of Event	Type of event, how large an area, how big a storm or magnitude of earthquake, tsunami, etc. Numbers of personnel likely to be effected. Likely resources needed.	"Mission Disaster Relief Officer (MDRO) through established contacts including: h"	Chief of Mission (CoM), the embassy's Emergency Action Committee (EAC) and the USAID Office Foreign Disaster Assistance (OFDA) Principal Regional Advisor				Data and voice	Overview brief

Scope and Magnitude of Event	Type of event, how large an area, how big a storm or magnitude of earthquake, tsunami, etc. Numbers of personnel likely to be effected. Likely resources needed.	"Mission Disaster Relief Officer (MDRO) through established contacts including: h"	Chief of Mission (CoM), the embassy's Emergency Action Committee (EAC) and the USAID Office Foreign Disaster Assistance (OFDA) Principal Regional Advisor				Data and voice	Overview brief
Security Clearance Information	Information regarding the Security Clearance of individuals.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data	
Security Clearance Information	Information regarding the Security Clearance of individuals.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data	

Security Policy and Instructions	Set of laws, rules, and practices that regulate how sensitive (SBU and classified) information is managed, protected, and distributed by an AIS. NOTE: System security policy interprets regulatory and operational requirements for a particular system and states how that system will satisfy those requirements. All systems or networks that process SBU or classified information will have a security policy. Security Policy and Instructions focuses on the creation of specific policy parameters and the negotiation/modification of these parameters. The input is the invocation of the policy manager to actively create/negotiate security policy parameters for a given service/service set and specified information/objects. The output is instructions concerning the new/modified policy parameters that constrain/enable service execution.	"AFDIR 33-303"	"AFDIR 33-303, definition for System Security Policy."	NCOW	"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Service Desk Procedures	Planned procedures for operating the service desk.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Service Request Response	The Service Provider's response to the request for service/information. Provides feedback to the Subscriber concerning the status of the pending service request. Bundle Includes: Audit Controls COI Tables COI Roles COI Membership List Shared Workspace Controls Information Creation Controls COI Policy-Enforcement Mechanisms Information Advertisement Confirmation of Delivery IDM Response Notification Help Desk Information Modified Information Object Retrieved Information Object				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

	• Customized Presentation Data							

Service Request Response	The Service Provider's response to the request for service/information. Provides feedback to the Subscriber concerning the status of the pending service request. Bundle Includes: Audit Controls COI Tables COI Roles COI Membership List Shared Workspace Controls Information Creation Controls COI Policy-Enforcement Mechanisms Information Advertisement Confirmation of Delivery IDM Response Notification Help Desk Information Modified Information Object Retrieved Information Object				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

	• Customized Presentation Data							
Shared Workspace Controls	Controls used to establish and manage a shared workspace for the COI. Includes: - Application Use Controls - Information Exchange Controls				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

	- Information Disposition Controls							
Significant Event Log	Daily significant events	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data	Website
Significant Event Log	Daily significant events	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011				Data	Website

SITREP - JTF	Information on the disaster and status of response actions.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data and voice	Email; phone; face to face
SITREPS					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
SITREPS - Out					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Situation Report - DART	Information on the disaster and status of response actions.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data and voice	Email; phone; face to face
Status Updates	Information on the disaster and status of response actions.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data and voice	Email; phone; face to face
Status Updates	Information on the disaster and status of response actions.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005				Data and voice	Email; phone; face to face
Subscriber Information Request					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Subscriber Profile	All requirements, criteria and other pertinent user information in a proper format and submit as the current User/Entity profile. Define and implement the basic attributes of the user's profile that are determined by the organization to which the user belongs and the user's role in that organization. Example attributes include user's roles, areas of responsibility, clearances, accesses, and communications medium. The Subscriber Profile is used to tailor the Network services to the Subscriber's preferences (font size, colors, default page, etc.).	NCOW			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Subscriber Request Response	Provides feedback to the Subscriber concerning the status of a pending request.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Subscriber Service Request	Subscriber Service Request represents a user request for a specific service or capability. This includes profile requests, information publication requests, information acquisition requests, collaboration requests, and COI services requests. A Subscribers request for services from the network (information transport, file access, information dissemination, etc.).				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Subscriber Service Request Response	Subscriber Service Request Response to a user request for a specific service or capability. This includes profile requests, information publication requests, information acquisition requests, collaboration requests, and COI services requests. A Subscribers request for services from the network (information transport, file access, information dissemination, etc.).				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Training	Training required to gain access to the AF Network and other related training requirements				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
UIS Directives	Directives issued both to trigger specific actions as well as to inform effected organizations.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

UIS Plans	Plans for the operation of systems and networks.				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
UIS Policy & Guidance	GCC/JFC, and other Policy and Guidance that regulates Information Technology activities. UIS Policy & Guidance implements all mandatory and discretionary protection policies relevant to the GIG enterprise level. It also implements discretionary protection policies within any given domain. Implementation activities include setting parameters in mechanisms used for protection policy enforcement, deployment and configuration of protection devices, and re-configuration activities to meet changes in threat posture, changes in performance capabilities, and/or changes in protection policy (e.g., INFOCON Directives).	NCOW			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Web Services Request					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project

Annex N3 - High Level Operational Concept Graphic "As-Is" Operational Viewpoint (OV-1)

The complexities of operating and sharing information with an evolving and often unfamiliar community of interest place a premium on the Department of Defense's (DOD) ability to understand the nuances of potential stakeholder organizations' cultures, needs, strengths and limitations. The high level operational concept, as shown in the unclassified information sharing (UIS) "As-Is" Operational Viewpoint (OV) -1 below, describes current UIS capabilities during a notional humanitarian assistance/disaster relief (HA/DR) effort (Figure N3-1).

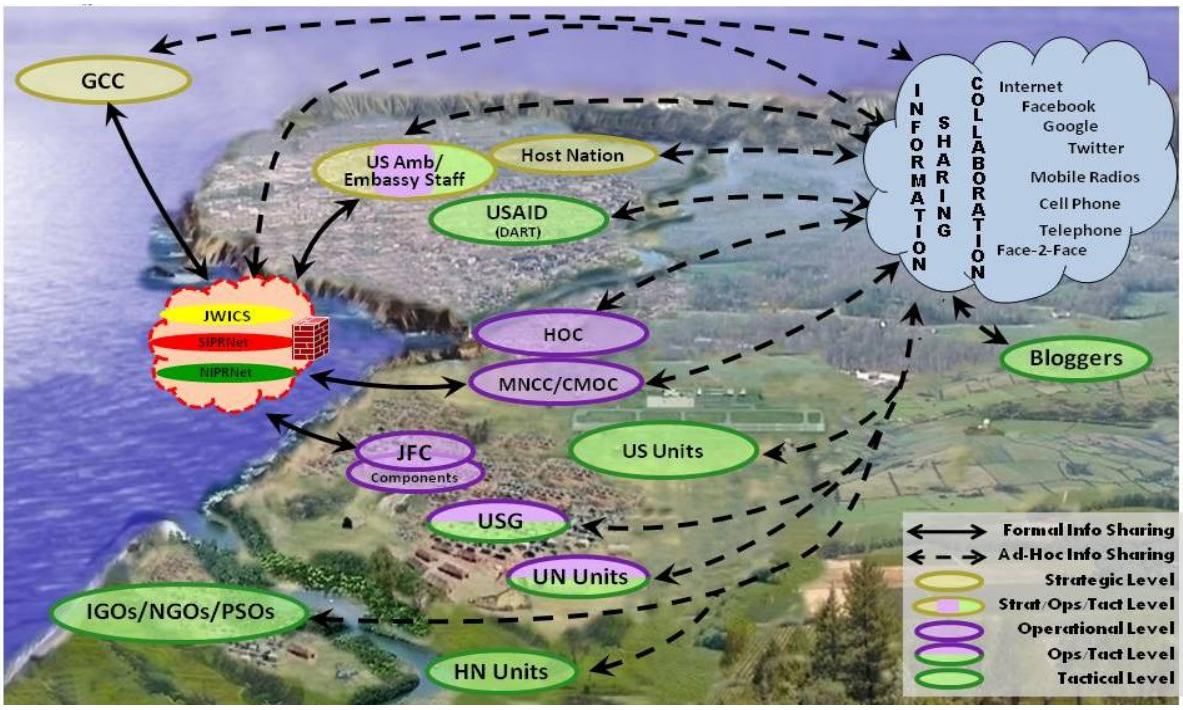


Figure N3-1 UIS "As-Is" High Level Operational Viewpoint (OV-1)

DOD's role in HA/DR, also termed as foreign humanitarian assistance (FHA), consists of DOD activities in support of the United States Agency for International Development (USAID) or Department of State (DOS), conducted outside the United States (U.S.), its territories, and possessions to relieve or reduce human suffering, disease, hunger, or privation. While, U.S. military forces are not the primary U.S. Government (USG) means of providing FHA, the foreign assistance they are tasked to provide is designed to supplement or complement the efforts of the host nation civil authorities or agencies that may have the primary responsibility for providing that assistance.

DOD has unique assets for effective response and can play a key role in foreign humanitarian crises. The U.S. military possesses exceptional operational reach that can be employed to enhance an initial response. Additionally, U.S. military capabilities in logistics, command and control (C2), communications, and mobility are able to provide rapid and robust response to dynamic and evolving situations among vastly different military, civilian, and government entities. HA/DR operations require coordination and collaboration among many agencies, both governmental and nongovernmental, with

U.S. military forces often tasked in a supporting role. As such, the combatant commander (CCDR) or joint force commander may not be responsible for determining the mission (relief missions, dislocated civilian support missions, security missions, technical assistance and support functions, and foreign consequence management) or specifying roles and responsibilities among the participating agencies. During HA/DR operations unity of command may not be possible, but the requirement for unity of effort becomes paramount.

Information sharing is critical to the efficient pursuit of a common humanitarian purpose. No single responding entity can be the source of all of the required data and information. Making critical information widely available to multiple responding civilian and military elements not only reduces duplication of effort, but also enhances coordination and collaboration and provides a common knowledge base so that critical information can be pooled, analyzed, compared, contrasted, validated, and reconciled. Information sharing is not primarily a technology issue; rather, the challenges are largely social, institutional, cultural, and organizational. These impediments limit and shape the willingness of civilian and military personnel and organizations to openly cooperate and share information and capabilities. Issues complicating effective coordination include:

- lack of understanding about the information culture of partners
- suspicions regarding the balance between information sharing and intelligence gathering
- tensions between military needs for classification (secrecy) of data, versus the civilian need for transparency
- differences in the C2 style of military operations versus civilian activities
- the compatibility and interoperability of planning tools and processes.[1]

The sharing of information is particularly critical to effective HA/DR because no single responding entity can be the source of all of the required data and information. Making critical information widely available to multiple responding civilian and military elements not only reduces duplication of effort, but also enhances coordination and collaboration and provides a common knowledge base so that critical information can be pooled, analyzed, compared, contrasted, validated, and reconciled. Civil-military collaboration networks need to be designed to dismantle traditional institutional stovepipes and facilitate the sharing of information among civilian and military organizations.

The UIS "as-is" OV-1 describes the current situation defined by the difference between required capabilities and identified operational gaps. The capabilities required by combatant commands and subordinate staffs (e.g., joint task force (JTF) headquarters, Service components) to effectively employ UIS include:[2]

[1] Joint Chiefs of Staff, Foreign Humanitarian Assistance, Joint Pub 3-29 (Washington, DC: 17 Mar 2009).
[2] USJFCOM J9, *Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Baseline Assessment Report*, v. 1.3, 16 May 2011, pgs. 136-144.

- clear and simplified lines of authority for managing information sharing risk and adjudicating competing DOD guidance for information release
- a UIS portal capability integrating/federating synchronous, asynchronous, and multi-mode services, including language translation, display fusion, social media integration and collaboration services
- a validated UIS Operating Concept
- standard operating procedures for implementing the UIS Operating Concept
- an automated cross domain capability from existing SECRET Internet Protocol Router Network (SIPRNET) and the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) to the UIS portal enabling agile information sharing and collaboration
- an unclassified information sharing capability (UISC) enabling mobile terminal device users through synchronization services, Geographic Information System integration, sufficient application support for minimal portal collaboration, and a connection interface facilitating low cost bulk provision of devices
- a Knowledge Management/Information Management (KM/IM) UIS portal structure reducing learning/training requirements for intended users
- policies balancing enclave security concerns with UIS policy intent
- enhancing UIS information and collaboration tools while a unifying technical solution is implemented
- standing UIS protocol and procedure templates supporting rapid integration with non-enduring and ad hoc mission partners
- a web based UISC accommodating multimedia information sharing and collaboration among the spectrum of potential mission partners to include both real and virtual members
- standing UIS protocols and procedures for engagement with UIS enduring partners
- procedural enablers to make UIS training more efficient and effective, accelerate user access to information, and empower KM/IM (i.e., document retention policy, metadata policy, library structure, document content and labeling standards, file and folder naming conventions, user friendliness, disaster recovery plan, prime source designation, access and control rules for information, help desk provisioning, action tracking, and version control)
- a uniform interpretation of [information management and sharing] policies
- a collaborative portal available via the internet

- a UIS portal emphasizing open source software, enterprise business practices, and modularity permitting integration and federation of rapidly emerging social networks and intergovernmental organizations (IGO)/nongovernmental (NGO) enclave systems
- a UISC unconstrained by geographical locations
- a UISC with sufficient interoperability at link, transport, network, and application layer
- a UISC supporting both enduring and ad hoc communities
- a UISC that is rapidly scalable without losing information sharing and collaboration functionalities
- a guide book for cultural engagement with enduring UIS partners, particularly NGOs and IGOs
- a UIS portal centrally funded and provisioned to ensure uninterrupted service across all DOD enclaves
- a UISC accommodating through physical or procedural mechanisms, information exchange with non-internet protocol networks such as High Frequency Packet or other data signaling protocols, radio voice nets, telephonic information, or face-to-face networks

The CCDRs have identified the following gaps and shortfalls in their current capabilities at the combatant command and JTF levels.[3]

- Staffs lack sufficient knowledge/skills/abilities to understand the roles, responsibilities, limitations, authorities, potential contributions, and information exchange requirements of interagency and other potential mission partners, resulting in ineffective information exchange.
- Inconsistent information management schemes among existing DOD web portal implementations and standards impede information sharing with mission partners, resulting in needless duplication of information, inefficient searches, lapses in event coordination, poor presentation of information to target audiences, and general information overload.
- Staffs are impeded in rapidly establishing dynamic information sharing environments and/or sharing of information (e.g., Government-provided imagery products) by inadequate procedures and restrictive interpretation and inflexibility of information sharing policies. Solution(s) are required to address both crisis and deliberate planning responses.
- Information sharing with USG agencies and other mission partners is impeded by the incompatibility between DOD's hierarchical information exchange methodologies/processes, and decentralized or ad hoc processes employed by USG agencies and other mission partners.

[3] USJFCOM J9, *Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Baseline Assessment Report*, v. 1.3, 16 May 2011, pgs. 183-184.

- Diverse cultural and operational habits among staffs lead to work on multiple classified and unclassified government networks, as well as public domains. Manual cross domain transfer mechanisms currently in place are cumbersome and inefficient, adversely affecting operations.
- Without a common strategy and standard procedures for effective integration, staffs lack the ability to access and interpret valuable information in the public domain, such as social media.
- Staffs lack a DOD UISC that is flexible, accessible, user-friendly, and interoperable across the broadest pool of mission partners. This UISC should be standard across DOD to minimize the need to train on a new tool when DOD personnel transition to a new area of responsibility.
- Staffs lack processes and procedures to include mission partners in existing DOD systems and networks for information sharing, and access mission partners systems and networks for information sharing.
- Staffs' ability to collaborate is impaired by damaged, underdeveloped, or disparately developed network infrastructure in affected nations.

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project

Annex N4 - High Level Operational Concept Graphic Unclassified Information Sharing (UIS)"To-Be" Operational Viewpoint (OV-1)

1. Operational Problem

Unclassified information sharing (UIS) mission partners and stakeholder participant organizations continue to face rapid and accelerating advances in information technology. This proliferation of capabilities and technology choices contribute to an overwhelming UIS information overload to those organizations.[1]

In addition to challenges posed by information technology innovations and communications infrastructure improvements, the U.S. military faces growing requirements to interact with new and unfamiliar partners. Building unity of effort across this diverse group of mission partners poses a significant challenge in operations, particularly those involving non-combat missions where the military is in a supporting role.

Part of this challenge arises in accommodating the institutional autonomy of new mission partners and stakeholder organizations that bring different organizational cultures, procedures, languages and agendas.[2] Mission partners are defined as the expanse of possible actors with whom the Department of Defense (DOD) may share information, whether organizations or national governments. They include: federal, non-DOD departments and agencies; state, local and tribal government departments and agencies; foreign governments, militaries, and organizations; nongovernmental organizations (NGOs); intergovernmental organizations (IGOs); private sector companies and organizations, including private sector organizations (PSOs); and international organizations.[3] Stakeholder participant organizations include, but are not limited to NGOs and members of the public and private sectors involved with the same community of interest (COI) or issue. Viewed collectively, these participant actors comprise the extended enterprise[4] for unclassified information sharing.

Existing policies, processes and procedural issues, such as the lack of compatible procedures and a missing general consensus on business rules, complicate and inhibit effective cooperation. Strong, hierarchy-based organizational cultures, while naturally building internal homogenous worldviews among members, tend to inhibit external networking efforts to build trust and create a shared understanding with other organizations.[5] Additionally, the military's best efforts at coordination are confounded by outdated regulatory and legal policies that impede information sharing and dissemination as well as strict organizational cultures that do not provide incentives for collaboration.

Continued mission success requires sustained and habitual information sharing across domains with a broad range of mission partners and stakeholder participant organizations in the extended

---

[1] ASD (NII)/DOD CIO, *Department of Defense Information Sharing Strategy*: 4 May 2007.
[2] Joint Staff, *Unclassified Information Sharing Capability (UISC) Concept of Operations*, 15 Nov 10, p.1.
[3] Joint Staff J8, *Department of Defense (DOD) Multinational And Other Mission Partners (MNMP) Command And Control (C2) Information Sharing Capability Concept Of Operations*, Pre-decisional Draft v.1.
[4] Adapted from OASD/NII, *Department of Defense Information Sharing Implementation Plan*, April 2009.
[5] Schein, E. H. (1990). *Organizational Culture*. American Psychologist, 45(2), 110

enterprise. Despite efforts to achieve this goal, DOD has been largely unsuccessful in establishing effective mechanisms for developing and nurturing essential relationships that consistently facilitate common or compatible procedures, generate consensus on business rules, and stimulate effective cooperation.

2. Vision

The way ahead for UIS is to pursue a combination of proven best practices, and experimentally validated UIS procedures, architectures, and information exchange requirements, while DOD implements an initial technical capability. The technical approach should be focused on UIS agility and adaptation that provides flexibility in the context of dynamic mission requirements and a constantly evolving public information sharing domain, characterized by the prevalence of unstructured data and distributed or ad hoc organizational structures. Successful DOD adoption of standard information sharing procedures, protocols, templates and business rules, developed with an appreciation for the requirements of mission partners, will begin the process of overcoming cultural and organizational impediments. For the military culture, it represents a redressing of the balance between protection and sharing of information through the application of risk management. For non-DOD partners, visibility into the range of organizational goals, objectives, and common approaches to problem solving, can mitigate information sharing obstacles, especially between military and NGOs.

3. Operational Capabilities[6]

Building on work already done by various organizations in UIS and command and control (C2) concept development and experimentation, UIS development should focus on updating and refining standard procedures, architectures and information exchange requirements. The development work can be explored and refined within a single mission area (e.g. humanitarian assistance / disaster relief (HA/DR) but should be considered for application across the spectrum of operations.

Specific procedural requirements of combatant command and subordinate staffs include:

- Continuous update of quick reference guides to the roles and responsibilities of potential mission partners.
- An electronic, searchable handbook-like reference document for using UIS to support mission requirements.
- Continuous validation of processes and procedures for the expedited release of controlled unclassified information to support mission requirements.
- Expanded and refined processes and procedures for the transfer of imagery data using UIS to support mission requirements.

[6] IMISAS Baseline Assessment Report (Draft), ver. 1.3, 16 May 2011.

- Incentives to promote information sharing and the rapid establishment of dynamic information sharing environments.
- Revised procedures and authorities for the handling of unclassified information to support mission requirements.
- Consideration of UIS processes and procedures in other mission areas such as Homeland Defense/Civil Support.

The development of a UIS architecture defined by information exchange requirements would describe potential partners, integral processes and activities, and required supporting technology. The following are required to inform UIS development:

- Definition of touch points or interactions with the extended enterprise of mission partners and stakeholder participant organizations.
- Refinement of a common lexicon and ontology in support of the UIS information management scheme, using commonly available (e.g., extensible markup language (.XML)) frameworks.
- Development and refinement of partnerships and/or legal relationships between government and private sector companies with respect to information management schemes that could be applied to UIS.
- Description of the unclassified information flow between strategic, operational and tactical forces.
- UIS modernization aligned with National Information Exchange Model information exchange standards and processes.
- Refinement of unclassified information exchange requirements.
- Development of pre-planned templates for recurring information sharing requirements using UIS.

For UIS to be effective, DOD's technical capabilities must support the Department's information sharing and collaboration requirements, particularly with non-DOD mission partners. As DOD implements their initial UIS capability in the public domain, best practices and lessons learned from technical demonstrations and experimentation should be applied to accelerate the evolution of capabilities. These capabilities must satisfy not only DOD requirements but be compatible and interoperable with mission partners. Capabilities already identified by the combatant commanders include:

- Federated UIS search capabilities aligned with information sharing modernization efforts in the public sector.
- Graduated user account permissions and methodologies for anticipated and unanticipated users to facilitate allocating access to different levels of information based on trust.

- UIS capabilities to provide updates to mission partners and capture data through dynamic sources (e.g., social media, hotlines, news).
- UIS capabilities to access information in the public domain, such as social media.
- Integrated portal (e.g. SharePoint) capabilities that are interoperable across the broadest pool of mission partners.
- A rapid user registration system with the capability and capacity to support the expansion of the UIS COI during crisis.
- UIS capabilities to accommodate disconnected, intermittent, and low bandwidth (DIL) user access, including mobile devices.
- UIS capabilities to access, gather, process, and analyze information as public domain capabilities and frameworks, such as social media, continue to improve and modernize.
- UIS capabilities to leverage modernization and improvements to commercial off-the-shelf or government off-the-shelf products which support a user-defined operating picture.

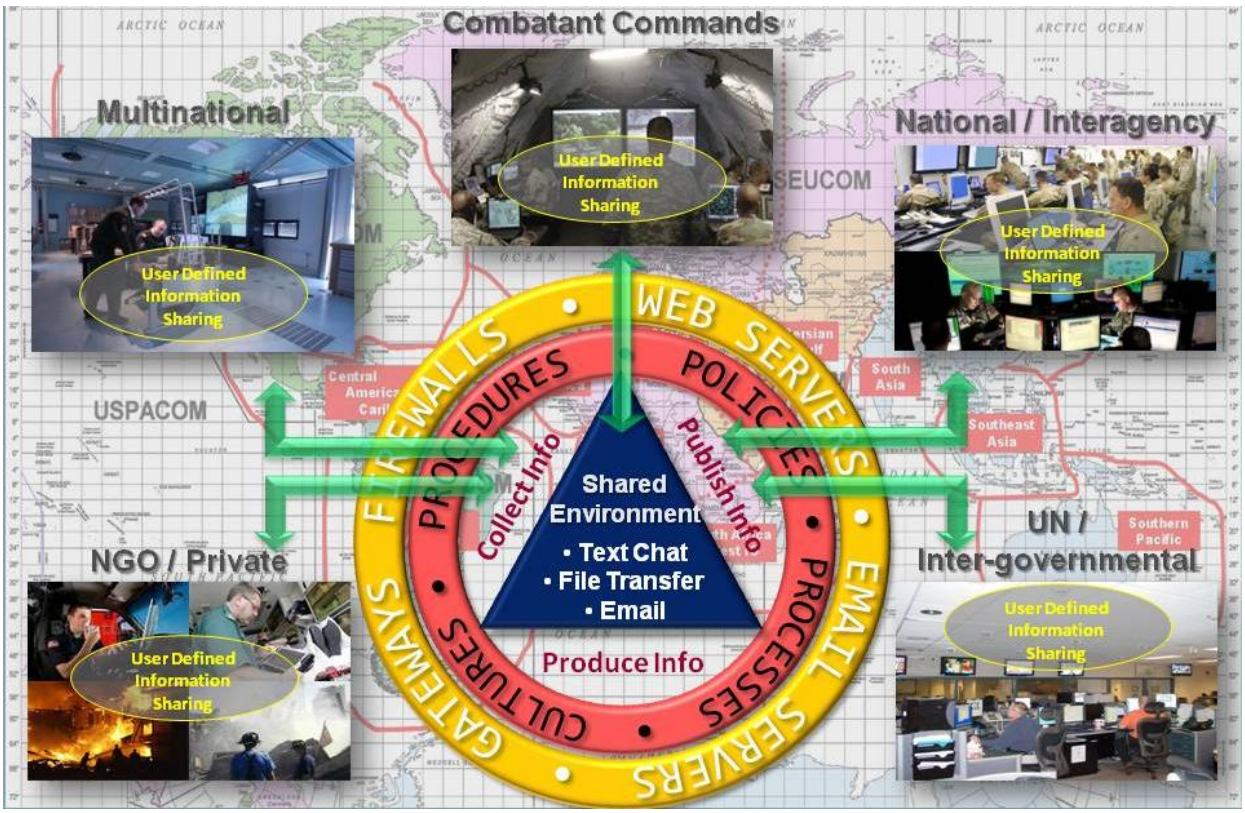


Figure N4-1 UIS "To-Be" High Level Operational Viewpoint (OV-1)

The above capabilities are reflected in the UIS "To-Be" Operational Viewpoint (OV) -1, (Figure N4-1), which portrays a combatant commander's UIS requirements for an HA/DR operation conducted in the near-term or next 5 years. In addition to DOD forces at the strategic, operational and tactical levels, mission partners include United States Government agencies, multinational, intergovernmental, nongovernmental and private sector organizations, and disconnected, intermittent, and low bandwidth users. UIS procedures provide a gateway between DOD systems and the public domain. As depicted, the public domain is an essential requirement for collaboration and sharing of unclassified information with the majority of mission partners.

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project

Annex N5 - Unclassified Information Sharing (UIS) Operational Resource Flow Description
OV-2

1. Department of Defense Architecture Framework (DODAF) Operational Viewpoint (OV) 2

The aim of the Operational Resource Flow Description (OV- 2) is to record the operational characteristics for the community of anticipated users relevant to the architectural description and their collaboration needs, as expressed in needlines and information flows. A needline documents the required or actual exchanges of information. A needline is a conduit for one or more information exchanges, i.e., it represents a logical bundle of information flows; the needline does not indicate how the transfer is implemented. The OV-2 is not a communications link or communications network diagram but a high-level definition of the logical requirement for information exchange.

The specific application of the OV-2 is to describe a logical pattern of resource (information, funding, personnel, or materiel) flows. The purpose of an OV-2 model is to describe a logical pattern of resource flows. The logical pattern need not correspond to specific organizations, systems or locations, allowing resource flows to be established without prescribing the way that the resource flows are handled and without prescribing solutions. The OV-2 is intended to track the need for resource flows between specific operational activities and locations that play a key role in the architectural description. The OV-2 does not depict the physical connectivity between the activities and locations. The logical pattern established in an OV-2 model may act as the backbone onto which architectural elements may be overlaid - e.g., a systems viewpoint (SV) 1, Systems Interface Description, model can show which systems are providing the necessary capability.

The main features of this model are the operational resource flows, the location (or type of location / environment) where the resources need to be or are deployed, and the needlines that indicate a need to exchange or share resources. An OV-2 indicates the key players and those interactions necessary to conduct the corresponding operational activities of an OV-5a, Operational Activity Decomposition Tree, or OV-5b, Operational Activity Model.

An OV-2 can also define a need to exchange items between operational activities and locations, and external resources; i.e., operational activities, locations or organizations that are not strictly within the scope of the subject architectural description but which interface to it either as important sources of items required within the architectural description or important destinations for items provided within the architectural description.

The OV-2 is intended to track the need to exchange items between key operational activities and locations within the architectural description. The OV-2 does not depict the physical connectivity between the operational activities and locations. The needlines established in an OV-2 can be realized by resources and their interactions in a SV-1 model or services view (SvcV) 1, Services Context Description model. There may not be a one-to-one correspondence between an operational activity and a location in an OV-2 and a resource in the SV-1 Systems Interface Description model or SvcV-1 Services Context Description model. For example, an operational activity and location may be realized by two systems, where one provides backup for the other, or it may be that the functionality of an operational activity has to be split between two locations for practical reasons.

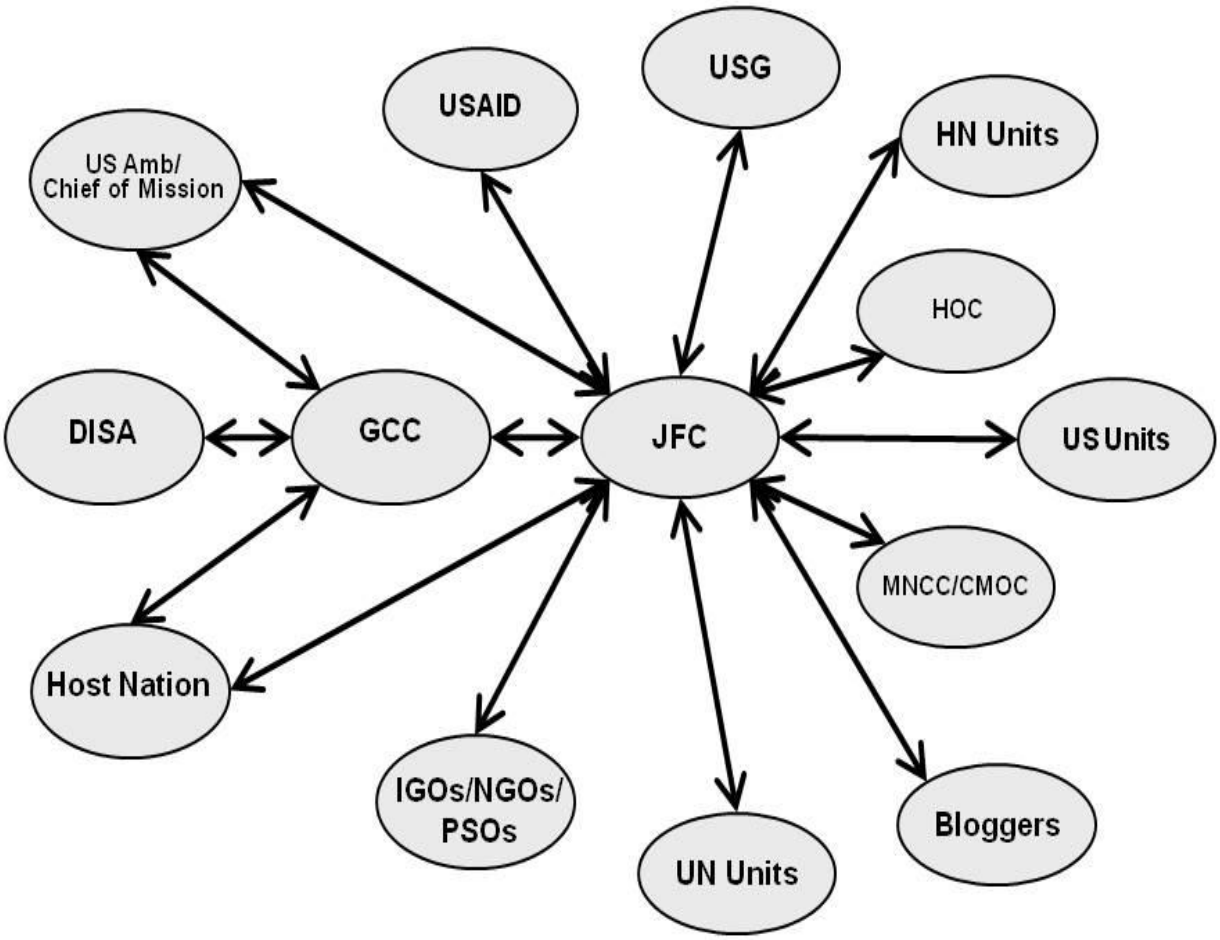


Figure N5-1 – Operational Resource Flow (OV-2)

2. Unclassified Information Sharing (UIS) OV-2

The UIS OV-2, Figure N5-1, shows the principal organizations and operational resource flows for Department of Defense (DOD) support in a foreign humanitarian assistance (FHA) scenario. The architecture is oriented to focus on the resource flows between the key military organizations at the strategic-theater (geographic combatant commander (GCC) Figure N5-2) and operational (joint force commander (JFC) Figure N5-3,) levels, and their DOD and non-DOD partners. For clarity of the OV-2, the needlines are shown from the GCC or the JFC, however, in practice; both may have some information sharing requirements with a range of non-DOD partners depending on the operational situation.

The Defense Information Systems Agency (DISA) is the primary provider for voice, video and data services to the warfighter, including those Internet-based capabilities used in support of UIS. While the primary needline is between DISA and the GCC, DISA support continues to the JFC and subordinate U.S. tactical forces (depicted as US Units, multinational forces coordination center (MNCC) or civil-military operations center (CMOC).

In the initial phase of an FHA scenario, the GCC and U.S. embassy (U.S. Ambassador, Chief of Mission) in the affected country will share information on the effects of the disaster and needs of the host nation (HN), and coordinate potential DOD responses. Also in the planning phase of an FHA operation, the GCC will share information with HN counterparts to coordinate the U.S. military response. While not explicitly shown in the OV-2, the JFC could also have information sharing and coordination requirements with the U.S. embassy and the HN, as well as HN units, should a joint task force (JTF) be established to conduct humanitarian assistance/disaster relief (HA/DR) operations.

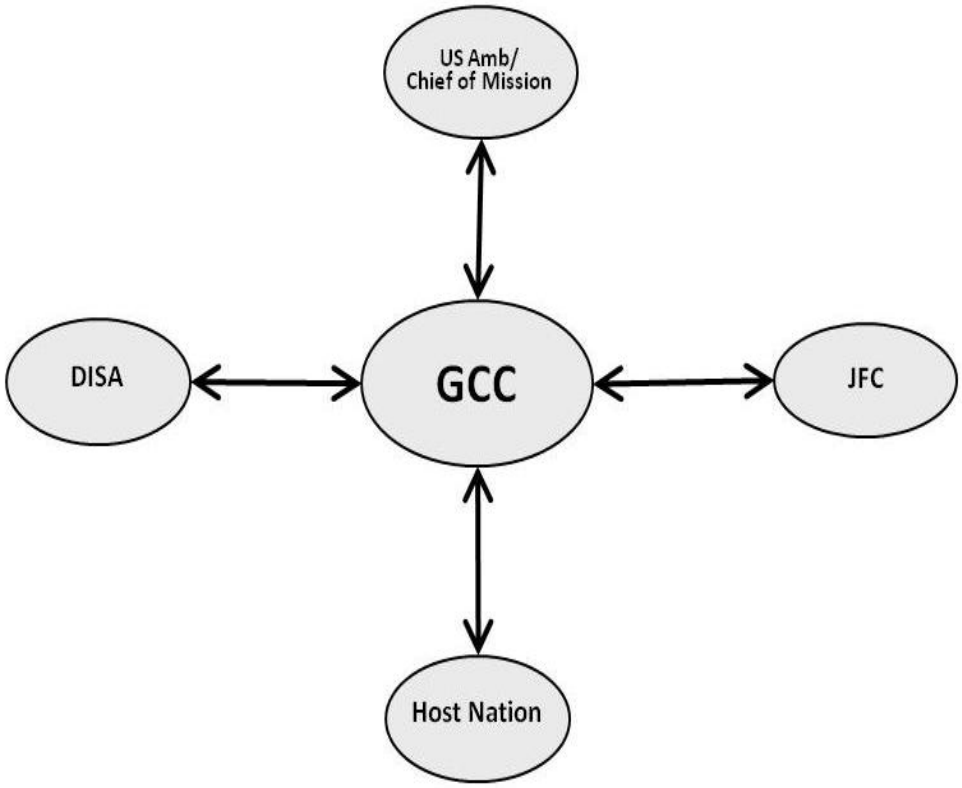


Figure N5-2 – GCC Operational Resource Flow (OV-2)

The U.S. Agency for International Development (USAID) will be a key partner whenever DOD provides FHA and there will always be a need to share information and assessments, and coordinate DOD support in the affected nation. As the DOD role in HA/DR operations is normally in support of another U.S. agency, there will be a requirement for interagency coordination in developing the unified U.S. government (USG) approach to the crisis.

The humanitarian assistance community of interest (COI) is diverse and there are growing requirements to interact with intergovernmental organizations (IGO) like the United Nation (UN), North Atlantic Treaty Organization (NATO) or the African Union, who may have a leadership role in the crisis response and provide subordinate units (e.g. UN units) as part of the relief effort. A humanitarian operations center (HOC), made up of international and interagency representatives, may be established to coordinate the overall relief strategy and unity of effort among all participants

in a large foreign humanitarian assistance operation. Additionally, there are numerous nongovernmental organizations (NGO) and private sector organizations (PSO) that may already be active in the affected area or join the relief effort. There are a range of information sharing and coordination requirements between the JFC and these organizations that will depend on the operational situation, the organization's mission and their desire to interact with DOD forces.

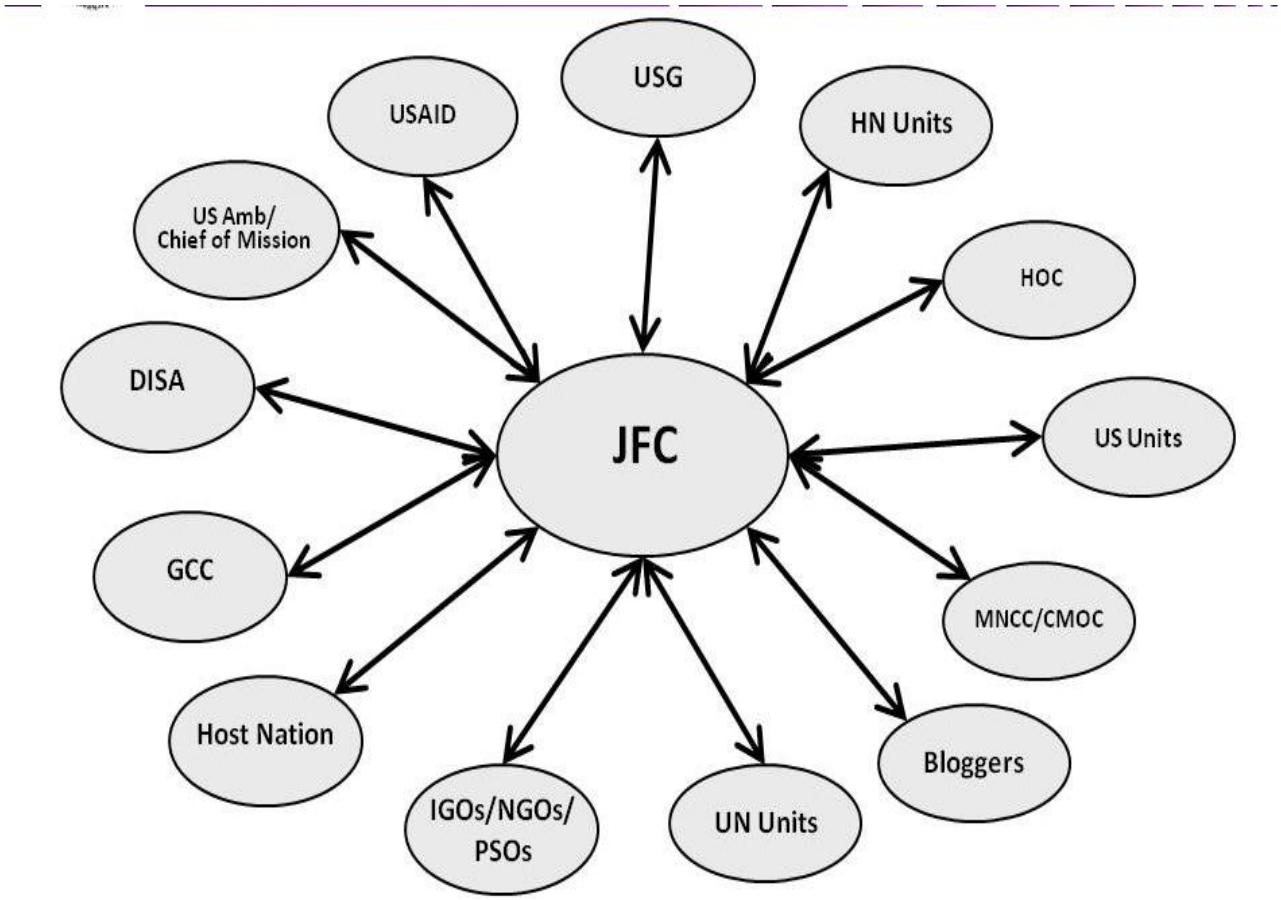


Figure N5-3 – JFC Operational Resource Flow (OV-2)

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project

Annex N6 - Unclassified Information Sharing (UIS)
Operational Resource Flow Matrix
OV-3

1. Department of Defense Architecture Framework (DODAF) Operational Viewpoint (OV) 3

The mapping of the resource flows to the needlines of the Operational Resource Flow Description (OV-2) occurs in the Operational Resource Flow Matrix (OV-3). The OV-3 viewpoint identifies the resource transfers that are necessary to support operations to achieve a specific operational task. This view is initially constructed from the information contained in the OV-2, but the OV-3 provides a more detailed definition of the resource flows for operations within a community of anticipated users. The operational resource flow matrix details resource flow exchanges by identifying which operational activities and locations exchange what resources, with whom, why the resource is necessary, and the key attributes of the associated resources. The focus is on identifying resource flow exchanges that cross the capability boundary.

Resource flow exchanges express the relationship across the three basic architecture data elements for the view (operational activities, operational locations, and resource flows) with a focus on the specific aspects of the resource flow and the resource content. The OV-3 is one of a suite of operational views that address the resource content of the operational architecture (the others being OV-2 and OV-5). The OV-3 identifies resource elements and relevant attributes of the resource flows, and associates the exchange to the producing and consuming operational activities and locations and to the needline that the resource flow satisfies. Needlines are logical requirements-based collaboration relationships between operational activities and nodes (as shown in the OV-2).

The emphasis in this view is on the logical and operational characteristics of the resource flows being exchanged, with focus on the resource flows crossing the capability boundary. It is important to note that OV-3 is not intended to be an exhaustive listing of all the details contained in every resource flow of every operational activity and nodes associated with the UIS Architecture. Rather, this view is intended to capture the most important aspects of selected resource flows.

2. OV-3 Matrix

The OV-3 matrix is provided in Annex N7 of the Final Report.

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project

Annex N8 - Unclassified Information Sharing (UIS) Organizational Relationships Chart OV-4

For the UIS architecture, the Organizational Relationships Chart, Operational Viewpoint (OV)-4, is based on the model contained in joint doctrine, *Interorganizational Coordination During Joint Operations* (Figure N8-1).

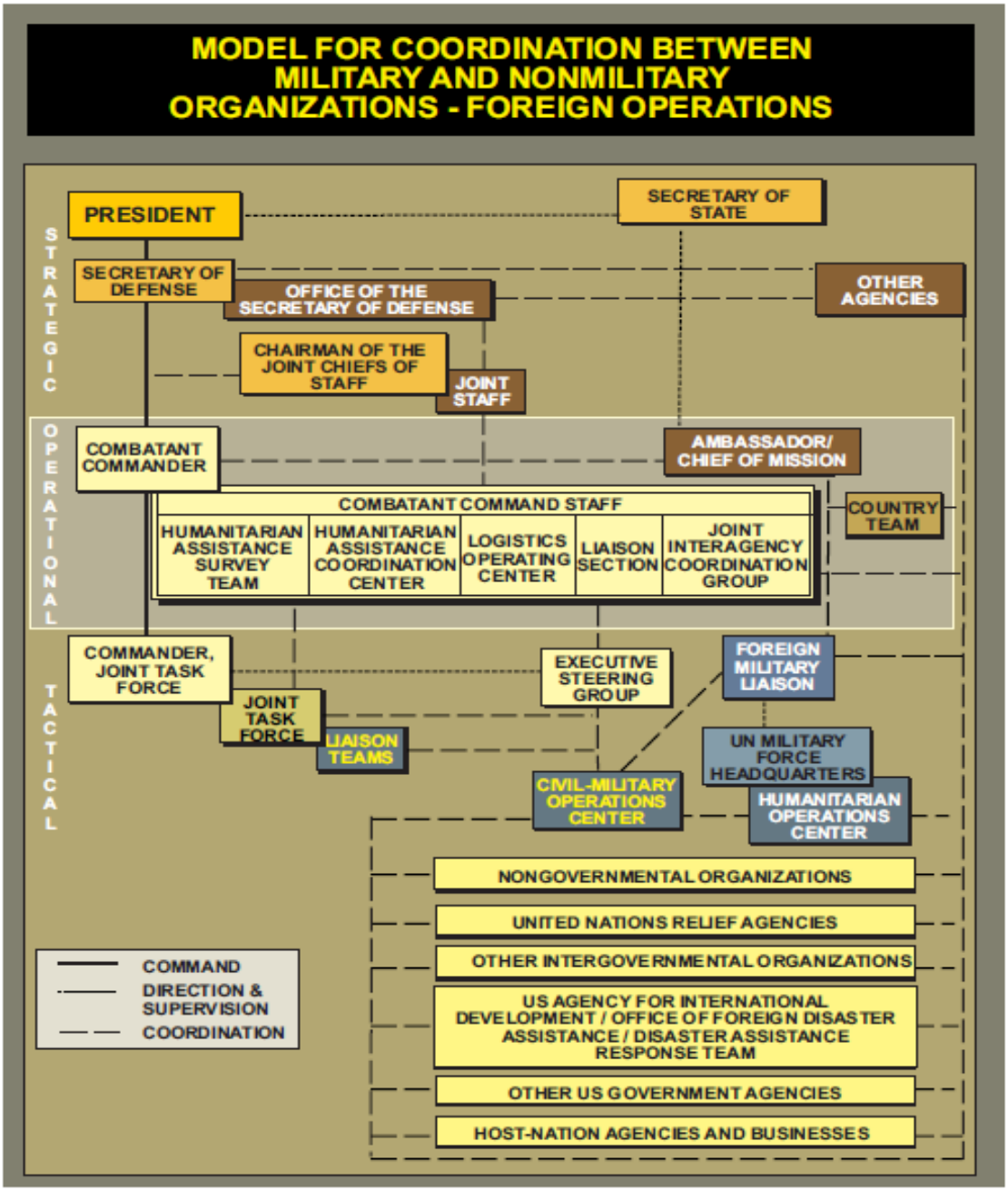


Figure N8-1 – Notional Structure for Coordination among Military and Nonmilitary Organizations - Foreign Operations[1]

[1] Joint Chiefs of Staff, Interorganizational Coordination During Joint Operations, Joint Pub 3-08 (Washington, DC: 24 June 2011.

This OV-4 (Figure N8-2) illustrates the organizational context, role or other relationships among organizations that are the performers in the architecture.

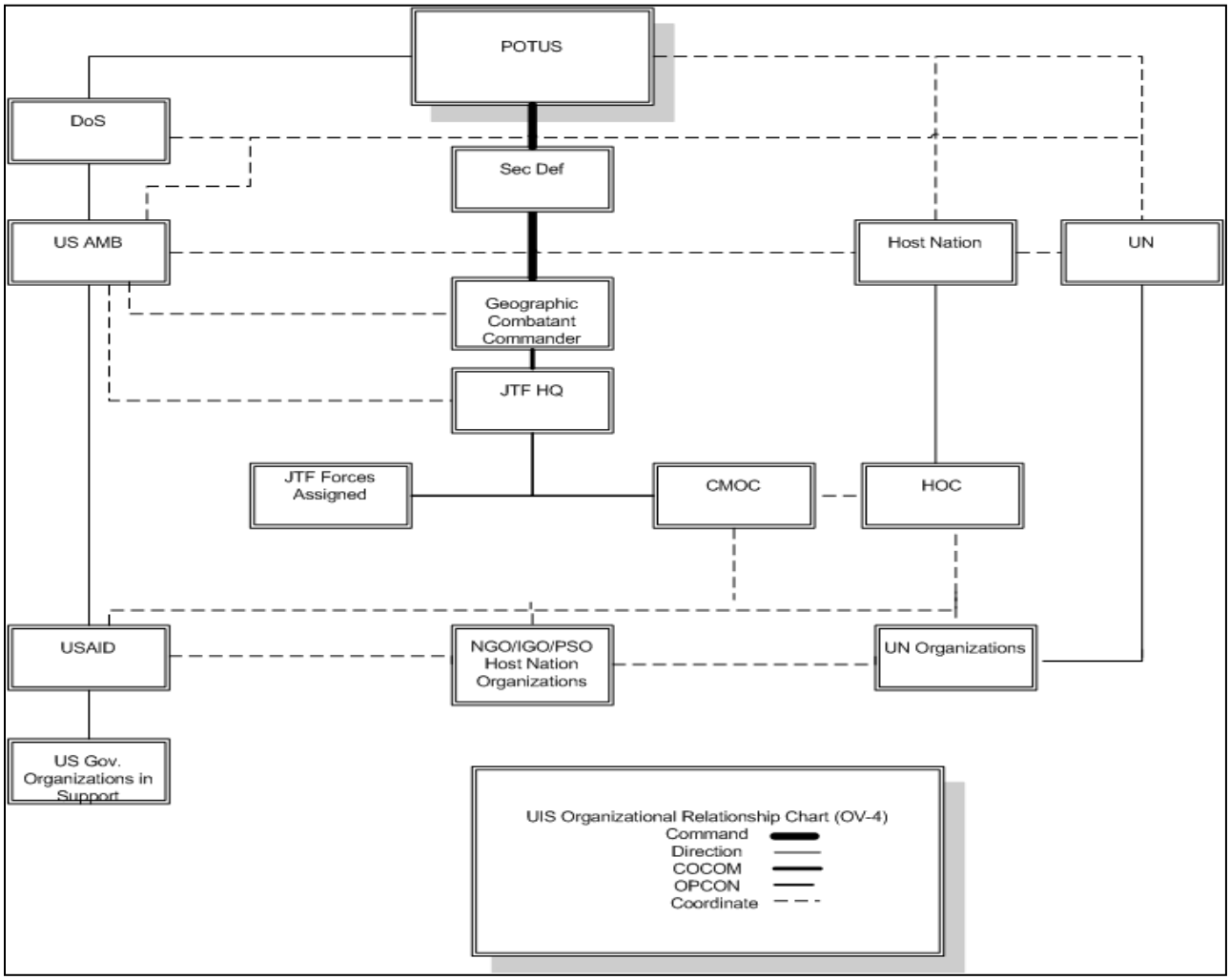


Figure N8-2 – UIS Organizational Relationships Chart (OV-4)

The UIS OV-4 shows the various relationships that can exist between organizations and sub-organizations within the architecture. These relationships can include supervisory reporting, command and control relationships, and command-subordinate relationships. Another type of relationship is a coordination relationship between equals, where two organizations coordinate or collaborate without one having a supervisory or command relationship over the other. Organizational relationships are important to depict in an architecture model, because they can illustrate fundamental roles (e.g., who or what type of skill is needed to conduct operational activities) as well as management relationships (e.g., command structure or relationship to other key players). Additionally, organizational relationships can provide insight for the information sharing depicted in the UIS Operational Resource Flow Description, OV-2.

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project

Annex N9 - Unclassified Information Sharing (UIS) Operational Activity Decomposition Tree Operational Viewpoint (OV) 5a

1. Operational Activity Hierarchy Tree

The decomposition levels and the amount of detail shown on the Unclassified Information Sharing (UIS) Operational Activity Decomposition Tree Operational Viewpoint (OV) 5a are aligned with the operational nodes that are responsible for conducting the operational activities (shown on corresponding Operational Resource Flow Description (OV-2) products). It is important to note the OV-5a is only as exhaustive as necessary to attain the objectives for the architecture as stated in the All Viewpoint (AV) 1, Overview and Summary Information. The initial decomposition of the *UIS – Provide Unclassified Information Sharing* into its three main activities – *UIS 1.0 Provide for UIS*, *UIS 2.0 Perform UIS Management*, and *UIS 3.0 Provide UIS Services* is shown in Figure N9-1. These activities are further decomposed on successive pages. Activity descriptions are contained in section 5.

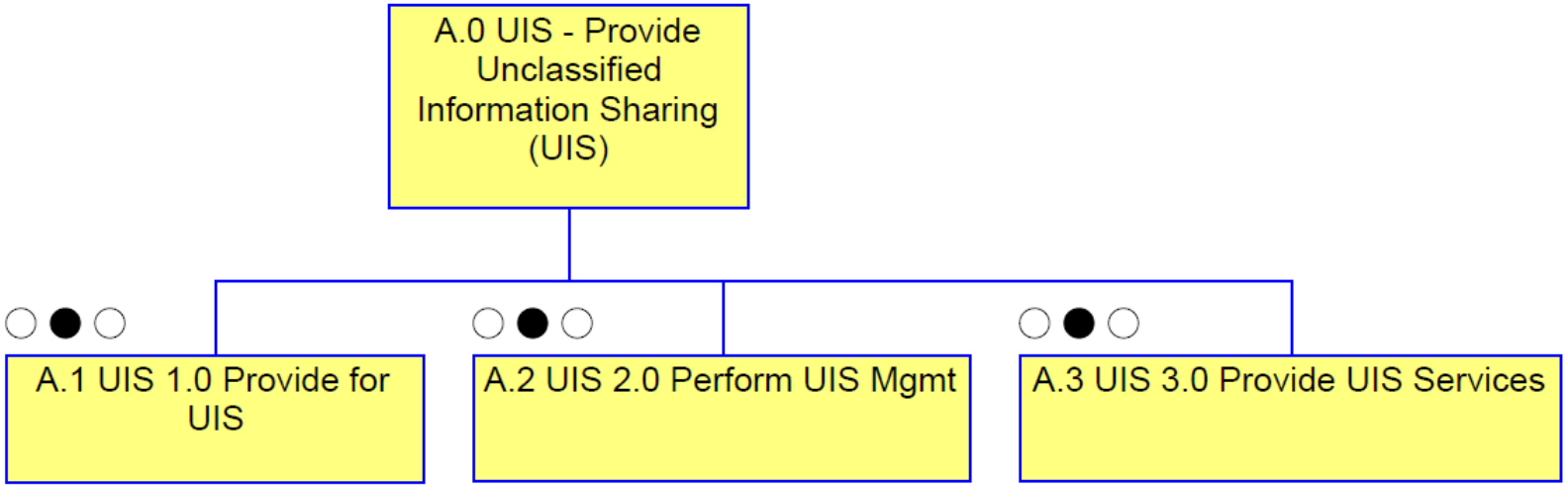


Figure N9-1 – A.0 UIS *Provide UIS* Initial Decomposition

2. UIS 1.0 Provide for UIS

Descriptions of *UIS 1.0 Provide for UIS* (Figure N9-2) and its sub-activities can be found starting at section 5, page N9-7.

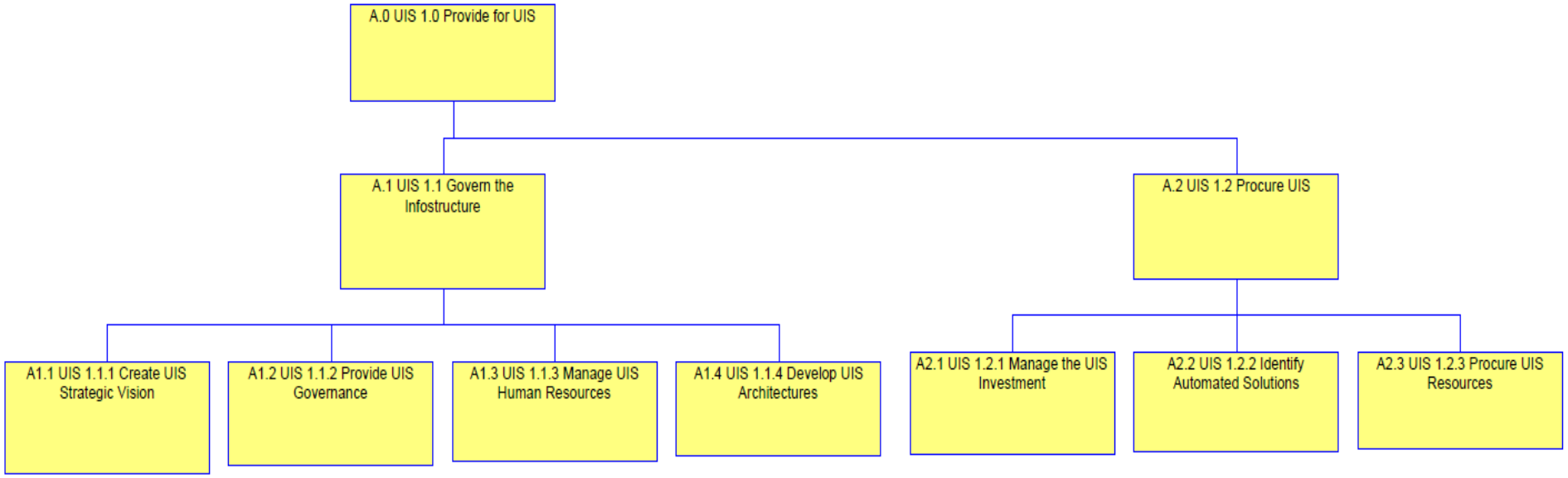


Figure N9-2 - UIS 1.0 *Provide for UIS* Decomposition

3. UIS 2.0 UIS Management

Descriptions of the *UIS 2.0 Perform UIS Management* (Figure N9-3) and its sub-activities can be found starting at section 5, page N9-8.

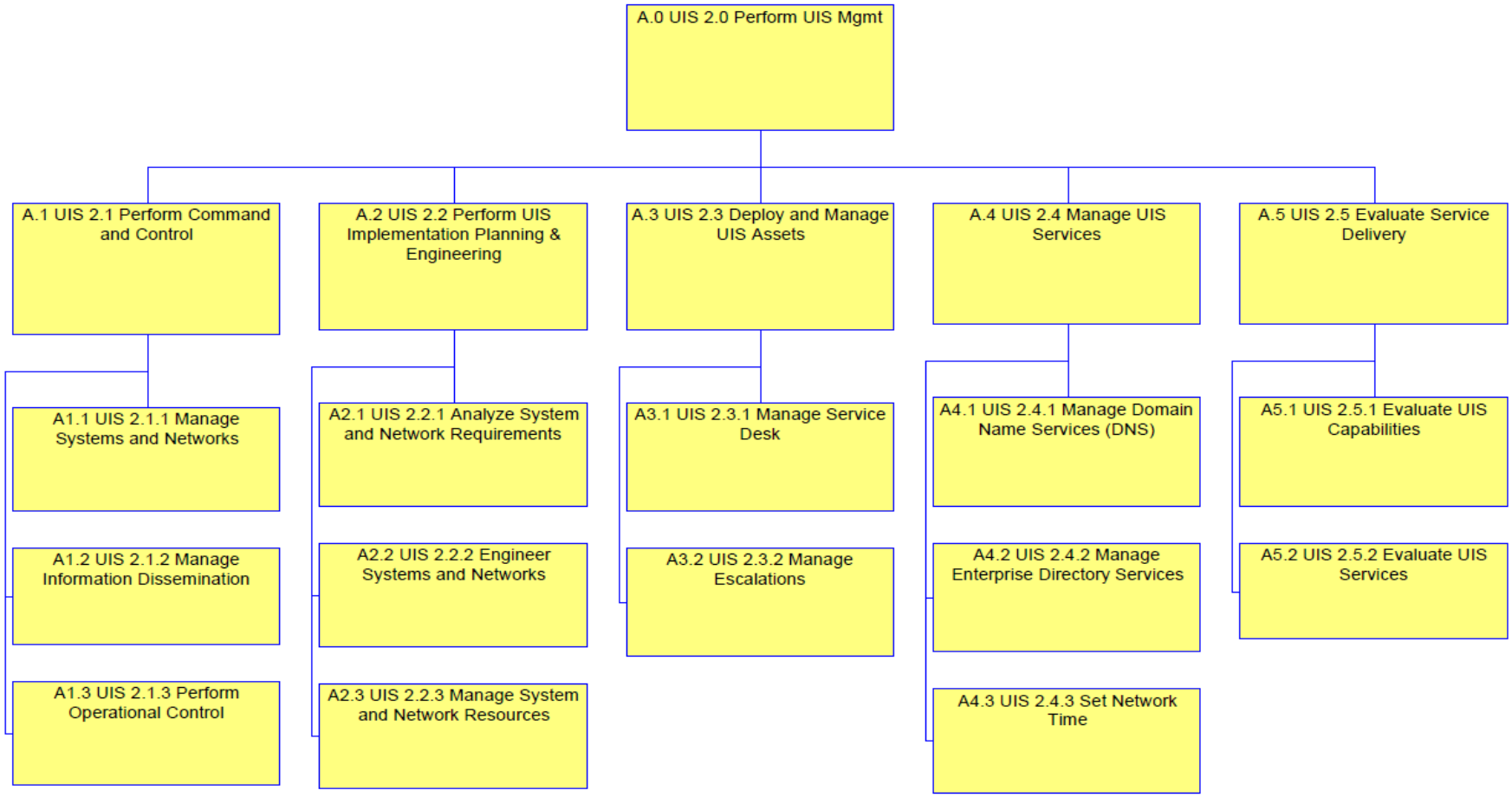


Figure N9-3 - UIS 2.0 *UIS Management* Decomposition

4. UIS 3.0 Provide UIS Services

Descriptions of the *UIS 3.0 Provide UIS Services* (Figure N9-4) and its sub-activities can be found starting at section 5, page N9-11. A more detailed view of sub-activities UIS 3.3.1 *Provide Community of Interest* and *UIS 3.3.2 Provide Information Sharing Services* is provided in section 4.1.

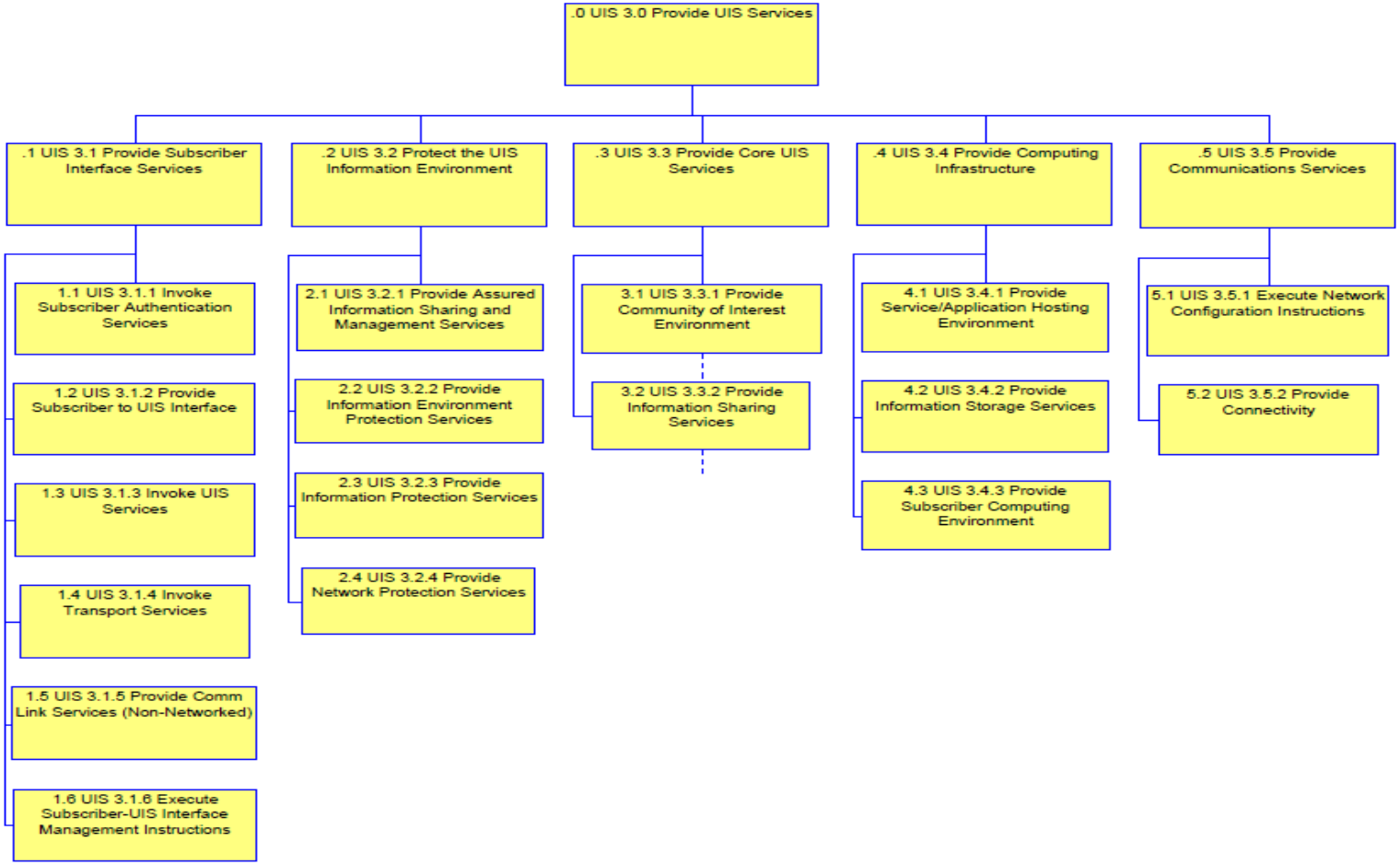


Figure N9-4 - UIS 3.0 *Provide UIS Services* Decomposition

4.1 UIS 3.3 Provide UIS Core Services

Descriptions of the *UIS 3.3 Provide Core UIS Services* and its sub-activities can be found starting at section 5, page N9-13. These activities are the focus of IMISAS project experimentation.

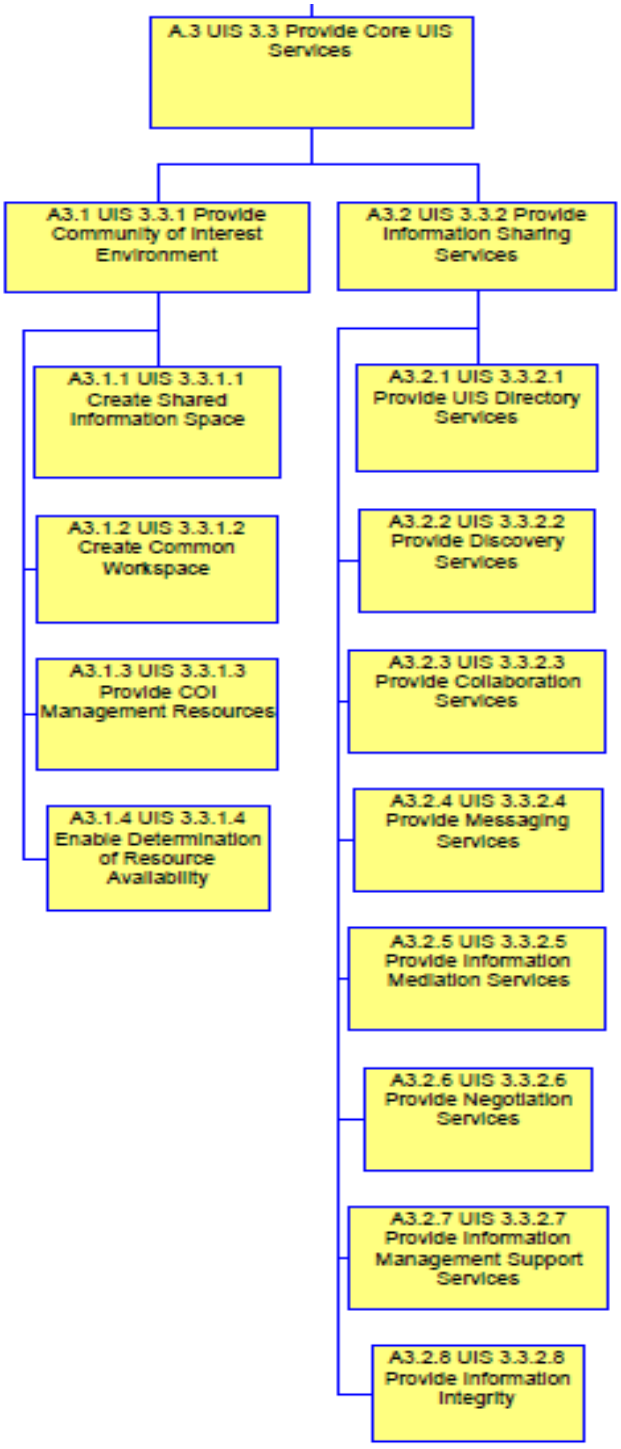


Figure N9-5 - UIS 3.3 *Provide UIS Core Services* Decomposition

5. Activity Descriptions

Name	Description	Ops Nodes
UIS 1.0 Provide for UIS	This activity includes acquiring, managing, and sustaining UIS assets and their associated needs in support of providing UIS capabilities. This enables consumers to use the services and agencies to manage them. This activity includes the full range of support throughout an UIS asset lifecycle.	DOD
UIS 1.1 Govern the Infostructure	Encompasses the activities necessary to direct and manage the information infrastructure from the senior leader level.	DOD
UIS 1.1.1 Create UIS Strategic Vision	This activity encompasses the activities necessary to generate the strategic vision and guidance necessary to implement UIS operations.	DOD
UIS 1.1.2 Provide UIS Governance	Establishing an effective governance framework includes defining organizational structures, processes, leadership, roles and responsibilities to ensure that enterprise UIS investments are aligned and delivered in accordance with enterprise strategies and objectives.	DOD
UIS 1.1.3 Manage UIS Human Resources	A competent workforce is acquired and maintained for the creation and delivery of UIS services to the business. This is achieved by following defined and agreed-upon practices supporting recruiting, training, evaluating performance, promoting and terminating. This process is critical, as people are important assets, and governance and the internal control environment are heavily dependent on the motivation and competence of personnel.	DOD
UIS 1.1.4 Develop UIS Architectures	This parent activity covers all of the processes necessary to develop, vet, and approve architectural information within the UIS family of architectures	DOD
UIS 1.2 Procure UIS	Performing essential planning, design and purchase actions to identify automated solutions, manage the UIS investment and procure UIS resources.	DOD
UIS 1.2.1 Manage the UIS Investment	A framework is established and maintained to manage UIS-enabled investment programs and that encompasses cost, benefits, prioritization within budget, a formal budgeting process and management against the budget. Stakeholders are consulted to identify and control the total costs and benefits within the context of the UIS strategic and tactical plans, and initiate corrective action where needed. The process fosters partnership between UIS and business stakeholders; enables the effective and efficient use of UIS resources; and provides transparency and accountability into the total cost of ownership (TCO), the realization of business benefits and the return on investment (ROI) of UIS-enabled investments.	DOD

UIS 1.2.2 Identify Automated Solutions	The need for a new application or function requires analysis before acquisition or creation to ensure that business requirements are satisfied in an effective and efficient approach. This process covers the definition of the needs, consideration of alternative sources, review of technological and economic feasibility, execution of a risk analysis and cost-benefit analysis, and conclusion of a final decision to 'make' or 'buy'. All these steps enable organizations to minimize the cost to acquire and implement solutions whilst ensuring that they enable the business to achieve its objectives.	DOD
UIS 1.2.3 Procure UIS Resources	UIS resources, including people, hardware, software and services, need to be procured. This requires the definition and enforcement of procurement procedures, the selection of vendors, the setup of contractual arrangements, and the acquisition itself. Doing so ensures that the organization has all required UIS resources in a timely and cost-effective manner.	DOD
UIS 2.0 Perform UIS Management	This activity consists of the planning, organizing, coordinating, and controlling the establishment, maintenance, and dissolution of all the capabilities of and services provided by the UIS environment. It comprises the development of the environment's capabilities, the management of its system and network configurations, as well as the conduct of its administration, monitoring, and response activities. It also consists of performance of all UIS activities necessary to manage and protect the flow of information within the information environment. These activities are performed by UIS Personnel. It takes functional and operational performance requirements as inputs and produces operational capabilities within the information environment. This activity is controlled by the operational environment; plans; policies; guidance; laws and regulations; tactics, techniques, and procedures; standards; and funding.	DIAS
UIS 2.1 Perform Command and Control	To perform command and control (C2) of network and system operations, to include control and management oversight of all operations and security aspects for the network. C2 of system and network management is the set of activities required to provide direction and reporting over fault, configuration, accounting, performance, and security and system management activities within the network.	DISA
UIS 2.1.1 Manage Systems and Networks	Systems and network management includes the set of activities required to provide fault, configuration, accounting, performance, and security management within the network.	DISA

UIS 2.1.2 Manage Information Dissemination	Dissemination Management is the set of activities required to dynamically manage competing Subscriber requirements and to automatically allocate Information infrastructure resources to service those demands. This activity focuses on the regulation of content placement activities (e.g., publish and subscribe, content mirroring, content migration). The activity provides the capability to establish, select, and manage both general and specific information dissemination channels. The activity provides regulatory measures for governing repositories, directories, catalogs, and dissemination-related metadata. It has the primary control over publish and subscribe mechanisms. Information dissemination relies on commonly-understood metadata "tags" to distribute information products from the Producer to the Consumers.	DISA
UIS 2.1.3 Perform Operational Control	Activities essential to maintaining control and management of a resilient operational infrastructure, such as establishing and maintaining appropriate network operations situational awareness, planning and executing operational actions, and evaluating, selecting and executing operational courses of action.	DISA
UIS 2.2 Perform UIS Implementation Planning & Engineering	The aim of this planning and engineering activity is to design the UIS services and infrastructure required to support the mission and its needs. This requires a process of identifying the customers with shared interests, determining the technical capability required to support the UIS services demanded, designing the appropriate architectures and selecting the UIS components to form the 'provided' capability. After strategy is defined, implementation and engineering planning must be accomplished. An implementation plan must be created to describe the implementation in more detail and add additional information that enables the project organization to execute implementation in a proper way. The implementation plan should contain at least the following information: - Overview of the parties involved; - Description of the solution to be implemented; - Implementation strategy; - Migration strategy; - Back-out scenarios and procedures; - Risks and Risk Management; - Decision tree; - Necessary changes managed by Change Management; - Migration plan; - Overview of necessary resources; - Implementation schedule; - Site surveys; - Provision for feedback of early implementation experience	DISA
UIS 2.2.1 Analyze System and Network Requirements	Analyze requirements documents to develop an engineering solution.	DISA
UIS 2.2.2 Engineer Systems and Networks	Develop Systems and Networks from established and approved requirements.	DISA
UIS 2.2.3 Manage System and Network Resources	Management of finances, people, and equipment.	DISA

UIS 2.3 Deploy and Manage UIS Assets	Deploy and provide management over the people, money, and equipment needed to operate, and maintain systems, networks, and services.	DISA
UIS 2.3.1 Manage Service Desk	The Service desk/support center extends the range of services and offers a more global-focused approach, allowing business processes to be integrated into the Service Management infrastructure. It not only handles incidents, problems and questions, but also provides an interface for other activities such as customer change requests, maintenance contracts, software licenses, Service Level Management, Configuration Management, Availability Management, Financial Management for UIS Services, and UIS Service Continuity Management.	DISA
UIS 2.3.2 Manage Escalations	Even in the best-supported operations, service breaches will occur. What is then important is to successfully manage the service breach, by recording the breach details and escalating to the Problem Management team, where appropriate.	DISA
UIS 2.4 Manage UIS Services	Initiates a set of services/activities that manage Enterprise Information Technology Services available to the Subscriber. Includes activities needed to negotiate Quality of Service (QoS) and cost agreements, and to bind the Subscriber and the Provider once an agreement has been reached. The end result of this negotiation is the Service Level Management (SLM), which is essential in any organization so that the level of UIS Service needed to support the business can be determined, and monitoring can be initiated to identify whether the required service levels are being achieved	DISA
UIS 2.4.1 Manage Domain Name Services (DNS)	Provides enterprise-wide hostname and internet protocol (IP) address resolution for enterprise services, C2 nodes, and mission applications. Manage Domain Name Services - ensure domain name services and active directory structures are configured properly to facilitate IP address to host name resolution. Area of focus of this activity is TCP/IP and active directory services domain name structure.	DISA
UIS 2.4.2 Manage Enterprise Directory Services	Directory Services are used to manage system-network resources (including access control lists and user privileges). Directory Services differs from a directory in that it is both the directory information source and the services making the information available and usable to the user's applications. A meta-data service offers the ability to synchronize authoritative data between disparate but connected directories. Includes support for: Entity Directory; Authentication and Authorization Directory; Network Directory; Meta-directories and Connectors; Information Assurance Services; Domain, Tree and Forest Management; Print Services; Routing and remote access; Group policy and policies for sites, domains, users, and computers; Message Queuing Services; Quality of Service (QoS); Distributed File System; Network Management; Electronic Mail; Backup and Restore Services; Directory Management; and Exchange Migration	DISA

UIS 2.4.3 Set Network Time	Activities required to establish and distribute network time.	DISA
UIS 2.5 Evaluate Service Delivery	This activity identifies and documents the service level management processes which are needed to assess, evaluate and sustain an adequate service level for all customers in accordance with the SLM defined in "Manage UIS Services". This is a cyclical process, where previous service level agreements and targets are re-evaluated periodically to see where improvements can be made.	DISA
UIS 2.5.1 Evaluate UIS Capabilities	This activity ensures that all capabilities required to support information technology (IT) services function correctly, reliably, and according to standards as set by Baseline Services and above-baseline SLA contained within the command, control, communications, computers and information management (C4IM) Service Catalog.	DISA
UIS 2.5.2 Evaluate UIS Services	Evaluate the C4IM and underpinning UIS services necessary to conduct combatant command (COCOM) operations and business activities. Activity should result in an overarching Service Improvement Plan (SIP) and underpinning infrastructure, staffing, and training plans focused upon specific UIS capabilities.	DISA
UIS 3.0 Provide UIS Services	This activity provides capabilities that enable users to dynamically interact, share, and use information to operate in a net-centric manner. These services consist of core services, community of interest (COI) services, and environment control services. Note: these services have also been referred to as Global Information Grid (GIG) Enterprise Services (GES).	GCC JFC DISA
UIS 3.1 Provide Subscriber Interface Services	A set of services provided at the Subscriber interface that provide presentation services to the Subscriber (Input/Output), and translate the Subscriber's requests for Net-Centric services into the proper form/format for communication with Network Service Providers.	GCC JFC DISA
UIS 3.1.1 Invoke Subscriber Authentication Services	Invokes a set of services to authenticate the Subscriber onto the network and provide access to resources within the Community of Interest. Receives and processes the Network Authentication response to ensure that the User is connected to the true network before providing Subscriber credentials to the network. Translates the identification provided by the Subscriber (User ID and Password, palm scan, retinal scan, etc.) into a set of electronic credentials that are presented to the Information Assurance services. This activity enables the periodic login of a user that has a current account with the information environment. A user may have multiple accounts and each account may provide multiple roles for the user. Provides authentication and authorization for the user.	DISA
UIS 3.1.2 Provide Subscriber to UIS Interface	Accepts audio, video, data, and imagery inputs (Subscriber Input) from the Subscriber and provides the appropriate electrical/electronic interface to the Global Information Grid (GIG). Converts electrical/electronic signals from the Global Information Grid (GIG) into audio, video, data, and imagery outputs (Subscriber Output) for the Subscriber.	DISA

UIS 3.1.3 Invoke UIS Services	Initiates a set of services/activities that provide UIS Services to the Subscriber. Includes activities needed to query catalogs, directories, and discovery services to locate a source (provider) for the requested information or service, negotiate Quality of Service (QoS) and cost agreements, and to bind the Subscriber and the Provider once an agreement has been reached.	GCC JFC
UIS 3.1.4 Invoke Transport Services	The set of services that interacts with services in the Network Service Provider Node and/or the Network Management Node to move (transport) data and information in a networked environment.	GCC JFC
UIS 3.1.5 Provide Comm Link Services (Non-Networked)	Provides information transport services in a non-networked environment (e.g., non-networked point-to-point radio link).	
UIS 3.1.6 Execute Subscriber-UIS Interface Management Instructions	Executes network management instructions (fault, configuration, accounting, performance, and security management instructions) received from UIS and provides status information back to UIS.	GCC JFC
UIS 3.2 Protect the Enterprise Information Environment	This activity depicts the capability required to Protect the Enterprise Information Environment and associated services from internal and external threats.	DISA DOD
UIS 3.2.1 Provide Assured Information Sharing and Management Services	This activity provides the ability to securely and dynamically share information. It provides an authorized user timely exchange of information without special technical training or special security clearances to obtain the right information, at the right time, at the right place, and displayed in the right format during normal, degraded, and disconnected conditions, while denying adversaries and unauthorized users access to that same information or service. It enables exchanging information within and between security domains and Communities of Interest (COIs), at multiple levels of sensitivities, and, between authorized users within the DOD, other US Government departments and agencies, law enforcement agencies, selected non-government and private sector entities, allied nations and coalition partners, as appropriate, under normal, degraded, and disconnected conditions. Assured Information Sharing enables the timely, automated, and flexible creation and management of COIs. It also provides for dynamic, trusted and authenticated user access, as well as enabling the sharing of user identity and access rights throughout the enterprise.	DISA DOD

UIS 3.2.2 Provide Information Environment Protection Services	This activity provides the ability to monitor, search for, detect, track, and respond to attacks by adversaries within the net-centric environment. Involves integrating a security management infrastructure with the overall management and operation of the environment and deployed to provide net-centric IA services. To manage IA effectively within a security management infrastructure needs to be integrated with the overall management and operation of the environment and deployed to provide net-centric IA services. Any circumstance or event with the potential to adversely impact an IA through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.	DISA DOD
UIS 3.2.3 Provide Information Protection Services	This activity delivers Assured Resource (Systems and Networks) Availability and Assured Information Protection. Actions include recognition of attacks as they are initiated or are progressing, efficient and effective response actions to counter the attack and safely and securely recover from such attacks, and reconstituting new capabilities from reserve or reallocated assets when original capabilities are destroyed. Information Protection Services are focused on Assured Resource (Systems and Networks) Availability and on Assured Information Protection. The objectives of this focus are achieved by instituting agile capabilities to resist adversarial attacks, through recognition of such attacks as they are initiated or are progressing, through efficient and effective response actions to counter the attack and safely and securely recover from such attacks; and by reconstituting new capabilities from reserve or reallocated assets when original capabilities are destroyed.	DISA DOD
UIS 3.2.4 Provide Network Protection Services	Delivers mechanisms that provide network protection to include network encryption, physical isolation, high assurance guards, and firewalls. Mechanisms are used to create a collection of system high networks and enclaves. Enclave protection mechanisms are also used to provide security within specific security domains. In general, enclave protection mechanisms are installed as part of an Intranet used to connect networks that have similar security requirements and have a common security domain. A site may have multiple security domains with protection mechanisms tailored to the security requirements of specific customers.	DISA DOD
UIS 3.3 Provide Core UIS Services	This activity enables warfighters/operators to exercise control over enterprise information and services through a loosely coupled, distributed infrastructure that leverages service modularity, multimedia connectivity, metadata, and collaboration to provide an environment that promotes unifying actions among all UIS participants.	GCC JFC

UIS 3.3.1 Provide Community of Interest Environment	This activity provides functions developed by a community of interest (COI) for its specific missions or, for the common use of other COIs. A function that is initially specific to a COI can satisfy the requirements of other COIs and become a common function. Furthermore, any COI function can become a core application/ function. Communities of Interest: Collaborative groups of users, who must exchange information in pursuit of their shared goals, interests, missions, or business processes, and who, therefore must have a shared vocabulary for the information they exchange. DOD Directive: Data Sharing in a Net-Centric Department of Defense A Community of Interest is the collection of people that are concerned with the exchange of information in some subject area. The community is made up of the users/operators that actually participate in the exchange; the system builders ...., and the functional proponents that define the requirements and acquire the systems on the behalf of the Users. The subject area is the COI domain - whatever the people in the COI need to communicate about.	GCC JFC
UIS 3.3.1.1 Create Shared Information Space	Activities required establishing a shared information space for COI members. The "information space" is used to aggregate, integrate, fuse, and disseminate information to users.	GCC JFC
UIS 3.3.1.2 Create Common Workspace	Activities required to establish a shared workspace for COI members.	GCC JFC
UIS 3.3.1.3 Provide COI Management Resources	Activities required for COI Managers to establish COI member roles, membership lists, profiles, access controls, and policy-based network instructions.	GCC JFC
UIS 3.3.1.4 Enable Determination of Resource Availability	Activities required to allow COI members to determine the availability (presence and status) of COI resources (information objects, members, storage services, communications resources, etc.).	GCC JFC

UIS 3.3.2 Provide Information Sharing Services	Information Management Services include those activities that provide life-cycle management of Subscriber data without regard to data content or meaning. Information Management: The creation, use, sharing, and disposition of information as a resource critical to the effective and efficient operation of functional activities. The structuring of functional processes to produce and control the use of data and information within functional activities, information systems, and computing and communications infrastructure.	GCC JFC
UIS 3.3.2.1 Provide UIS Directory Services	A directory is an information resource used to store information about objects. A directory service can make those objects and their content available to user applications. The data in the directory may come from a number of authoritative data sources. Provides the directory management organization and processes required to create a scalable, secure, and manageable infrastructure for deploying and maintaining directory services. Directory Services Profile VS., 13 Jan 03 COIs will establish their own set of one or more directories. The COI will be responsible for configuring and maintaining the configuration of the directories.	GCC JFC
UIS 3.3.2.2 Provide Discovery Services	This set of services enables the formulation of search activities within shared space repositories (e.g., catalogs, directories, registries). It provides the means to articulate the required service argument, provide search service capabilities, locate repositories to search and return search results or, if necessary, initiates a tasking to the system to obtain the requested information.	GCC JFC
UIS 3.3.2.3 Provide Collaboration Services	This activity provides and controls the shared resources, capabilities, and communications that allow real-time collaborative interactions among participating group members. This environment provides synchronous collaboration capabilities; asynchronous collaboration can occur through other net-centric services and applications that are provided within the information environment.	GCC JFC
UIS 3.3.2.4 Provide Messaging Services	Messaging Services are all formal (organizational) messaging services, to include e-mail, Defense Message System (DMS), and instant messaging services. Provides services to support asynchronous and synchronous information exchange. This activity consists of all activities needed to support formal (organizational and/or structured) and informal (email and/or unstructured) messaging services. It includes support for tactical requirements. It supports the composition and validation of outgoing messages (message preparation). It supports the processing of incoming messages, including subsequent distribution to intended recipients as users of the information environment. The activity establishes and conducts message (bulletin) board services. It also supports official message traffic.	GCC JFC
UIS 3.3.2.5 Provide Information Mediation Services	This activity enables transformation processing (translation, aggregation, and integration), situational awareness support (correlation and fusion), negotiation (brokering, trading and auctioning services) and publishing.	GCC JFC

UIS 3.3.2.6 Provide Negotiation Services	This set of services applies protocols to establish the most appropriate service capabilities in response to service invocations. The request for data or services may be brokered to provide specific objects and/or object methods. The request for data or services may be supported by trader services that exchange information among brokers. The request for data or services may also be negotiated based upon the attributes of the persona of the requesting principal or upon the service that best matches the request.	GCC JFC
UIS 3.3.2.7 Provide Information Management Support Services	Activities required supporting the use of Information Objects during business, combat support, or war fighting activities.	GCC JFC
UIS 3.3.2.8 Provide Information Integrity	1) This activity provides protection against unauthorized modification or destruction of information. This protection supports information in storage, in transit and when processing. This capability maintains the quality of information, reflecting the logical correctness and reliability of the data. It ensures the logical completeness of the hardware and software implementing the data protection mechanisms and the consistency of the related data store structures. 2) Activities required to protect Information Objects and meta-data resident in a database or data warehouses (e.g., file encryption, records locking, and access controls).	GCC JFC
UIS 3.4 Provide Computing Infrastructure	Computing Infrastructure includes those activities that provide a secure, robust, and cost effective computing environment to host core, network, and mission/community of interest (COI) application software; capabilities that enable information storage/retrieval and continuity of operations/disaster recovery (COOP/DR); and common resources that enable user input and information processing, output, and display.	GCC JFC
UIS 3.4.1 Provide Service/Application Hosting Environment	Provides an architecturally compliant, consistent, reliable, and secure computing environment (consisting of application software and associated utilities) to support enterprise applications. This environment includes common enterprise application/functions that are available to all users, including administrators.	
UIS 3.4.2 Provide Information Storage Services	This activity provides storage/retrieval services for individuals and groups, as well as for other core services (such as messaging, collaboration, mediation, and discovery services). A data store is the actual warehousing of the data on some medium such as optical disk, tape, or hard drive.	
UIS 3.4.3 Provide Subscriber Computing Environment	This activity provides the computing environment through which a subscriber gains access to the information infrastructure services it invokes. This activity: - Provides the subscriber's presentation services (such as input/output) - Translates the subscriber's requests for net-centric services into the proper format for communication with network service providers	

UIS 3.5 Provide Communications Services	Communications Services provide the Subscriber with a full range of information transport services for voice, data, video, imagery, etc. Communications Services provide an integrated network that is managed and configured to provide an information transfer utility for Information infrastructure Subscribers.	
UIS 3.5.1 Execute Network Configuration Instructions	Network Configuration Instructions are the policy based instructions from the network manager. These would include instructions to improve the availability, security, reliability, integrity and performance of the network.	
UIS 3.5.2 Provide Connectivity	This activity focuses on providing communication operations across wired and wireless networks that provide connection between nodes and/or different networks in a way that is transparent to the warfighter.	DISA
UIS 3.5.3 Provide Bulk In-Transit Information Encryption	This activity encrypts information between two points in the system, normally using higher-level protocols (e.g., secure sockets layer/transport layer security (SSL/TLS))	DISA
UIS 3.5.4 Transport Information	This process moves information across the communications channel. It includes: - The transmission and reception of electrical signals; signal regeneration, amplification, relay, and re-transmission; - Routing and switching of the communications path; and - Gateway services required for signal protocol conversion as needed.	DISA

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project

Annex N10 - Unclassified Information Sharing (UIS) Operational Activity Model Operational Viewpoint (OV) 5b

1. Operational Activity Model

The Operational Activity Model Operational Viewpoint (OV) 5b describes operational activities; Input/Output (I/O) flows between activities, and I/O flows to and from activities that are outside the scope of the architecture. I/O flows of operational activities relate to information elements in the Operational Resource Flow Matrix (OV-3), and are further characterized by the information exchange attributes described in the OV-3. I/Os that are produced or consumed by operational activities that cross operational node boundaries are carried by needlines described in the Operational Resource Flow Description (OV-2).

The OV-5b uses standard terminology to ensure precise communication. Box meanings are named descriptively with verbs or verb phrases and are split and clustered in decomposition diagramming. Arrow meanings are bundled and unbundled in diagramming and the arrow segments are labeled with nouns or noun phrases to express meanings. Arrow-segment labels are prescriptive, constraining the meaning of their segment to apply exclusively to the particular data or objects that the arrow segment graphically represents.

Each side of the function box has a standard meaning in terms of box/arrow relationships. The side of the box with which an arrow interfaces reflects the arrow's role. Arrows entering the left side of the box are inputs. Inputs are transformed or consumed by the operational activity to produce outputs. Arrows leaving a box on the right side are outputs. Outputs are the data or objects produced by the operational activity. An example is shown in Figure N10-1.

FigureN10-1 - OV-5b Graphic Example

2. UIS – Provide Unclassified Information Sharing Context

The diagram in Figure N10-2 shows the top level or context operational activity of the UIS OV-5b. It shows the interface between the *UIS Provide Unclassified Information Sharing* and the *Perform External Activities* which is an aggregation of the activities of the operational nodes described in the OV-2.

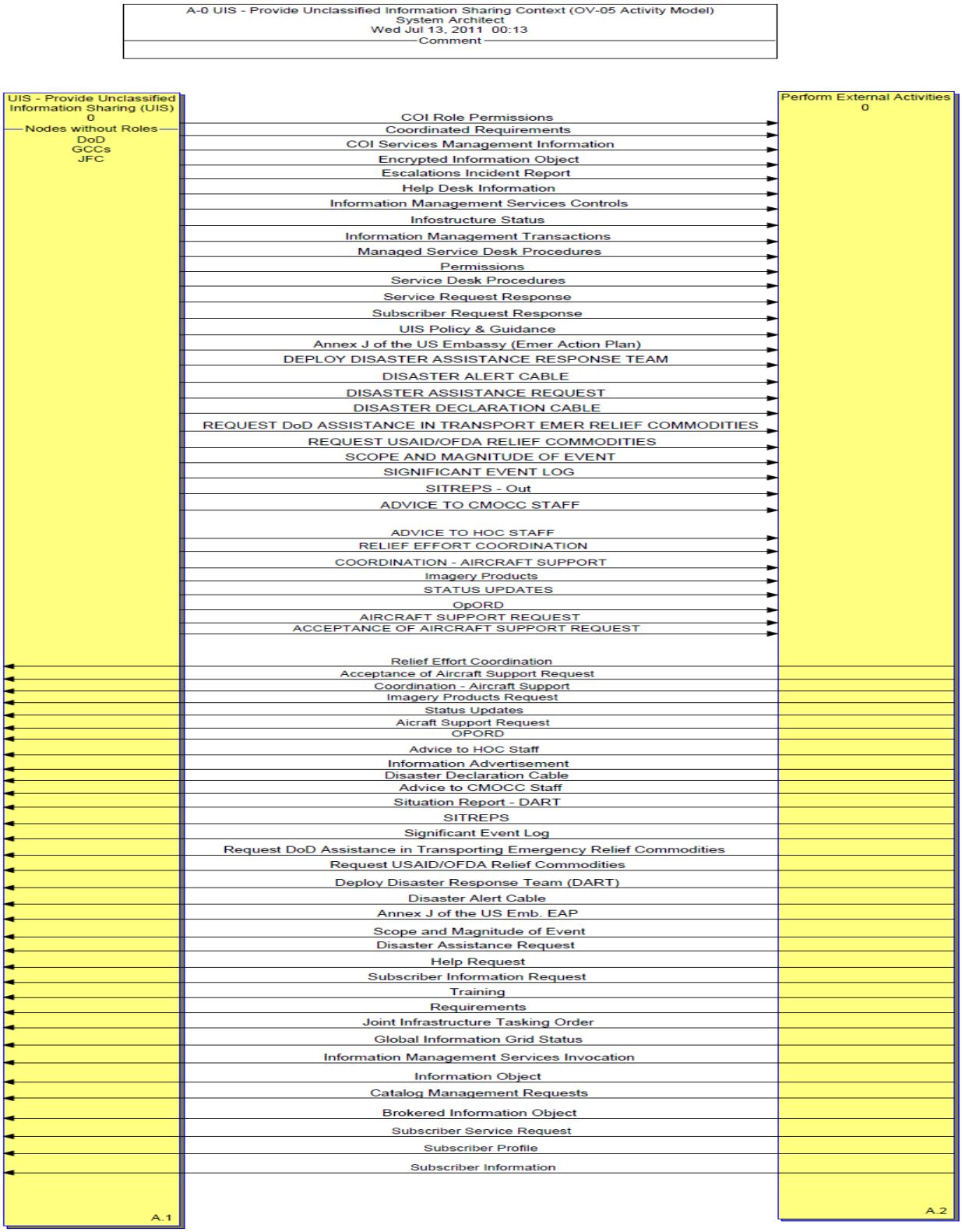


Figure N10-2 - A0 level UIS Activities

Figure N10-3 shows the first level activities of Unclassified Information Sharing (UIS) – Provide Unclassified Information Sharing: *UIS 1.0 Provide for UIS*, *UIS 2.0 Perform UIS Management*, and *UIS 3.0 Provide UIS Services*.

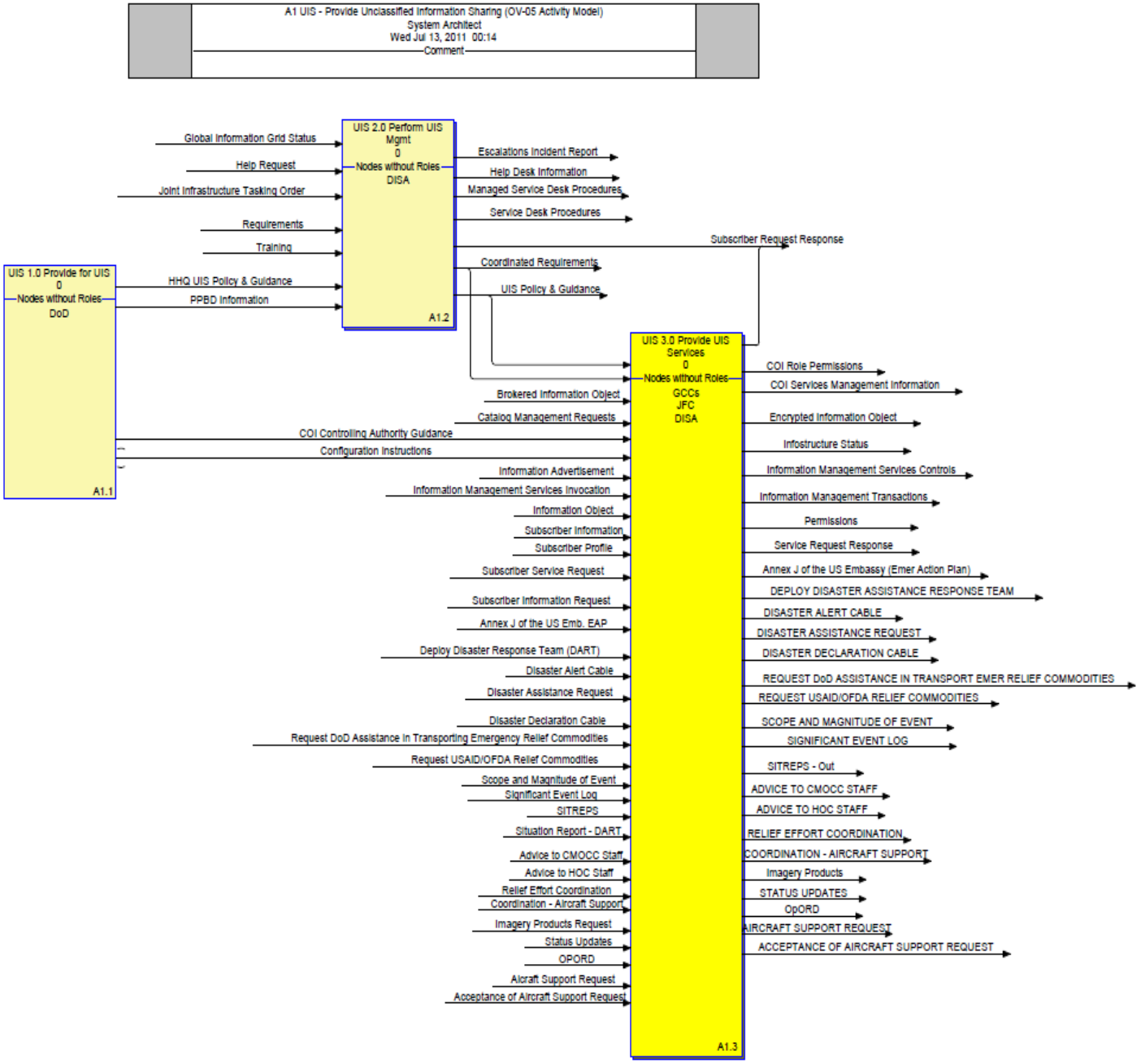


Figure N10-3 - A1 Level UIS Activities

UIS 3.0 activities are decomposed in Figure N10-4, showing *UIS 3.1 Provide Subscriber Interface Services, 3.2 Protect the UIS Information Environment, UIS 3.3 Provide Core UIS Services, UIS 3.4 Provide Computing Infrastructure,* and *UIS 3.5 Provide Communications Services*.

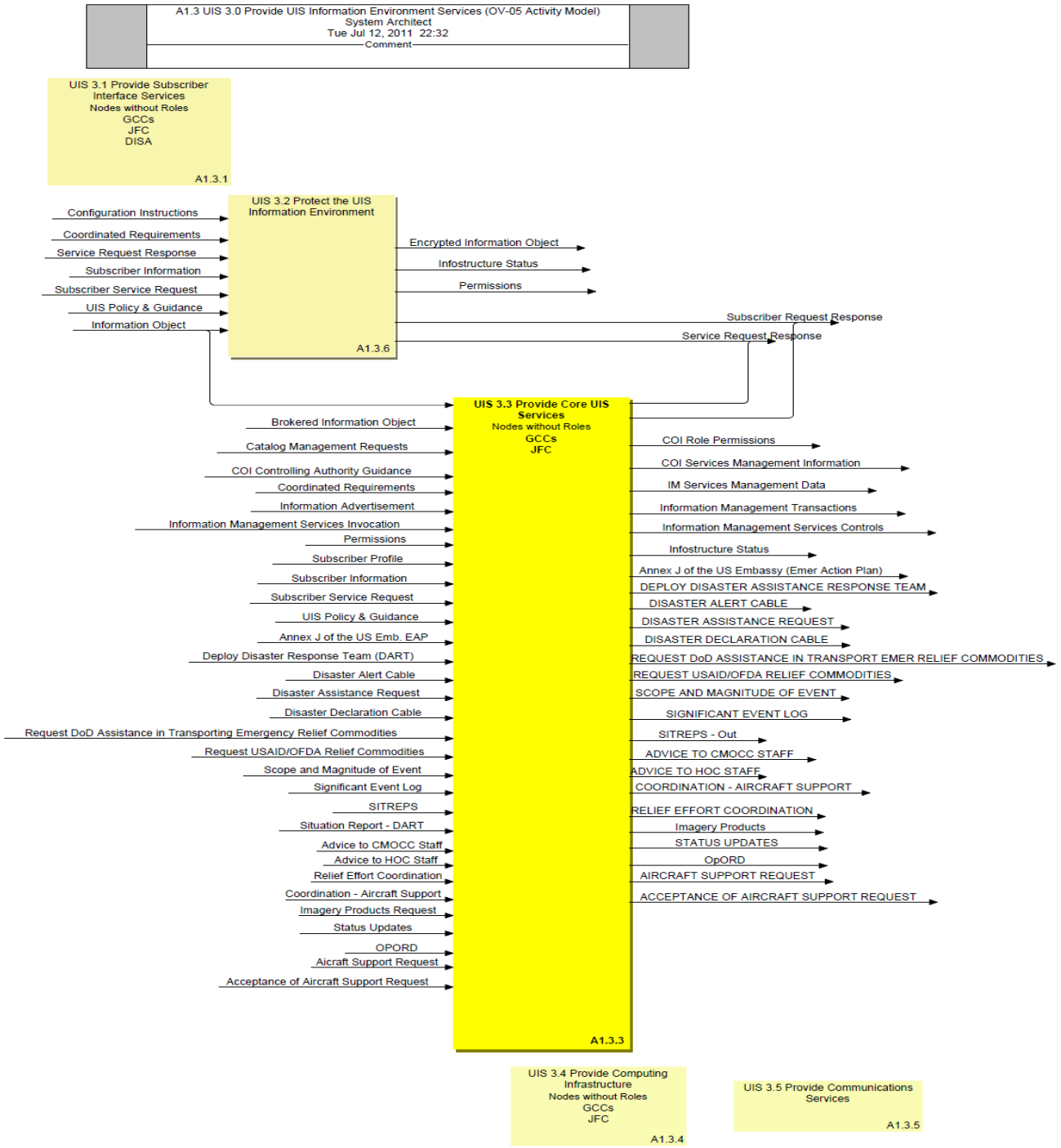


Figure N10-4 - UIS 3.0 Activities

The IMISAS Project focused on UIS 3.3, *Provide Core UIS Services*, which is decomposed in Figure N10-5.

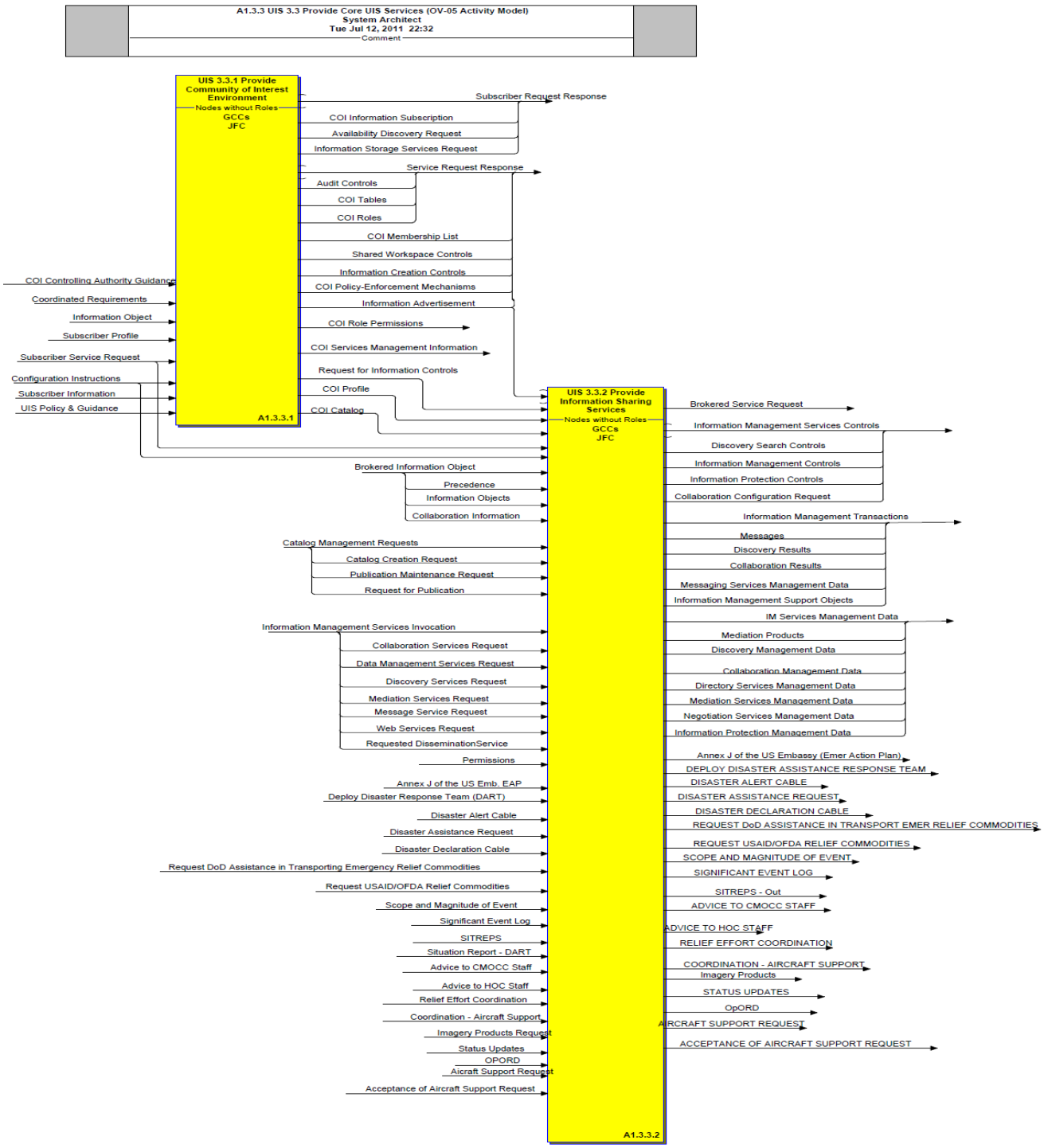


Figure N10-5 - UIS 3.3 Provide Core UIS Services Decomposition

The activities of interest, *UIS 3.3.1 Create Shared Information Environment* is decomposed in Figure N10-6 and *UIS 3.3.2* Provide Information Sharing Services, is decomposed in Figure N10-7. Activities are described at section 3; input and output descriptions can be found in section 4.

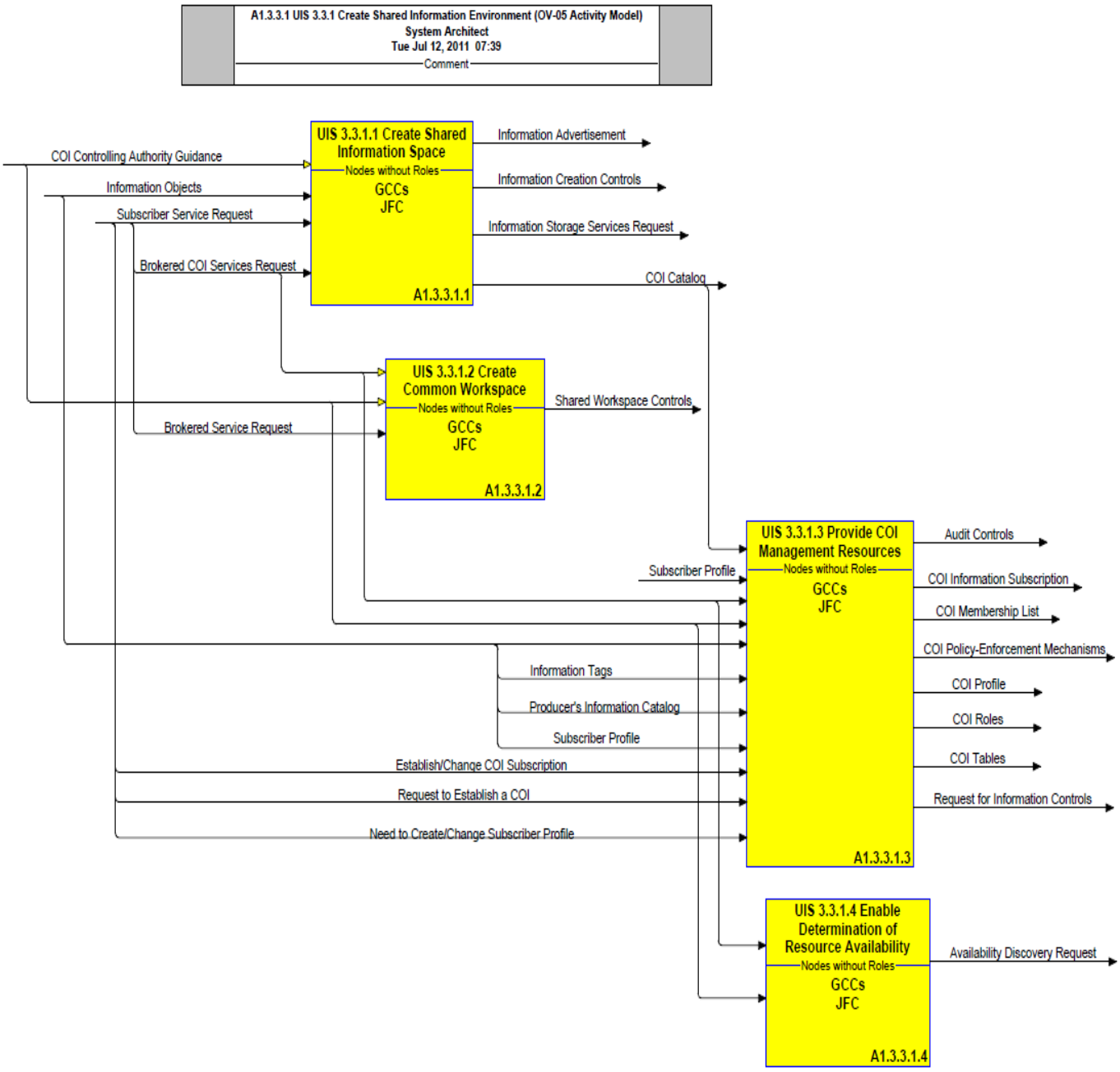


Figure N10-6 - UIS 3.3.1 Activities

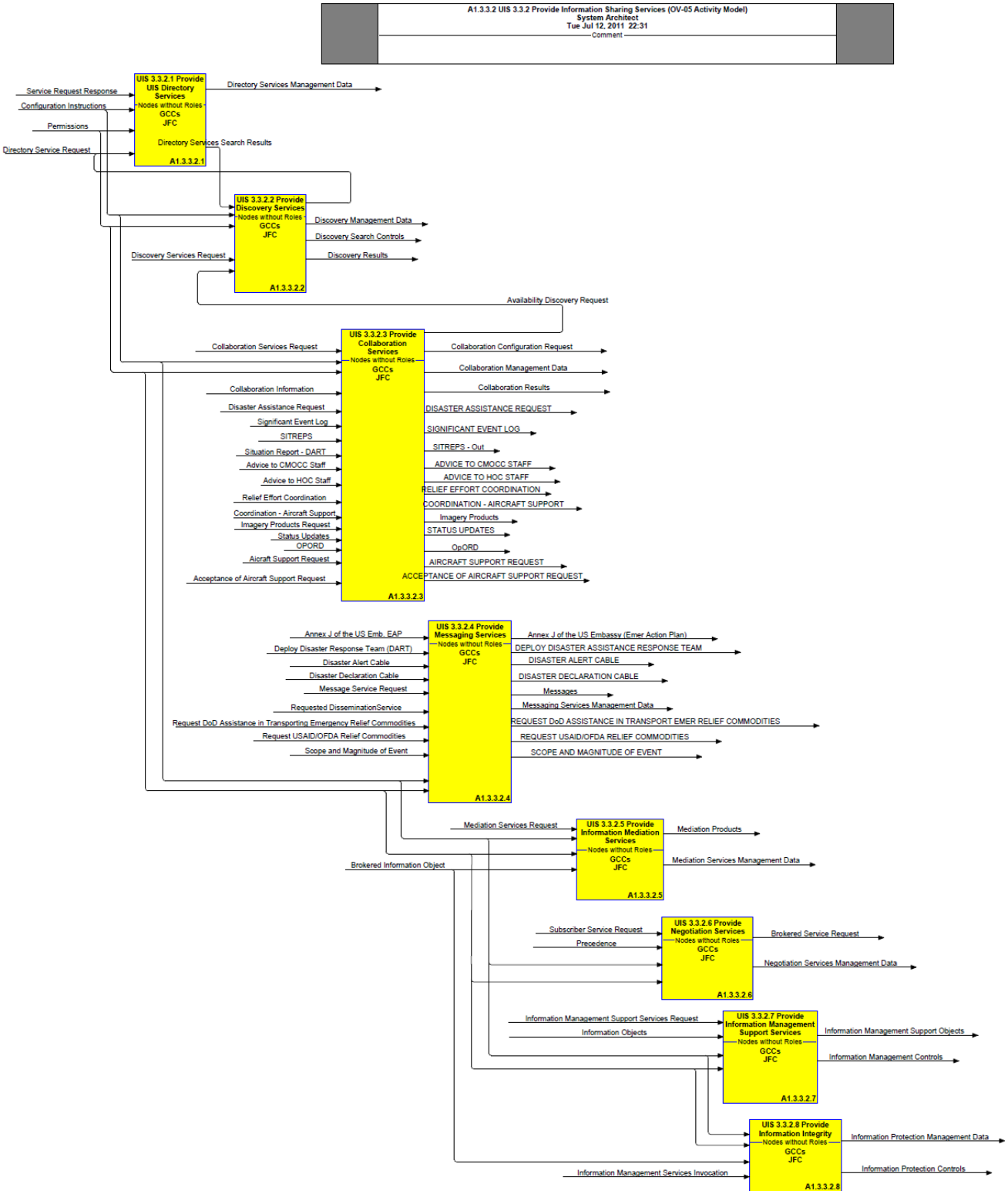


Figure N10-7 - UIS 3.3.2 Activities

Figures N10-8 through N10-14 are examples of each of the Operational Nodes that might interact with the combatant commander (COCOM) during humanitarian response/disaster relief (HA/DR) operations and represent an initial development within the UIS Architecture.

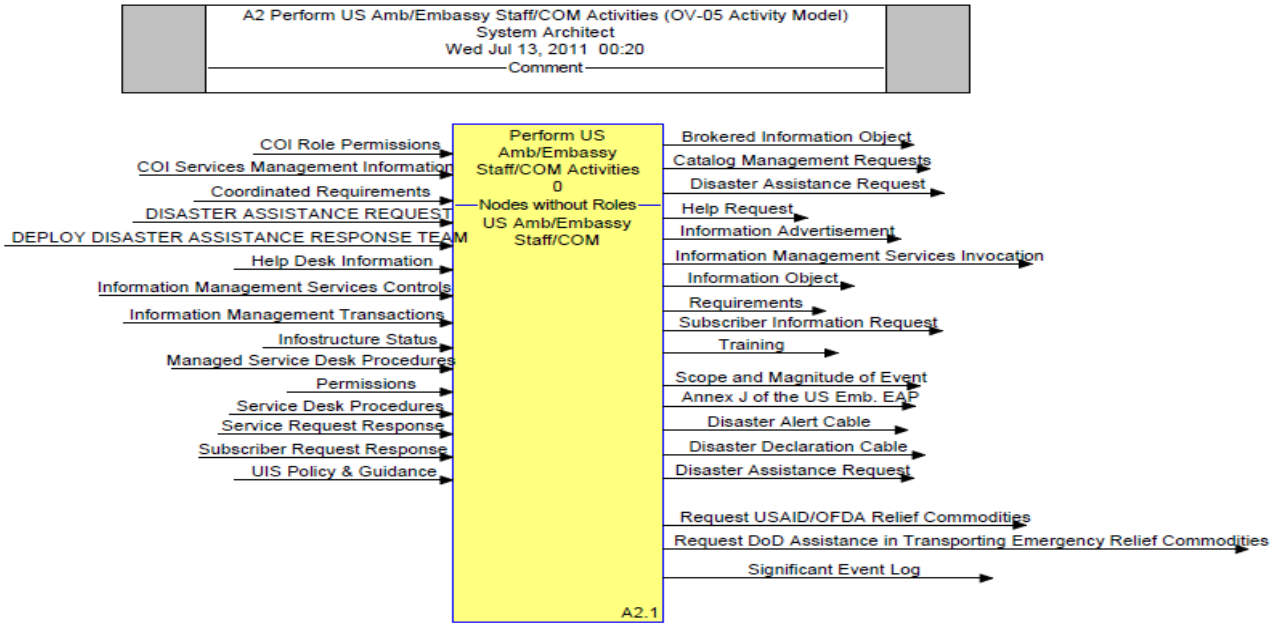
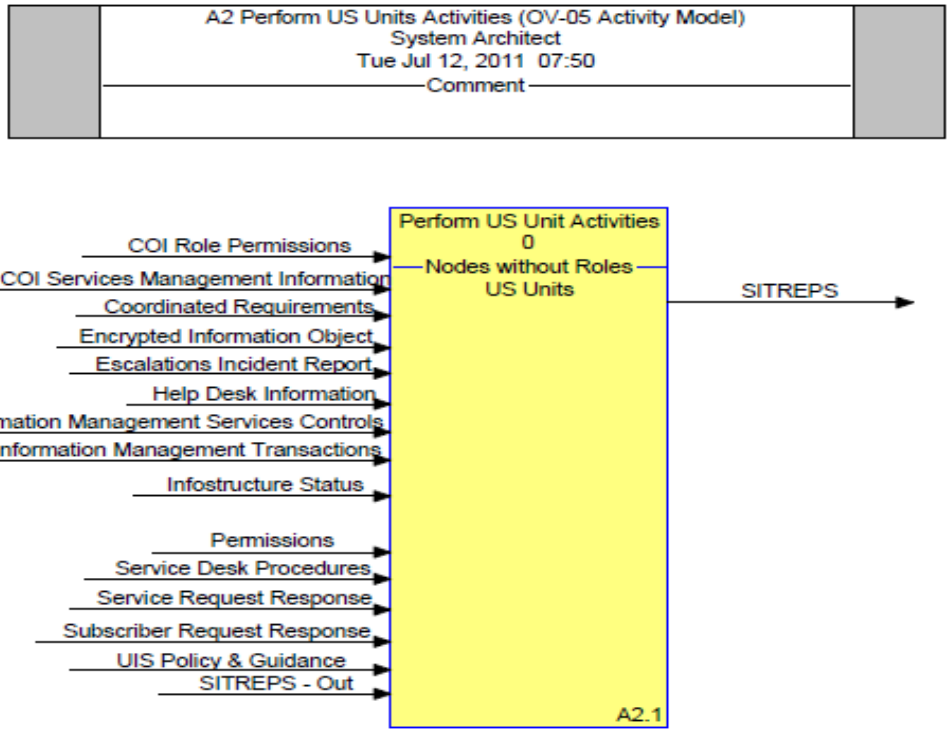


Figure N10-8 - U.S. Embassy Activities



FigureN10- 9 - U.S. Military Unit Activities

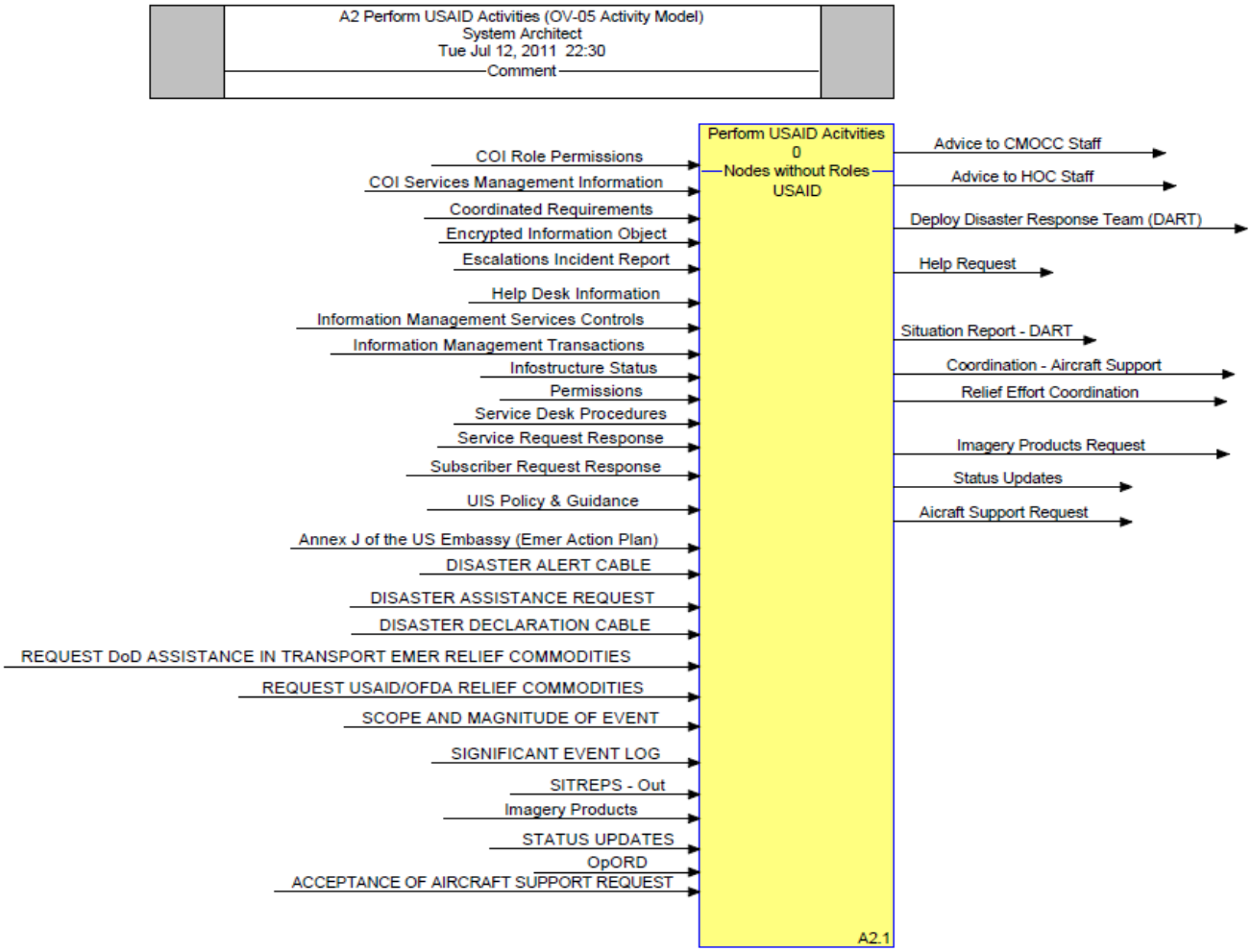


Figure N10-10 - USAID Activities

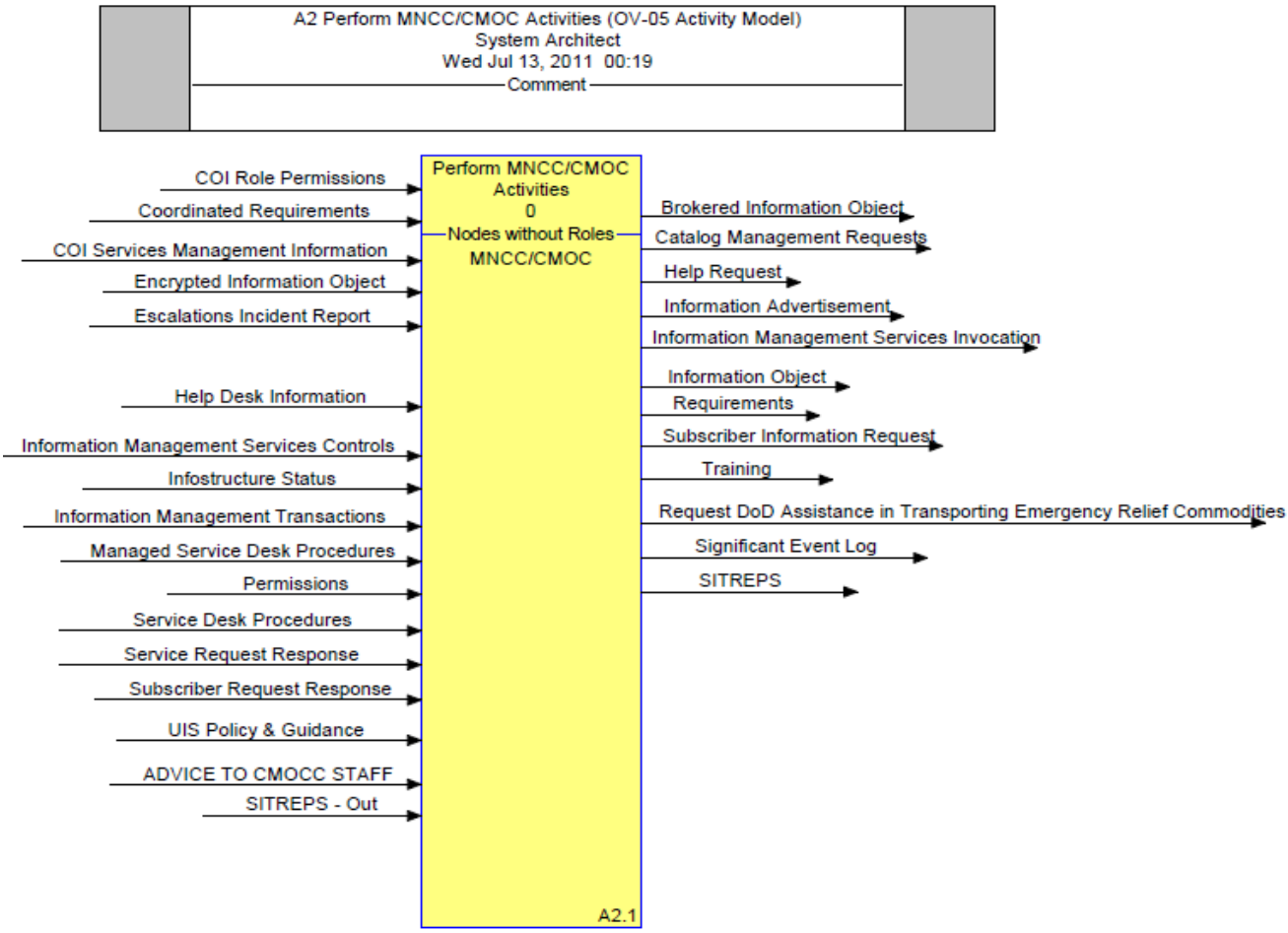


Figure N10-11 - MNCC/CMOC Activities

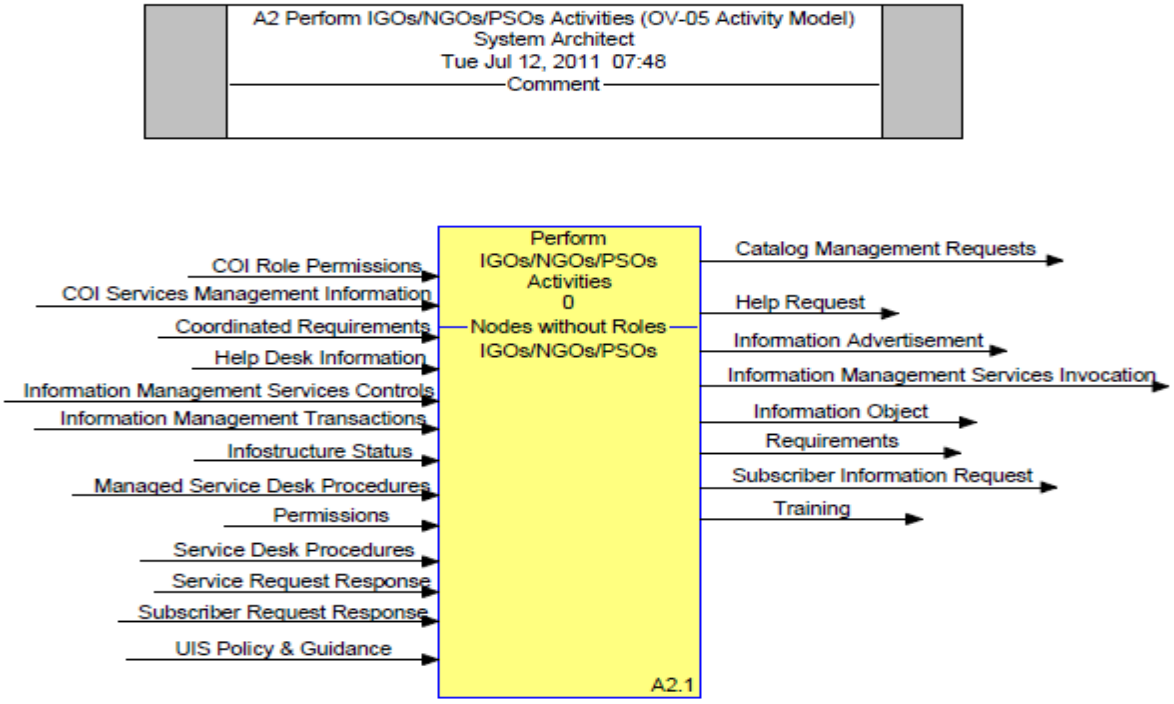


Figure N10-12 - IGO/NGO/PSO Activities

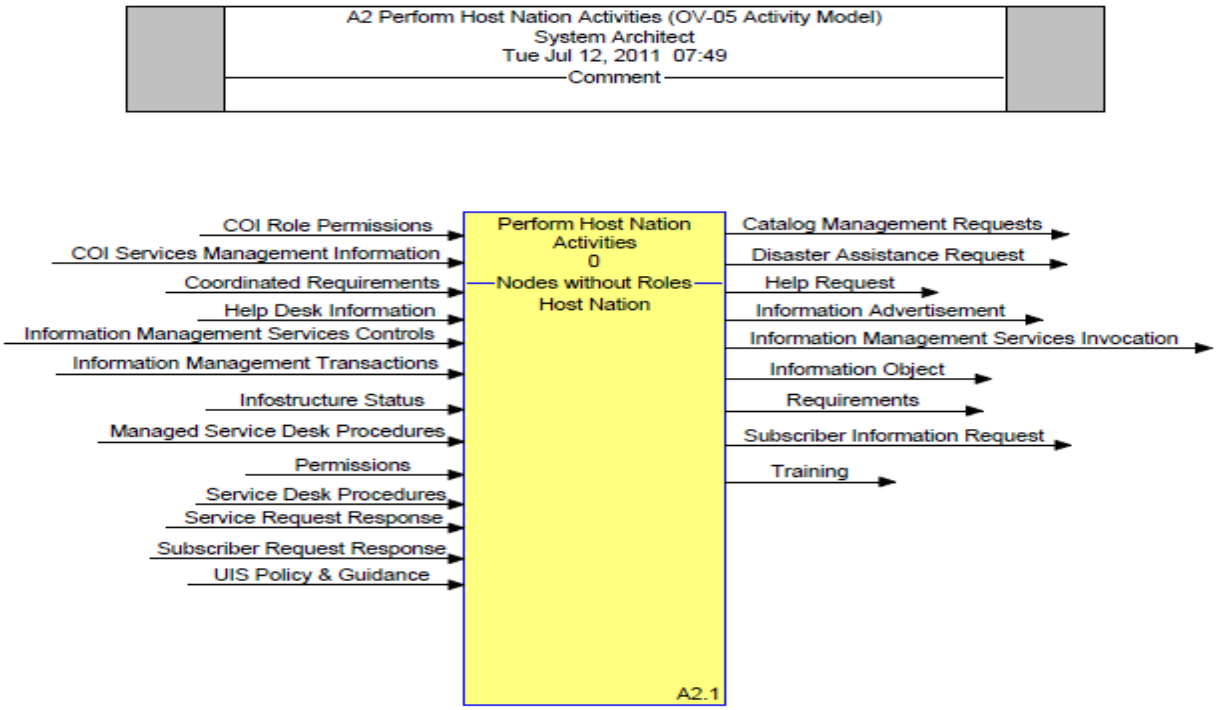


Figure N10-13 - Host Nation Activities

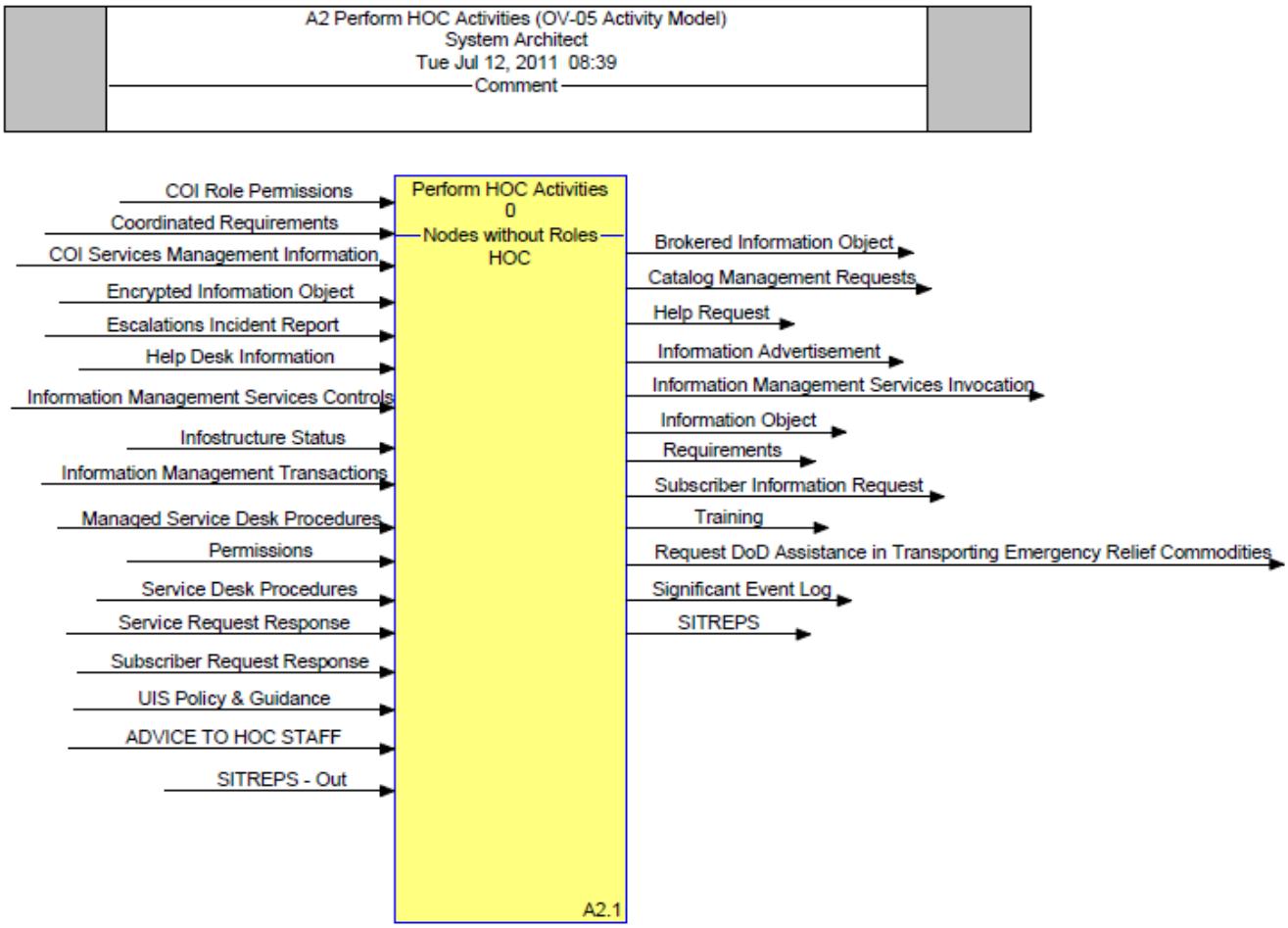


Figure N10-14 - HOC Activities

3. Operational Activities

Name	Description	Operational Nodes
Perform DISA Activities	For modeling purposes Only.	DISA
Perform Bloggers Activities	For modeling purposes only	Bloggers
Perform External Activities	Aggregate of external activities performed by operational nodes (OPNodes) external to the Geographic Combatant Commander (GCC)/Joint Force Commander (JFC), e.g., Ambassador/Embassy Staff, Host Nation, Multinational Force Coordination Center (MNCC)/Civil-Military Operations Center (CMOC), Intergovernmental Organizations (IGOs)/Nongovernmental Organizations (NGOs)/Private Sector Organizations (PSOs), U.S. Government (USG) agencies, etc.	
Perform GCC Activities	External activities of the GCC to the UIS Architecture	GCCs
Perform HN Units Activities	For modeling purposes only	"HN Units"
Perform HOC Activities	For modeling purposes only	HOC
Perform Host Nation Activities	For modeling purposes only	"Host Nation"
Perform IGOs/NGOs/PSOs Activities	For modeling purposes only	"IGOs/NGOs/PSOs"
Perform MNCC/CMOC Activities	For modeling purposes only	"MNCC/CMOC"
Perform UN Units Activities	For modeling purposes only	"UN Units"
Perform US Amb/Embassy Staff/COM Activities	For modeling purposes only.	"US Amb/Embassy Staff/COM"
Perform US Unit Activities	For modeling purposes only	"US Units"
Perform USAID	For modeling purposes only.	USAID

Acitvities		
UIS - Provide Unclassified Information Sharing (UIS)	The UIS is defined as the computers, ancillary equipment, software, firmware, and similar procedures, services, people, and related resources used in the acquisition, storage, manipulation, protection, management, movement, control, display, switching, interchange, transmission, or reception of data or information in any format including audio, video, imagery, or data, not including the information itself whether supporting UIS. This model describes the activities involved required to establish, operate, and maintain the Infostructure from the UIS provider's point of view. This model describes how the UIS ops activities will support the DoD UIS Implementation Sharing Plan.	DoD "JFC - UIS" "GCC - UIS"
UIS 1.0 Provide for UIS	This activity includes acquiring, managing, and sustaining UIS assets and their associated needs in support of providing UIS capabilities. This enables consumers to use the services and agencies to manage them. This activity includes the full range of support throughout an UIS Asset lifecycle.	DoD
UIS 2.0 Perform UIS Mgmt	This activity consists of the planning, organizing, coordinating, and controlling the establishment, maintenance, and dissolution of all the capabilities of and services provided by the UIS environment. It comprises the development of the environment's capabilities, the management of its system and network configurations, as well as the conduct of its administration, monitoring, and response activities. It also consists of performance of all UIS activities necessary to manage and protect the flow of information within the information environment. These activities are performed by UIS Personnel. It takes functional and operational performance requirements as inputs and produces operational capabilities within the information environment. This activity is controlled by the operational environment; plans; policies; guidance; laws and regulations; tactics, techniques, and procedures; standards; and funding.	DISA
UIS 2.1 Perform Command and Control	To perform Command and Control (C2) of network and system Operations, to include control and management oversight of all operations and security aspects for the network. C2 over system and network Management is the set of activities required to provide direction and reporting over fault, configuration, accounting, performance, and security & system management activities within the network.	DISA

UIS 2.1.1 Manage Systems and Networks	System and Network Management is the set of activities required to provide fault, configuration, accounting, performance, and security management within the network.	DISA
UIS 2.1.2 Manage Information Dissemination	Dissemination Management is the set of activities required to dynamically manage competing Subscriber requirements and to automatically allocate Infostructure resources to service those demands. This activity focuses on the regulation of content placement activities (e.g., publish and subscribe, content mirroring, content migration). The activity provides the capability to establish, select, and manage both general and specific information dissemination channels. The activity provides regulatory measures for governing repositories, directories, catalogs, and dissemination-related metadata. It has the primary control over publish and subscribe mechanisms. Information dissemination relies on commonly-understood metadata "tags" to distribute information products from the Producer to the Consumers.	DISA
UIS 2.1.3 Perform Operational Control	Activities essential to maintaining control and management of a resilient operational infrastructure, such as establishing and maintaining appropriate network operations situational awareness, planning and executing operational actions, and evaluating, selecting and executing operational courses of action.	DISA
UIS 2.2 Perform UIS Implementation Planning & Engineering	The aim of this planning and engineering activity is to design the UIS services and infrastructure required to support the mission and its needs. This requires a process of identifying the customers with shared interests, determining the technical capability required to support the UIS services demanded, designing the appropriate architectures and selecting the UIS components to form the 'provided' capability. After strategy is defined, implementation and engineering planning must be accomplished. An implementation plan must be created to describe the implementation in more detail and add additional information that enables the project organization to execute implementation in a proper way. The implementation plan should contain at least the following information: -	DISA

	Overview of the parties involved; - Description of the solution to be implemented; - Implementation strategy; - Migration strategy; - Back-out scenarios and procedures; - Risks and Risk Management; - Decision tree; - Necessary changes managed by Change Management; - Migration plan; - Overview of necessary resources; - Implementation schedule; - Site surveys; - Provision for feedback of early implementation experience	
UIS 2.2.1 Analyze System and Network Requirements	Analyze requirements documents to develop an engineering solution.	DISA
UIS 2.2.2 Engineer Systems and Networks	Develop Systems and Networks from established and approved requirements.	DISA
UIS 2.2.3 Manage System and Network Resources	Management of finances, people, and equipment.	DISA
UIS 2.3 Deploy and Manage UIS Assets	Deploy and provide management over the people, money, and equipment needed to operate, and maintain systems, networks, and services.	DISA
UIS 2.3.1 Procure Asset	In order to procure assets, there must be a valid need for the assets, there must be finances available to support the procurement, and there must be a procurement vehicle for the acquisition of the asset. Examples of assets include hardware, software, applications, and web services.	DISA
UIS 2.3.2 Deploy New Asset	This activity deploys newly acquired assets into the ConstellationNet in accordance with current policies.	DISA
UIS 2.3.3 Identify Asset	In order to properly manage an IT asset, the asset manager must know if its existence, must know the attributes which make it unique, and must know its planned lifecycle.	DISA
UIS 2.3.4 Report Asset Information / Metrics	The AFKS / GCSS-AF systems are used to report on assets within the enterprise and to maintain metrics on their use.	DISA
UIS 2.3.5 Manage Asset Configuration	The process of identifying and defining Configuration Items in a system, recording and reporting the status of Configuration Items, and verifying the completeness and correctness of Configuration Items. Applies to existing systems as well as assets acquired from the Procure Asset activity. Provides a logical model of the infrastructure or a service by identifying, controlling, maintaining and verifying the versions of Configuration Items (CIs) in existence.	DISA
UIS 2.3.6 Manage	The Service desk/support center extends the range of services and offers a more	DISA

Service Desk	global-focused approach, allowing business processes to be integrated into the Service Management infrastructure. It not only handles incidents, problems and questions, but also provides an interface for other activities such as customer change requests, maintenance contracts, software licenses, Service Level Management, Configuration Management, Availability Management, Financial Management for IT Services, and IT Service Continuity Management.	"JFC - UIS" "GCC - UIS"
UIS 2.3.6.1 Manage Service Desk Procedures	When designing your processes and procedures, and taking the broad view, you will need to: review their validity on a regular basis, and update as required, involve all relevant parties, allocate sufficient time and resources, consider alternatives (e.g. information being computerized rather than in printed form) and provide new reference materials based on incident and problem trend analyses. Includes collecting and managing customer information.	DISA "JFC - UIS" "GCC - UIS"
UIS 2.3.6.2 Provide Help Desk Services		DISA "JFC - UIS" "GCC - UIS"
UIS 2.3.6.3 Manage Escalations	Even in the best-supported operations, services breaches will occur. What is then important is to successfully manage the service breach, by recording the breach details and escalating to the Problem Management team, where appropriate.	DISA "GCC - UIS"
UIS 2.3.7 Remove Existing Asset	As assets reach the end of their established lifecycles, they must be removed from the enterprise in accordance with established policies.	"GCC - UIS"
UIS 2.4 Manage UIS Services	Initiates a set of services/activities that manage UIS Information Technology Services available to the Subscriber. Includes activities needed to negotiate Quality of Service (QoS) and cost agreements, and to bind the Subscriber and the Provider once an agreement has been reached. The end result of this negotiation is the Service Level Management (SLM), which is essential in any organization so that the level of UIS Service needed to support the business can be determined, and monitoring can be initiated to identify whether the required service levels are being achieved	DISA
UIS 2.4.1 Manage Domain Name Services (DNS)	Provides enterprise wide hostname and IP address resolution for CII Enterprise services, C2 nodes, and mission applications. Manage Domain Name Services - ensure domain name services and active directory	DISA

	structures are configured properly to facilitate IP address to host name resolution. Area of focus of this activity is TCP/IP and active directory services domain name structure.	
UIS 2.4.2 Manage Enterprise Directory Services	Directory Services are used to manage system-network resources (including access control lists and user privileges). Directory Services differs from a directory in that it is both the directory information source and the services making the information available and usable to the user's applications. A meta-data service offers the ability to synchronize authoritative data between disparate but connected directories. Includes support for: Entity (ID) Directory; Authentication and Authorization Directory; Network Directory; Meta-directories and Connectors; Information Assurance Services; Domain, Tree and Forest Management; Print Services; Routing and remote access; Group policy and policies for sites, domains, users, and computers; Message Queuing Services; Quality of Service (QoS); Distributed File System; Network Management; Electronic Mail; Backup and Restore Services; Directory Management; and Exchange Migration	DISA
UIS 2.4.3 Set Network Time	Activities required to establish and distribute network time.	DISA
UIS 2.5 Evaluate Service Delivery	This activity identifies and documents the service level management processes which are needed to assess, evaluate and sustain an adequate service level for all customers in accordance with the SLM defined in "Manage UIS Services". This is a cyclical process, where previous service level agreements and targets are re-evaluated periodically to see where improvements can be made.	DISA
UIS 2.5.1 Evaluate UIS Capabilities	This activity ensures that all capabilities required to support IT services function correctly, reliably, and according to standards as set by Baseline Services and above-baseline SLA contained within the C4IM Service Catalog.	DISA
UIS 2.5.2 Evaluate UIS Services	Evaluate the C4IM and underpinning UIS Services necessary to conduct COCOM Operations and Business activities. Activity should result in an overarching Service Improvement Plan (SIP) and underpinning infrastructure, staffing, and training plans focused upon specific UIS capabilities.	DISA

UIS 3.0 Provide UIS Services	This activity provides capabilities that enable users to dynamically interact, share, and use information to operate in a net-centric manner. These services consist of core services, COI services, and environment control services. Note: these services have also been referred to as GIG Enterprise Services (GES).	"JFC - UIS" DISA "GCC - UIS"
UIS 3.1 Provide Subscriber Interface Services	A set of services provided at the Subscriber interface that provide presentation services to the Subscriber (Input/Output), and translate the Subscriber's requests for Net-Centric services into the proper form/format for communication with Network Service Providers.	"JFC - UIS" DISA "GCC - UIS"
UIS 3.2 Protect the UIS Information Environment	This set of activities depict the capability required to Protect the UIS Information Environment and associated services from internal and external threats.	DISA DoD "GCC - UIS"
UIS 3.2.1 Provide Assured Information Sharing and Management Services	This activity provides the ability to securely and dynamically share information. It provides an authorized user timely exchange of information without special technical training or special security clearances to obtain the right information, at the right time, at the right place, and displayed in the right format during normal, degraded, and disconnected conditions, while denying adversaries and unauthorized users access to that same information or service. It enables exchanging information within and between security domains and Communities of Interest (COIs), at multiple levels of sensitivities, and, between authorized users within the DOD, other US Government departments and agencies, law enforcement agencies, selected non-government and private sector entities, allied nations and coalition partners, as appropriate, under normal, degraded, and disconnected conditions. Assured Information Sharing enables the timely, automated, and flexible creation and management of COIs. It also provides for dynamic, trusted and authenticated user access, as well as enabling the sharing of user identity and access rights throughout the enterprise.	DISA DoD
UIS 3.2.2 Provide Information Environment Protection Services	This activity provides the ability to monitor, search for, detect, track, and respond to attacks by adversaries within the net-centric environment. Involves integrating a security management infrastructure with the overall management and operation of the environment and deployed to provide net-centric IA services.	DISA DoD

	To manage IA effectively within a security management infrastructure needs to be integrated with the overall management and operation of the environment and deployed to provide net-centric IA services. Any circumstance or event with the potential to adversely impact an IA through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.	
UIS 3.2.3 Provide Information Protection Services	This activity delivers Assured Resource (Systems and Networks) Availability and Assured Information Protection. Actions include recognition of attacks as they are initiated or are progressing, efficient and effective response actions to counter the attack and safely and securely recover from such attacks, and reconstituting new capabilities from reserve or reallocated assets when original capabilities are destroyed. Information Protection Services are focused on Assured Resource (Systems and Networks) Availability and on Assured Information Protection. The objectives of this focus are achieved by instituting agile capabilities to resist adversarial attacks, through recognition of such attacks as they are initiated or are progressing, through efficient and effective response actions to counter the attack and safely and securely recover from such attacks; and by reconstituting new capabilities from reserve or reallocated assets when original capabilities are destroyed.	DISA DoD
UIS 3.2.4 Provide Network Protection Services	Delivers mechanisms that provide network protection to include network encryption, physical isolation, high assurance guards, and firewalls. Mechanisms are used to create a collection of system high networks and enclaves. Enclave protection mechanisms are also used to provide security within specific security domains. In general, enclave protection mechanisms are installed as part of an Intranet used to connect networks that have similar security requirements and have a common security domain. A site may have multiple security domains with protection mechanisms tailored to the security requirements of specific customers.	DISA DoD
UIS 3.3 Provide Core UIS Services	This activity enables warfighters/operators to exercise control over enterprise information and services through a loosely coupled, distributed infrastructure that leverages service modularity, multimedia connectivity, metadata, and collaboration to provide an environment that promotes unifying actions among all UIS participants.	"JFC - UIS" "GCC - UIS"
UIS 3.3.1 Provide Community of Interest Environment	This activity provides functions developed by a COI for its specific missions or, for the common use of other COIs. A function that is initially specific to a COI can satisfy the requirements of other COIs and become a common function. Furthermore, any COI function can become a core application/function.	"JFC - UIS" "GCC - UIS"

	Communities of Interest: Collaborative groups of users, who must exchange information in pursuit of their shared goals, interests, missions, or business processes, and who, therefore must have a shared vocabulary for the information they exchange. DoD Directive: Data Sharing in a Net-Centric Department of Defense A Community of Interest is the collection of people that are concerned with the exchange of information in some subject area. The community is made up of the users/operators that actually participate in the exchange; the system builders ...., and the functional proponents that define the requirements and acquire the systems on the behalf of the Users. The subject area is the COI domain - whatever the people in the COI need to communicate about.	
UIS 3.3.1.1 Create Shared Information Space	Activities required to establish a shared information space for COI members. The "information space" is used to aggregate, integrate, fuse, and disseminate information to users.	MAJCOM "JFC - UIS" "GCC - UIS"
UIS 3.3.1.2 Create Common Workspace	Activities required to establish a shared workspace for COI members.	"JFC - UIS" "GCC - UIS"
UIS 3.3.1.3 Provide COI Management Resources	Activities required for COI Managers to establish COI member roles, membership lists, profiles, access controls, and policy-based network instructions.	"JFC - UIS" "GCC - UIS"
UIS 3.3.1.4 Enable Determination of Resource Availability	Activities required to allow COI members to determine the availability (presence and status) of COI resources (information objects, members, storage services, communications resources, etc).	"JFC - UIS" "GCC - UIS"
UIS 3.3.2 Provide Information Sharing Services	Information Management Services include those activities that provide life-cycle management of Subscriber data without regard to data content or meaning. Information Management: The creation, use, sharing, and disposition of information as a resource critical to the effective and efficient operation of functional activities. The structuring of functional processes to produce and control the use of data and information within functional activities, information systems, and computing and communications infrastructure.	"JFC - UIS" "GCC - UIS"

UIS 3.3.2.1 Provide UIS Directory Services	A directory is an information resource used to store information about objects. A directory service can make those objects and their content available to user applications. The data in the directory may come from a number of authoritative data sources. Provides the directory management organization and processes required to create a scalable, secure, and manageable infrastructure for deploying and maintaining directory services. Directory Services Profile ver. 1.9, 13 Jan 03 COIs will establish their own set of one or more directories. The COI will be responsible for configuring and maintaining the configuration of the directories.	"JFC - UIS" "GCC - UIS"
UIS 3.3.2.2 Provide Discovery Services	This set of services enables the formulation of search activities within shared space repositories (e.g., catalogs, directories, registries). It provides the means to articulate the required service argument, provide search service capabilities, locate repositories to search and return search results or, if necessary, initiates a tasking to the system to obtain the requested information.	"JFC - UIS" "GCC - UIS"
UIS 3.3.2.3 Provide Collaboration Services	This activity provides and controls the shared resources, capabilities, and communications that allow real-time collaborative interactions among participating group members. This environment provides synchronous collaboration capabilities; asynchronous collaboration can occur through other net-centric services and applications that are provided within the information environment.	"JFC - UIS" "GCC - UIS"
UIS 3.3.2.4 Provide Messaging Services	Messaging Services are all formal (organizational) messaging services, to include e-mail, Defense Message Service (DMS), and instant messaging services. Provides services to support asynchronous and synchronous information exchange. This activity consists of all activities needed to support formal (organizational and/or structured) and informal (email and/or unstructured) messaging services. It includes support for tactical requirements. It supports the composition and validation of outgoing messages (message preparation). It supports the processing of incoming messages, including subsequent distribution to intended recipients as users of the information environment. The activity establishes and conducts message (bulletin) board services. It also supports official message traffic.	"JFC - UIS" "GCC - UIS"
UIS 3.3.2.5 Provide Information Mediation Services	This activity enables transformation processing (translation, aggregation, and integration), situational awareness support (correlation and fusion), negotiation (brokering, trading and auctioning services) and publishing.	"JFC - UIS" "GCC - UIS"
UIS 3.3.2.6 Provide	This set of services applies protocols to establish the most appropriate service	"JFC - UIS"

Negotiation Services	capabilities in response to service invocations. The request for data or services may be brokered to provide specific objects and/or object methods. The request for data or services may be supported by trader services that exchange information among brokers. The request for data or services may also be negotiated based upon the attributes of the persona of the requesting principal or upon the service that best matches the request.	"GCC - UIS"
UIS 3.3.2.7 Provide Information Management Support Services	Activities required to support the use of Information Objects during business, combat support, or warfighting activities.	"JFC - UIS" "GCC - UIS"
UIS 3.3.2.8 Provide Information Integrity	1) This activity provides protection against unauthorized modification or destruction of information. This protection supports information in storage, in transit and when processing. This capability maintains the quality of information, reflecting the logical correctness and reliability of the data. It ensures the logical completeness of the hardware and software implementing the data protection mechanisms and the consistency of the related data store structures. 2) Activities required to protect Information Objects and meta-data resident in a database or data warehouses (e.g., file encryption, records locking, and access controls).	"JFC - UIS" "GCC - UIS"
UIS 3.4 Provide Computing Infrastructure	Computing Infrastructure includes those activities that provide a secure, robust, and cost effective computing environment to host core, network, and mission/community of interest (COI) application software; capabilities that enable information storage/retrieval and continuity of operations/disaster recover (COOP/DR); and common resources that enable user input and information processing, output, and display.	"JFC - UIS" "GCC - UIS"
UIS 3.5 Provide Communications Services	Communications Services provide the Subscriber with a full range of information transport services for voice, data, video, imagery, etc. Communications Services provide an integrated network that is managed and configured to provide an information transfer utility for Infostructure Subscribers.	

4. Inputs/Outputs

Name	Purpose	Ref1	Ref1 Detail	Ref2	Ref2 Detail	Ped1	Ped1 Detail	Format	Transfer Mechanism
Acceptance of Aircraft Support Request	Acceptance of request for relief supplies to be lifted by U.S. military aircraft.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
ACCEPTANCE OF AIRCRAFT SUPPORT REQUEST	Acceptance of request for relief supplies to be lifted by U.S. military aircraft.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
Add Requestor to Streaming Video Group						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Advice to HOC Staff	Information on humanitarian support to the relief community.							Data and voice	Email; phone; face to face
Advice to CMOC Staff	Information on military support to the relief community.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face

ADVICE TO CMOC STAFF	Information on military support to the relief community.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
ADVICE TO HOC STAFF	Information on humanitarian support to the relief community.							Data and voice	Email; phone; face to face
Aircraft Support Request	Request for relief supplies to be lifted by U.S. military aircraft.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
AIRCRAFT SUPPORT REQUEST	Request for relief supplies to be lifted by U.S. military aircraft.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
Annex J of the US Emb. EAP	Annex J (Mission Disaster Relief Plan) of the US Embassy Emergency Action Plan (EAP)	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Written document

Annex J of the US Embassy (Emer Action Plan)	Annex J (Mission Disaster Relief Plan) of the US Embassy Emergency Action Plan (EAP)	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Written document
Approved Operational Changes	Approved changes to the operational infostructure.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Change History	Records of changes to assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Configuration Information	Details on the current configuration of assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Cost Data	Costs of operation of IT assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Dependencies	Dependencies between assets on the network.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Asset Discovery Policy	Policy for the timely discovery of assets on the network.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Identification Information	Identifying information for managed objects on the network.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Information	Identification and operational information on assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Information Collection Policy	Policy regarding the detail and extent of information to be collected on assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Lifecycle Policy	Plans for lifecycle replacement of IT assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Metrics	Measurable information regarding the status and performance of assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Asset Purchasing Catalog	The catalog of assets that are available to be purchased.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Assigned Asset Lifecycles	Asset Lifecycles associated with identified assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Audio and Video Collaboration Results	Results of audio or video collaboration.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Audit Controls	A set of instructions to network equipment to implement the Audit Services request. Audit trail records from all available sources are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with DoD information system IA procedures	"GIG IA"	"GIG IA Component of the GIG Integrated Architecture"			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Availability Discovery Request	Request to Discovery Services to search for persons or resources needed to conduct collaboration.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Brokered COI Services Request	Request establishment of a Community of Interest (COI) with definition of information requirements, membership, subscriber profiles, catalog and services administration. Includes requests by the COI policy manager to actively create/negotiate policy parameters for a given service/service set and specified information/objects.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Brokered Information Object	Information Objects that have been brokered or prioritized for service delivery.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Brokered Service Request	The Brokered Service Request is produced after the Subscriber’s Service Request is compared to other pending service requests, the Subscriber's Profile, and the Commander's Information Policy. It is a response to a Subscribers Service Request. Applies Commander's information policy and network resource status. The Brokered Service Request is the allocation of infostructure resources in support of the Information Network.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Catalog Advertisements	IDM services will enable producers of information to post the descriptions of their information products rapidly and send advertisements to interested users.	"IDM CRD"	22 Jan 01, Pg 24			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Catalog Creation Request						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Catalog Management Requests	Request for services to create, update, and maintain catalog information. Bundle includes: - Catalog Creation Request - Request for publication - Publication Maintenance Request					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Change Request	Request to change any portion of the infrastructure, whether a physical change, a software change, a configuration change, or any other.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Catalog	Catalog of Services or Information Objects available to COI members.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Controlling Authority Guidance	Guidance provided by the Controlling Authority of the Community of Interest.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Directory	The vocabulary (i.e. metadata elements) and the sources for the metadata organized according to the taxonomy / ontology that the COI has developed.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

COI Directory Creation Request	Request to generate a directory from a COI's taxonomy and / or ontology and metadata from authoritative data sources.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Directory Management Data	Data that will be used to manage a COI's directory.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Information Subscription	COI Member's request to subscribe to Information Objects. Subscribers may chose to receive update notifications only or may chose to receive the updated Information Objects.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Membership List	Community Of Interest (COI) Membership List represents user support provided by COI Services for a COI. Includes membership, user role, catalog, subscription administration, and Roles Based Access Control (RBAC) support.	"NCOW"				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Policy-Enforcement Mechanisms	A set of policy-based controls to COI resources to enforce COI policies and is performed through various policy-enforcement mechanisms distributed throughout the information environment.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

COI Profile	The Subscriber's Profile updated to include information about his/her role and associated rights and privileges within the COI. Community of Interest (COI) Profiles represent a user/entity request to establish a COI identity. The request includes all pertinent information required to initiate the COI profile and accesses authorization. This includes all user profiles associated with the COI upon authentication. Operate and manage the dynamic and automatic feedback mechanisms that enable the profile to "learn" and "anticipate" the user's needs based on his usage patterns and patterns of similarly profiled users. Implement a combination of human and automated means to review, verify, and validate both the user and provider-specified portions of the dynamic profile.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Role Permissions	Permissions assigned to a COI Role					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Roles	Roles and Responsibilities within a Community of Interest.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

COI Services Management Information	Data concerning the configuration, performance, use, status, and security of Community of Interest (COI) Services. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Tables	Tables (directories, indexes, registries, metadata repositories, etc) required to manage COI resources and Information Objects.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Collaboration Configuration Request	A request to UIS Configuration Management to change the configuration of network equipment to allocate or de-allocate resources required for collaboration.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Collaboration Information	Audio, video, multimedia, or data information objects from one or more collaboration participants.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Collaboration Management Data	Data concerning the configuration, performance, use, status, and security of collaborative resources. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Collaboration Results	Information objects that are produced during collaboration. Examples include: audio, video, multimedia files and associated records.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Collaboration Services Request	Request for the creation and use of a collaborative work environment. The users may be members of a persistent Community of Interest (COI) or an ad hoc group needing collaboration services. The work environment be persistent or temporary (needed only for the duration of the collaboration).					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Commander's Information Policy	Consists of operational authorities' policy on use of infostructure and rules governing the classification, releasability and priority of the information presented to the infostructure. Instructions, directions or policy specific to a unit, organization or operation that has local implications for guidance in security and Information Assurance conditions.	"ICD GIG ES dated 03/22/2004"	ICD GIG ES dated 03/22/2004			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Configuration Change Instructions	Change Configuration Instructions are sent to Infostructure components to initiate a change in their configuration. These can include commands to update software components, change routing tables, activate spare equipment, etc.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Configuration Instructions	Instructions to configure infostructure equipment. Network Configuration Instructions are the policy based instructions from the network manager. These would include instructions to improve the availability, security, reliability, integrity, and performance of the network. Instructions or policy created by systems administrators, policy analyst, and CND analyst that propose guides and updates for any instructions on the proper procedures for configuration, changes, or updates for Information Assurance process that include IDS, COMSEC, EMSEC, and KMI., VPN management and other IA processes. Information generated from managed IA activity include raw audit data configuration information, request for access, request to perform transactions and credentials.	"GIG NetOps"	"GIG NetOps, Ver 3.0"	"GIG IA IFTR "	"GIG IA IFTR - Identity Management and Authentication"	"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Configuration Management Plan	Process for managing configurations of systems and networks.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Contract Payment Policy	UIS policy for how/when contracts will be paid.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Contract Payment Records	Records of actual payments made against contracts.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Contract Payment Schedules	Planned payment schedules for contracts.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Contract Reports	Summary of the status of existing contracts.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Coordinated Requirements	Requirements for infostructure services that have been processed, prioritized, coordinated, and a decision has been made to either act on, table, or deny the requirement.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Coordination	Information on the disaster and status of response actions.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09	Data and voice	Email; phone; face to face
Coordination - Aircraft Support	Information about commodities and delivery requirements.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face

COORDINATION - AIRCRAFT SUPPORT	Information about commodities and delivery requirements.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
Coordination - CMOC						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Cost Data	UIS Cost data.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Country advisories	Warning to American citizens of danger in the relief area and information about how to locate American Citizens (AMCITS) in the relief area.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and voice	Email; phone; face to face
Country update to impending disaster to include maps	GIS tools, geographical representation of relief area and actions.	"OCHA website: Information Management: Services"	http://www.unocha.org/what-we-do/information-management/im-services					Data	Posted on Reliefweb
Data Management Services Request						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

DEPLOY DISASTER ASSISTANCE RESPONSE TEAM	Team composition, capabilities, support needs	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG
Deploy Disaster Assistance Response Team (DART)	Team composition, capabilities, support needs	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG
Depreciation Schedules	Planned reduction in value of UIS assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Design Requirements	System design requirements. - Performance and Quality - Security - Capacity/Size					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Directory Service Request	A request to: - modify the structure of the directory, - manipulate (create, read, update, delete) the directory entry for an information object.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Directory Services Catalog	Catalog of Directory Services metadata holdings.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Directory Services Management Data	Data concerning the configuration, performance, use, status, and security of Directory Services. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Directory Services Search Results	Results returned from search in Directory Services.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Disaster Alert Cable	Background, current situation, anticipated course of action.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Cable (Message)(DOS equivalent to DMS)
DISASTER ALERT CABLE	Background, current situation, anticipated course of action.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Cable (Message)(DoS equivalent to DMS)

Disaster Assistance Request	Request for up to $50,000 USD. Designates specific humanitarian and disaster relief organization to receive.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Cable (Message); email; fax
DISASTER ASSISTANCE REQUEST	Request for up to $50,000 USD. Designates specific humanitarian and disaster relief organization to receive.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Cable (Message); email; fax
Disaster Declaration Cable	1. The disaster is of such a magnitude that it is beyond the host country's ability to respond adequately; the host country has requested or will accept USG assistance, and it is in the interest of the USG to provide assistance. 2. The extent to which the host country needs assistance; 3. The intended use of requested resources, including recommended organizations through which funds will be channeled. 4. Estimated number of killed, injured, affected, displaced and homeless; immediate humanitarian needs; background info i.e. geo location, infrastructure, crops, livestock; other donor efforts; info from available assessment reports.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Cable (Message) (DoS equivalent to DMS); email; FAX

DISASTER DECLARATION CABLE	1. The disaster is of such a magnitude that it is beyond the host country's ability to respond adequately; the host country has requested or will accept USG assistance, and it is in the interest of the USG to provide assistance. 2. The extent to which the host country needs assistance; 3. The intended use of requested resources, including recommended organizations through which funds will be channeled. 4. Estimated number of killed, injured, affected, displaced and homeless; immediate humanitarian needs; background info i.e. geo location, infrastructure, crops, livestock; other donor efforts; info from available assessment reports.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Cable (Message) (DoS equivalent to DMS); email; FAX
DISASTER RELIEF GUIDANCE	Resources and agencies available	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG
Disaster relief guidance	Resources and agencies available	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG

Disaster Relief Guidance						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Discovery Management Data	Data concerning the configuration, performance, use, status, and security of Discovery Services. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Discovery Results	Location of requested data or service. Once the location of the requested Service or Information is known, the Subscriber, and Application, or another Service can request the Information or invoke the Service.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Discovery Search Controls	Controls used to search repositories for the requested information, service, or metadata. Bundle includes: Service Search Controls Information Search Controls Person Search Controls Metadata Search Controls					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Discovery Services Request	Subscriber Request to search the network for information and/or services. Includes Availability Discovery Request.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
DNS Response	DNS information response to DNS Query					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Encrypted Information Object	Information Objects that have been encrypted to provide Confidentiality of data-in-transit over backbone networks must be maintained using appropriate encryption measures as per the classification or sensitivity level of the data.	"CJCSI 6510.01E"	"CJCSI 6510.01E, IA Computer Network Defense"			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Escalations Incident Report	Report of escalations incidents which operate in a planned and measurable fashion.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Establish/Change COI Subscription	Subscriber's request to establish or change the subscription to a Community of Interest (COI).					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Global Information Grid Status	Status of the GIG infostructure					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Help Desk Information	Assistance and problem resolution information provided to the Requester.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Help Request	A Subscriber's request for UIS assistance. Help requests may be received via e-mail, or web interface.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

HHQ UIS Policy & Guidance	DoD and other Policy and Guidance that regulates Information Technology activities. UIS Policy & Guidance implements all mandatory and discretionary protection policies relevant to the GIG enterprise level. It also implements discretionary protection policies within any given domain. Implementation activities include setting parameters in mechanisms used for protection policy enforcement, deployment and configuration of protection devices, and re-configuration activities to meet changes in threat posture, changes in performance capabilities, and/or changes in protection policy (e.g., INFOCON Directives).					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Identified Assets	Assets existing on the network.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

IM Services Management Data	Data concerning the configuration, performance, use, status, and security of Information Management Services. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel. Bundle includes: Discovery Management Data Collaboration Management Data Messaging Services Management Data Mediation Services Management Data Negotiation Services Management Data Information Protection Management Data					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Imagery Assessment	Imagery Products and Assessment	"https://www.cia.gov/library/reports/archived-reports-1/Ann_Rpt_2003/snp.html"						Data	Posted on Reliefweb; Email with attachment
Imagery Products	Geo-rectified products	"USSOUTHCOM and JTF-Haiti… Some Challenges and Considerations in Forming a Joint"	US Joint Forces Command Joint, Center for Operational Analysis					Data	Posted on Reliefweb; Webpage; Email with attachment
Imagery Products Request	Geo-rectified products	"Joint Lessons Learned: Keys to Successful International Humanitarian Assistance"	Joint Center for Operational Analysis, US Joint Forces Command, Norfolk, Virginia					Data and voice	Email; phone; face to face

IMAGERY PRODUCTS REQUEST	Geo-rectified products	"Joint Lessons Learned: Keys to Successful International Humanitarian Assistance"	Joint Center for Operational Analysis, US Joint Forces Command, Norfolk, Virginia					Data and voice	Email; phone; face to face
Incident Escalation Policy	Plans for when/how to escalate incidents to higher levels of support.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Advertisement						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Creation Controls	Controls the development and release of new information objects into the shared information space.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Management Controls	A set of instructions to network equipment to implement the policy-based Information Management request.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Management Services Controls	A set of instructions to network equipment to implement the policy-based Information Management request.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Information Management Services Invocation	Information Management Services Invocation is the approved and brokered Subscriber's request for NCES information management services like Discovery, Collaboration, Messaging, or Mediation. Bundle includes: - Discovery Services Request - Collaboration Services Request - Message Services Request - Mediation Services Request - Data Management Services Request - Web Services Request					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Management Support Objects	Information Objects that have been created of modified during the Information Management Support activities.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Management Support Services Request	A Subscriber's request for Records Mgt, Workflow Mgt, or Data Administration services.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Information Management Transactions	Output from Information Management activities. Bundle includes: Discovery Services Search Results Collaboration Information Objects Messages Mediation Products Records Documents Workflow Products Table Updates					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Object	An Information Object includes audio, video, data, or sensor information and their meta data tags. This ICOM may also be used in a plural context					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Protection Controls	A set of instructions to network equipment to implement the policy-based Information Protection Services.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Protection Management Data	Data concerning the configuration, performance, use, status, and security of Information Protection Services resources. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Information Storage Services Request	Request to Enterprise Storage Management Services to store, retrieve, or move information. Bundle includes: Modified Tables Updated Metadata Replicated Directory Updated Authoritative Source Data					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Storage Services Response	Response from Provide Information Storage Services					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Tags	Information Tags are metadata (data about data) All data, that will be exchanged or has the potential to be exchanged, will be tagged in accordance with the current JTA standard for tagged data items (XML).	"IDM CRD"	22 Jan 2001, pg 38			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Infostructure Events	Occurrences within the ConstellationNet Infostructure. This includes both normal and anomalous events.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Infostructure Reports	Analysis of Infostructure Data.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Infostructure Status	Infostructure Status focuses on the reporting requirements at various levels of NetOps management to ensure NetOps Personnel can maintain GIG situational awareness. Situational-awareness requirements, policy, guidance, monitoring capabilities, and standard NetOps operating procedures control this activity. NetOps personnel perform this activity. Infostructure Status is the standardized NetOps status derived from situational awareness capabilities, following reporting procedures, an established reporting hierarchy, and identified authorities for overseeing and controlling NetOps. Bundle includes: • Net-Centric Services Management Data • SSPI Status • Network Status • NCES Status • Storage Management Data					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
INFOSTRUCTURE STATUS									
IT Contract Support Requirements	Requirements for provision of IT Contract Support					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

IT Policy & Guidance	DoD, AF, MAJCOM, and other Policy and Guidance that regulates Information Technology activities. IT Policy & Guidance implements all mandatory and discretionary protection policies relevant to the GIG enterprise level. It also implements discretionary protection policies within any given domain. Implementation activities include setting parameters in mechanisms used for protection policy enforcement, deployment and configuration of protection devices, and re-configuration activities to meet changes in threat posture, changes in performance capabilities, and/or changes in protection policy (e.g., INFOCON Directives).					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
JFC UIS Policy & Guidance	JFC Policy and Guidance that regulates UIS activities. JFC Policy & Guidance implements all mandatory and discretionary protection policies relevant to the UIS. It also implements discretionary protection policies within any given domain. Implementation activities include setting parameters in mechanisms used for protection policy enforcement, deployment and configuration of protection devices, and re-configuration activities to meet changes in threat posture, changes in performance capabilities, and/or changes in protection policy (e.g., INFOCON Directives).					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Joint Infrastructure Tasking Order	A Joint order, typically from JTF-GNO, that directs configuration, implementation, or other types of action to be taken with regards to information, information protection, and other infrastructure issues					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Managed Assets	Assets that are properly configuration controlled.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Managed Configuration Plan	Actively maintained and supported plan for managing configuration of systems and networks.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Managed Service Desk Procedures	Service desk operations and procedures handled in a planned and controlled fashion.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Mediation Products	Information objects that have been produced or altered through the use of Mediation Services.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Mediation Services Management Data	Data concerning the configuration, performance, use, status, and security of Mediation Services resources. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Mediation Services Request	Request to provide mediation services.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Message Service Request	Request to provide support for asynchronous and synchronous information exchange.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Messages	Synchronous or asynchronous messages for distribution.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Messaging Services Management Data	Data concerning the configuration, performance, use, status, and security of Messaging Services resources. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Mission Requirements	Requirements Documents received from Subscribers, COI Managers, Systems Program Officers (SPOs), Program Management Offices (PMOs) and others.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Need to Create/Change Subscriber Profile	(Boundary Input), represents a Subscriber's requirement to create or change a Subscriber Profile.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Negotiation Services Management Data	Data concerning the configuration, performance, use, status, and security of Negotiation Services resources. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Network Time	Updated standard time for the network.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
OPORD	Detailed instructions for executing the Humanitarian Assistance/Disaster Relief operation.	"USSOUTHCOM and JTF-Haiti… Some Challenges and Considerations in Forming a Joint"	US Joint Forces Command Joint, Center for Operational Analysis					Data	Posted on Reliefweb; Webpage; Email with attachment
OpORD	Detailed instructions for executing the Humanitarian Assistance/Disaster Relief operation.	"USSOUTHCOM and JTF-Haiti… Some Challenges and Considerations in Forming a Joint"	US Joint Forces Command Joint, Center for Operational Analysis					Data	Posted on Reliefweb; Webpage; Email with attachment
Paid Contracts	Contracts that have had all or some payments made.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Permissions	Permissions determine the data and applications that may be accessed for each role that is assigned the set of permissions that are necessary for the user to perform his required tasks. Is the act of allowing and authorizing use of specific resources for use in accessing networks? These resources can be identified and allowed for use in many ways that may include file, directory and object access. Normally the access controls that are required and placed on a resource are the permissions granted for access to that resource or a particular object. It focuses on capabilities for enabling and/or disabling entity permissions, rights, or privileges associated with locally or remotely entering host systems. Permission restrictions may be based on time-of-day, user location, device identity, port identity, etc. Authorization Restriction Parameters may be static or dynamic. UIS Security Administrators construct this type of authorization based on local and enterprise-wide policy, and deconflicts this type of authorization with other types of authorization being employed. This activity is controlled by access and usage policies that respond to evaluated threats.	"NIST/ITL Bulletin"	"NIST/ITL Bulletin, An Introduction to Role-Based Access Control"			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

PPBD Information	Planning, Programming, & Budgeting Decision information is used to govern fiscal expenditures supporting the EIE					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Precedence	An information flow precedence tag (e.g., routine, priority, emergency)					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Producer's Information Catalog	Catalog/index of information Producers products and product updates.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Publication Maintenance Request						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Relief Effort Coordination	Information about the plans and execution of DART's relief efforts.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
RELIEF EFFORT COORDINATION	Information about the plans and execution of DART's relief efforts.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face

REQUEST DoD ASSISTANCE IN TRANSPORT EMER RELIEF COMMODITIES	Type, amount, location, destination, Required Delivery Date (RDD), capacity limitations at reception area	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG
Request DoD Assistance in Transporting Emergency Relief Commodities	Type, amount, location, destination, Required Delivery Date (RDD), capacity limitations at reception area	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG
Request for Information Controls	Request to establish new information/objects either by information collection means or as a result of exploiting, interpreting, assessing, or analyzing existing data to provide additional insights.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Request for Publication						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Request Streaming Video Service	A Request from streaming video services					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Request to Establish a COI	(Boundary Input), represents a requirement to establish a Community of Interest (COI). Gartner defines Community of Interest as "Also know as a community of practice, this group of people associated and linked in a network of communication or knowledge network because of their shared interest or shared responsibility for a subject area. ... Communities continually emerge and dissolve, and their membership, processes and knowledge continually change and evolve. Source: Gartner's Glossary of Terms Used for the Knowledge Workplace: 2004 Update. Bundle includes: COI Membership List COI Member Designation COI Role Descriptions COI Policies	"NCOW: Need to Operate as a COI: (Boundary Input) "	Represents a user requirement to initiate and operate as a COI typically based on missions, tasks, or objectives.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Request USAID/OFDA Relief Commodities						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
REQUEST USAID/OFDA RELIEF COMMODITIES	Material available from USAID/OFDA stockpiles	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG

Request USAID/OFDA relief commodities	Material available from USAID/OFDA stockpiles	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG
Requested Dissemination Service	The Requested Dissemination Services are provided once the Subscriber's Credentials have been authenticated, the appropriate policies have been reviewed, and the required permissions have been granted. Bundle includes: - Smart Push Data - Search Results - IDM Catalog Data					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Requirements	Requirements Documents received from Subscribers, COI Managers, Systems Program Officers (SPOs), Program Management Offices (PMOs) and others.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Scope and Magnitude of Event	Type of event, how large an area, how big a storm or magnitude of earthquake, tsunami, etc. Numbers of personnel likely to be effected. Likely resources needed.	"Mission Disaster Relief Officer (MDRO) through established contacts including: h"	Chief of Mission (CoM), the embassy's Emergency Action Committee (EAC) and the USAID Office Foreign Disaster Assistance (OFDA) Principal Regional Advisor					Data and voice	Overview brief
SCOPE AND MAGNITUDE OF EVENT	Type of event, how large an area, how big a storm or magnitude of earthquake, tsunami, etc. Numbers of personnel likely to be effected. Likely resources needed.	"Mission Disaster Relief Officer (MDRO) through established contacts including: h"	Chief of Mission (CoM), the embassy's Emergency Action Committee (EAC) and the USAID Office Foreign Disaster Assistance (OFDA) Principal Regional Advisor					Data and voice	Overview brief
Security Clearance Information	Information regarding the Security Clearance of individuals.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09	Data	Cable (Message); email; fax
SECURITY CLEARANCE INFORMATION						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Security Policy and Instructions	Set of laws, rules, and practices that regulate how sensitive (SBU and classified) information is managed, protected, and distributed by an AIS. NOTE: System security policy interprets regulatory and operational requirements for a particular system and states how that system will satisfy those requirements. All systems or networks that process SBU or classified information will have a security policy. Security Policy and Instructions focuses on the creation of specific policy parameters and the negotiation/modification of these parameters. The input is the invocation of the policy manager to actively create/negotiate security policy parameters for a given service/service set and specified information/objects. The output is instructions concerning the new/modified policy parameters that constrain/enable service execution.	"AFDIR 33-303"	"AFDIR 33-303, definition for System Security Policy."	NCOW		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Service Desk Procedures	Planned procedures for operating the service desk.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Service Request Response	The Service Provider's response to the request for service/information. Provides feedback to the Subscriber concerning the status of the pending service request. Bundle Includes: Audit Controls COI Tables COI Roles COI Membership List Shared Workspace Controls Information Creation Controls COI Policy-Enforcement Mechanisms Information Advertisement Confirmation of Delivery IDM Response Notification Help Desk Information Modified Information Object Retrieved Information Object • Customized Presentation Data					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Shared Information	Assured Information Sharing (AIS) provides the ability to securely and dynamically share information. It enables the ability to exchange information within and between security domains and Communities of Interest (COIs), at multiple levels of sensitivities, and, between authorized users within the Department of Defense (DOD), other United States (US) government departments and agencies, law enforcement agencies, selected non-government and private sector entities, allied nations, and coalition partners. AIS facilitates the timely, automated, and flexible creation and management of COIs, and provides for dynamic, trusted, and authenticated user access, as well as enabling the sharing of user identity and access rights throughout the enterprise.	"GIG IA"	"GIG IA Capability Roadmap for AIS, Ver 1.0"			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Shared Workspace Controls	Controls used to establish and manage a shared workspace for the COI. Includes: - Application Use Controls - Information Exchange Controls - Information Disposition Controls					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Significant Event Log	Daily significant events	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Website
SIGNIFICANT EVENT LOG	Daily significant events	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Website
SITREP - JTF	Information on the disaster and status of response actions.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
SITREPS						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
SITREPS - Out						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Situation Report - DART	Information on the disaster and status of response actions.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09	Data and voice	Email; phone; face to face
Situational Awareness Data	Improvements in the marking of situational awareness information (such that unclassified situational awareness data resident in secret tactical networks is distinguished from secret situational data) and the ability of CDSs to process situational awareness data for transfer to unclassified networks. Information objects that support Situational Awareness.	"GIG IA"	"GIG IA Component of the GIG Integrated Architecture"			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Status Updates	Information on the disaster and status of response actions.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
STATUS UPDATES	Information on the disaster and status of response actions.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
Status of approaching natural disaster	Information on type of disaster likely to occur and likelihood of striking country.							Data and voice	Alert posted on Embassy web site
Streaming Multimedia	Multi-media information content (including video) presented as a data stream.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Streaming Multi-media	Multi-media information content (including video) presented as a data stream.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Subscriber Information	Subscriber Information to be Stored, Processed, Published, or Transmitted across the network. This includes voice, video, data and imagery.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Subscriber Information Request						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Subscriber Profile	All requirements, criteria and other pertinent user information in a proper format and submit as the current User/Entity profile. Define and implement the basic attributes of the user's profile that are determined by the organization to which the user belongs and the user's role in that organization. Example attributes include user's roles, areas of responsibility, clearances, accesses, and communications medium. The Subscriber Profile is used to tailor the Network services to the Subscriber's preferences (font size, colors, default page, etc).	NCOW				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Subscriber Request	Subscriber request is a generic bundle of several different types of requests.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Subscriber Request Response	Provides feedback to the Subscriber concerning the status of a pending request.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Subscriber Service Request	Subscriber Service Request represents a user request for a specific service or capability. This includes profile requests, information publication requests, information acquisition requests, collaboration requests, and COI services requests. A Subscribers request for services from the network (information transport, file access, information dissemination, etc).					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Subscriber Service Request Response	Subscriber Service Request Response to a user request for a specific service or capability. This includes profile requests, information publication requests, information acquisition requests, collaboration requests, and COI services requests. A Subscribers request for services from the network (information transport, file access, information dissemination, etc).					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Training	Training required to gain access to the AF Network and other related training requirements					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
UIS Directives	Directives issued both to trigger specific actions as well as to inform effected organizations.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
UIS Plans	Plans for the operation of systems and networks.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
UIS Policy & Guidance	GCC/JFC, and other Policy and Guidance that regulates Information Technology activities. UIS Policy & Guidance implements all mandatory and discretionary protection policies relevant to the GIG enterprise level. It also implements discretionary protection policies within any given domain. Implementation activities include setting parameters in mechanisms used for protection policy enforcement, deployment and configuration of protection devices, and re-configuration activities to meet changes in threat posture, changes in performance capabilities, and/or changes in protection policy (e.g., INFOCON Directives).	NCOW				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Validated Asset Requirements	Requirements for asset changes which have been validated as supporting mission requirements.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Validated Contracts	Contracts shown to be necessary and appropriate.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Video Stream Availability Notification Message						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Vulnerability and Damage Assessments	Assess damage suffered	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09	Data	MSG
VULNERABILITY AND DAMAGE ASSESSMENTS						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Web Services Request						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

THIS PAGE INTENTIONALLY BLANK

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project

Annex N11 - Unclassified Information Sharing (UIS) Operational Activity Model Operational Viewpoint (OV) 5b

1. Operational Activity Model

The Operational Activity Model Operational Viewpoint (OV) 5b describes operational activities; Input/Output (I/O) flows between activities, and I/O flows to and from activities that are outside the scope of the architecture. I/O flows of operational activities relate to information elements in the Operational Resource Flow Matrix (OV-3), and are further characterized by the information exchange attributes described in the OV-3. I/Os that are produced or consumed by operational activities that cross operational node boundaries are carried by needlines described in the Operational Resource Flow Description (OV-2).

The OV-5b uses standard terminology to ensure precise communication. Box meanings are named descriptively with verbs or verb phrases and are split and clustered in decomposition diagramming. Arrow meanings are bundled and unbundled in diagramming and the arrow segments are labeled with nouns or noun phrases to express meanings. Arrow-segment labels are prescriptive, constraining the meaning of their segment to apply exclusively to the particular data or objects that the arrow segment graphically represents.

Each side of the function box has a standard meaning in terms of box/arrow relationships. The side of the box with which an arrow interfaces reflects the arrow's role. Arrows entering the left side of the box are inputs. Inputs are transformed or consumed by the operational activity to produce outputs. Arrows leaving a box on the right side are outputs. Outputs are the data or objects produced by the operational activity. An example is shown in Figure N11-1.

Figure N11-1 - OV-5b Graphic Example

2. UIS – Provide Unclassified Information Sharing Context

The diagram in Figure N11-2 shows the top level or context operational activity of the UIS OV-5b. It shows the interface between the *UIS Provide Unclassified Information Sharing* and the *Perform External Activities* which is an aggregation of the activities of the operational nodes described in the OV-2.

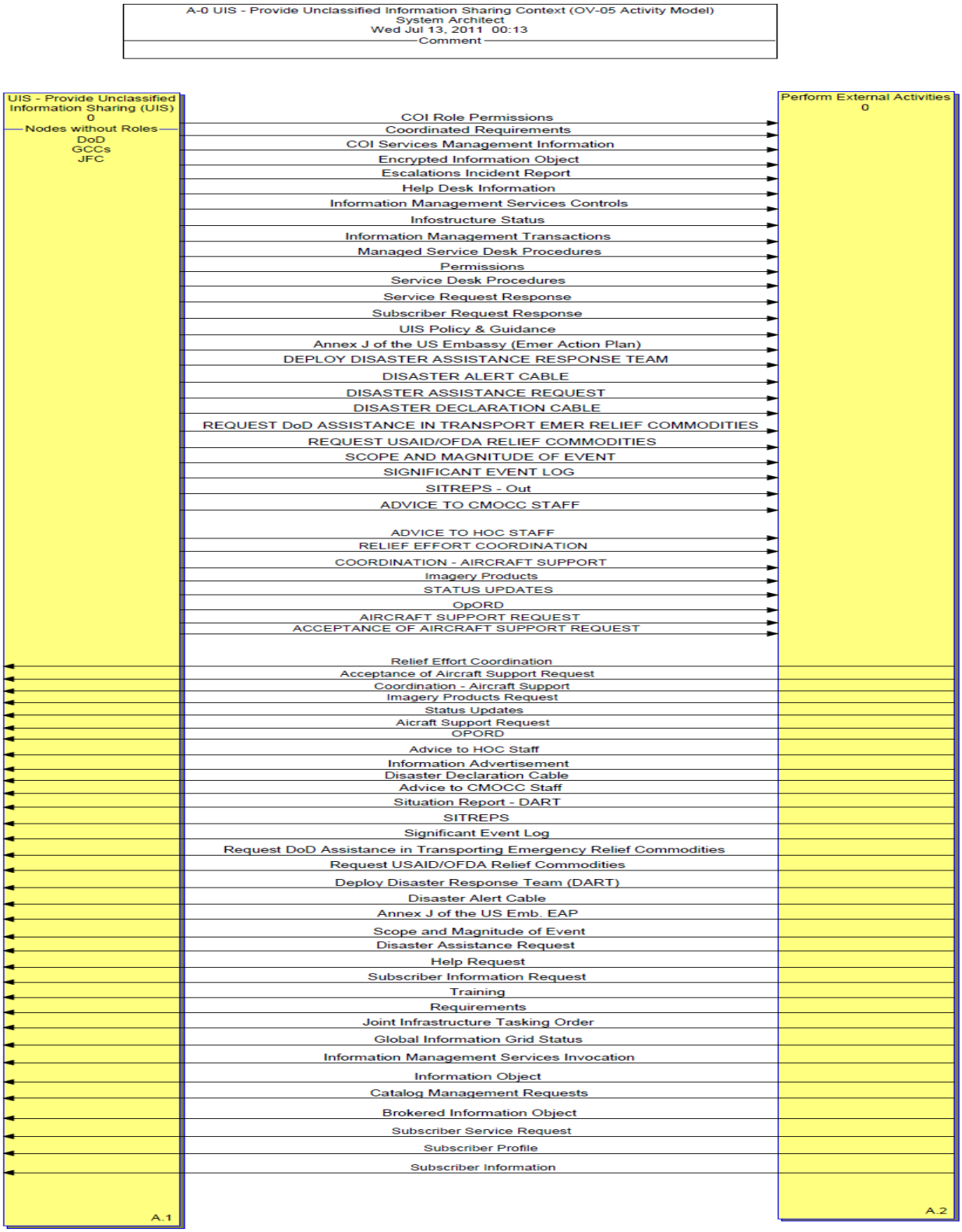


Figure N11-2 - A0 level UIS Activities

Figure N11-3 shows the first level activities of Unclassified Information Sharing (UIS) – Provide Unclassified Information Sharing: *UIS 1.0 Provide for UIS*, *UIS 2.0 Perform UIS Management*, and *UIS 3.0 Provide UIS Services*.

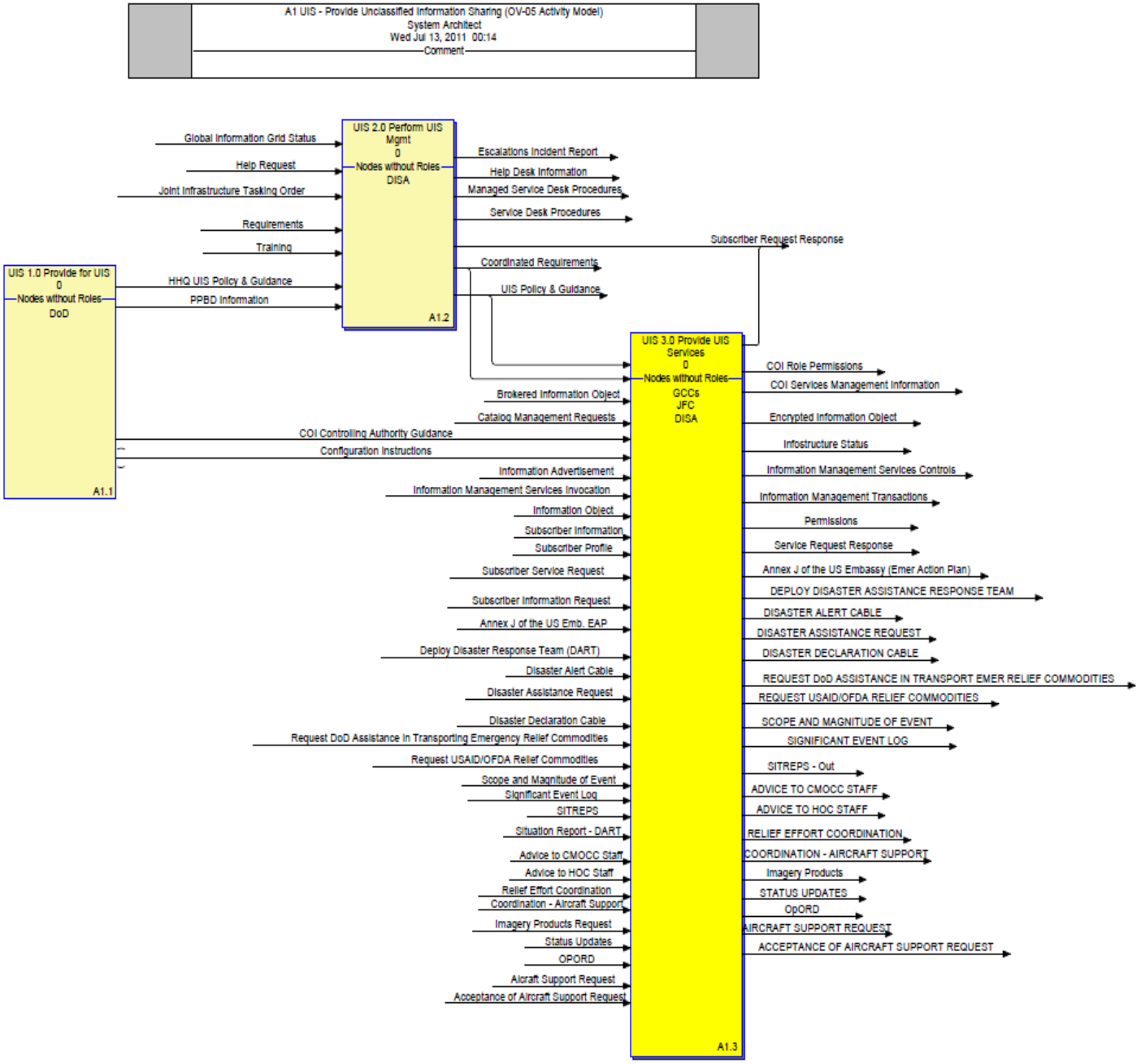


Figure N11-3 - A1 Level UIS Activities

UIS 3.0 activities are decomposed in Figure N11-4, showing *UIS 3.1 Provide Subscriber Interface Services, 3.2 Protect the UIS Information Environment, UIS 3.3 Provide Core UIS Services, UIS 3.4 Provide Computing Infrastructure,* and *UIS 3.5 Provide Communications Services*.

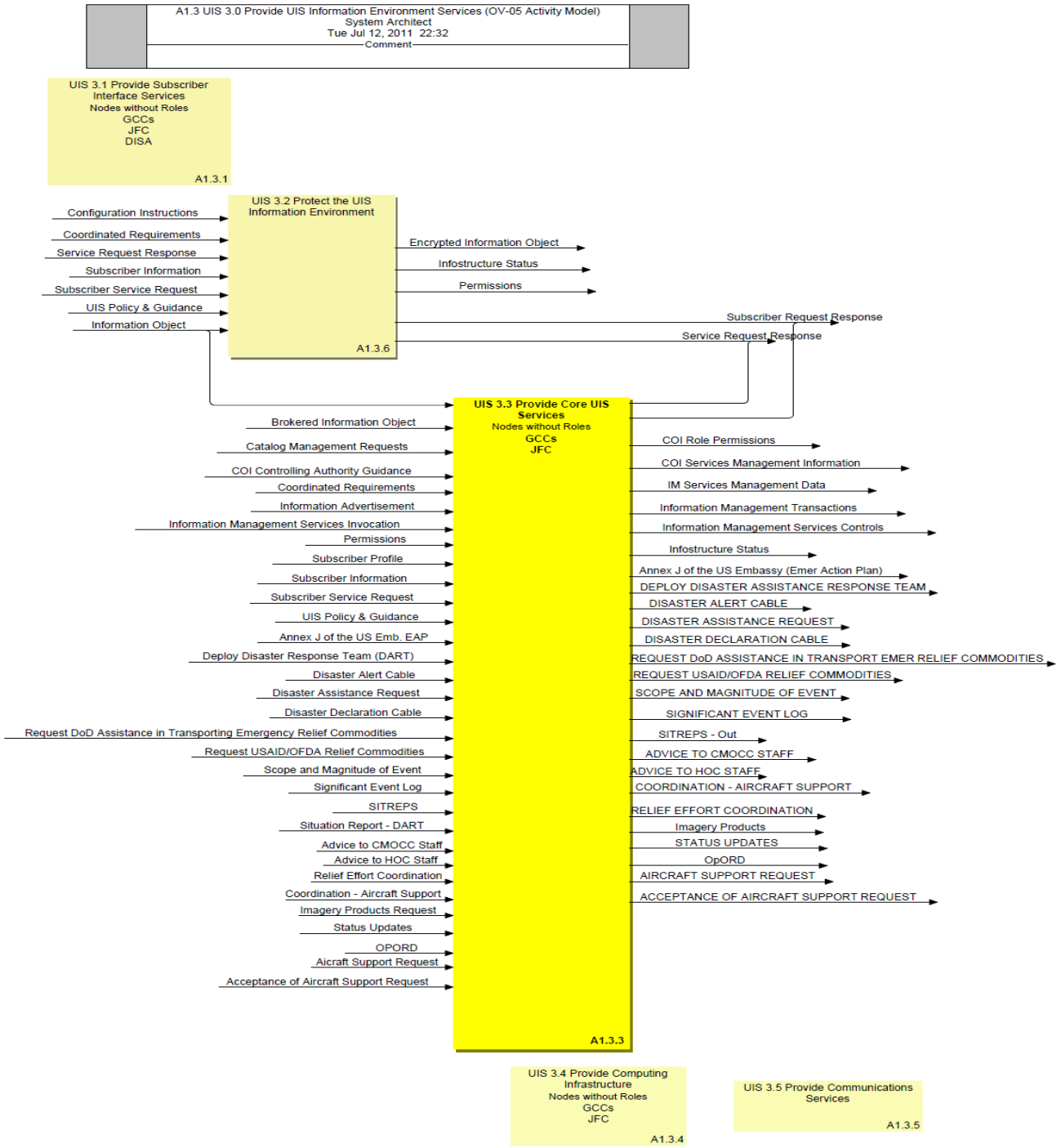


Figure N11-4 - UIS 3.0 Activities

The IMISAS Project focused on UIS 3.3, *Provide Core UIS Services*, which is decomposed in Figure N11-5.

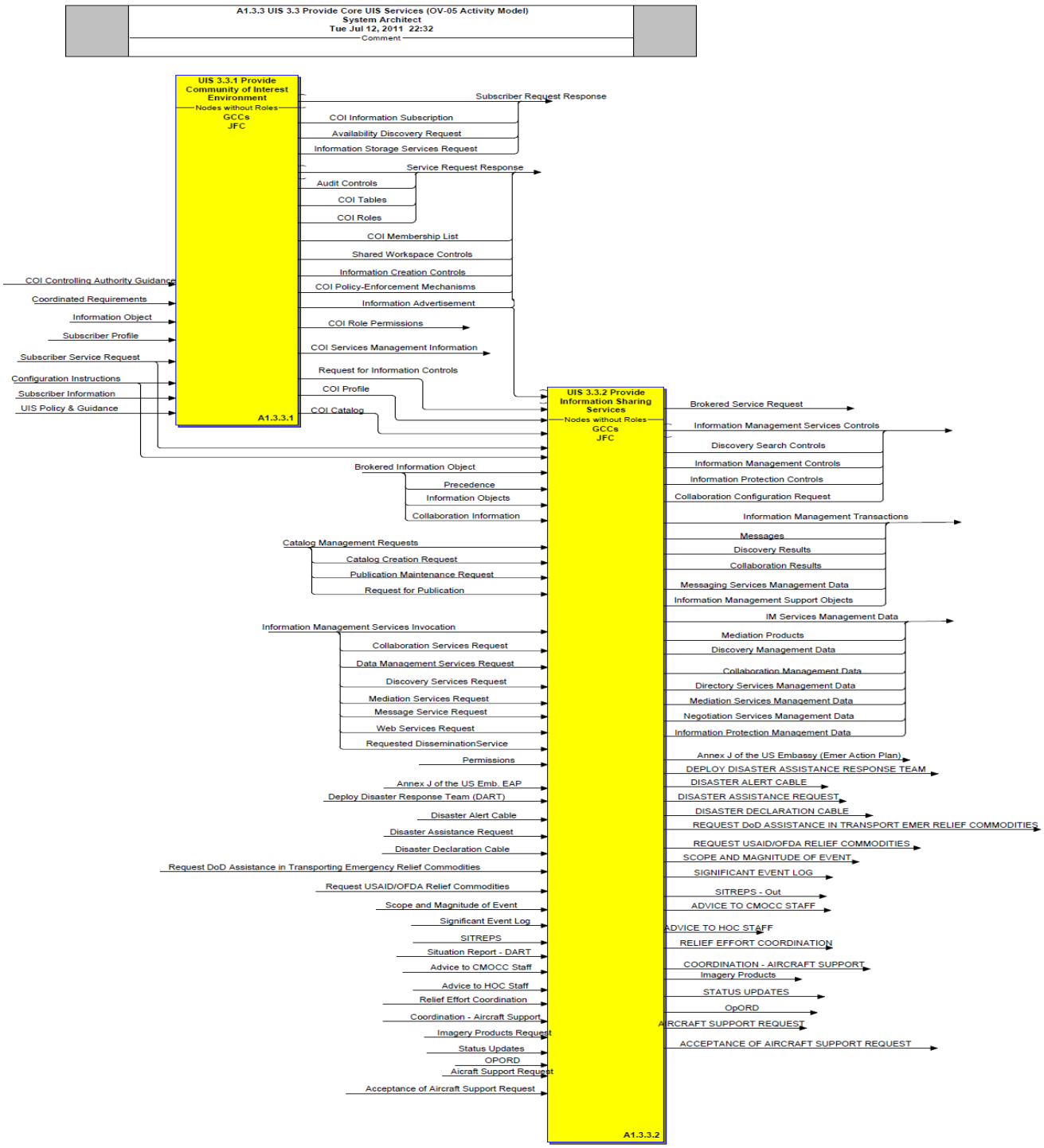


Figure N11-5 - UIS 3.3 Provide Core UIS Services Decomposition

The activities of interest, *UIS 3.3.1 Create Shared Information Environment* is decomposed in Figure N11-6 and *UIS 3.3.2* Provide Information Sharing Services, is decomposed in Figure N11-7. Activities are described at section 3; input and output descriptions can be found in section 4.

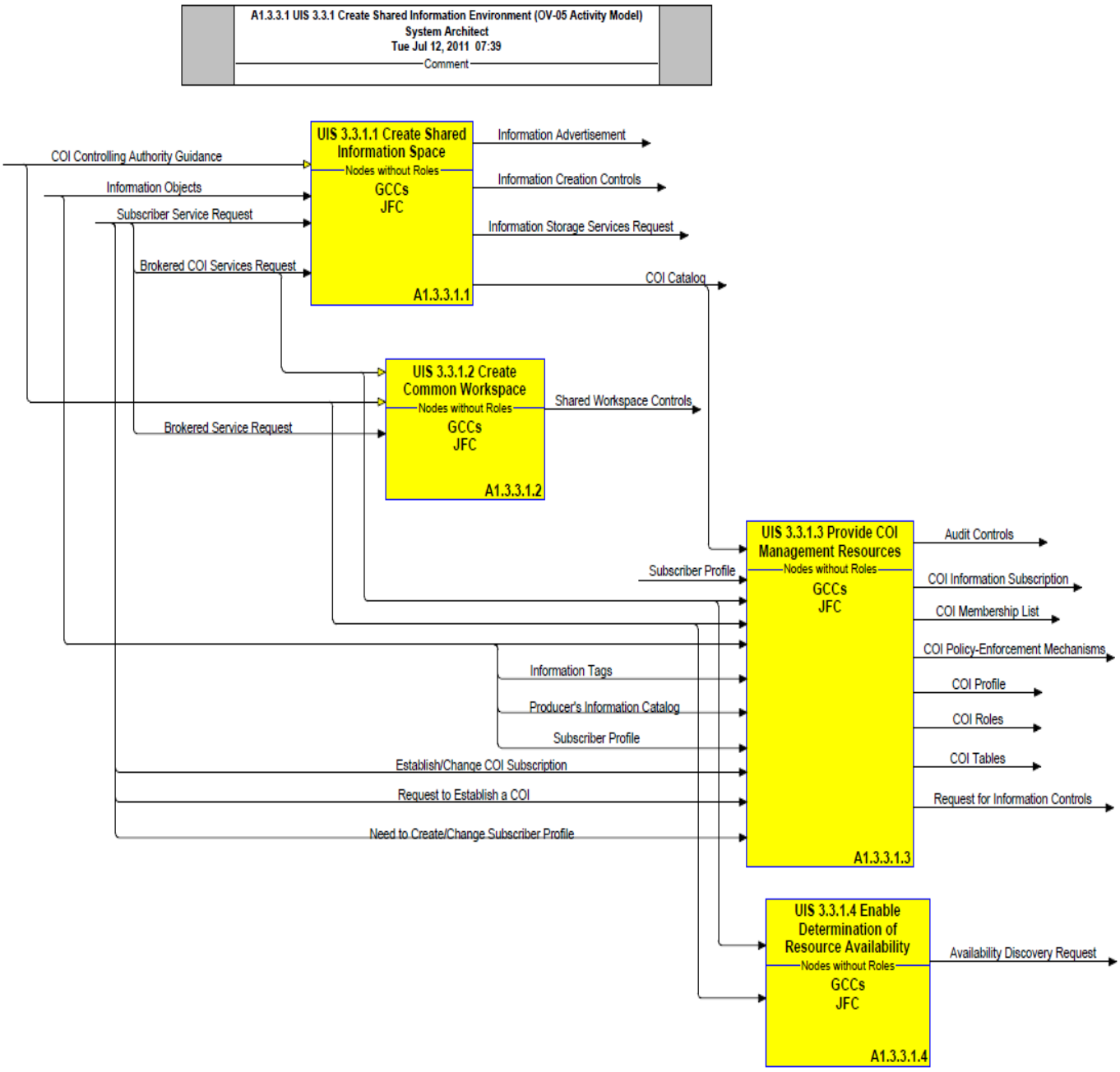


Figure N11-6 - UIS 3.3.1 Activities

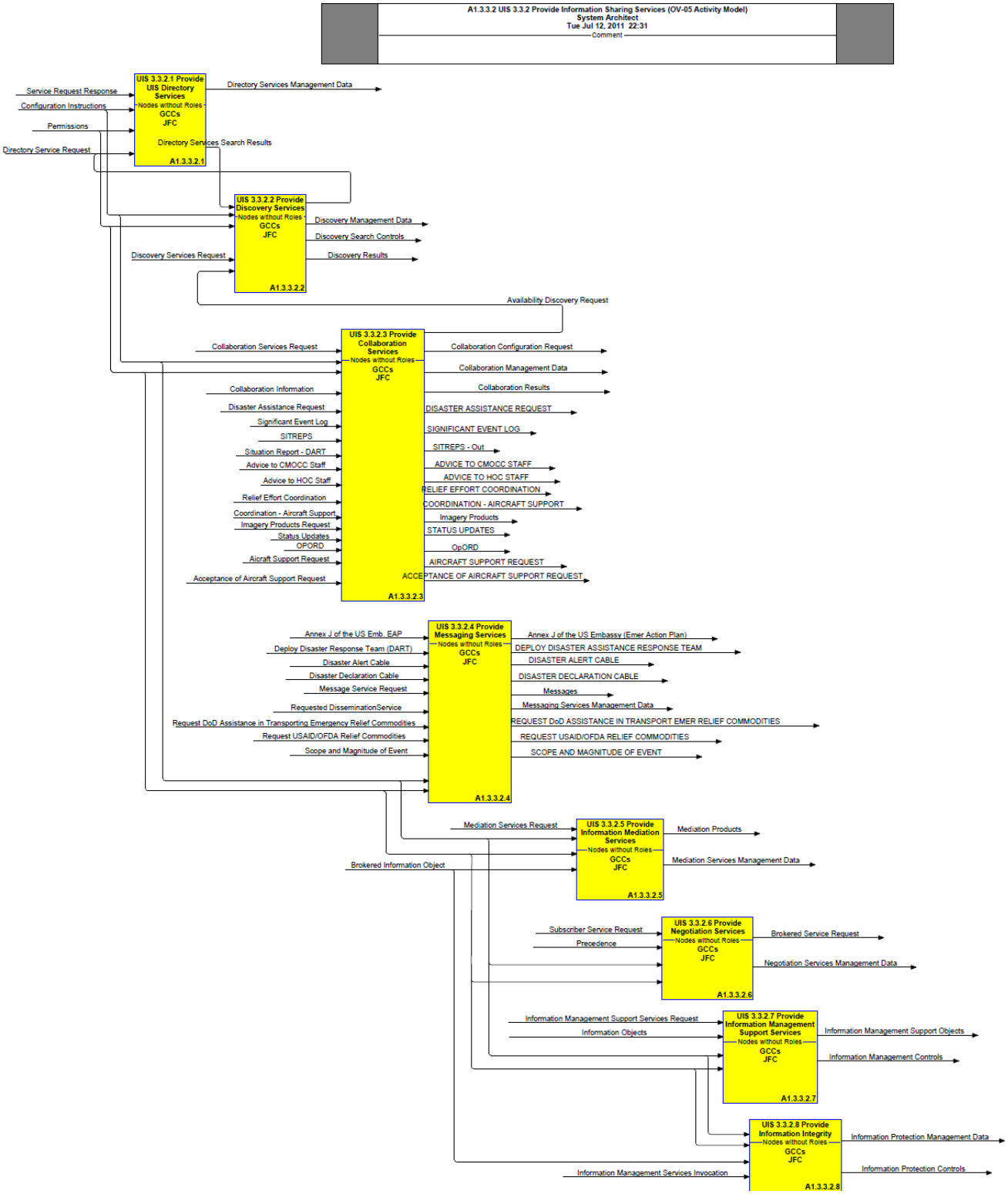


Figure N11-7 - UIS 3.3.2 Activities

Figures N11-8 through N11-14 are examples of each of the Operational Nodes that might interact with the combatant commander (COCOM) during humanitarian response/disaster relief (HA/DR) operations and represent an initial development within the UIS Architecture.

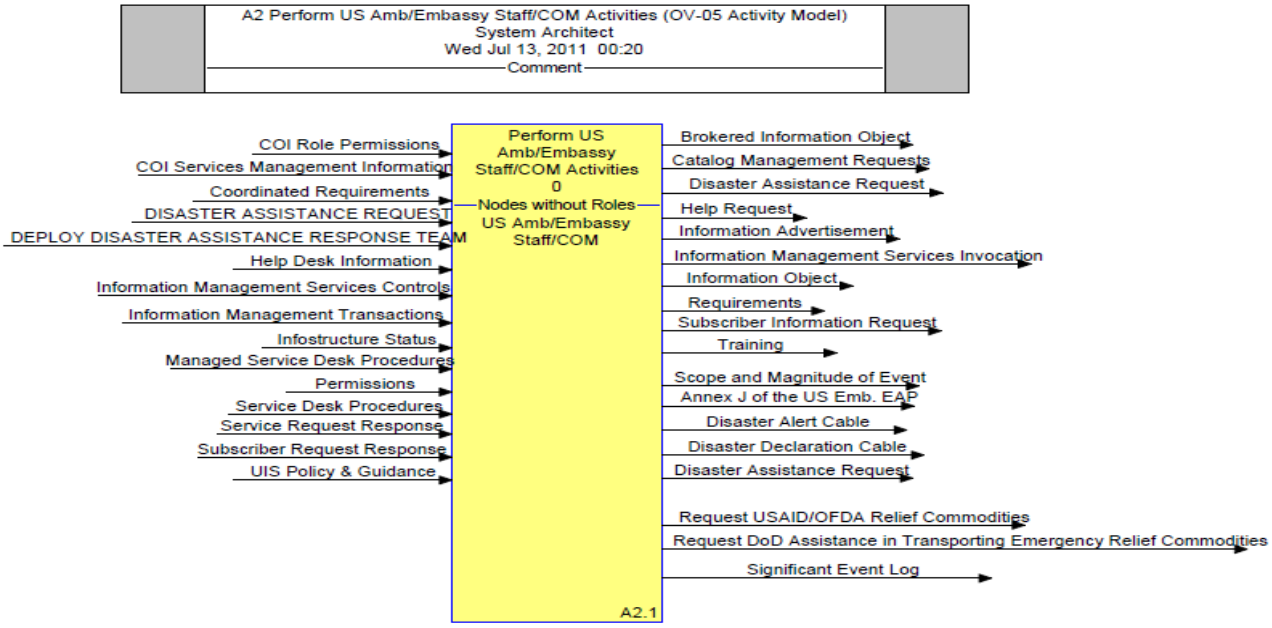


Figure N11-8 - U.S. Embassy Activities

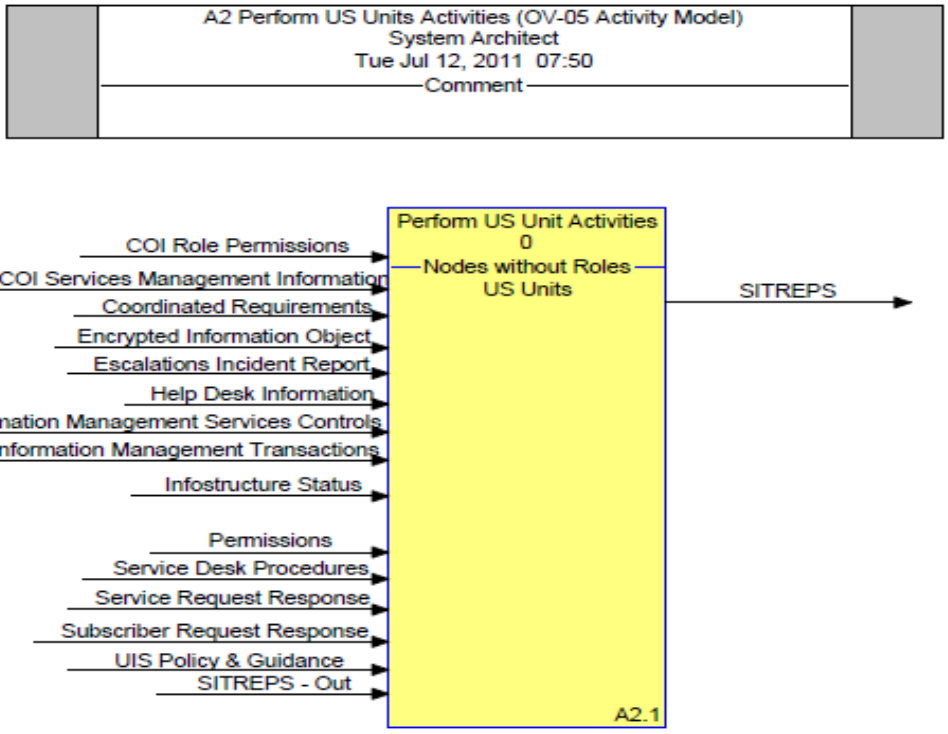


Figure N11- 9 - U.S. Military Unit Activities

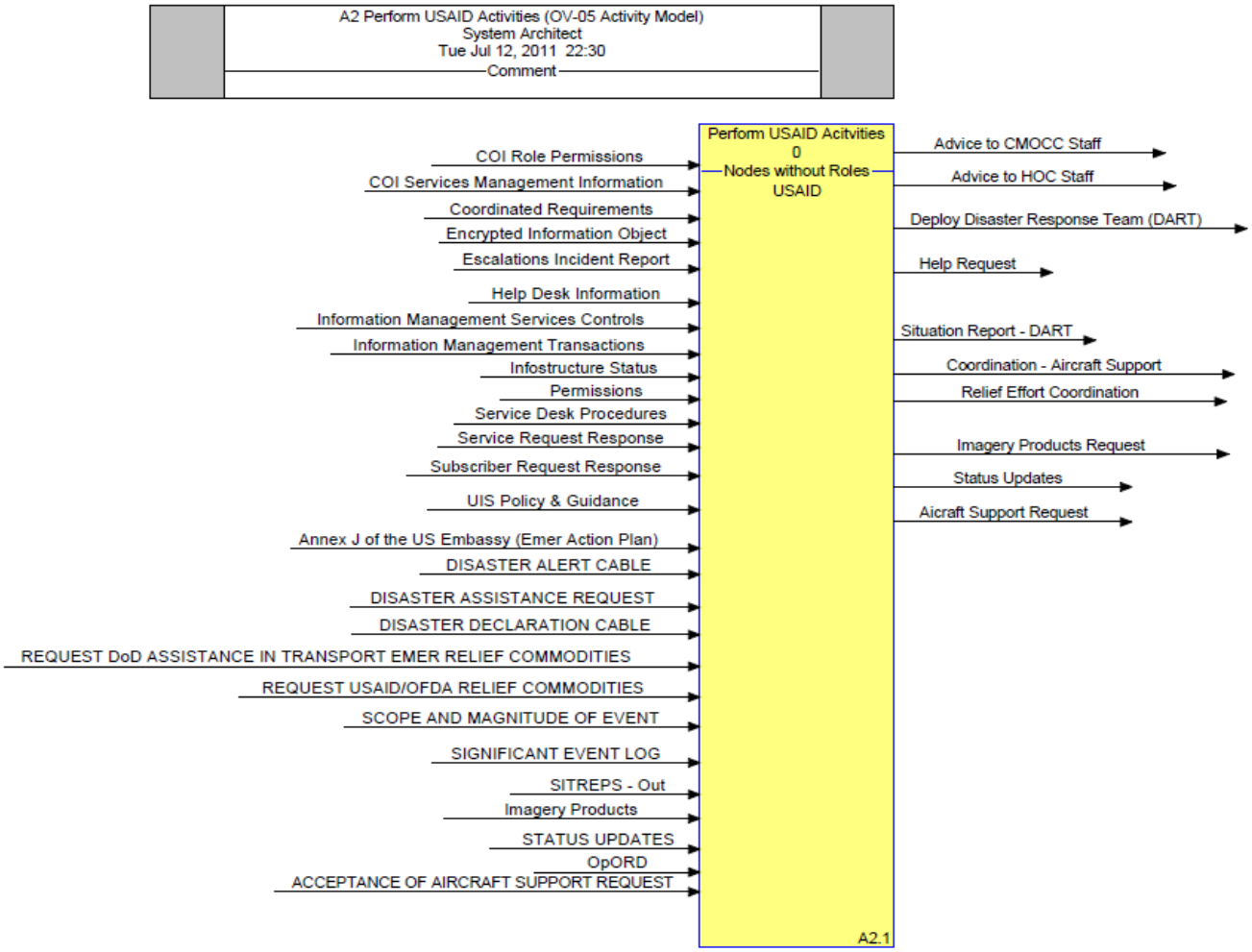


Figure N11-10 - USAID Activities

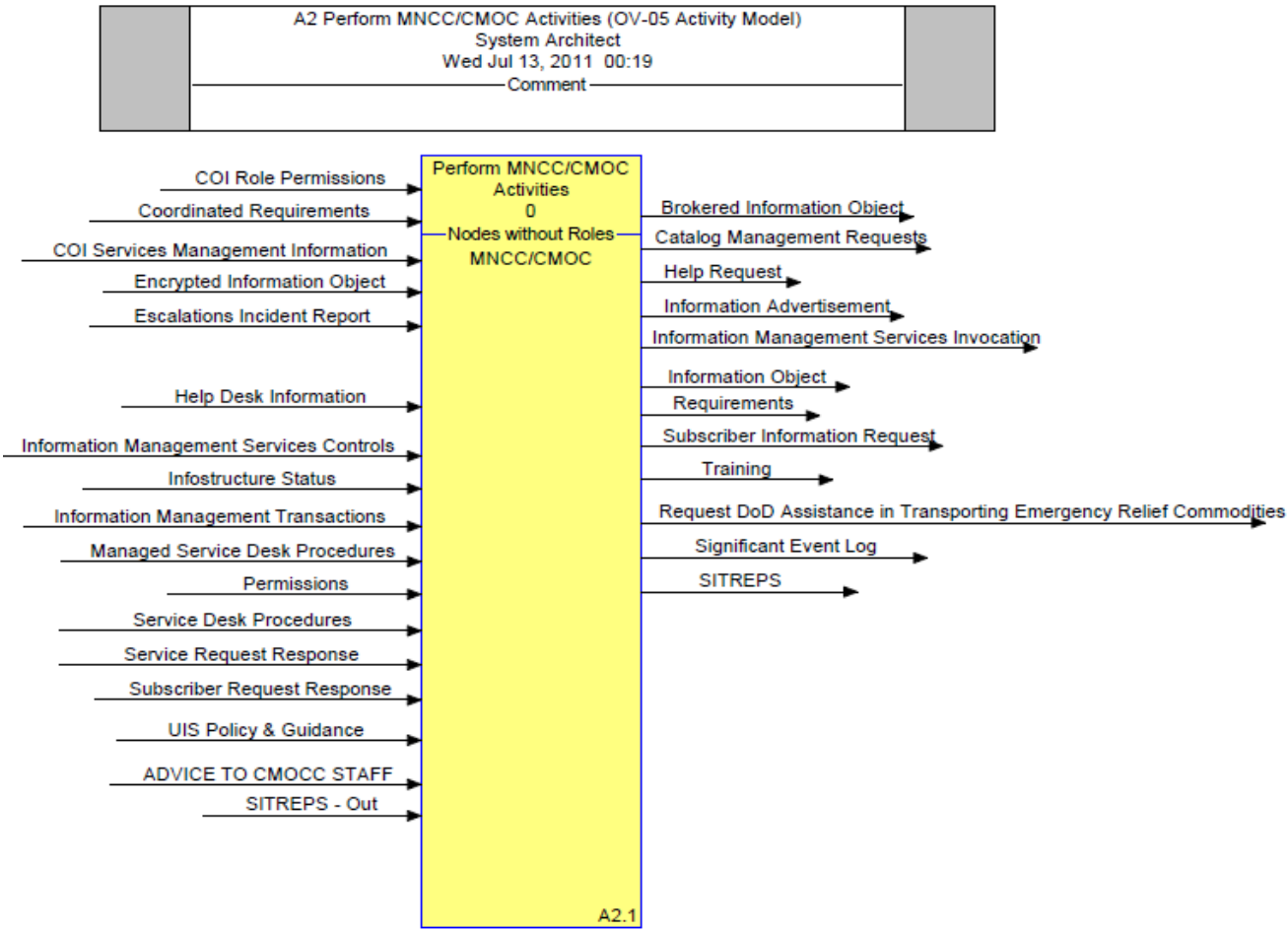


Figure N11-11 - MNCC/CMOC Activities

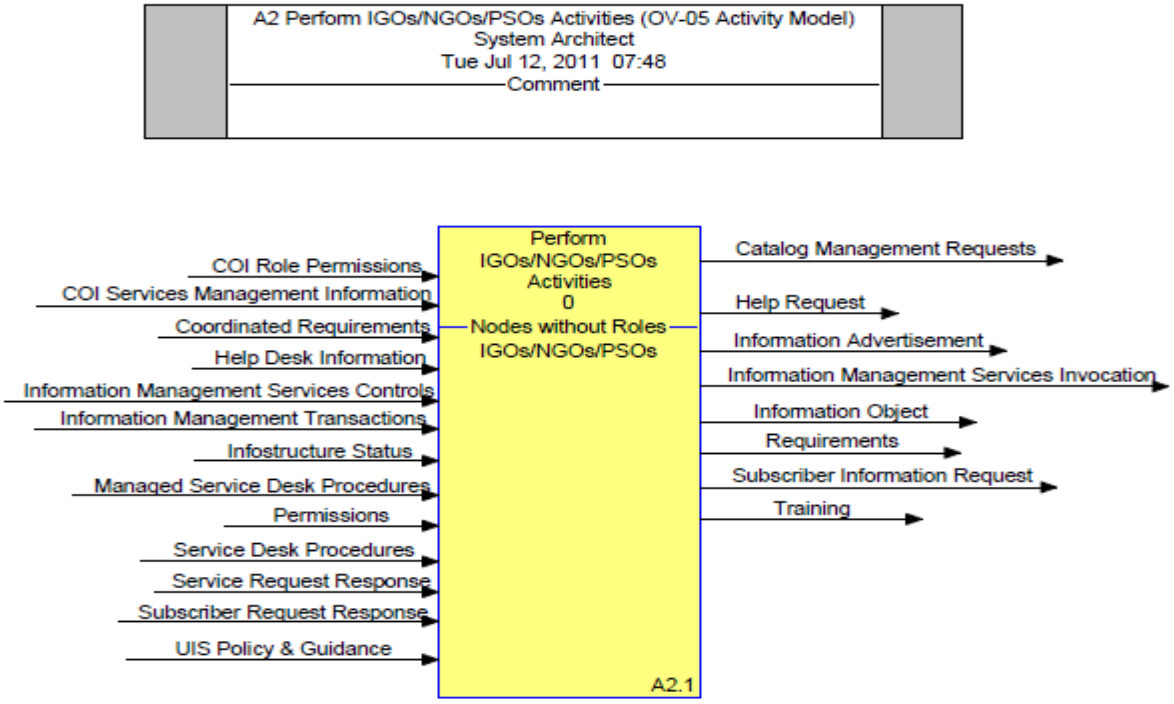


Figure N11-12 - IGO/NGO/PSO Activities

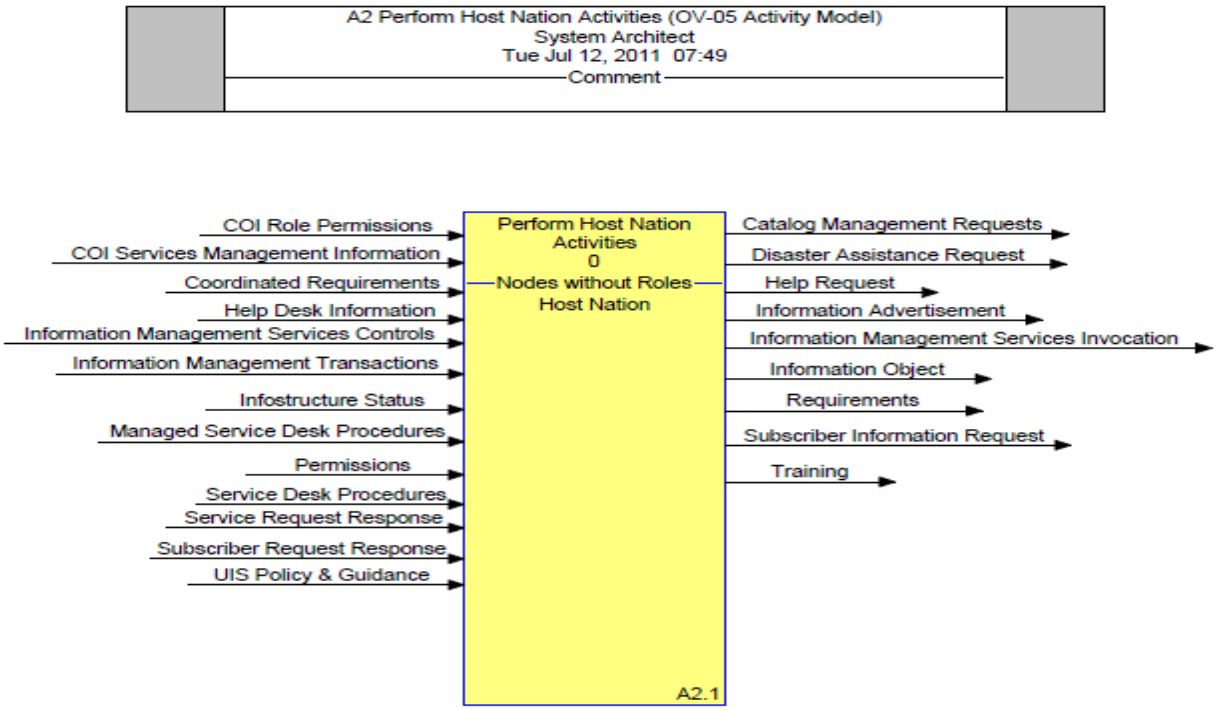


Figure N11-13 - Host Nation Activities

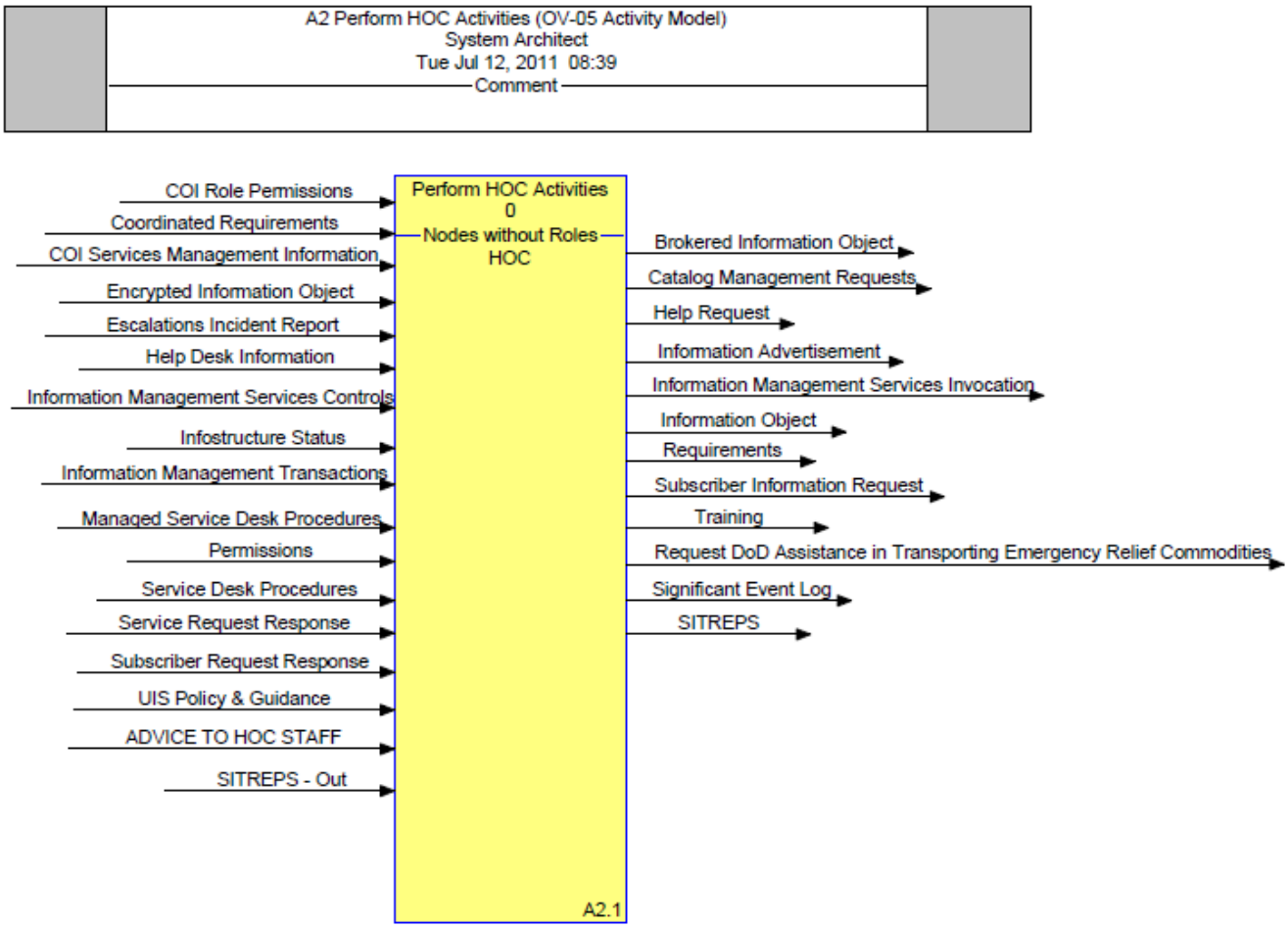


Figure N11-14 - HOC Activities

3. Operational Activities

Name	Description	Operational Nodes
Perform DISA Activities	For modeling purposes Only.	DISA
Perform Bloggers Activities	For modeling purposes only	Bloggers
Perform External Activities	Aggregate of external activities performed by operational nodes (OPNodes) external to the Geographic Combatant Commander (GCC)/Joint Force Commander (JFC), e.g., Ambassador/Embassy Staff, Host Nation, Multinational Force Coordination Center (MNCC)/Civil-Military Operations Center (CMOC), Intergovernmental Organizations (IGOs)/Nongovernmental Organizations (NGOs)/Private Sector Organizations (PSOs), U.S. Government (USG) agencies, etc.	
Perform GCC Activities	External activities of the GCC to the UIS Architecture	GCCs
Perform HN Units Activities	For modeling purposes only	"HN Units"
Perform HOC Activities	For modeling purposes only	HOC
Perform Host Nation Activities	For modeling purposes only	"Host Nation"
Perform IGOs/NGOs/PSOs Activities	For modeling purposes only	"IGOs/NGOs/PSOs"
Perform MNCC/CMOC Activities	For modeling purposes only	"MNCC/CMOC"
Perform UN Units Activities	For modeling purposes only	"UN Units"
Perform US Amb/Embassy Staff/COM Activities	For modeling purposes only.	"US Amb/Embassy Staff/COM"
Perform US Unit Activities	For modeling purposes only	"US Units"

Perform USAID Acitvities	For modeling purposes only.	USAID
UIS - Provide Unclassified Information Sharing (UIS)	The UIS is defined as the computers, ancillary equipment, software, firmware, and similar procedures, services, people, and related resources used in the acquisition, storage, manipulation, protection, management, movement, control, display, switching, interchange, transmission, or reception of data or information in any format including audio, video, imagery, or data, not including the information itself whether supporting UIS. This model describes the activities involved required to establish, operate, and maintain the Infostructure from the UIS provider's point of view. This model describes how the UIS ops activities will support the DoD UIS Implementation Sharing Plan.	DoD "JFC - UIS" "GCC - UIS"
UIS 1.0 Provide for UIS	This activity includes acquiring, managing, and sustaining UIS assets and their associated needs in support of providing UIS capabilities. This enables consumers to use the services and agencies to manage them. This activity includes the full range of support throughout an UIS Asset lifecycle.	DoD
UIS 2.0 Perform UIS Mgmt	This activity consists of the planning, organizing, coordinating, and controlling the establishment, maintenance, and dissolution of all the capabilities of and services provided by the UIS environment. It comprises the development of the environment's capabilities, the management of its system and network configurations, as well as the conduct of its administration, monitoring, and response activities. It also consists of performance of all UIS activities necessary to manage and protect the flow of information within the information environment. These activities are performed by UIS Personnel. It takes functional and operational performance requirements as inputs and produces operational capabilities within the information environment. This activity is controlled by the operational environment; plans; policies; guidance; laws and regulations; tactics, techniques, and procedures; standards; and funding.	DISA
UIS 2.1 Perform Command and Control	To perform Command and Control (C2) of network and system Operations, to include control and management oversight of all operations and security aspects for the network. C2 over system and network Management is the set of activities required to provide	DISA

	direction and reporting over fault, configuration, accounting, performance, and security & system management activities within the network.	
UIS 2.1.1 Manage Systems and Networks	System and Network Management is the set of activities required to provide fault, configuration, accounting, performance, and security management within the network.	DISA
UIS 2.1.2 Manage Information Dissemination	Dissemination Management is the set of activities required to dynamically manage competing Subscriber requirements and to automatically allocate Infostructure resources to service those demands. This activity focuses on the regulation of content placement activities (e.g., publish and subscribe, content mirroring, content migration). The activity provides the capability to establish, select, and manage both general and specific information dissemination channels. The activity provides regulatory measures for governing repositories, directories, catalogs, and dissemination-related metadata. It has the primary control over publish and subscribe mechanisms. Information dissemination relies on commonly-understood metadata "tags" to distribute information products from the Producer to the Consumers.	DISA
UIS 2.1.3 Perform Operational Control	Activities essential to maintaining control and management of a resilient operational infrastructure, such as establishing and maintaining appropriate network operations situational awareness, planning and executing operational actions, and evaluating, selecting and executing operational courses of action.	DISA
UIS 2.2 Perform UIS Implementation Planning & Engineering	The aim of this planning and engineering activity is to design the UIS services and infrastructure required to support the mission and its needs. This requires a process of identifying the customers with shared interests, determining the technical capability required to support the UIS services demanded, designing the appropriate architectures and selecting the UIS components to form the 'provided' capability. After strategy is defined, implementation and engineering planning must be accomplished. An implementation plan must be created to describe the implementation in more detail and add additional information that enables the project organization to execute	DISA

	implementation in a proper way. The implementation plan should contain at least the following information: - Overview of the parties involved; - Description of the solution to be implemented; - Implementation strategy; - Migration strategy; - Back-out scenarios and procedures; - Risks and Risk Management; - Decision tree; - Necessary changes managed by Change Management; - Migration plan; - Overview of necessary resources; - Implementation schedule; - Site surveys; - Provision for feedback of early implementation experience	
UIS 2.2.1 Analyze System and Network Requirements	Analyze requirements documents to develop an engineering solution.	DISA
UIS 2.2.2 Engineer Systems and Networks	Develop Systems and Networks from established and approved requirements.	DISA
UIS 2.2.3 Manage System and Network Resources	Management of finances, people, and equipment.	DISA
UIS 2.3 Deploy and Manage UIS Assets	Deploy and provide management over the people, money, and equipment needed to operate, and maintain systems, networks, and services.	DISA
UIS 2.3.1 Procure Asset	In order to procure assets, there must be a valid need for the assets, there must be finances available to support the procurement, and there must be a procurement vehicle for the acquisition of the asset. Examples of assets include hardware, software, applications, and web services.	DISA
UIS 2.3.2 Deploy New Asset	This activity deploys newly acquired assets into the ConstellationNet in accordance with current policies.	DISA
UIS 2.3.3 Identify Asset	In order to properly manage an IT asset, the asset manager must know if its existence, must know the attributes which make it unique, and must know its planned lifecycle.	DISA
UIS 2.3.4 Report Asset Information / Metrics	The AFKS / GCSS-AF systems are used to report on assets within the enterprise and to maintain metrics on their use.	DISA
UIS 2.3.5 Manage Asset Configuration	The process of identifying and defining Configuration Items in a system, recording and reporting the status of Configuration Items, and verifying the completeness and correctness of Configuration Items. Applies to existing systems as well as assets acquired from the Procure Asset activity.	DISA

	Provides a logical model of the infrastructure or a service by identifying, controlling, maintaining and verifying the versions of Configuration Items (CIs) in existence.	
UIS 2.3.6 Manage Service Desk	The Service desk/support center extends the range of services and offers a more global-focused approach, allowing business processes to be integrated into the Service Management infrastructure. It not only handles incidents, problems and questions, but also provides an interface for other activities such as customer change requests, maintenance contracts, software licenses, Service Level Management, Configuration Management, Availability Management, Financial Management for IT Services, and IT Service Continuity Management.	DISA "JFC - UIS" "GCC - UIS"
UIS 2.3.6.1 Manage Service Desk Procedures	When designing your processes and procedures, and taking the broad view, you will need to: review their validity on a regular basis, and update as required, involve all relevant parties, allocate sufficient time and resources, consider alternatives (e.g. information being computerized rather than in printed form) and provide new reference materials based on incident and problem trend analyses. Includes collecting and managing customer information.	DISA "JFC - UIS" "GCC - UIS"
UIS 2.3.6.2 Provide Help Desk Services		DISA "JFC - UIS" "GCC - UIS"
UIS 2.3.6.3 Manage Escalations	Even in the best-supported operations, services breaches will occur. What is then important is to successfully manage the service breach, by recording the breach details and escalating to the Problem Management team, where appropriate.	DISA "GCC - UIS"
UIS 2.3.7 Remove Existing Asset	As assets reach the end of their established lifecycles, they must be removed from the enterprise in accordance with established policies.	"GCC - UIS"
UIS 2.4 Manage UIS Services	Initiates a set of services/activities that manage UIS Information Technology Services available to the Subscriber. Includes activities needed to negotiate Quality of Service (QoS) and cost agreements, and to bind the Subscriber and the Provider once an agreement has been reached. The end result of this negotiation is the Service Level Management (SLM), which is essential in any organization so that the level of UIS Service needed to support the business can be determined, and monitoring can be	DISA

	initiated to identify whether the required service levels are being achieved	
UIS 2.4.1 Manage Domain Name Services (DNS)	Provides enterprise wide hostname and IP address resolution for CII Enterprise services, C2 nodes, and mission applications. Manage Domain Name Services - ensure domain name services and active directory structures are configured properly to facilitate IP address to host name resolution. Area of focus of this activity is TCP/IP and active directory services domain name structure.	DISA
UIS 2.4.2 Manage Enterprise Directory Services	Directory Services are used to manage system-network resources (including access control lists and user privileges). Directory Services differs from a directory in that it is both the directory information source and the services making the information available and usable to the user's applications. A meta-data service offers the ability to synchronize authoritative data between disparate but connected directories. Includes support for: Entity (ID) Directory; Authentication and Authorization Directory; Network Directory; Meta-directories and Connectors; Information Assurance Services; Domain, Tree and Forest Management; Print Services; Routing and remote access; Group policy and policies for sites, domains, users, and computers; Message Queuing Services; Quality of Service (QoS); Distributed File System; Network Management; Electronic Mail; Backup and Restore Services; Directory Management; and Exchange Migration	DISA
UIS 2.4.3 Set Network Time	Activities required to establish and distribute network time.	DISA
UIS 2.5 Evaluate Service Delivery	This activity identifies and documents the service level management processes which are needed to assess, evaluate and sustain an adequate service level for all customers in accordance with the SLM defined in "Manage UIS Services". This is a cyclical process, where previous service level agreements and targets are re-evaluated periodically to see where improvements can be made.	DISA
UIS 2.5.1 Evaluate UIS Capabilities	This activity ensures that all capabilities required to support IT services function correctly, reliably, and according to standards as set by Baseline Services and above-	DISA

	baseline SLA contained within the C4IM Service Catalog.	
UIS 2.5.2 Evaluate UIS Services	Evaluate the C4IM and underpinning UIS Services necessary to conduct COCOM Operations and Business activities. Activity should result in an overarching Service Improvement Plan (SIP) and underpinning infrastructure, staffing, and training plans focused upon specific UIS capabilities.	DISA
UIS 3.0 Provide UIS Services	This activity provides capabilities that enable users to dynamically interact, share, and use information to operate in a net-centric manner. These services consist of core services, COI services, and environment control services. Note: these services have also been referred to as GIG Enterprise Services (GES).	"JFC - UIS" DISA "GCC - UIS"
UIS 3.1 Provide Subscriber Interface Services	A set of services provided at the Subscriber interface that provide presentation services to the Subscriber (Input/Output), and translate the Subscriber's requests for Net-Centric services into the proper form/format for communication with Network Service Providers.	"JFC - UIS" DISA "GCC - UIS"
UIS 3.2 Protect the UIS Information Environment	This set of activities depict the capability required to Protect the UIS Information Environment and associated services from internal and external threats.	DISA DoD "GCC - UIS"
UIS 3.2.1 Provide Assured Information Sharing and Management Services	This activity provides the ability to securely and dynamically share information. It provides an authorized user timely exchange of information without special technical training or special security clearances to obtain the right information, at the right time, at the right place, and displayed in the right format during normal, degraded, and disconnected conditions, while denying adversaries and unauthorized users access to that same information or service. It enables exchanging information within and between security domains and Communities of Interest (COIs), at multiple levels of sensitivities, and, between authorized users within the DOD, other US Government departments and agencies, law enforcement agencies, selected non-government and private sector entities, allied nations and coalition partners, as appropriate, under normal, degraded, and disconnected conditions. Assured Information Sharing enables the timely, automated, and flexible creation and management of COIs. It also provides for dynamic, trusted and authenticated user access, as well as enabling the sharing of	DISA DoD

	user identity and access rights throughout the enterprise.	
UIS 3.2.2 Provide Information Environment Protection Services	This activity provides the ability to monitor, search for, detect, track, and respond to attacks by adversaries within the net-centric environment. Involves integrating a security management infrastructure with the overall management and operation of the environment and deployed to provide net-centric IA services. To manage IA effectively within a security management infrastructure needs to be integrated with the overall management and operation of the environment and deployed to provide net-centric IA services. Any circumstance or event with the potential to adversely impact an IA through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.	DISA DoD
UIS 3.2.3 Provide Information Protection Services	This activity delivers Assured Resource (Systems and Networks) Availability and Assured Information Protection. Actions include recognition of attacks as they are initiated or are progressing, efficient and effective response actions to counter the attack and safely and securely recover from such attacks, and reconstituting new capabilities from reserve or reallocated assets when original capabilities are destroyed. Information Protection Services are focused on Assured Resource (Systems and Networks) Availability and on Assured Information Protection. The objectives of this focus are achieved by instituting agile capabilities to resist adversarial attacks, through recognition of such attacks as they are initiated or are progressing, through efficient and effective response actions to counter the attack and safely and securely recover from such attacks; and by reconstituting new capabilities from reserve or reallocated assets when original capabilities are destroyed.	DISA DoD
UIS 3.2.4 Provide Network Protection Services	Delivers mechanisms that provide network protection to include network encryption, physical isolation, high assurance guards, and firewalls. Mechanisms are used to create a collection of system high networks and enclaves. Enclave protection mechanisms are also used to provide security within specific security domains. In general, enclave protection mechanisms are installed as part of an Intranet used to connect networks that have similar security requirements and have a common security domain. A site may have multiple security domains with protection mechanisms tailored to the security requirements of specific customers.	DISA DoD
UIS 3.3 Provide Core	This activity enables warfighters/operators to exercise control over enterprise	"JFC - UIS"

UIS Services	information and services through a loosely coupled, distributed infrastructure that leverages service modularity, multimedia connectivity, metadata, and collaboration to provide an environment that promotes unifying actions among all UIS participants.	"GCC - UIS"
UIS 3.3.1 Provide Community of Interest Environment	This activity provides functions developed by a COI for its specific missions or, for the common use of other COIs. A function that is initially specific to a COI can satisfy the requirements of other COIs and become a common function. Furthermore, any COI function can become a core application/function. Communities of Interest: Collaborative groups of users, who must exchange information in pursuit of their shared goals, interests, missions, or business processes, and who, therefore must have a shared vocabulary for the information they exchange. DoD Directive: Data Sharing in a Net-Centric Department of Defense A Community of Interest is the collection of people that are concerned with the exchange of information in some subject area. The community is made up of the users/operators that actually participate in the exchange; the system builders ...., and the functional proponents that define the requirements and acquire the systems on the behalf of the Users. The subject area is the COI domain - whatever the people in the COI need to communicate about.	"JFC - UIS" "GCC - UIS"
UIS 3.3.1.1 Create Shared Information Space	Activities required to establish a shared information space for COI members. The "information space" is used to aggregate, integrate, fuse, and disseminate information to users.	MAJCOM "JFC - UIS" "GCC - UIS"
UIS 3.3.1.2 Create Common Workspace	Activities required to establish a shared workspace for COI members.	"JFC - UIS" "GCC - UIS"
UIS 3.3.1.3 Provide COI Management Resources	Activities required for COI Managers to establish COI member roles, membership lists, profiles, access controls, and policy-based network instructions.	"JFC - UIS" "GCC - UIS"
UIS 3.3.1.4 Enable Determination of Resource Availability	Activities required to allow COI members to determine the availability (presence and status) of COI resources (information objects, members, storage services, communications resources, etc).	"JFC - UIS" "GCC - UIS"

UIS 3.3.2 Provide Information Sharing Services	Information Management Services include those activities that provide life-cycle management of Subscriber data without regard to data content or meaning. Information Management: The creation, use, sharing, and disposition of information as a resource critical to the effective and efficient operation of functional activities. The structuring of functional processes to produce and control the use of data and information within functional activities, information systems, and computing and communications infrastructure.	"JFC - UIS" "GCC - UIS"
UIS 3.3.2.1 Provide UIS Directory Services	A directory is an information resource used to store information about objects. A directory service can make those objects and their content available to user applications. The data in the directory may come from a number of authoritative data sources. Provides the directory management organization and processes required to create a scalable, secure, and manageable infrastructure for deploying and maintaining directory services. Directory Services Profile ver. 1.9, 13 Jan 03 COIs will establish their own set of one or more directories. The COI will be responsible for configuring and maintaining the configuration of the directories.	"JFC - UIS" "GCC - UIS"
UIS 3.3.2.2 Provide Discovery Services	This set of services enables the formulation of search activities within shared space repositories (e.g., catalogs, directories, registries). It provides the means to articulate the required service argument, provide search service capabilities, locate repositories to search and return search results or, if necessary, initiates a tasking to the system to obtain the requested information.	"JFC - UIS" "GCC - UIS"
UIS 3.3.2.3 Provide Collaboration Services	This activity provides and controls the shared resources, capabilities, and communications that allow real-time collaborative interactions among participating group members. This environment provides synchronous collaboration capabilities; asynchronous collaboration can occur through other net-centric services and applications that are provided within the information environment.	"JFC - UIS" "GCC - UIS"
UIS 3.3.2.4 Provide Messaging Services	Messaging Services are all formal (organizational) messaging services, to include e-mail, Defense Message Service (DMS), and instant messaging services. Provides services to support asynchronous and synchronous information exchange. This activity consists of all activities needed to support formal (organizational and/or structured) and informal (email and/or unstructured) messaging services. It includes	"JFC - UIS" "GCC - UIS"

	support for tactical requirements. It supports the composition and validation of outgoing messages (message preparation). It supports the processing of incoming messages, including subsequent distribution to intended recipients as users of the information environment. The activity establishes and conducts message (bulletin) board services. It also supports official message traffic.	
UIS 3.3.2.5 Provide Information Mediation Services	This activity enables transformation processing (translation, aggregation, and integration), situational awareness support (correlation and fusion), negotiation (brokering, trading and auctioning services) and publishing.	"JFC - UIS" "GCC - UIS"
UIS 3.3.2.6 Provide Negotiation Services	This set of services applies protocols to establish the most appropriate service capabilities in response to service invocations. The request for data or services may be brokered to provide specific objects and/or object methods. The request for data or services may be supported by trader services that exchange information among brokers. The request for data or services may also be negotiated based upon the attributes of the persona of the requesting principal or upon the service that best matches the request.	"JFC - UIS" "GCC - UIS"
UIS 3.3.2.7 Provide Information Management Support Services	Activities required to support the use of Information Objects during business, combat support, or warfighting activities.	"JFC - UIS" "GCC - UIS"
UIS 3.3.2.8 Provide Information Integrity	1) This activity provides protection against unauthorized modification or destruction of information. This protection supports information in storage, in transit and when processing. This capability maintains the quality of information, reflecting the logical correctness and reliability of the data. It ensures the logical completeness of the hardware and software implementing the data protection mechanisms and the consistency of the related data store structures. 2) Activities required to protect Information Objects and meta-data resident in a database or data warehouses (e.g., file encryption, records locking, and access controls).	"JFC - UIS" "GCC - UIS"

UIS 3.4 Provide Computing Infrastructure	Computing Infrastructure includes those activities that provide a secure, robust, and cost effective computing environment to host core, network, and mission/community of interest (COI) application software; capabilities that enable information storage/retrieval and continuity of operations/disaster recover (COOP/DR); and common resources that enable user input and information processing, output, and display.	"JFC - UIS" "GCC - UIS"
UIS 3.5 Provide Communications Services	Communications Services provide the Subscriber with a full range of information transport services for voice, data, video, imagery, etc. Communications Services provide an integrated network that is managed and configured to provide an information transfer utility for Infostructure Subscribers.	

4. Inputs/Outputs

Name	Purpose	Ref1	Ref1 Detail	Ref2	Ref2 Detail	Ped1	Ped1 Detail	Format	Transfer Mechanism
Acceptance of Aircraft Support Request	Acceptance of request for relief supplies to be lifted by U.S. military aircraft.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
ACCEPTANCE OF AIRCRAFT SUPPORT REQUEST	Acceptance of request for relief supplies to be lifted by U.S. military aircraft.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
Add Requestor to Streaming Video Group						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Advice to HOC Staff	Information on humanitarian support to the relief community.							Data and voice	Email; phone; face to face
Advice to CMOC Staff	Information on military support to the relief community.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face

ADVICE TO CMOC STAFF	Information on military support to the relief community.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
ADVICE TO HOC STAFF	Information on humanitarian support to the relief community.							Data and voice	Email; phone; face to face
Aircraft Support Request	Request for relief supplies to be lifted by U.S. military aircraft.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
AIRCRAFT SUPPORT REQUEST	Request for relief supplies to be lifted by U.S. military aircraft.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
Annex J of the US Emb. EAP	Annex J (Mission Disaster Relief Plan) of the US Embassy Emergency Action Plan (EAP)	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Written document

Annex J of the US Embassy (Emer Action Plan)	Annex J (Mission Disaster Relief Plan) of the US Embassy Emergency Action Plan (EAP)	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Written document
Approved Operational Changes	Approved changes to the operational infostructure.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Change History	Records of changes to assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Configuration Information	Details on the current configuration of assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Cost Data	Costs of operation of IT assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Asset Dependencies	Dependencies between assets on the network.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Discovery Policy	Policy for the timely discovery of assets on the network.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Identification Information	Identifying information for managed objects on the network.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Information	Identification and operational information on assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Information Collection Policy	Policy regarding the detail and extent of information to be collected on assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Lifecycle Policy	Plans for lifecycle replacement of IT assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Asset Metrics	Measurable information regarding the status and performance of assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Asset Purchasing Catalog	The catalog of assets that are available to be purchased.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Assigned Asset Lifecycles	Asset Lifecycles associated with identified assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Audio and Video Collaboration Results	Results of audio or video collaboration.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Audit Controls	A set of instructions to network equipment to implement the Audit Services request. Audit trail records from all available sources are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with DoD information system IA procedures	"GIG IA"	"GIG IA Component of the GIG Integrated Architecture"			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Availability Discovery Request	Request to Discovery Services to search for persons or resources needed to conduct collaboration.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Brokered COI Services Request	Request establishment of a Community of Interest (COI) with definition of information requirements, membership, subscriber profiles, catalog and services administration. Includes requests by the COI policy manager to actively create/negotiate policy parameters for a given service/service set and specified information/objects.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Brokered Information Object	Information Objects that have been brokered or prioritized for service delivery.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Brokered Service Request	The Brokered Service Request is produced after the Subscriber’s Service Request is compared to other pending service requests, the Subscriber's Profile, and the Commander's Information Policy. It is a response to a Subscribers Service Request. Applies Commander's information policy and network resource status. The Brokered Service Request is the allocation of infostructure resources in support of the Information Network.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Catalog Advertisements	IDM services will enable producers of information to post the descriptions of their information products rapidly and send advertisements to interested users.	"IDM CRD"	22 Jan 01, Pg 24			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Catalog Creation Request						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Catalog Management Requests	Request for services to create, update, and maintain catalog information. Bundle includes: - Catalog Creation Request - Request for publication - Publication Maintenance Request					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Change Request	Request to change any portion of the infrastructure, whether a physical change, a software change, a configuration change, or any other.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Catalog	Catalog of Services or Information Objects available to COI members.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Controlling Authority Guidance	Guidance provided by the Controlling Authority of the Community of Interest.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Directory	The vocabulary (i.e. metadata elements) and the sources for the metadata organized according to the taxonomy / ontology that the COI has developed.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

COI Directory Creation Request	Request to generate a directory from a COI's taxonomy and / or ontology and metadata from authoritative data sources.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Directory Management Data	Data that will be used to manage a COI's directory.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Information Subscription	COI Member's request to subscribe to Information Objects. Subscribers may chose to receive update notifications only or may chose to receive the updated Information Objects.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Membership List	Community Of Interest (COI) Membership List represents user support provided by COI Services for a COI. Includes membership, user role, catalog, subscription administration, and Roles Based Access Control (RBAC) support.	"NCOW"				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Policy-Enforcement Mechanisms	A set of policy-based controls to COI resources to enforce COI policies and is performed through various policy-enforcement mechanisms distributed throughout the information environment.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

COI Profile	The Subscriber's Profile updated to include information about his/her role and associated rights and privileges within the COI. Community of Interest (COI) Profiles represent a user/entity request to establish a COI identity. The request includes all pertinent information required to initiate the COI profile and accesses authorization. This includes all user profiles associated with the COI upon authentication. Operate and manage the dynamic and automatic feedback mechanisms that enable the profile to "learn" and "anticipate" the user's needs based on his usage patterns and patterns of similarly profiled users. Implement a combination of human and automated means to review, verify, and validate both the user and provider-specified portions of the dynamic profile.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Role Permissions	Permissions assigned to a COI Role					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Roles	Roles and Responsibilities within a Community of Interest.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

COI Services Management Information	Data concerning the configuration, performance, use, status, and security of Community of Interest (COI) Services. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
COI Tables	Tables (directories, indexes, registries, metadata repositories, etc) required to manage COI resources and Information Objects.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Collaboration Configuration Request	A request to UIS Configuration Management to change the configuration of network equipment to allocate or de-allocate resources required for collaboration.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Collaboration Information	Audio, video, multimedia, or data information objects from one or more collaboration participants.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Collaboration Management Data	Data concerning the configuration, performance, use, status, and security of collaborative resources. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Collaboration Results	Information objects that are produced during collaboration. Examples include: audio, video, multimedia files and associated records.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Collaboration Services Request	Request for the creation and use of a collaborative work environment. The users may be members of a persistent Community of Interest (COI) or an ad hoc group needing collaboration services. The work environment be persistent or temporary (needed only for the duration of the collaboration).					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Commander's Information Policy	Consists of operational authorities' policy on use of infostructure and rules governing the classification, releasability and priority of the information presented to the infostructure. Instructions, directions or policy specific to a unit, organization or operation that has local implications for guidance in security and Information Assurance conditions.	"ICD GIG ES dated 03/22/2004"	ICD GIG ES dated 03/22/2004			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Configuration Change Instructions	Change Configuration Instructions are sent to Infostructure components to initiate a change in their configuration. These can include commands to update software components, change routing tables, activate spare equipment, etc.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Configuration Instructions	Instructions to configure infostructure equipment. Network Configuration Instructions are the policy based instructions from the network manager. These would include instructions to improve the availability, security, reliability, integrity, and performance of the network. Instructions or policy created by systems administrators, policy analyst, and CND analyst that propose guides and updates for any instructions on the proper procedures for configuration, changes, or updates for Information Assurance process that include IDS, COMSEC, EMSEC, and KMI., VPN management and other IA processes. Information generated from managed IA activity include raw audit data configuration information, request for access, request to perform transactions and credentials.	"GIG NetOps"	"GIG NetOps, Ver 3.0"	"GIG IA IFTR "	"GIG IA IFTR - Identity Management and Authentication"	"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Configuration Management Plan	Process for managing configurations of systems and networks.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Contract Payment Policy	UIS policy for how/when contracts will be paid.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Contract Payment Records	Records of actual payments made against contracts.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Contract Payment Schedules	Planned payment schedules for contracts.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Contract Reports	Summary of the status of existing contracts.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Coordinated Requirements	Requirements for infostructure services that have been processed, prioritized, coordinated, and a decision has been made to either act on, table, or deny the requirement.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Coordination	Information on the disaster and status of response actions.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09	Data and voice	Email; phone; face to face
Coordination - Aircraft Support	Information about commodities and delivery requirements.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face

COORDINATION - AIRCRAFT SUPPORT	Information about commodities and delivery requirements.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
Coordination - CMOC						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Cost Data	UIS Cost data.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Country advisories	Warning to American citizens of danger in the relief area and information about how to locate American Citizens (AMCITS) in the relief area.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and voice	Email; phone; face to face
Country update to impending disaster to include maps	GIS tools, geographical representation of relief area and actions.	"OCHA website: Information Management: Services"	http://www.unocha.org/what-we-do/information-management/im-services					Data	Posted on Reliefweb

Data Management Services Request						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
DEPLOY DISASTER ASSISTANCE RESPONSE TEAM	Team composition, capabilities, support needs	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG
Deploy Disaster Assistance Response Team (DART)	Team composition, capabilities, support needs	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG
Depreciation Schedules	Planned reduction in value of UIS assets.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Design Requirements	System design requirements. - Performance and Quality - Security - Capacity/Size					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Directory Service Request	A request to: - modify the structure of the directory, - manipulate (create, read, update, delete) the directory entry for an information object.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Directory Services Catalog	Catalog of Directory Services metadata holdings.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Directory Services Management Data	Data concerning the configuration, performance, use, status, and security of Directory Services. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Directory Services Search Results	Results returned from search in Directory Services.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Disaster Alert Cable	Background, current situation, anticipated course of action.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Cable (Message)(DOS equivalent to DMS)

DISASTER ALERT CABLE	Background, current situation, anticipated course of action.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Cable (Message)(DoS equivalent to DMS)
Disaster Assistance Request	Request for up to $50,000 USD. Designates specific humanitarian and disaster relief organization to receive.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Cable (Message); email; fax
DISASTER ASSISTANCE REQUEST	Request for up to $50,000 USD. Designates specific humanitarian and disaster relief organization to receive.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Cable (Message); email; fax

Disaster Declaration Cable	1. The disaster is of such a magnitude that it is beyond the host country's ability to respond adequately; the host country has requested or will accept USG assistance, and it is in the interest of the USG to provide assistance. 2. The extent to which the host country needs assistance; 3. The intended use of requested resources, including recommended organizations through which funds will be channeled. 4. Estimated number of killed, injured, affected, displaced and homeless; immediate humanitarian needs; background info i.e. geo location, infrastructure, crops, livestock; other donor efforts; info from available assessment reports.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Cable (Message) (DoS equivalent to DMS); email; FAX
DISASTER DECLARATION CABLE	1. The disaster is of such a magnitude that it is beyond the host country's ability to respond adequately; the host country has requested or will accept USG assistance, and it is in the interest of the USG to provide assistance. 2. The extent to which the host country needs assistance; 3. The intended use of requested resources, including recommended organizations through which funds will be channeled. 4. Estimated number of killed, injured, affected, displaced and homeless; immediate humanitarian needs; background info i.e. geo location, infrastructure, crops, livestock; other donor efforts; info from available assessment reports.	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Cable (Message) (DoS equivalent to DMS); email; FAX

DISASTER RELIEF GUIDANCE	Resources and agencies available	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG
Disaster relief guidance	Resources and agencies available	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG
Disaster Relief Guidance						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Discovery Management Data	Data concerning the configuration, performance, use, status, and security of Discovery Services. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Discovery Results	Location of requested data or service. Once the location of the requested Service or Information is known, the Subscriber, and Application, or another Service can request the Information or invoke the Service.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Discovery Search Controls	Controls used to search repositories for the requested information, service, or metadata. Bundle includes: Service Search Controls Information Search Controls Person Search Controls Metadata Search Controls					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Discovery Services Request	Subscriber Request to search the network for information and/or services. Includes Availability Discovery Request.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
DNS Response	DNS information response to DNS Query					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Encrypted Information Object	Information Objects that have been encrypted to provide Confidentiality of data-in-transit over backbone networks must be maintained using appropriate encryption measures as per the classification or sensitivity level of the data.	"CJCSI 6510.01E"	"CJCSI 6510.01E, IA Computer Network Defense"			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Escalations Incident Report	Report of escalations incidents which operate in a planned and measurable fashion.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Establish/Change COI Subscription	Subscriber's request to establish or change the subscription to a Community of Interest (COI).					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Global Information Grid Status	Status of the GIG infostructure					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Help Desk Information	Assistance and problem resolution information provided to the Requester.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Help Request	A Subscriber's request for UIS assistance. Help requests may be received via e-mail, or web interface.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

HHQ UIS Policy & Guidance	DoD and other Policy and Guidance that regulates Information Technology activities. UIS Policy & Guidance implements all mandatory and discretionary protection policies relevant to the GIG enterprise level. It also implements discretionary protection policies within any given domain. Implementation activities include setting parameters in mechanisms used for protection policy enforcement, deployment and configuration of protection devices, and re-configuration activities to meet changes in threat posture, changes in performance capabilities, and/or changes in protection policy (e.g., INFOCON Directives).					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Identified Assets	Assets existing on the network.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

IM Services Management Data	Data concerning the configuration, performance, use, status, and security of Information Management Services. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel. Bundle includes: Discovery Management Data Collaboration Management Data Messaging Services Management Data Mediation Services Management Data Negotiation Services Management Data Information Protection Management Data					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Imagery Assessment	Imagery Products and Assessment	"https://www.cia.gov/library/reports/archived-reports-1/Ann_Rpt_2003/snp.html"						Data	Posted on Reliefweb; Email with attachment
Imagery Products	Geo-rectified products	"USSOUTHCOM and JTF-Haiti… Some Challenges and Considerations in Forming a Joint"	US Joint Forces Command Joint, Center for Operational Analysis					Data	Posted on Reliefweb; Webpage; Email with attachment
Imagery Products Request	Geo-rectified products	"Joint Lessons Learned: Keys to Successful International Humanitarian Assistance"	Joint Center for Operational Analysis, US Joint Forces Command, Norfolk, Virginia					Data and voice	Email; phone; face to face

IMAGERY PRODUCTS REQUEST	Geo-rectified products	"Joint Lessons Learned: Keys to Successful International Humanitarian Assistance"	Joint Center for Operational Analysis, US Joint Forces Command, Norfolk, Virginia					Data and voice	Email; phone; face to face
Incident Escalation Policy	Plans for when/how to escalate incidents to higher levels of support.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Advertisement						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Creation Controls	Controls the development and release of new information objects into the shared information space.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Management Controls	A set of instructions to network equipment to implement the policy-based Information Management request.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Management Services Controls	A set of instructions to network equipment to implement the policy-based Information Management request.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Information Management Services Invocation	Information Management Services Invocation is the approved and brokered Subscriber's request for NCES information management services like Discovery, Collaboration, Messaging, or Mediation. Bundle includes: - Discovery Services Request - Collaboration Services Request - Message Services Request - Mediation Services Request - Data Management Services Request - Web Services Request					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Management Support Objects	Information Objects that have been created of modified during the Information Management Support activities.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Management Support Services Request	A Subscriber's request for Records Mgt, Workflow Mgt, or Data Administration services.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Information Management Transactions	Output from Information Management activities. Bundle includes: Discovery Services Search Results Collaboration Information Objects Messages Mediation Products Records Documents Workflow Products Table Updates					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Object	An Information Object includes audio, video, data, or sensor information and their meta data tags. This ICOM may also be used in a plural context					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Protection Controls	A set of instructions to network equipment to implement the policy-based Information Protection Services.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Protection Management Data	Data concerning the configuration, performance, use, status, and security of Information Protection Services resources. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Information Storage Services Request	Request to Enterprise Storage Management Services to store, retrieve, or move information. Bundle includes: Modified Tables Updated Metadata Replicated Directory Updated Authoritative Source Data					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Storage Services Response	Response from Provide Information Storage Services					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Information Tags	Information Tags are metadata (data about data) All data, that will be exchanged or has the potential to be exchanged, will be tagged in accordance with the current JTA standard for tagged data items (XML).	"IDM CRD"	22 Jan 2001, pg 38			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Infostructure Events	Occurrences within the ConstellationNet Infostructure. This includes both normal and anomalous events.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Infostructure Reports	Analysis of Infostructure Data.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Infostructure Status	Infostructure Status focuses on the reporting requirements at various levels of NetOps management to ensure NetOps Personnel can maintain GIG situational awareness. Situational-awareness requirements, policy, guidance, monitoring capabilities, and standard NetOps operating procedures control this activity. NetOps personnel perform this activity. Infostructure Status is the standardized NetOps status derived from situational awareness capabilities, following reporting procedures, an established reporting hierarchy, and identified authorities for overseeing and controlling NetOps. Bundle includes: • Net-Centric Services Management Data • SSPI Status • Network Status • NCES Status • Storage Management Data					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
INFOSTRUCTURE STATUS									
IT Contract Support Requirements	Requirements for provision of IT Contract Support					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

IT Policy & Guidance	DoD, AF, MAJCOM, and other Policy and Guidance that regulates Information Technology activities. IT Policy & Guidance implements all mandatory and discretionary protection policies relevant to the GIG enterprise level. It also implements discretionary protection policies within any given domain. Implementation activities include setting parameters in mechanisms used for protection policy enforcement, deployment and configuration of protection devices, and re-configuration activities to meet changes in threat posture, changes in performance capabilities, and/or changes in protection policy (e.g., INFOCON Directives).					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
JFC UIS Policy & Guidance	JFC Policy and Guidance that regulates UIS activities. JFC Policy & Guidance implements all mandatory and discretionary protection policies relevant to the UIS. It also implements discretionary protection policies within any given domain. Implementation activities include setting parameters in mechanisms used for protection policy enforcement, deployment and configuration of protection devices, and re-configuration activities to meet changes in threat posture, changes in performance capabilities, and/or changes in protection policy (e.g., INFOCON Directives).					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Joint Infrastructure Tasking Order	A Joint order, typically from JTF-GNO, that directs configuration, implementation, or other types of action to be taken with regards to information, information protection, and other infrastructure issues					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Managed Assets	Assets that are properly configuration controlled.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Managed Configuration Plan	Actively maintained and supported plan for managing configuration of systems and networks.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Managed Service Desk Procedures	Service desk operations and procedures handled in a planned and controlled fashion.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Mediation Products	Information objects that have been produced or altered through the use of Mediation Services.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Mediation Services Management Data	Data concerning the configuration, performance, use, status, and security of Mediation Services resources. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Mediation Services Request	Request to provide mediation services.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Message Service Request	Request to provide support for asynchronous and synchronous information exchange.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Messages	Synchronous or asynchronous messages for distribution.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Messaging Services Management Data	Data concerning the configuration, performance, use, status, and security of Messaging Services resources. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Mission Requirements	Requirements Documents received from Subscribers, COI Managers, Systems Program Officers (SPOs), Program Management Offices (PMOs) and others.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Need to Create/Change Subscriber Profile	(Boundary Input), represents a Subscriber's requirement to create or change a Subscriber Profile.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Negotiation Services Management Data	Data concerning the configuration, performance, use, status, and security of Negotiation Services resources. May include log files and other data reported to COI Managers, UIS or Information Assurance personnel.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Network Time	Updated standard time for the network.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
OPORD	Detailed instructions for executing the Humanitarian Assistance/Disaster Relief operation.	"USSOUTHCOM and JTF-Haiti… Some Challenges and Considerations in Forming a Joint"	US Joint Forces Command Joint, Center for Operational Analysis					Data	Posted on Reliefweb; Webpage; Email with attachment
OpORD	Detailed instructions for executing the Humanitarian Assistance/Disaster Relief operation.	"USSOUTHCOM and JTF-Haiti… Some Challenges and Considerations in Forming a Joint"	US Joint Forces Command Joint, Center for Operational Analysis					Data	Posted on Reliefweb; Webpage; Email with attachment
Paid Contracts	Contracts that have had all or some payments made.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Permissions	Permissions determine the data and applications that may be accessed for each role that is assigned the set of permissions that are necessary for the user to perform his required tasks. Is the act of allowing and authorizing use of specific resources for use in accessing networks? These resources can be identified and allowed for use in many ways that may include file, directory and object access. Normally the access controls that are required and placed on a resource are the permissions granted for access to that resource or a particular object. It focuses on capabilities for enabling and/or disabling entity permissions, rights, or privileges associated with locally or remotely entering host systems. Permission restrictions may be based on time-of-day, user location, device identity, port identity, etc. Authorization Restriction Parameters may be static or dynamic. UIS Security Administrators construct this type of authorization based on local and enterprise-wide policy, and deconflicts this type of authorization with other types of authorization being employed. This activity is controlled by access and usage policies that respond to evaluated threats.	"NIST/ITL Bulletin"	"NIST/ITL Bulletin, An Introduction to Role-Based Access Control"			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

PPBD Information	Planning, Programming, & Budgeting Decision information is used to govern fiscal expenditures supporting the EIE					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Precedence	An information flow precedence tag (e.g., routine, priority, emergency)					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Producer's Information Catalog	Catalog/index of information Producers products and product updates.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Publication Maintenance Request						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Relief Effort Coordination	Information about the plans and execution of DART's relief efforts.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
RELIEF EFFORT COORDINATION	Information about the plans and execution of DART's relief efforts.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face

REQUEST DoD ASSISTANCE IN TRANSPORT EMER RELIEF COMMODITIES	Type, amount, location, destination, Required Delivery Date (RDD), capacity limitations at reception area	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG
Request DoD Assistance in Transporting Emergency Relief Commodities	Type, amount, location, destination, Required Delivery Date (RDD), capacity limitations at reception area	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG
Request for Information Controls	Request to establish new information/objects either by information collection means or as a result of exploiting, interpreting, assessing, or analyzing existing data to provide additional insights.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Request for Publication						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Request Streaming Video Service	A Request from streaming video services					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Request to Establish a COI	(Boundary Input), represents a requirement to establish a Community of Interest (COI). Gartner defines Community of Interest as "Also know as a community of practice, this group of people associated and linked in a network of communication or knowledge network because of their shared interest or shared responsibility for a subject area. ... Communities continually emerge and dissolve, and their membership, processes and knowledge continually change and evolve. Source: Gartner's Glossary of Terms Used for the Knowledge Workplace: 2004 Update. Bundle includes: COI Membership List COI Member Designation COI Role Descriptions COI Policies	"NCOW: Need to Operate as a COI: (Boundary Input) "	Represents a user requirement to initiate and operate as a COI typically based on missions, tasks, or objectives.			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Request USAID/OFDA Relief Commodities						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

REQUEST USAID/OFDA RELIEF COMMODITIES	Material available from USAID/OFDA stockpiles	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG
Request USAID/OFDA relief commodities	Material available from USAID/OFDA stockpiles	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data and Voice	MSG
Requested Dissemination Service	The Requested Dissemination Services are provided once the Subscriber's Credentials have been authenticated, the appropriate policies have been reviewed, and the required permissions have been granted. Bundle includes: - Smart Push Data - Search Results - IDM Catalog Data					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Requirements	Requirements Documents received from Subscribers, COI Managers, Systems Program Officers (SPOs), Program Management Offices (PMOs) and others.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Scope and Magnitude of Event	Type of event, how large an area, how big a storm or magnitude of earthquake, tsunami, etc. Numbers of personnel likely to be effected. Likely resources needed.	"Mission Disaster Relief Officer (MDRO) through established contacts including: h"	Chief of Mission (CoM), the embassy's Emergency Action Committee (EAC) and the USAID Office Foreign Disaster Assistance (OFDA) Principal Regional Advisor					Data and voice	Overview brief
SCOPE AND MAGNITUDE OF EVENT	Type of event, how large an area, how big a storm or magnitude of earthquake, tsunami, etc. Numbers of personnel likely to be effected. Likely resources needed.	"Mission Disaster Relief Officer (MDRO) through established contacts including: h"	Chief of Mission (CoM), the embassy's Emergency Action Committee (EAC) and the USAID Office Foreign Disaster Assistance (OFDA) Principal Regional Advisor					Data and voice	Overview brief
Security Clearance Information	Information regarding the Security Clearance of individuals.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09	Data	Cable (Message); email; fax

SECURITY CLEARANCE INFORMATION						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Security Policy and Instructions	Set of laws, rules, and practices that regulate how sensitive (SBU and classified) information is managed, protected, and distributed by an AIS. NOTE: System security policy interprets regulatory and operational requirements for a particular system and states how that system will satisfy those requirements. All systems or networks that process SBU or classified information will have a security policy. Security Policy and Instructions focuses on the creation of specific policy parameters and the negotiation/modification of these parameters. The input is the invocation of the policy manager to actively create/negotiate security policy parameters for a given service/service set and specified information/objects. The output is instructions concerning the new/modified policy parameters that constrain/enable service execution.	"AFDIR 33-303"	"AFDIR 33-303, definition for System Security Policy."	NCOW		"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Service Desk Procedures	Planned procedures for operating the service desk.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Service Request Response	The Service Provider's response to the request for service/information. Provides feedback to the Subscriber concerning the status of the pending service request. Bundle Includes: Audit Controls COI Tables COI Roles COI Membership List Shared Workspace Controls Information Creation Controls COI Policy-Enforcement Mechanisms Information Advertisement Confirmation of Delivery IDM Response Notification Help Desk Information Modified Information Object Retrieved Information Object • Customized Presentation Data					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Shared Information	Assured Information Sharing (AIS) provides the ability to securely and dynamically share information. It enables the ability to exchange information within and between security domains and Communities of Interest (COIs), at multiple levels of sensitivities, and, between authorized users within the Department of Defense (DOD), other United States (US) government departments and agencies, law enforcement agencies, selected non-government and private sector entities, allied nations, and coalition partners. AIS facilitates the timely, automated, and flexible creation and management of COIs, and provides for dynamic, trusted, and authenticated user access, as well as enabling the sharing of user identity and access rights throughout the enterprise.	"GIG IA"	"GIG IA Capability Roadmap for AIS, Ver 1.0"			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Shared Workspace Controls	Controls used to establish and manage a shared workspace for the COI. Includes: - Application Use Controls - Information Exchange Controls - Information Disposition Controls					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Significant Event Log	Daily significant events	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Website
SIGNIFICANT EVENT LOG	Daily significant events	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011					Data	Website
SITREP - JTF	Information on the disaster and status of response actions.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
SITREPS						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
SITREPS - Out						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Situation Report - DART	Information on the disaster and status of response actions.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09	Data and voice	Email; phone; face to face
Situational Awareness Data	Improvements in the marking of situational awareness information (such that unclassified situational awareness data resident in secret tactical networks is distinguished from secret situational data) and the ability of CDSs to process situational awareness data for transfer to unclassified networks. Information objects that support Situational Awareness.	"GIG IA"	"GIG IA Component of the GIG Integrated Architecture"			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Status Updates	Information on the disaster and status of response actions.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
STATUS UPDATES	Information on the disaster and status of response actions.	"USAID Field Operations Guide for Disaster Assessment and Response (Appendix F)"	version 4.0, September 2005					Data and voice	Email; phone; face to face
Status of approaching natural disaster	Information on type of disaster likely to occur and likelihood of striking country.							Data and voice	Alert posted on Embassy web site
Streaming Multimedia	Multi-media information content (including video) presented as a data stream.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Streaming Multi-media	Multi-media information content (including video) presented as a data stream.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Subscriber Information	Subscriber Information to be Stored, Processed, Published, or Transmitted across the network. This includes voice, video, data and imagery.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Subscriber Information Request						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Subscriber Profile	All requirements, criteria and other pertinent user information in a proper format and submit as the current User/Entity profile. Define and implement the basic attributes of the user's profile that are determined by the organization to which the user belongs and the user's role in that organization. Example attributes include user's roles, areas of responsibility, clearances, accesses, and communications medium. The Subscriber Profile is used to tailor the Network services to the Subscriber's preferences (font size, colors, default page, etc).	NCOW				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Subscriber Request	Subscriber request is a generic bundle of several different types of requests.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Subscriber Request Response	Provides feedback to the Subscriber concerning the status of a pending request.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Subscriber Service Request	Subscriber Service Request represents a user request for a specific service or capability. This includes profile requests, information publication requests, information acquisition requests, collaboration requests, and COI services requests. A Subscribers request for services from the network (information transport, file access, information dissemination, etc).					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Subscriber Service Request Response	Subscriber Service Request Response to a user request for a specific service or capability. This includes profile requests, information publication requests, information acquisition requests, collaboration requests, and COI services requests. A Subscribers request for services from the network (information transport, file access, information dissemination, etc).					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Training	Training required to gain access to the AF Network and other related training requirements					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
UIS Directives	Directives issued both to trigger specific actions as well as to inform effected organizations.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
UIS Plans	Plans for the operation of systems and networks.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
UIS Policy & Guidance	GCC/JFC, and other Policy and Guidance that regulates Information Technology activities. UIS Policy & Guidance implements all mandatory and discretionary protection policies relevant to the GIG enterprise level. It also implements discretionary protection policies within any given domain. Implementation activities include setting parameters in mechanisms used for protection policy enforcement, deployment and configuration of protection devices, and re-configuration activities to meet changes in threat posture, changes in performance capabilities, and/or changes in protection policy (e.g., INFOCON Directives).	NCOW				"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Validated Asset Requirements	Requirements for asset changes which have been validated as supporting mission requirements.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Validated Contracts	Contracts shown to be necessary and appropriate.					"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Video Stream Availability Notification Message						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		
Vulnerability and Damage Assessments	Assess damage suffered	"Per USAID cable MRN 11 STATE 4720/150531Z JAN 11"	Subject: USAID/DCHA Office of U.S. Foreign Disaster Assistance Guidance for Disaster Planning and Response - FY 2011			"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09	Data	MSG
VULNERABILITY AND DAMAGE ASSESSMENTS						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

Web Services Request						"USAF AFNet 2012 Arch Vers 1.0"	2-Oct-09		

THIS PAGE INTENTIONALLY BLANK

United States Joint Staff
Joint and Coalition Warfighting (JCW)

Interagency and Multinational Information Sharing Architecture and Solutions (IMISAS) Project

Annex O - White Paper on Unclassified Information Sharing (UIS)

Approved For Public Release - 28 October 2011

Executive Summary

Building on a strong foundation of current concepts, this near-term (five-year) vision for fostering unclassified information sharing (UIS) proposes "realm of the possible" areas to explore with broader conceptual frameworks, subsequent capability development activities, and joint experimentation. UIS focuses on a dynamic mix of *mission partners*, including United States military and government agencies, foreign governments and their militaries, international organizations, regional organizations, and state, local and tribal authorities. Although not a focus area, the UIS trade space also includes *stakeholder participant organizations*[1], such as nongovernmental organizations and members of the public and private sectors.

In the near-term future operating environment, UIS mission partners and stakeholder participant organizations face rapid and accelerating advances in information technology. Nurturing the rapid and accelerating growth of human knowledge, this proliferation of capabilities and technology choices may contribute to an overwhelming information overload among those organizations.

Existing policy, processes and procedural issues, such as the lack of compatible procedures and even general consensus on business rules, complicate and inhibit effective cooperation. Strong, hierarchy-based organizational cultures, while naturally building internal homogenous worldviews among members, tend to inhibit external networking efforts to build trust and create shared understanding with other organizations.

Best practices, as well as logically and experimentally derived solutions, can reveal "realm of the possible" capabilities, achievable in the next five years. The proposed UIS "success mechanism" blends aspects of changing technologies, policies, and organizational cultures. Proposed solutions include revising and updating UIS procedures, architectures, and information exchange requirements. A focus on agility and adaptation provides flexibility in the context of dynamic mission requirements and constantly evolving public information sharing domain, characterized by the prevalence of unstructured data and distributed, ad hoc, or post-bureaucratic organizational structures. Finally, proposed UIS solutions outline several areas where cost-benefit or feasibility analyses can provide value to decision makers.

---

[1] Adapted from "Designing an Inclusive Simulation Environment: Understanding the Landscape of Non-military Humanitarian Assistance and Disaster Relief Actors." World Cares Center, New York, NY, 2010. Source identifies "groups without government affiliation" as NGOs, Community-based Organizations, Faith-based Organizations, Private Sector Organizations and Corporations, and Host Country Civil Society.

Mission partners and stakeholder participant organizations willingly participate in a wide-range of mission areas, such as humanitarian assistance/disaster relief (HA/DR). Leveraging UIS capabilities will include the following foreseeable benefits: (1) achieving compatibility of effort across mission and coalition operations; (2) improving the speed and execution of cooperation; (3) achieving rapid adaptability across mission and coalition operations; and (4) improving the ability to anticipate events and resource needs, providing an initial situational advantage, and setting the conditions for success. As UIS approaches mature into an enterprise solution, these benefits can be logically extensible to other mission areas, such as Homeland Defense/Civil Support.

TABLE OF CONTENTS

1.0 Purpose O-1
2.0 Scope O-1
3.0 Military Problem O-5
4.0 Solution O-10
5.0 Risks and Mitigations O-18
6.0 Implications O-19
Appendix – References O-21

Approved For Public Release - 28 October 2011

Unclassified Information Sharing (UIS)

1.0 Purpose

This document describes a vision for unclassified information sharing (UIS) among mission partners and stakeholder participant organizations. The purpose is to generate an effective discourse, collectively explore tomorrow's "realm of the possible," and provide a conceptual foundation for subsequent capability development activities and joint experimentation.

2.0 Scope

"DOD must coordinate internally and with multiple mission partners in a variety of scenarios and situations that require immediate response. The ability to share information during such times is critical to operational success."[2]

The Capstone Concept for Joint Operations (CCJO) identifies the United States (U.S.) military's need for "integrated national and multinational operations, which in turn will require close cooperation with partners that may have very different organizational processes and cultures in a variety of standard and nonstandard relationships."[3] Whether formed in humanitarian assistance/disaster relief (HA/DR) mission contexts or in other areas, maintaining and adapting these relationships presents a unique set of challenges and opportunities for UIS among stakeholder communities, especially when extended to other mission spaces.

Information sharing is "making information available to participants (people, processes, or systems)," which "includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant."[4] ***Mission partners*** are defined as the expanse of possible actors with whom the Department of Defense (DOD) may coordinate and therefore share information, whether with organizations or national governments. They include: federal non-DOD departments and agencies, state, local, and tribal government departments and agencies, nongovernmental organizations (NGOs), intergovernmental organizations (IGOs), private sector companies and organizations including international

[2] OASD/NII, *Department of Defense Information Sharing Implementation Plan*, April 2009.
[3] *Capstone Concept for Joint Operations*, Version 3.0, 15 Jan 09, p. 33.
[4] *Department of Defense Information Sharing Strategy*, 4 May 2007

organizations, foreign governments, and militaries.[5] ***Stakeholder participant organizations*** include, but are not limited to, some NGOs and members of the public and private sectors involved with the same community of interest (COI) or issue who would reject affiliation as a DOD mission partner. Viewed collectively, these participant actors comprise the UIS ***extended enterprise.***[6]

Based on the *DOD Information Sharing Implementation Plan*, this document envisions a future state in which "transparent, open, agile, timely, and relevant information sharing occurs to promote freedom of maneuverability across a trusted information environment."[7] Building on the foundation of the *Unclassified Information Sharing Capability (UISC) Concept of Operations*[8] and the *Department of Defense Information Sharing Implementation Plan*,[9] this concept is grounded in the anticipated initial operational capability (IOC) for a common suite of UIS tools as expressed in the policy, processes and procedures, organizational culture and technology domains.

> *"Simply making enormous amounts of data and information available and introducing new technologies is not enough to ensure efficient coordination and effective decision-making. Strong management, proper resourcing, advanced training and recognized standards and policies are necessary to take full advantage of data and information for strategic analysis and operational applications."*[10]

Policies, Processes and Procedures focus on implementing current strategies, such as activities directed in the *DOD Information Sharing Implementation Plan*, toward realizing a "whole of

---

[5] Joint Staff, J8, DDC4 CCD, *Department Of Defense (DOD) Multinational And Other Mission Partners (MNMP) Information Sharing Capability (ISC) Concept of Operations*, Draft v. 1.8.

[6] Adapted from OASD/NII, *Department of Defense Information Sharing Implementation Plan*, April 2009. In "Designing an Inclusive Simulation Environment: Understanding the Landscape of Non-military Humanitarian Assistance and Disaster Relief Actors," the World Cares Center similarly refers to an "ecosystem of disaster relief." Both sources underscore a broad scope of different actors involved in HA/DR crisis situations, representing a wide range of perspectives, approaches, and goals.

[7] Appendix A, OASD/NII, *Department of Defense Information Sharing Implementation Plan*, April 2009

[8] United States Joint Chiefs of Staff, J-3, *Unclassified Information Sharing Capability (UISC) Concept of Operations*, 10 November 2010.

[9] OASD/NII, *Department of Defense Information Sharing Implementation Plan*, April 2009.

[10] Dennis King. *The Haiti Earthquake: Breaking New Ground in the Humanitarian Information Landscape*. Humanitarian Exchange Magazine, October 2010.

government" approach to information sharing. While global market forces in the commercial sector spawn frequent and significant information technology innovations, it is likely that bureaucratic policies and procedures will evolve at a much slower pace, inhibiting the realization of the full potential for information sharing in the years to come. That being said, based on validated procedures for information sharing, combatant commander and joint force commander staffs will still routinely engage with members of the extended enterprise. Standing protocols and procedure templates will foster rapid integration with non-enduring or ad hoc mission partners while standardized procedures will minimize the need for training when extended enterprise personnel transition to new missions in other global regions. A more adaptive and flexible approach to information sharing policies will enable military commanders to include the extended enterprise in their existing systems and social networks for information sharing. Commanders will also rapidly establish dynamic information sharing environments, especially in the context of social media.

> *"The chasm between military and civilian actors remains a source of serious challenges. The origins of these challenges are legion: lack of trust, lack of interoperability (technical, semantic, and willingness to work together), lack of shared information, lack of collaboration mechanisms, cultural differences (national and professional), and so forth."*[11]

> *"Successful information sharing requires a major cultural shift across the DOD. There is an established mindset of information "ownership." The new mindset must be one of information "stewardship." The best technology, processes, and policies will not make this successful if the people do not embrace the new cultural norms."*[12]

Organizational Cultures recognize the influences of organizational defense mechanisms, where habitual frictions, miscommunications, and lack of trust continue to inhibit free and open discourse. Noted Massachusetts Institute of Technology professor, Edgar Schein, defines an organization's culture as "what a group learns over a period of time as that group solves its

---

[11] Alberts, David S., Reiner K. Huber, and James Moffat. NATO NEC C2 Maturity Model, Command and Control Research Program, Jan 10

[12] *Department of Defense Information Sharing Strategy*: 4 May 2007

problems of survival in an external environment and its problems of internal integration."[13] In a stressful and ambiguous environment, an organization's culture provides its security blanket, born in "automatic patterns of perceiving, thinking, feeling, and behaving," where culture is to the group "what defense mechanisms are for the individual."[14] Comprehensive cultural engagement with members of the extended enterprise will not achieve immediate results but, over time, will help to generate a greater appreciation of others. Widely circulated among stakeholders and highlighted in professional military education and other training programs, lessons learned, guidebooks, and standard operating procedures will help to generate a shared understanding and a consensus interpretation of collective information sharing policies among extended enterprise members. By providing visibility into the range of organizational goals, objectives, and common approaches to problem solving, extended enterprise members can mitigate information sharing obstacles, especially between military and non-military actors. Reflecting their charter requirements of impartiality and neutrality, some private organizations and NGOs will still seek to avoid appearances of alignment with military or government organizations, especially when it would engender possible reprisal from local actors. That being said, working together during major HA/DR events may soften these edges and reduce organizational and cultural frictions in years to come.

> *"[The goal is] an unclassified, loosely-coupled, web-enabled software platform delivering the capability for a disparate set of participants to connect, collaborate, plan and coordinate; network socially and professionally; have situational awareness; and document the activities of multiple communities of interest and practice."*[15]

Technology includes the link, transport, network and application layers and the common suite of UIS tools that enhance the extent and timeliness of information sharing and increase the effectiveness of combatant and joint force commander staffs and other responders. These capabilities will include powerful language translation tools with sufficient fidelity and accuracy to render actionable translations across the range of languages and dialects in the joint operating environment. Participation among a wide-range of potential mission partners and other

---

[13] Schein, E. H. (1990). Organizational culture. *American Psychologist*, *45*(2), 110
[14] Ibid.
[15] *Unclassified Information Sharing Capability (UISC) Concept of Operations*, JCS J-3, 15 Nov 10, p.5.

organizations will be encouraged by intuitive interfaces and unobtrusive account access and management without imposing excessive needs for personal data. Available via the internet and across all DOD enclaves, the suite of UIS tools will be unconstrained by geographic location. While centrally funded and provisioned to ensure uninterrupted service, a de-centralized web-hosting physical location would prevent a single point of failure and facilitate continuity of operations. A distributed architecture design will mitigate service delays and loss of data from interruptions and time outs. But when disruptions do occur, effective plans, procedures, and embedded protocols will transition the extended enterprise to an alternative emergency infrastructure for collaboration. Social media (e.g., Facebook or Twitter) will be seamlessly integrated into currently available military UIS portals, greatly expanding potential sources of field data and enhancing the situational awareness of operational commanders and staffs. Enabling both synchronous and asynchronous communication frameworks, the suite of UIS tools will be rapidly scalable without losing core functionalities, such as accommodating multimedia exchanges among potential physical and virtual, extended enterprise members. Mobile device users will enjoy the same capabilities as fixed-site users through synchronization services, geographic information system integration, application support for minimal portal collaboration, and a connection interface that facilitates low-cost, widely-available devices.

3.0 Military Problem

"The challenge lies in achieving a relative unity of effort across a diverse group of contributors while preserving institutional autonomy across different organizational cultures, procedures, and languages. In order for combatant commands to better work with and engage their extended partners, they require an interoperable collaboration and information exchange capability."[16]

"Our ability to effectively solve today's problems while preparing for tomorrow's challenges will not only require us to work together within the Whole of Government, but effectively collaborate

[16] *Unclassified Information Sharing Capability (UISC) Concept of Operations*, JCS J-3, 15 Nov 10, p.1.

beyond traditional boundaries into national and international areas of expertise in an increasingly unified and collective approach. This trend necessitates multidimensional integration, smart organizations, and responsive policies which empower collaboration and knowledge sharing to operate at increasingly higher levels of performance."[17]

"The challenge of sharing within an environment of information overload is only likely to grow increasingly more difficult to manage as the globalization of distributed social networks or Web 2.0 makes our world even smaller and more interconnected."[18]

As problems of information stove-pipes and policy restrictions are addressed, fundamental military problems for UIS will likely shift to a related, but different issue. Much of the research indicates that rapid and accelerating advances in information technology and related disciplines will combine to produce overwhelming information overload. Viewed in a different perspective, perhaps our existing hierarchical processes aren't flexible enough to cope with managing the proliferation of available data, while alternative approaches, such as Wikipedia or companycommand.com have been more successful.

An Abundance of Technical Capability . . .

An examination of the past 50 years clearly reveals that any prediction of future information technologies quickly reduces to a low-probability guessing game. In the 1970s, Moore's law predicted that computer processing power would double every 18-24 months, a phenomenon that has proven to be generally true, if not a bit pessimistic. In that same decade, French economist Georges Anderla made a more telling observation regarding the rapid growth rate of knowledge—the real driver behind the need for more computing power and interpretive capabilities. He estimated that since ancient times humans had doubled their knowledge in the span of 1,500 years, doubled it again in another 250 years, doubled it once again in the ensuing 50 years, and have been continuing to double the amount of factual knowledge repetitively in

[17] Maj Gen P. K. Keen, USEUCOM Chief of Staff. Preface remarks to *Collaboration in the National Security Arena: Myths and Reality -- What Science and Experience can Contribute to its Success*, Strategic Multi-layer Assessment (SMA) Multi-agency/Multi-disciplinary White Papers in Support of Counter-Terrorism and Counter-WMD, Jun 09

[18] Ibid.

less than 10 years ever since with no indication of this acceleration slowing. In fact, in today's information revolution, human knowledge is estimated to be doubling once every 18 months.[19]

In today's environment and the near-future, our UIS way ahead may not be revealed by analyzing capability gaps, but recognizing capability opportunities. Ironically, we will likely be faced with a plethora of capabilities and technology choices that complicate and obscure any coherent modernization roadmap. We've already seen information overload inhibit our best efforts to generate a full and complete appreciation of the operating environment. Almost like the classic arms race, technological advances deliver newer and better information management capabilities while the sheer volume of user-generated information quickly rises above the ability to process it.

Not only are we challenged to harness all of this information, but moreover, how can we make sense of it? In an unpublished paper, Lt Col Soenke Marahrens, German Air Force, offers a more refined opinion, "For almost 150 years the military has been struggling to overcome the dilemma between 'never enough and always too much' information through changes like new forms of organization or by establishing new technology. Contrary to widespread opinion information overflow rarely is a problem of lower levels in the hierarchy of the armed forces. It is more likely a common problem for higher command levels. Instead, lower echelons more often suffer from the lack of information due to increasing data processing at the higher levels.[20]"

. . . and, Technology is Probably the Easiest Part

Success in tomorrow's missions will require sustained and habitual information sharing across domains with a broad range of mission partners and stakeholder participant organizations in the extended enterprise. Despite efforts to achieve this goal, DOD has been largely unsuccessful in establishing effective mechanisms for developing and nurturing essential relationships that consistently facilitate common or compatible procedures, generate consensus on business rules, and stimulate effective cooperation. As the proliferation of stakeholder organizations, both governmental and nongovernmental, continues to expand in today's fiscally challenging world economy, there is a decided tendency for organizations to grow more insular.

---

[19] Philosopher Robert Anton Wilson, extrapolates Anderla's predictions beyond 1973 in the audiobook, *Acceleration of Knowledge*.

[20] Marahrens, Soenke (n.d.). *Aspects of Military Command and Control for the 21st Century*.

"Culture, viewed as such taken-for-granted, shared, tacit ways of perceiving, thinking, and reacting, is one of the most powerful and stable forces operating in organizations."[21]

"Cultural change is critical to organizational transformation and is an organization's most difficult challenge."[22]

"The heterogeneous make-up of the enterprise implies that no single element is in charge of the entire endeavor." [23]

Like the two-faced Janus of Roman mythology, organizational culture can invoke both strengths and weaknesses. Internally, strong, organizational cultures build unit cohesion by developing relatively homogenous perceptions among members. But, outside the organization, these same common perceptions oftentimes inhibit efforts to create a shared understanding and build trust among others. Each of these aspects of organizational culture can greatly influence the effectiveness of information sharing.

A Bureaucratic Straightjacket?

An industrial age pioneer in social organizational structures, Max Weber grounded much of our understanding of bureaucratic organizations in sociology and organizational psychology.[24] According to Weber, bureaucracies exhibit a formal hierarchical structure of power and authority alongside a rationally derived and systematic division of labor. Anchored in a regulatory framework of formal and explicit procedures, bureaucratic governance consists of rule-based decisions and communications. Applied impersonally and consistently, decisions are recorded in permanent and authoritative texts, thus generating the need for effective information management technologies and processes.

---

[21] Schein, E. H. (1996). Culture: The missing concept in organizational studies. *Administrative Sciences Quarterly, 41*(2), 229.
[22] OASD/NII, *Department of Defense Information Sharing Implementation Plan*, April 2009.
[23] Alberts, David S., Reiner K. Huber, and James Moffat. NATO NEC C2 Maturity Model, Command and Control Research Program, Jan 10
[24] Weber, Max. (1968). *Economy and Society*. Roth, Guenther and Claus Wittich (Eds.). New York: Bedminister Press, 956-958.

Initially designed and later optimized for efficient and cost-effective production of industrial goods and services, some have criticized bureaucratic structures as anachronistic in the information age with today's changing focus on social networking and service provision. Moreover, bureaucracies oftentimes exhibit sub-optimization, where stove-piped sub-units pursue objectives that are not always in consonance with the larger organization's stated goals. Studies also indicate that today's bureaucratic funding and accountability mechanisms can reinforce stove-piped organizational procedures as well as tendencies toward functional insularity.[25] Military organization bureaucracies also exhibit a tendency for goal displacement, where zealous application of rules and regulations can sometimes take precedence over operational objectives.[26] When rules become ends unto themselves, it's easy for organizational members to blindly apply established procedures, sometimes in unsuitable situations, leading to counterproductive results.

Comparing failed information sharing initiatives in the context of e-government programs, several studies identify the very attributes of Weberian bureaucracy (i.e., hierarchy, division of labor, and rigidity of rules) as major impediments to progress.[27] Most note a serious gap between the rhetoric about e-government's potential for information sharing and the reality on the ground. Furthermore, in resource-constrained environments, a bureaucratic fortress mentality can inhibit open collaboration and teamwork, even while powerful information technology advances offer potentially valuable information sharing capabilities. The implication here is that in order to reform stove-piping, systems of accountability may need to be changed before benefits from information technology can be realized.[28] Leveraging information technologies to deliver services online cannot succeed without fundamental changes in the public sector's traditional structures, practices, and relationships between the state and its citizens.

---

[25] Selznik, P. (1980). TVA and the Grass Roots: A Study of Politics and Organization. Berkeley: University of California Press.
[26] Merton, R.K. (1957). *Social Theory and Social Structure*. New York: Free Press, 1957.
[27] See Jain, Aby. (2004). *Using the Lens of Max Weber's Theory of Bureaucracy to Examine E-Goverment Research*. Paper presented at 37th Hawaii International Conference on System Sciences, Marche, S., and McNiven, J. (2003). E-government and E-governance: the future isn't what it used to be," *Canadian Journal of Administrative Sciences* (20:1), 74-86, and Li, F. (2003). Implementing e-Government Strategy in Scotland: Current Situation and Emerging Issues. *Journal of Electronic Commerce in Organizations* (1:2), 44-65.
[28] Marche, S., and McNiven, J. (2003). E-government and E-governance: the future isn't what it used to be," *Canadian Journal of Administrative Sciences* (20:1), 74-86.

Mission Context in a Complex Operating Environment

Alberts, et al.,[29] describe ***complex endeavors*** as undertakings where:

- The number and diversity of participants is such that there are multiple, interdependent chains of command and the intents and priorities of the participants conflict with one another, or their components have significantly different weights, or the participants' perceptions of the situation differ in important ways.
- The effects space spans multiple domains. There is a lack of understanding of networked cause and effect relationships and a resulting inability to accurately predict relevant effects that are likely to arrive from alternative courses of action, and therefore, a lack of ability to appropriately react to undesirable effects by making timely decisions, developing appropriate plans, and taking the necessary actions.

Globalization trends and resulting geographically distributed social networks have outlined the complexity and dispersal of expertise. As the boundaries between analysts, operators, and collectors become increasingly fuzzy, no one person has the monopoly on what information is needed to get the job done. While we recognize the military's need for National-to-tactical integration, our best efforts are confounded by outdated regulatory and legal policies that impede information sharing and dissemination as well as strict organizational cultures that do not provide incentives for collaboration.

4.0 Solution

Capabilities outlined in the *Unclassified Information Sharing Capability (UISC) Concept of Operations*[30] and the *Department of Defense Information Sharing Implementation Plan*[31] describe an IOC for a common suite of UIS tools. Building on our understanding of logically derived and experimentally validated solutions, this document outlines a set of 'realm of the possible' capabilities, achievable in the next five years. The proposed UIS "success mechanism" blends aspects of technology, policy, and organizational cultures to establish a better way of realizing collective mission objectives. The next several sections offer a logical framework for

[29] Alberts, David S., Reiner K. Huber, and James Moffat. NATO NEC C2 Maturity Model, Command and Control Research Program, Jan 10.
[30] United States Joint Chiefs of Staff, J-3, *Unclassified Information Sharing Capability (UISC) Concept of Operations*, 10 November 2010.
[31] OASD/NII, *Department of Defense Information Sharing Implementation Plan*, April 2009.

describing the proposed solution focus areas as well as a rudimentary strategy for organizing actions toward achieving the UIS vision.

Capitalize on the Most Readily Available Solutions

Building on work already done by various organizations in UIS, command and control (C2) concept formation and experimentation, a suitable "low-hanging fruit" UIS development effort in the next five years should focus on refining and updating established (1) standard procedures, and (2) architectures and information exchange requirements in the HA/DR mission environment, while exploring logical extensions to other mission areas (i.e., Homeland Defense/Civil Support).

Procedures

- Refine procedures for combatant command and joint task force headquarters (JTF HQ) staffs using UIS to support mission requirements. Establish rigorous initial and continuing training mechanisms that promote and preserve individual and team skills in this critical area.
- Provide a continuous update process for quick reference guides to the roles and responsibilities of potential mission partners for the combatant commander and JTF HQ staffs using UIS to support mission requirements.
- Continue to evaluate and improve an electronically searchable, handbook-like reference document framework for combatant command and JTF HQ staffs using UIS to support mission requirements.
- Make the continuous validation of processes and procedures for the expedited release of controlled unclassified information to support mission requirements a priority for the commander and a desired learning objective for unit training.
- Expand processes and procedures for the transfer of imagery data using UIS to support mission requirements, such as current industrial standards or an interface to Google maps.
- Create incentives to promote information sharing and the rapid establishment of dynamic information sharing environments.
- Revise procedures and authorities for the handling of unclassified information to support mission requirements.

- Model the UIS procedure development and revision process for application in mission areas beyond HA/DR operations, such as Homeland Defense/Civil Support.[32]

Architectures and Information Exchange Requirements

- Define touch points or interactions (e.g., Twitter, Facebook, UIS portals, Adobe Connect Online) with the extended enterprise of mission partners and stakeholder participant organizations and test the utility beyond HA/DR mission environments through experimentation and analysis of real-world operations.
- Continue to refine a common lexicon and ontology in support of the UIS information management scheme, using commonly available (e.g., extensible markup language also referred to as XML) frameworks.
- Continue to refine the recommendations of partnerships and/or legal relationships between government and private sector companies with respect to information management schemes that could be applied to UIS.
- Describe the unclassified information flow between the JTF HQ, subordinate Civil-Military Operations Centers, and other tactical forces (e.g., provincial reconstruction teams) in support of missions beyond HA/DR operations.
- Continue UIS modernization aligned with National Information Exchange Model information exchange standards and processes.
- Update and refine combatant command and JTF HQ staff unclassified information exchange requirements supporting HA/DR operations, with logical extension to other mission areas, such as Homeland Defense/Civil Support.
- Develop pre-planned templates of recurring information sharing requirements using UIS to support combatant command and JTF HQ staff HA/DR mission requirements.
- Train combatant command and JTF HQ staff personnel for HA/DR mission with the use of existing governmental/non-governmental tools and applications.
- Explore pre-planned templates of recurring information sharing requirements using UIS to support combatant command, JTF HQ staff, and other partners[33] in Homeland Defense/Civil Support mission areas.

---

[32] Consider the UIS approach for baselining information sharing processes and procedures developed among the National Military Command Center, Global Situational Awareness Facility, Department of Homeland Security National Operations Center, NGB Joint Coordination Center, and the NORAD and USNORTHCOM Command Center.

Make Agility the Defining Characteristic of UIS

> *"Agility is the synergistic combination of robustness, resilience, responsiveness, flexibility, innovation, and adaptation. Agile organizations can recognize the dynamic nature of the situation and apply the appropriate C2 approach."*[34]

> *"C2 maturity changes over time, so applications may need to be segmented in order to focus on coherent patterns. These changes appear to be related primarily to changes in the mission. For example, crisis response and reconstruction levy different requirements and may develop very different command and control capacities and practices. Moreover, C2 maturity may change as a result of the introduction of new entities or the loss of entities in the endeavor."*[35]

Building on the existing conceptual constructs and experimentation efforts for UIS and C2, a more challenging UIS development effort in the next five years should focus on agility, tailoring and adapting the UIS in the context of, (1) dynamic mission requirements and (2) accelerating evolution of information sharing capabilities in the public domain.

Dynamic mission requirements

- Develop rapid and effective mechanisms for identifying the "five W's" (i.e., who, what, where, when, why) of mission partners to improve combatant command and JTF HQ staffs' knowledge, skills, and abilities to understand the roles, responsibilities, limitations, authorities, potential contributions, and information exchange requirements in dynamic mission environments.

---

[33] Consider organizations and initiatives such as the Federal Information Sharing Environment (ISE), Maritime Security, Aviation Security, the National Command and Coordination Capability (NCCC), the Joint Continental U.S. Communications Support Environment (JCCSE), and the Next Generation Air Transportation System (NextGen).

[34] Alberts, David S., Reiner K. Huber, and James Moffat. NATO NEC C2 Maturity Model, Command and Control Research Program, Jan 10

[35] Ibid.

- Deliver tailored UIS capabilities across all phases of an operation, focusing on essential shaping (Phase 0) activities that assure or solidify relationships with friends and allies in order to build information sharing relationships for potential missions.
- Test and evaluate whether the extant UIS has the capability and capacity to support combatant command and JTF HQ staffs in the conduct of operations beyond the HA/DR mission environment.
- Identify and evaluate whether necessary UIS tools are available on appropriate networks to support staff planning and execution beyond the HA/DR mission environment.
- Refine and update criteria and procedures for the rapid establishment of new UIS worksites to support combatant command and JTF HQ staff mission operations.
- Refine and update processes and procedures for posting communications in the UIS environment that provide better transparency and COI awareness and reduce duplicative communications.
- Refine and update authorities and procedures that enable collaboration among the combatant command staff, interagency, IGO, or NGO counterparts.
- Define, test and evaluate the potential UIS capabilities and skills required by a JTF to conduct operations.
- Develop rapid and effective mechanisms that tailor the UIS environment to meet mission requirements across the spectrum of contingency environments.

Evolution of public domain capabilities and frameworks

- Align federated search UIS search capabilities with information sharing modernization efforts in the public sector.
- Enhance/develop graduated user account permissions and methodologies (streamlining subscriber access administration procedures) for anticipated and unanticipated users to facilitate allocating access to different levels of information based on trust.
- Expand UIS capabilities to provide updates to mission partners and capture data through dynamic sources (e.g., social media, hotlines, news).
- Expand UIS capabilities to access and integrate information in the public domain, such as social media.
- Integrate portal capabilities on the UIS that are interoperable across the broadest pool of mission partners.
- Align UIS capabilities to accommodate user access via smart phone applications as they continue to modernize and improve capabilities.
- Align UIS capabilities to access, gather, process, and analyze information as public domain capabilities and frameworks, such as social media, continue to improve and modernize.

- Align UIS capabilities to leverage modernization and improvements to commercial off-the-shelf or government off-the-shelf products which support a user-defined operating picture.

Make the Public Domain the Defining Environment for UIS

"Hierarchical organizational structures often reinforce formalized, hierarchical information sharing over emerging ones. . . . Today's globally connected world is holding such traditional hierarchical cultures hostage through rapidly evolving technology."[36]

Although lacking clear definition and consensus among organizational researchers, one approach suggests that information age technologies influence an evolution toward post-bureaucratic organizational (PBO) structures.[37] This new social paradigm is already characterized by a reduction of formal levels of hierarchy, emphasizing flexible and context-tailored decision making over rule-following. Key actors are determined more by capability, knowledge and expertise appropriate to the task at hand rather than a hierarchical office holder. Time structures for the PBOs are built on the expectation of constant change or transformation as opposed to predictable bureaucratic time cycles, such as annual budgets. An atmosphere of trust and interdependence among organizational actors is grounded in shared mission defining values as well as more ephemeral 'marriages of convenience' occurring among unlikely partners, creating a more permeable boundary between the inside and outside of organizations as well. In this organizational environment, rapid and effective information sharing among stakeholders eclipses rule-based bureaucratic information notification as the dominant mechanism for collective mission accomplishment.

---

[36] Maj Gen P. K. Keen, USEUCOM Chief of Staff. Preface remarks to *Collaboration in the National Security Arena: Myths and Reality -- What Science and Experience can Contribute to its Success*, Strategic Multi-layer Assessment (SMA) Multi-agency/Multi-disciplinary White Papers in Support of Counter-Terrorism and Counter-WMD, Jun 09

[37] See Grey, C. and Garsten, C. (2000). Trust, Control and Post-Bureaucracy. *Organization Studies*, 22(1), 229-250. and Heckscher, C. (1994). Defining the Post-Bureaucratic Type. In *The Post-Bureaucratic Organization*, Charles Heckscher and Anne Donnellon (Eds.). Thousand Oaks, CA: Sage, 14-62.

Recognizing that unstructured frameworks are the norm for most information sharing, data specifications, and organizational designs in the public domain, the most challenging UIS development approach for the next five years would focus efforts on, (1) finding ways to adapt hierarchical/structured frameworks to function with decentralized/ad hoc frameworks into a coherent whole and (2) finding ways to access, gather, process, and analyze unstructured public domain data.

Blending structured/unstructured frameworks

- Continue to develop and test methodologies/processes to improve information sharing between DOD and mission partner hierarchical, decentralized or ad hoc unclassified information exchange structures.
- Continue to develop, and evaluate through experimentation, information sharing processes and procedures to include mission partners in existing DOD systems.
- Continue to develop, and evaluate through experimentation and training, information sharing cultures, processes and procedures to access mission partners systems.

Harnessing unstructured public domain data

- Explore whether military common data standards and protocols and tailored metadata will mitigate needless duplication of information, inefficient searches, lapses in event coordination, poor presentation of information to target audiences and remedy general information overload in the public domain for information sharing.
- Explore whether and how unstructured data and metadata can accommodate cross-domain transfers and whether business rules emulating guard functionalities can suitably deal with unstructured data.
- Explore how the management of metadata and access control can adequately protect data from being forwarded to undesirable third parties in the public sector domain.
- Test and evaluate the effectiveness of tools to identify knowledgeable users and sort, prioritize, and highlight unstructured data content.

Effective Decision-Making Mechanisms for UIS Development and Modernization

"One cannot and should not think about optimizing command and control in the 21st century. There is no single approach, no best system design or configuration, no best process for all situations and circumstances. Uncertainty in the mission space and complexity in the environment, the effects space, and the complexity inherent in a collective dominate. Since there are both

benefits and costs associated with operating a given C2 approach, there will not be a one-size-fits-all solution."[38]

"Case studies of several real-world contingency operations indicate that collective participants tend to seek only the minimum threshold of interactions rather than pay the price in time, energy, and resources needed for higher levels of cooperation and integration."[39]

Like most endeavors, UIS is situated in a framework of choices like the risk and reward calculation of information sharing versus operational security. A viable UIS development effort in the next five years would focus on similar cost-benefit and feasibility analyses of, (1) stakeholder participation and (2) the limits of technology in supporting information sharing in the public domain. Each of these continuous analyses should focus on identifying threshold capabilities in order to refine and validate UIS implementation requirements.

Stakeholder participation

- Conduct a cost-benefit analysis of the value of UIS capabilities.
- Conduct a cost-benefit analysis of providing information sharing services to participants with minimal technological resources (e.g., high frequency radio, mobile phone) and disconnected, intermittent, or low-bandwidth services.
- Conduct a cost-benefit analysis of UIS capabilities to make automatic recommendations in a restricted communications environment and gracefully degrade from high to low-bandwidth.
- Conduct a cost-benefit analysis of UIS capabilities to exchange information with disconnected intermittent low-bandwidth users.
- Conduct a cost-benefit analysis of UIS capabilities for short message service (SMS) coding of 911-type short codes and processing of information.
- Conduct a cost-benefit analysis of compression utilities and their effect on UIS.

[38] Alberts, David S., Reiner K. Huber, and James Moffat. NATO NEC C2 Maturity Model, Command and Control Research Program, Jan 10

[39] Ibid.

Limits of technology

- Conduct a feasibility analysis of automatic trust center capabilities in the UIS environment, focused on whether characterizations of trust among mission partners can provide sufficient validity and value in the operational context.
- Conduct a feasibility analysis of source authenticity and information reliability tools in the UIS environment for filtering and verification of real-time data from channels such as Twitter, SMS, email and really simple syndication, commonly referred to as RSS, feeds.
- Conduct a feasibility analysis of procedures and tools to enforce data standards and adherence to protocols on the UIS given the prevalence of unstructured data in the public domain.

5.0 Risks and Mitigations

Significant obstacles and risks will certainly complicate moving forward with the DOD UIS Enterprise. Some are a result of the current U.S. economic outlook, including anticipated reductions in the defense budget. Other obstacles may eclipse national economic concerns, such as today's clear and present dangers involving global information security. The approach to the DOD UIS Enterprise will be informed by some of these risks, but the challenges can be mitigated to some degree as well. For example:

The UIS approach will depend on a baseline, technical commonality (e.g., computer or other web-enabled device with access to the internet, such as desktop/laptop computers, netbooks, personal digital assistants, cell phones and smart phones) among the potential stakeholders/participants. As the technologies advance and capabilities increase, the extended enterprise risks leaving members behind.

- Mitigation: Since the private sector has habitually led modernization efforts for information technology, consider letting the marketplace define the set-point for extended enterprise members' collective capabilities.

The need for confidentiality when working with some governmental organizations has inhibited many NGOs from joining DOD-hosted collaboration portals.

- Mitigation: Consider an external/neutral forum to accommodate stakeholder participant organization interactions, using best practices from the economic, academic, and business communities.

Stakeholder participant organizations represent a wide variety of policies and procedures that govern participation, information sharing, and approach.

- Mitigation: Identify, categorize, and accept organizational policy, process and procedure differences with an eye toward discovering and correlating policy touch points among organizations that may improve information sharing.

Increasing global concerns for cyber security may impede further development of national policies and coordination strategies encouraging information sharing through the open internet.

- Mitigation: The DOD UIS Enterprise design and execution must fully align with national cyber network security measures, both hardware and policy related.

6.0 Implications

"The ability to share information within and among participating entities must be accompanied by changes in information sharing behaviors and policies including a move from decisions to share based on 'need to know' to information-sharing decisions based on an understanding of the 'need to share.' The resulting increases in information sharing will improve the quality and accessibility of available information which will, in turn, improve entity awareness and shared awareness."[40]

"The desired capability is simply to enable COCOMs and their respective real and virtual communities to share information, with whom, where, when, and as often as necessary, to better achieve mission success."[41]

The CCJO envisions a complex, future, operating environment, where military forces will rarely succeed alone, but instead, will operate in conjunction with other agencies of the U.S. and partner governments. The success of the endeavor will depend on the success of that partnership. The Defense Security Cooperation Agency manages HA/DR programs through the geographic combatant commands. These efforts are carried out by a wide range of organizations that include, but are not limited to, U.S. agencies, foreign militaries, foreign governments, NGOs, private voluntary organizations (PVO), industry partners, and academia.[42]

---

[40] Ibid.
[41] USSOUTHCOM, *Transformational Information-Sharing Cooperation (TISC) Concept of Operations*, 10 Jun 10
[42] *Capstone Concept for Joint Operations*, Version 3.0, 15 Jan 09.

As expressed in the *DOD Information Sharing Strategy*, the benefits of viable information sharing capabilities include: (1) achieving unity of effort across mission and coalition operations; (2) improving the speed and execution of decisions; (3) achieving rapid adaptability across mission and coalition operations; and (4) improving the ability to anticipate events and resource needs, providing an initial situational advantage, and setting the conditions for success.

This discussion of UIS is fundamentally about change. Aligning and balancing aspects of technology, policy, processes, procedures, and organizational culture will certainly be the biggest challenge. The past few years have shown us that technological change is relatively easy given the proliferation of technology-centric projects, programs, and initiatives funded by the U.S. Government and other members of the extended enterprise. Compared with technology, the policy, process and procedural changes are much more difficult and resultantly slower.

Even with catastrophic catalyst events, such as war, efforts to re-engineer large bureaucratic organizations have been mired in red tape, process inefficiencies, and stout resistance. In comparison with both technology and policy, organizational cultures change at a geological pace. Cultures tend to reproduce over time, with change largely relegated to minor, cosmetic adjustments. It also takes significant commitment by leadership, especially when confronted with inevitable resistance. That being said, the future does hold potential to form meaningful COIs from various organizational cultures, where UIS capabilities enable extended enterprise members to willingly participate, share resources, and tailor policies, processes and procedures to address the imperatives of working together toward compatible goals.

Appendix – References

Alberts, David S., John J. Garstka, Richard E. Hayes, and David T. Signori. *Understanding Information Age Warfare*. Washington, DC: CCRP, 2001.

Alberts, David S., Reiner K. Huber, and James Moffat. *NATO Network Enabled Capability (NEC) Command and Control (C2) Maturity Model*, Command and Control Research Program, Jan 2010.

ASD (NII)/DOD CIO, *Department of Defense Information Sharing Implementation Plan*, April 2009.

ASD (NII)/DOD CIO, *Department of Defense Information Sharing Strategy*, 04 May 2007.

ASD (NII)/DOD CIO, DODI 8110.01, *Multinational and Other Mission Partner (MNMP) Information-Sharing Capability Framework*, 9 Jun 2010.

Chairman Joint Chiefs of Staff Instruction (CJCSI) 6285.01B, *Multinational Information Sharing (MNIS) Operational Systems Requirements Management Process*, 13 Sep 2010.

Chairman of the Joint Chiefs of Staff Instruction 6285.01A, *Multinational Information Sharing Operational Requirements Management*, 16 May 2008.

Collaboration in the National Security Arena: *Myths and Reality -- What Science and Experience can Contribute to its Success, Strategic Multi-layer Assessment (SMA) Multi-agency/Multi-disciplinary White Papers in Support of Counter-Terrorism and Counter-WMD*, Jun 09.

Dennis King. The Haiti Earthquake: Breaking New Ground in the Humanitarian Information Landscape. Humanitarian Exchange Magazine, October 2010.

DOD Instruction 8220.02, *Information and Communications Technology (ICT) Capability for Support of Stabilization and Reconstruction, Disaster Relief, and Humanitarian and Civic Assistance Operations*, 30 Apr 2009.

Grey, C. and Garsten, C. (2000). Trust, Control and Post-Bureaucracy. *Organization Studies*, 22(1), 229-250.

Heckscher, C. (1994). Defining the Post-Bureaucratic Type. In *The Post-Bureaucratic Organization*, Charles Heckscher and Anne Donnellon (Eds.). Thousand Oaks, CA: Sage, 14-62.

Jain, Aby. (2004). *Using the Lens of Max Weber's Theory of Bureaucracy to Examine E-Government Research*. Paper presented at 37th Hawaii International Conference on System Sciences.

Joint Staff, *Unclassified Information Sharing Capability (UISC) CONOPS*, 15 November 2010.

Joint Staff, J8, DDC4 CCD, *Department Of Defense (DoD) Multinational And Other Mission Partners (MNMP) Information Sharing Capability (ISC) Concept of Operations*, Draft v. 1.8.

JP 1-02, *DOD Dictionary of Military and Associated Terms*, 12 April 2001, (as amended through 15 May 2011).

Kiernan, Kathleen, and Carl Hunt. *The Law Enforcement Perspective in US Interagency Collaboration: Leveraging the Whole of Government Approach*, in Collaboration in the National Security Arena: Myths and Reality -- What Science and Experience can Contribute to its Success, Strategic Multi-layer Assessment (SMA) Multi-agency/Multi-disciplinary White Papers in Support of Counter-Terrorism and Counter-WMD, Jun 09.

Maj Gen P. K. Keen, USEUCOM Chief of Staff. Preface remarks to *Collaboration in the National Security Arena: Myths and Reality -- What Science and Experience can Contribute to its Success*, Strategic Multi-layer Assessment (SMA) Multi-agency/Multi-disciplinary White Papers in Support of Counter-Terrorism and Counter-WMD, Jun 09.

Li, F. (2003). Implementing e-Government Strategy in Scotland: Current Situation and Emerging Issues. *Journal of Electronic Commerce in Organizations* (1:2), 44-65.

Lt Col Marahrens, Soenke (n.d.). *Aspects of Military Command and Control for the 21st Century*.

Marche, S., and McNiven, J. (2003). E-government and E-governance: the future isn't what it used to be," *Canadian Journal of Administrative Sciences* (20:1), 74-86.

Merton, R.K. (1957). *Social Theory and Social Structure*. New York: Free Press, 1957.

Schein, E. H. (1990). Organizational culture. *American Psychologist*, *45*(2), 110.

Schein, E. H. (1996). Culture: The missing concept in organizational studies. *Administrative Sciences Quarterly*, *41*(2), 229.

Schmitt, John F., *A Practical Guide for Developing and Writing Military Concepts. Defense Analysis Red Team (DART)*, Dec 2002.

Secretary of Defense Report, *Quadrennial Defense Review Report*, Feb 2010.

Selznik, P. (1980). TVA and the Grass Roots: A Study of Politics and Organization. Berkeley: University of California Press.

USJFCOM, *Multinational Information Sharing (MNIS) Initial Capabilities Document (ICD) Version v1.0*, 18 September 2006.

USJFCOM, *Multinational and other Mission Partners (MNMP) C2 Information Sharing Capability Definition Package*, 12 October 2010.

USPACOM, *Asia Pacific Area Network (APAN) CONOPS*, June 2009.

USSOUTHCOM, *Transformational Information-Sharing Cooperation (TISC) Concept of Operations*, 10 Jun 10.

Warfighter Challenges FY09 inputs for Joint Interagency and Multi-National Interoperability.

Weber, Max. (1968). *Economy and Society*. Roth, Guenther and Claus Wittich (Eds.). New York: Bedminister Press, 956-958.

World Cares Center (2010). Designing an Inclusive Simulation Environment: Understanding the Landscape of Non-military Humanitarian Assistance and Disaster Relief Actors. New York, NY.