



DoD CIO Interoperability Process

30 Apr 2012

Ed Zick
DoD CIO
edward.zick@osd.mil
(571) 372-4680

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 30 APR 2012	2. REPORT TYPE	3. DATES COVERED 00-00-2012 to 00-00-2012			
4. TITLE AND SUBTITLE DoD CIO Interoperability Process		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) Department of Defense Chief Information Officer (DoD CIO), Washington, DC, 20301		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 Presented at the 2012 DoD Enterprise Architecture, Miami, FL, April 30 - May 3, 2012					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 15	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



Purpose

The purpose of this brief is to:

- Describe the Enhanced Information Support Plan (EISP) Enterprise Service Version (ESV), a module within the GIG Technical Guidance Federation (GTG-F)
- Describe the benefits users experience when using the GTG-F to create and submit ISPs for review and approval
- Explain how the DoD CIO utilizes the EISP to collect and analyze information to assess interoperability compliance



The DoD CIO has released Interim Guidance for Interoperability and prescribed use of the GTG-F

Interim Guidance for the Interoperability of Information Technology (IT) and National Security Systems (NSS) was signed 27 March 2012

https://www.intelink.gov/wiki/Portal:GIG_Technical_Guidance


Unclassified ISPs shall be created, submitted, and approved using the **GIG Technical Guidance Federation (GTG-F)**

The GTG-F is available for use: <https://gtg.csd.disa.mil>

- Common Access Card (CAC) authentication is required to access the GTG-F

GTG Federation Processes for ISP Development and Assessment of IT and NSS:

- Wednesday, Track 1, 1615 – 1700
- Demonstration of the GTG-F, including an overview of the EISP, GTP, and IAM



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

MAR 27 2012


MEMORANDUM FOR: SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARY OF DEFENSE FOR ACQUISITION,
TECHNOLOGY, AND LOGISTICS
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
CHIEF INFORMATION OFFICERS, MILITARY DEPARTMENTS

SUBJECT: Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS)

Reference: "Memorandum of Understanding Between the Joint Staff J8 Directorate and the Department of Defense Chief Information Officer for Transfer of Functions and Associated Resources," August 26, 2011

Reference transferred specific functions from the Joint Staff (J8) to the DoD CIO to include responsibilities for interoperability of IT and NSS previously performed by the Joint Staff (J6). The purpose of this memorandum is to provide interim guidance for the review and approval of Information Support Plans (ISPs), and interoperability certification of IT and NSS. This interim guidance memorandum does not alter existing DoD authorities or command relationships.

The DoD CIO point of contact for this action is Mr. Kris Strance, kris.strance@osd.mil, 571-372-4670.


Teresa M. Takai

Attachment:
Interim Guidance for Interoperability of IT and NSS



The DoD CIO, in partnership with DISA, has developed and instituted the GTG-F to create a more efficient and effective Interoperability assessment process

Program Management Portal 1.3.1 UNCLASSIFIED

PM-P Home IAM Home GTPs DISR Admin Search My Settings Support Logout

Welcome Mr. Rich | Last log in 04 Apr 2012

Filter by Program Title

Page 1 of 6 (93 items) First Prev 1 2 3 4 5 6 7 8 Next Last

			Actions
Acquisition Document Development and Management	Type: Information Support Plan, Classification: UNCLASS ACAT Level: Non-ACAT, MS: EISP v2.3, Stage: Updated	Status: Version 1 Not Submitted POC: Michael Hucul	View Full Profile Access EISP Wizard Access GTP Wizard
Advanced Computer Flight Plan v4.5 (Overlay)		Status: Version 1 Not Submitted POC: Robert Ford	View Full Profile Access EISP Wizard Access GTP Wizard
AETC Decision Support System	Type: Information Support Plan, Classification: UNCLASS/FOUO ACAT Level: ACAT III, MS: MS C, Stage: Revised	Status: Version 1 Not Submitted POC: Richard Jernigan	View Full Profile Access EISP Wizard Access GTP Wizard
Agile transportation for the 21st Century		Status: Version 1 Not Submitted POC: Howard Snare	View Full Profile Access EISP Wizard Access GTP Wizard
Air Force Fitness Management System II	Type: Information Support Plan, Classification: UNCLASS ACAT Level: ACAT III, MS: MS B, Stage: Initial	Status: Version 1 Not Submitted POC: Thomas Talcott	View Full Profile Access EISP Wizard Access GTP Wizard
Air Force Medical Systems Information Test Bed		Status: Version 1 Not Submitted POC: Paul Agosta	View Full Profile Access EISP Wizard Access GTP Wizard

Legend: Read Write Owner

EISP - The Enhanced Information Support Plan (ISP) provides step by step guidance on creating an ISP. The EISP guides ISP developers through an analysis of their architecture data to identify critical information risks and issues within their program.

GTP - The Global Information Grid (GIG) Technical Profiles (GTP) module provides simple wizard to create a Standards View for an ISP, CDD/CPD, and Other artifacts.

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

- The GTG-F is hosted on the DISA DECC, driven by the Enhanced Information Support Plan (EISP), enabling compliance with the DoD Information Enterprise Architecture (DIEA), GTPs, and DoD IT Standards Registry (DISR) IT standards.
- The data captured within the EISP and GTP module is pushed to the Interoperability Assessment Module (IAM) which provides a streamlined staffing, review, and commenting process for Interoperability data.
- The GTG-F incorporates benefits of cloud computing, allowing users:
 - Access to the Federation from “anywhere” while protecting programmatic data via PKI CAC authentication
 - To collaborate with other GTG-F users on a single program
 - The ability to share information via Web Service

There are **over 140 active programs in the GTG-F** (as of 27 April 2012)



The GTG-F provides PMs with a data-centric interoperability and compliance analysis process

- Guides PMs to better identify interoperability risks, issues, and develop mitigation plans through the use of online templates, business rules, and data validation capabilities
- Automates some architecture imports from tools or repositories reducing duplication of effort and provides visibility into information needs, dependencies, and interface requirements, focusing on interoperability and integration
- Eliminates the need to manually produce a document for submission as the data entered into the process is automatically formatted for review
- Implements an online review process allowing PMs and reviewers real-time adjudication of comments made directly on the data thus reducing administrative and duplicative comments
- Automatic triggers ensure information risks are identified, standards are current, and other mandatory compliance areas are assessed
- Provides the DoD an efficient, data-centric process for collecting and standardizing interoperability information while providing a single repository through which the DoD can perform analysis and increase decision speed

Stryker Brigade Combat Team realized a 30-40% cost savings in development of their ISP via this data-centric process

Joint Staff ISP reviewers said EISP generated ISPs are more thoroughly written and do not lack required detail as often as legacy ISPs

OSD(Health Affairs)/TRICARE Management Activity is saving time and effort by reusing data from Version 2.0 by utilizing the XML import capability within the EISP ESV



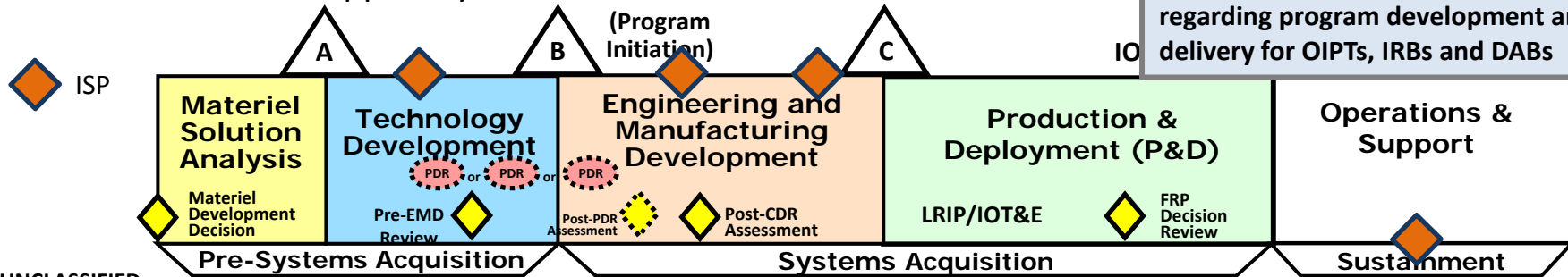
The EISP enables interoperability and compliance risk assessment within the acquisition process

- The EISP is the DoD CIO's **primary source** to collect and analyze information to ensure interoperability and compliance in these areas:
 - Integrated Architecture
 - DoD Information Enterprise Architecture
 - Standards
 - Net-Centric Strategy
 - Information Assurance
 - Web Services
 - Secure Information Exchanges

- Interoperability and compliance risk assessment provides the DoD CIO a **methodology to assess compliance** in the DoD Decision Support System

This data is being used as part of the DoD CIO's Technical Assessment on the IT Dashboard

Also, this data is being used to develop the DoD CIO position regarding program development and delivery for OIPTs, IRBs and DABs





Integrated Architecture

- The EISP Process Analysis section uses a program's architecture data to perform analysis that drives a PM to identify risks and issues within their program
- The EISP captures program architecture data across the Enterprise, in a standard format, to allow for the sharing and reuse of ISP information as well as for cross-program and Portfolio-level analysis

EISP ONLINE Release 1.3.1 Build 02 #417
ENHANCED INFORMATION SUPPORT PLAN

Navigation: EISP Home | PM-P Home | Admin | Program Info | Program Data | Overview | Analysis | Appendices | Supporting Docs | Feedback? | Logout

Welcome Mr. Rich

Caution: Currently, the EISP ESV will time out without warning users and any unsaved information will be lost. Users should save often to avoid timing out and prevent data loss. An automated warning capability is being developed for a future release.

Process Analysis

Time Phases | Performers | Systems | JCAs | Activities | Information Needs | System Implementations | Risks & Issues

Process Analysis Tree Elements | **Edit Performer**

This listing shows only the elements pertaining to the current time phase. To change the time phase, click on the "Time Phase" link below.

- Time Phase
- AH-1Z IOC
- Performers (Operational Nodes)
- Systems (System Nodes)
- Joint Capability Areas (JCAs)
- Activities (Operational Activities)
- Information Needs
- System Implementations
- Risks and Issues
- Supporting Documentation

Click here to view the complete tree.

[View the Tree](#) | [Import AV2](#)

Please enter the following information for the node. Please note, * indicates a required field.

*Performer Name: USMC Light/Attack Helicopter

*Performer Number: 1

*Internal/External: Internal

Description: Provides offensive air support, utility support, armed escort and airborne supporting arms coordination during naval expeditionary operations or joint and combined operations.

Performer Type: Marines

NOTE: All classified graphics must be appropriately labeled before they can be included in the template.

[ISP/TISP Product Matrix](#)

Figure Number	Graphics	Graphic Titles	Caption	Architecture Product	Preview	Action
1	null	AH-1Z Operational Node Connectivity Diagram		OV-2		Edit Delete

[Add Graphic](#)

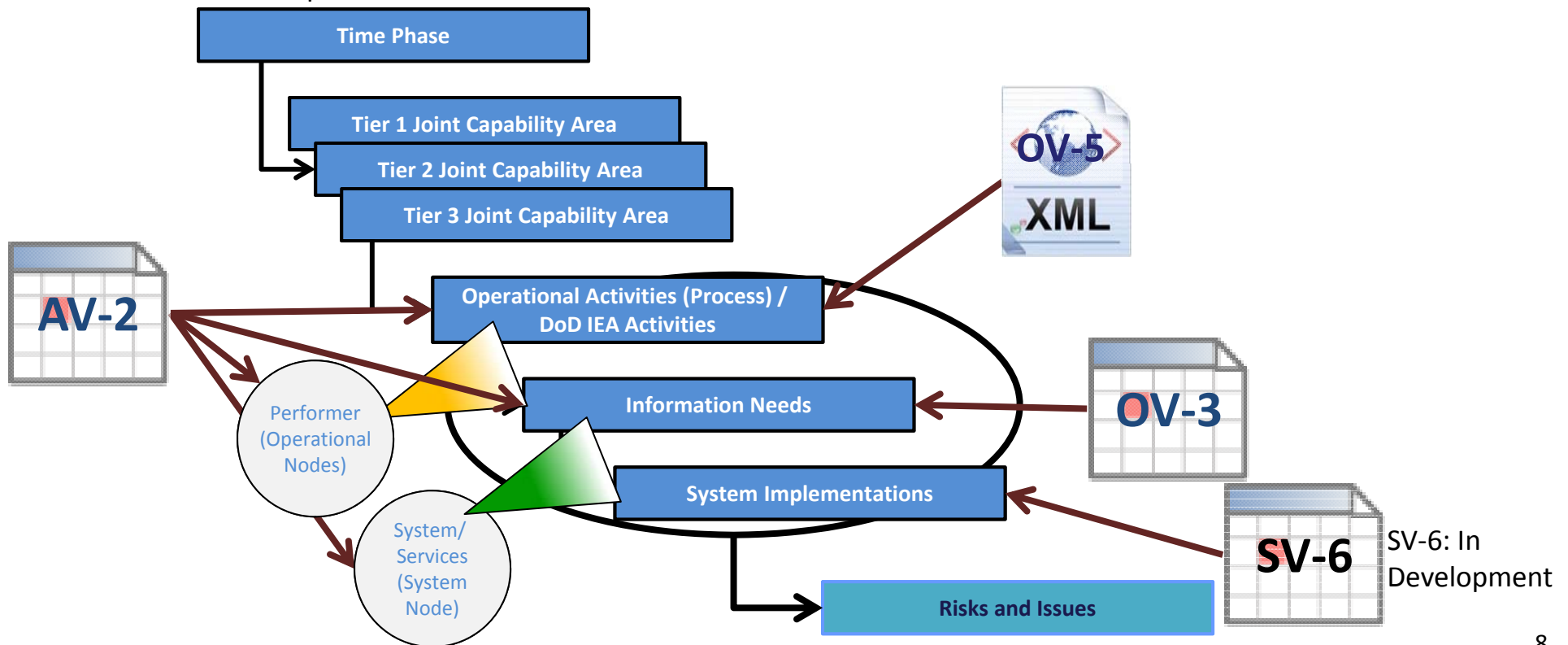
Operations
[Modify](#) [Delete](#)

DoD Architecture Framework (DoDAF)
<http://dodcio.defense.gov/dodaf20.aspx>



The EISP ESV allows users to import data into the Process Analysis section to reduce the burden on ISP developers and to assist in the DoD CIO's risk and issue analysis

- In the Process Analysis section, the ISP developer is asked to enter their detailed warfighter or business process related data
 - The EISP ESV contains the ability to automatically import pieces of required data directly into the Process Analysis section, reducing the amount of manual data entry
 - The information collected by the DoD CIO drives PMs to identify risks and issues that, if not properly managed, will limit or restrict the ability of a program to be operationally employed in accordance with requirements.





DoD Information Enterprise Architecture

- The EISP collects the data elements required by the DoD IEA and allows users to tailor the DoD IEA Activity model to their specific program
- The EISP automatically generates the DoD IEA Compliance Assessment Table from the data entered in the process
- DoD IEA V2.0 requirements are being researched and generated for a future EISP release

EISP ONLINE Release 1.3.1 Build 02 #417
ENHANCED INFORMATION SUPPORT PLAN

EISP Home PM-P Home Admin Program Info Program Data Overview Analysis Appendices Supporting Docs Feedback? Logout

Welcome Mr. Rich

Caution: Currently, the EISP ESV will time out without warning users and any unsaved information will be lost. Users should save often to avoid timing out and prevent data loss. An automated warning capability is being developed for a future release.

Analysis

Process Analysis DoD IEA NR-KPP Statement CPM Information Assurance Strategy Status

Overview DIEA Analysis DIEA Net-Centric Architectural Descriptions

Other Information Needs and Additional Operational Risks Radio Frequency Spectrum Needs Status Miscellaneous Analysis Supporting Documentation

DoD IEA Overview

To complete this section, refer to the DoD Information Enterprise Architecture Guidance for the EISP, available [here](#).

Perspectives
Select one or more of the perspectives of the DoD Information Enterprise (IE) relevant to the program.
* At least one perspective is required.

Production/Provision Management/Operational Consumption/Use

Where in the architecture description are the perspectives discussed?
Text:
Describe the net-centric assumptions contained in the AV-1.
Text:
Designate where in the architecture description are applicable DoD IEA Activities addressed. For each option selected, state exactly where in the Activity or Process Model the DoD IEA Activity has been incorporated.

Activity

Activity Model

Activity Model Decomposes DoD IEA Activities DoD IEA Activities Added Directly to Activity Model

DoD IEA Activities Incorporated into Activity Definitions Other

Process

DoD Information Enterprise Architecture (DoD IEA) Version 1.2
<http://dodcio.defense.gov/Home/Initiatives/DIEA.aspx>



Standards

- The GTG-F GIG Technical Profiles Wiki is located at: https://www.intelink.gov/wiki/Portal:GIG_Technical_Guidance/GTG_GTPs

GIG TECHNICAL PROFILES
1.3.1.04

PM-P Home GTPs DISR Home Admin Search My Settings Support Logout

Welcome, Brian Rich (DoD CIO)

AH-1Z DEMO

Step 1: Questionnaire Step 2: GTPs Step 3: Declaration Step 4: Standards Step 5: Review & Finish

GTPs List GTPs Tree

Below is a list of GTPs identified by answers to the Questionnaire. You may examine each GTP or begin responding to the guidance statements and standards within each GTP in the Declaration and Standards View.

GTP Title	Version #	Status	Version Date	Reference ID	DIEA Area
Internet Protocol - Core IPv6	1.0.0	Final	Jan 15, 2010	GTP-0001.0006	Communications

Previous Next

GIG Technical Profiles (GTP) Module
<https://gtg.csd.disa.mil>



Net-Centric Data Strategy

- The EISP collects information to analyze and assess a program's compliance with the Net-Centric Data Strategy through the collection of Data Sharing Characteristics:

- DDMS
- MDR Registered
- Web Service
- NCES Registered
- Discoverable
- IPv6 Capable
- Tagged

EISP ONLINE Release 1.3.1 Build 02 #417
ENHANCED INFORMATION SUPPORT PLAN

EISP Home PM-P Home Admin Program Info Program Data Overview Analysis Appendices Supporting Docs Feedback? Logout

Welcome Mr. Rich

Caution: Currently, the EISP ESV will time out without warning users and any unsaved information will be lost. Users should save often to avoid timing out and prevent data loss. An automated warning capability is being developed for a future release.

Process Analysis

Time Phases > Performers > Systems > JCAs > Activities > Information Needs > System Implementations > Risks & Issues

Process Analysis Tree Elements **Go/No Go Message System Implementation**

This listing shows only the elements pertaining to the current time phase. To change the time phase, click on the "Time Phase" link below.

- Time Phase
 - AH-1Z IOC
- Performers (Operational Nodes)
- Systems (System Nodes)
- Joint Capability Areas (JCAs)
- Activities (Operational Activities)
- Information Needs
- System Implementations
 - Go/No Go Message System Implementation
 - Request for Information/Intelligence Update System Implementation
 - Aircraft Status System Implementation
 - Airspace Control Message System Implementation
 - Airspace Control Message System Implementation
 - Navigation Information System Implementation
 - IFF Interrogation System Implementation

Enter the following regarding the System Implementations required to complete the activities that have been identified in this section.

System Implementation Name: Go/No Go Message System Implementati

Information Need Source(s): USMC Light/Attack

System Implementation Source(s): Show/Hide All

Information Need Consumer(s): Unit Level Aircraft Maintenance

System Implementation Consumer(s): Show/Hide All

Transport Methodology: IP-Routed Data/Web Service/VOIP ?

Uses DISN Uses Wireless Capability

By selecting IP-Routed Data/Web Service/VOIP as the Transport Methodology, we require users to select their Data Sharing Characteristics. If the exchange is exposing Data (to include VOIP), the user must indicate DDMS compliance and whether the exchange is Discoverable by a Federated Search. If the exchange is exposing a Service, the user must select Web Service and indicate whether it is MDR and NCES registered. For all exchanges, the user must indicate whether it is IPv6 capable.

Data Sharing Characteristics

DDMS MDR Registered Web Service NCES Registered

Discoverable IPv6 Capable Tagged Other

Risks and Issues can only be added to System Implementations when the parent Information Need is Critical, is

DAG Ch. 7.4 Net-Centric Information Sharing Data Strategy
<https://acc.dau.mil/CommunityBrowser.aspx?id=334048&lang=en-US>



Information Assurance

- The EISP collects references to a program’s IA Strategy and PPP so that reviewers and analysts may access the IA information they require
 - By doing so, the EISP does not recreate IA information that exists in an authoritative data source
 - Through analysis of Minimum Parameters, the EISP is able to analyze IA at the critical link level
- IA Policies for reference:
 - DoDD 5000.1 The Defense Acquisition System
 - DODI 5000.2 Operation of the Defense
 - DODD 8500.01E Information Assurance
 - DoDI 8500.2 Information Assurance Implementation
 - DoDI 8580.1 Information Assurance in the Defense
 - DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process
 - DoDI 5200.40 DoD Information Technology Security Certification and Accreditation Process

EISP ONLINE Release 1.3.1 Build 02 #417
ENHANCED INFORMATION SUPPORT PLAN

Navigation: EISP Home PM-P Home Admin Program Info Program Data Overview Analysis Appendices Supporting Docs Feedback? Logout

Welcome Mr. Rich

Caution: Currently, the EISP ESV will time out without warning users and any unsaved information will be lost. Users should save often to avoid timing out and prevent data loss. An automated warning capability is being developed for a future release.

Analysis

Process Analysis > DoD IEA > NR-KPP Statement > CPM > Information Assurance Strategy Status

Other Information Needs and Additional Operational Risks > Radio Frequency Spectrum Needs Status > Miscellaneous Analysis > Supporting Documentation

Information Assurance Strategy Status

Enter the following information about your Information Assurance Strategy, if it is complete. This information is not a requirement for an Information Support Plan. Please note, * indicates a required field.

Information Assurance Strategy Status

* Program Protection Plan Reference:	TBD
Program Protection Plan Completion Date:	19 Apr 2010 <input type="checkbox"/> To Be Determined (TBD)
* IA Strategy Title:	Information Assurance (IA) Strategy Light/Attack Helicopter Program (H-1) ACAT ID, May 2006
* IA Strategy Location:	Light/Attack Helicopter Program Office (PMΔ-278)
IA Strategy Status:	Approved by Service
IA Strategy Completion Date:	17 May 2006 <input type="checkbox"/> To Be Determined (TBD)

Point of Contact

Last Name	First Name	Rank	Job Title	Email	Action
THERE ARE NO POINT OF CONTACTS.					
Add Contact					

Supporting Documentation

Additional Descriptive Notes:
Keywords:
ISP Author Notes:

Information Assurance Policy References
<http://www.dtic.mil/whs/directives/index.html>



GTG-F Configuration Control Board (CCB) will be stood up to incorporate feedback, changes, and policy updates into the process

- The GTG-F CCB will include members from the DoD CIO, DISA, and the DoD Components
 - Members will provide inputs as to which changes and enhancements should be included in each release
- Users may add new GTG-F requirements in the GTG-F Software Forge community:
https://software.forge.mil/sf/projects/gtg_f
- The EISP is continuing to evolve and bring additional capabilities online, including:
 - Additional, and improved, architecture imports to reduce burden on PMs
 - Streamlined PDF to reduce size and complexity of ISP output
- The EISP will be updated to accommodate new policy and guidance
 - CJCSCI 6212.01F
 - DoD IEA Version 2.0



Summary

- The Interim Guidance for the Interoperability of Information Technology (IT) and National Security Systems (NSS), signed 27 March 2012, prescribes the use of the GTG-F to create and submit ISPs and GTPs for review and approval
 - <https://gtg.csd.disa.mil>
- The GTG-F provides PMs with a data-centric interoperability compliance analysis process that saves ISP developers time and money vs. the legacy process through the automatic import of architecture data, use of online templates, business rules, and data validation capabilities, and references to authoritative data sources
- The EISP, and the GTG-F, will continue to evolve to incorporate new capabilities, streamline the process for PMs, and create an effective and efficient process to collect Interoperability data

- POCs

EISP Help Desk
eisp_help@bah.com

GTG-F Help Desk
EE3TechSupport@disa.mil