



*Report of the*  
**Defense Science Board Task Force  
on Achieving Interoperability in a  
Net-Centric Environment**

# **Creating an Assured Joint DOD and Interagency Interoperable Net-Centric Enterprise**



**March 2009**

Office of the Under Secretary of Defense  
for Acquisition, Technology, and Logistics  
Washington, D.C. 20301-3140

# 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 <b>MAR 2009</b>	2. REPORT TYPE	3. DATES COVERED <b>00-00-2009 to 00-00-2009</b>			
4. TITLE AND SUBTITLE <b>Creating an Assured Joint DOD and Interagency Interoperable Net-Centric Enterprise</b>		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) <b>Office of the Under Secretary of Defense, For Acquisition, Technology, and Logistics, Washington, DC, 20301-3140</b>		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 <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>	<b>Same as Report (SAR)</b>	<b>174</b>	



*Report of the*  
**Defense Science Board**  
**Task Force on Achieving Interoperability**  
**in a Net-Centric Environment**

# **Creating an Assured Joint DOD and Interagency Interoperable Net-Centric Enterprise**

**March 2009**

Office of the Under Secretary of Defense  
For Acquisition, Technology, and Logistics  
Washington, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB).

The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions and recommendations in this report do not necessarily represent the official position of the Department of Defense. The Task Force on Achieving Interoperability in a Net-Centric Environment completed its information gathering in October 2008.

This report is unclassified and cleared for public release.



DEFENSE SCIENCE  
BOARD

OFFICE OF THE SECRETARY OF DEFENSE  
3140 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3140

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (ACQUISITION,  
TECHNOLOGY & LOGISTICS)

SUBJECT: Final Report of the Defense Science Board Task Force on Achieving  
Interoperability in a Net-Centric Environment

I am pleased to forward the final report of the Defense Science Board (DSB) Task Force on Achieving Interoperability in a Net-Centric Environment, chaired by The Honorable Arthur L. Money and LTG(R) William J. Hilsman.

As requested in the Terms of Reference, the Task Force was asked to assess the requirements for military operations in a net-centric environment, the use of a single autonomous agency as one mechanism to achieving interoperability, a standards-only approach allowing independent development and the development of a virtual test, integration and certification capability to assure interoperability. In doing so the Task Force was cognizant of the multiple organizations (Military Departments, domestic support operations, coalition partners and non-traditional partners) involved in DoD operations.

The final report addresses the Terms of Reference tasking and provides findings and recommendations that recognize our shift from "network enabled to network dependent" and the criticality in creating an interoperable net-centric environment that is necessary for national security. The report proposes a 500-day action plan which first establishes the governance system and the subsequent actions toward implementation of the Task Force recommendations.

I endorse all of the Task Force's recommendations and propose you review the Task Force Chairmen's letter and report.

A handwritten signature in black ink that reads "William Schneider, Jr." with a stylized flourish at the end.

William Schneider, Jr.  
DSB Chairman





DEFENSE SCIENCE  
BOARD

OFFICE OF THE SECRETARY OF DEFENSE  
3140 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3140

February 13, 2009

MEMORANDUM TO THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Defense Science Board Task Force on Achieving Interoperability in a Net-Centric Environment

The final report of the Defense Science Board (DSB) Task Force on Achieving Interoperability in a Net-Centric Environment is attached. Our task force has analyzed the results to date of ten years of Department of Defense (DOD) efforts to achieve interoperability in a net-centric environment. We have observed that during this time, the United States has fully entered the cyber area of national security operations. During the year the DSB studied the issues, attention to net-centric and cyber issues increased noticeably resulting in acknowledgement by our task force that the net-centric environment and the cyber environment share the same space. We, therefore, felt that the issue of a net-centricity could no longer be addressed separately from the cyber issue. This report uses the term “net-centric/cyber” in recognition of this shift.

With multiple inputs from combatant commanders fighting in today’s net-centric/cyber environment, the key message we heard was, “We are no longer network enabled. We are now network dependent.” The task force reached an overall conclusion that without an integrated net-centric/cyberspace plan, threats from adversaries in cyberspace represent a clear and present danger to the national security of the United States.

Even as the task force concluded that the United States is well into the next generation of warfare—cyber warfare—it is far from achieving the goals of assured interoperability in a net-centric environment. DOD is equally far from creating an interoperable net-centric environment that is necessary for national security.

The task force members stressed that this report should invoke action. We, therefore, recommend a governance structure and have outlined a 500-day plan of action as a key part of the report. The primary finding in this study is that the major impediment to attaining an assured joint DOD and interagency interoperable net-centric enterprise is governance—the “who is in charge?” issue.


The report defines the process for establishing and managing the enterprise and the key enabling network architecture. It focuses on key data strategies as a part of the enterprise. It lays out a test, evaluation, and certification process for all networks and also

offers opportunities for rapidly moving IT systems from the drawing board to the field. It addresses other key issues including training our people and strengthening our industry partnership.

A key area of the report is based on three years of previous DSB studies on information assurance that becomes critical the further we move into the net-centric/cyber era. Combatant commanders, as well as our Terms of Reference (TOR), noted the criticality of teaming with our interagency partners. We agreed, but as we progressed, a complete look at all of our interagency partners was beyond the time allotted for this study. However, recognizing that interagency operations between the Department of Defense and the Department of Homeland Security (DHS) have reached a critical stage, the task force provides an in-depth look at the relationships between these two agencies in the report. Working directly with the leadership of U.S. Northern Command (USNORTHCOM), the National Guard Bureau (NGB), and DHS, the report lays out actions for specific programs that will provide immediate results in building a net-centric enterprise as a part of the DOD/DHS partnership.

The primary recommendation of the report is for the Secretary of Defense to issue a directive letter establishing a Net-Centric/Cyber Council co-chaired by the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff to manage the implementation of the DOD program.

With the plan for DOD defined in Part I and for interagency interoperability in Part II, we have presented a path forward in a 500-day plan in Part III. The task force urges the Secretary of Defense to put this plan into action with his directive letter within 30 days after the approval of this report.



---

The Honorable Art Money  
Co-Chair



---

Lieutenant General Bill Hilsman, USA (ret.)  
Co-Chair



# Table of Contents

Executive Summary.....	ix
Chapter 1: Introduction.....	1
Chapter 2: Governance for the Assured Interoperable Net-Centric Enterprise.....	7
<b>Part I: Challenges Within the Department of Defense</b>	
Chapter 3: Defense Communications and Networks.....	17
Chapter 4: Service Oriented Architectures .....	49
Chapter 5: Interoperability and Information Assurance.....	61
Chapter 6: Joint DOD Test, Evaluation, and Certification.....	77
<b>Part II: Interagency Challenges</b>	
Chapter 7: Interagency Interoperability: Redefining “Jointness” .....	87
Chapter 8: The Human Dimension .....	107
<b>Part III: Actions for the First 500 Days</b>	
Chapter 9: Actions for the First 500 Days .....	115
Appendix A: Relevant Government Directives, Letters, and Memoranda.....	123
Appendix B Draft Directive.....	125
Appendix C: Challenges for Network Technologies.....	127
Terms of Reference .....	135
Task Force Membership .....	139
Presentations to the Task Force .....	143
Glossary.....	149



# Executive Summary

Achieving interoperability in a net-centric environment is fundamental to achieving the full potential of transformation. This fact is recognized by the terms of reference of this study and by previous studies completed both inside and outside the Department of Defense (DOD).

DOD is not yet organized, trained, equipped, or in many cases adequately focused on threats to cyberspace-enabled operations. The task force reached an overall conclusion that without an integrated net-centric/cyberspace plan, threats from cyber-intelligent adversaries represent a clear and present danger to U.S. national security.

Major steps are therefore recommended in this report to move to an assured “joint DOD” interoperable net-centric force within DOD. Additional recommendations from the task force focus on improvements at DOD and the Department of Homeland Security (DHS) to promote an integrated homeland defense and homeland security mission. The task force acknowledged that an interoperable, net-centric enterprise<sup>1</sup> designed to enable the best offense may make it easier for an adversary to attack and penetrate the network. Therefore, the task force also addressed risk assessment in relation to creating a sustainable network architecture.

## Evolving Definitions

**net-centricity:** The DOD vision of net-centricity—the capability to discover, access, trust, and use information—is a continuously-evolving, complex community of people, devices, information and services interconnected by a communications network to achieve optimal benefit of resources and better synchronization of events and their consequences.

**interoperability:** The ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. Interoperability includes both the technical exchange of information and the end-to-end operational effectiveness.

**cyberspace:** A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

---

1. An *enterprise* in this context is defined as any company, business, or organization engaged in a purposeful endeavor.

## Task Force Operation and Approach

The terms of reference directs the task force, at a minimum, to assess the requirement for military operations in a net-centric environment. It also directs the task force to (1) assess the use of a single, autonomous agency as a mechanism to achieve interoperability; (2) utilize a standards-only approach to allow independent development of systems certified to the standards; (3) develop virtual test, evaluation, and certification capabilities to assure interoperability of military operations in a net-centric environment; and (4) enable each model to establish and maintain configuration management among the multiple organizations involved in DOD operations. Finally, the task force was directed to (5) assess the potential to use current systems to incrementally evolve to net-centric capability.

Recognizing the critical and complex nature of the issues, the task force engaged members and government advisors from a comprehensive cross-section of DOD and DHS operations and industry.<sup>2</sup> Nineteen meetings held between August 2007 and October 2008 provided input from senior leadership across the government, including the intelligence community, DHS and DOD combatant commanders, the Joint Chiefs of Staff, the Office of the Secretary of Defense (OSD) staff, defense agencies, and the military Services.<sup>3</sup>

The task force puts forth a plan to create an assured Joint DOD and interagency interoperable net-centric enterprise aligned with DOD and national cyber strategies that enables U.S. decision and execution superiority—at all levels of decision making across the federal, state, and local government, to include out to the tactical edge.

While the primary focus of the task force was interoperability within DOD, the task force was also directed to study interagency interoperability. Early in its operation, the task force surveyed progress toward DOD interoperability with the intelligence community and noted excellent progress in their partnership. This was not the case for the relationship between DOD and DHS. For this reason, the task force focused on improvements to the relationship among the OSD, the United States Northern Command (USNORTHCOM), the uniformed Services, the National Guard Bureau, and DHS as a critical partnership for both homeland defense and homeland security.

---

2. A full list of task force members and advisors is provided at the end of this document.

3. A full list of presentations to the task force is provided at the end of this document.

## The Value of Interoperability

The United States has undeniably entered the cyber era of national security operations. Attention to these issues increased noticeably over the course of this study, resulting in an acknowledgement by the task force that operations in a net-centric environment will be heavily influenced by cyber activities in the net generation of warfare in this report. The phrase “net-centricity/cyber” is used to represent this new meaning.

Numerous examples were presented where interoperability was degraded or lost because of people thinking locally rather than globally. These cases ranged from program managers who had difficult resource choices to make, to unit commanders who spent pre-deployment money to buy software from a local company, to organizations buying their own network servers and laying their own fiber networks in theater instead of using those already available. This data was primarily anecdotal, and as a result, the task force did not find a way to quantify the value of achieving interoperability, nor could the penalty in security for widespread interoperability of information systems be quantified. However, the task force agreed on the overwhelming benefit of assured interoperability for DOD and the nation.

The input received provided a consistent picture of the need for an assured joint DOD interoperable net-centric environment. Key briefings from DOD combatant commanders highlighted a sea change to a world where U.S. forces are no longer network enabled; they are network dependent. Discussions with senior commanders describing the battle space of today clearly showed they understood the need for integrated information inputs from all sources and the need to manage assets in what has been well defined as a net-centric environment. These commanders understood that speed, accuracy, and reliability from the network were key to their operations. They know a transition has taken place from "warfare of the past" to "cyber warfare of the future". They also understood that DOD still has a long way to go to reach the goal of achieving interoperability with information assurance in a net-centric environment.

The task force also received inputs describing the need for a 24/7/365 assured joint DOD interagency interoperable net-centric capability for homeland defense and homeland security. This capability is necessary for federal, state, and local systems, units, and forces to provide and accept services among response teams. It is also necessary for the utilization of information and services gained through

shared communications, coordination, and collaboration to enable effective operation in homeland defense, homeland security, and defense support of civil authorities. A further need was identified for interoperable systems to enable these organizations to plan, design, build, acquire, test, train, and operate together.

Information sharing is a key national goal and assured interoperability and net-centricity is a key enabler to allow the desired information sharing. The overarching national security vision is to create an assured joint DOD and interagency interoperable net-centric enterprise along with critical integration with the cyber strategy that enables U.S. decision superiority—at all levels of decision making, to include at the tactical edge.<sup>4</sup> This goal envisions an information advantage for U.S. forces and mission partners by providing a rich data environment in which appropriate information and services are visible, accessible, understandable, and trusted.

## Where We Are Today

The U.S. government is far from achieving the goals of assured interoperability in a net-centric environment and equally far from having the ability to operate in the cyber environment of today and in the future.

Multiple inputs from the combatant commanders confirmed that DOD is highly dependent on communication and data networks for fundamental mission operations, yet there is insufficient joint DOD, interagency, or multinational interoperability. As a result, DOD is duplicating efforts and overspending in attempts to field an assured and interoperable enterprise both overseas and within the homeland.

DOD itself is not adequately equipped to provide the warfighter—the decision maker in the battlefield—all the modalities of assured net-centric interoperability. A successful net-centric strategy must integrate offensive and defensive cyber capabilities and take appropriate risks and challenges into account. Established interoperability can mean the difference in adapting and fielding new capabilities quickly.

---

4. The *network edge* in this context refers to portions of the network, usually located at long physical distances from the core, where bandwidth is limited.

Cyber offensive and defensive technologies (developed by both sides) have far outdistanced DOD requirements and acquisition process. Cyber technology for hardware, software, and systems is as available to adversaries as it is to U.S. forces.

## Impediments to Success

The task force asked representatives from the OSD Staff, the Joint Staff, combatant commanders, defense agencies, the Services, and the National Guard Bureau to discuss their vision for the future and to list the impediments that would delay or interfere with attaining the vision. The vast majority of these views recognized a similar desired future state and the same impediments to success.

Five critical success factors have been identified by DHS as essential to interoperable systems. These five factors—governance, standard operating procedures, technology, training and exercises, and usage—have been captured in “the Interoperability Continuum”<sup>5</sup> and are intended to serve as a tool to improve emergency response communications interoperability. The task force endorses this framework, and addresses each of the five factors in this report.

The primary impediment to success is the governance of the net-centric enterprise within DOD. A lack of definition and a related lack of enterprise-focused management within agencies and Services was also cited. A number of process and technical impediments were also cited, including the lack of a systems architecture and systems engineering. A related need was identified to provide interoperable network services across all DOD missions and across all modalities—wired, wireless, and satellite communications. A related need is for ever-increasing bandwidth and spectrum management.

Understanding the issues of interoperability, net-centricity, cyber offense, and cyber defense across the spectrum of national security is extremely difficult owing to the complexity of the issues and the fast-changing nature of the technologies. The issue is further complicated because the net-centric/cyber

---

5. More information on the interoperability continuum is available at [http://www.safecomprogram.gov/NR/rdonlyres/54F0C2DE-FA70-48DD-A56E-3A72A8F35066/0/Interoperability\\_Continuum\\_Brochure\\_2.pdf](http://www.safecomprogram.gov/NR/rdonlyres/54F0C2DE-FA70-48DD-A56E-3A72A8F35066/0/Interoperability_Continuum_Brochure_2.pdf)

domain does not fall within the purview of any single DOD area of responsibility and accountability.<sup>6</sup>

The lack of an integrated, heterogeneous, and dynamic network is a key impediment to interoperability. Integration of multiple types of networks of different generations into a single interoperable network can be carried out via gateways between disparate subnets and a master control plane. However, before a sensible, integrated heterogeneous defense network can be deployed, many difficult network problems need to be solved, particularly at or near the network edge and at subnet interfaces. The integrated defense network should support voice, video, data, hybrid Internet Protocol, and circuit-based services. It should have a two-tiered system of network services, where the first tier is a robust minimum “hard core” network service necessary for successful defense operations. This service will have modest rates but solid connectivity at all times with low delays. The second tier is a much higher rate “soft” network, which is less robust but has higher rates and supports data-intensive services such as Web browsing.

An issue that crossed both technology and policy is the need for a risk/challenge analysis of interoperability in an information assurance environment. Because increased functionality leads to increased dependence, interoperability demands strong, effective information assurance to reduce risk and ensure reliability. More importantly, interoperability increases the “circle of trust.” Enlarging the population of “insiders” represents a serious danger both in theory and practice and can increase the risk of penetration, compromise, or degradation. Conventional “good” information practices seek to limit the availability and exposure of information, limiting the circle of trust, and minimizing network size and complexity. While this improves assurance, these practices constrain functionality. In brief, interoperability and information assurance are in tension. Effective information assurance is expensive, often awkward, and constraining. As a consequence, it is critical to understand the real need for interoperability, along with its benefits, both advertised and realized.

It is also critical to understand the alternatives to and degrees of interoperability in order to quantify the value of incremental interoperability and to gauge how much information assurance is warranted. Finally, an understanding of the cost of planning for and “fighting through” degraded interoperability is

---

6. A number of recent directives and letters that support this goal are listed in Appendix A.



needed, including a plan to regain trust in the network and technology elements that enable interoperability.

Interagency collaboration and communication issues are also key factors for success. These include the lack of an integrated DOD/DHS program for the homeland defense and homeland security mission. Such an integrated program is needed to provide interagency collaboration on federated testing, networking, and the development of network architectures targeted at improving interagency exercises and experimentation, among other efforts. In addition, a program to facilitate cooperation between government, academia, and industry is also needed.

Cultural norms are also an impediment, including the slow pace of change to the “ways things have always been done.” This is reflected in the pace of acquisition that affects the ability to get information technology systems to the warfighter and homeland defender in a timely way. The lack of joint DOD and interagency training programs to educate federal leadership on the issues listed here was a primary focus needed on the human dimension. An equally important issue is the need for a stronger partnership between government and industry to achieve these goals.

All of these issues affect the information technology enterprise. The combatant commanders from the current theaters of war, Operation Iraqi Freedom and Operation Enduring Freedom, point to the need to better define DOD enterprise, manage its development and operation as an enterprise, and fund and program for it as an enterprise. An assured joint DOD and interagency interoperable net-centric enterprise is needed that can operate effectively in the cyber environment of current and future wars. The task force strongly agreed that this enterprise is so critical that direct involvement by the Secretary of Defense is needed to ensure its creation and successful implementation.

## Summary of Major Findings and Recommendations

### *Finding 1*

The major impediment to attaining an assured joint DOD and interagency interoperable net-centric enterprise is governance. To be effective, governance must be consistent and enforced.

#### RECOMMENDATION 1 SECRETARY OF DEFENSE INVOLVEMENT

To address gaps within DOD, the task force seeks Secretary of Defense involvement through a directive memorandum. Draft directive language that establishes a Net-Centric/Cyber Council is included in Appendix B. The task force also strongly recommends rapid implementation of the action items in the 500-day plan detailed in Part III of this report.

### *Finding 2*

Commanders in the field, whether overseas or in the homeland, depend on communications networks for successful operations. These systems frequently do not interoperate, are unnecessarily duplicated, and manage frequency and bandwidth poorly, both overseas and in the United States.

The goal for DOD is to establish a heterogeneous defense network with a master control plane that can integrate different types of networks originating from disparate subnets. This system must balance operational needs, network capacities, and technical capabilities.

#### RECOMMENDATION 2 NETWORK ARCHITECTURES

The Net-Centric/Cyber Council should charter and oversee a strong Network Systems Architecture Group assigned to the Defense Information Systems Agency (DISA) in order to define the defense network enterprise and to develop for DOD the supporting cost, budget, and Program Objective Memorandum data.

### ***Finding 3***

Using a service-oriented architecture (SOA) can enable government agencies to effectively and affordably address interoperability and information sharing challenges. The goal for DOD is to be able to understand the benefits and the risks of a SOA in addressing interoperability and information sharing challenges.

#### **RECOMMENDATION 3 SERVICE-ORIENTED ARCHITECTURE**

The Net-Centric/Cyber Council should direct DISA to establish a strong, senior-level technical and management-level leadership team, and a strong technical engineering team to address the development of a common SOA across DOD.

---

### ***Finding 4***

Despite the warnings in the 2006 Defense Science Board Summer Study on information assurance issues within DOD, potential adversaries continue to threaten the integrity and availability of military systems. DOD has not yet integrated information assurance as a part of the development of a joint DOD and interagency interoperable net-centric enterprise.

#### **RECOMMENDATION 4 INFORMATION ASSURANCE**

The Net-Centric/Cyber Council should direct United States Strategic Command to examine a few selected systems for risk assessment and for battle-mode requirements in order to create an information assessment capability and build a strong awareness campaign as the next steps in attaining information assurance in the enterprise.

---

### ***Finding 5***

Testing, evaluation, and certification that are performed by one Service or one agency are most often not accepted by other Services or agencies, with no common test methodology and no infrastructure to enable distributed testing. Similarly, there is no common test, evaluation, and/or certification capability for homeland defense, homeland security, and defense support of civil authorities accepted by DOD and DHS support systems. Numerous federal programs and models abound in this area. The goal for DOD and DHS is a federated, joint and

interagency integrated test, evaluation, and certification system and network with a “test by one, accept by all” mandate.

#### RECOMMENDATION 5 TEST, EVALUATION, AND CERTIFICATION

The Net-Centric/Cyber Council should direct the United States Joint Forces Command, supported by DISA and the Services, to establish a federated, virtual, joint, integrated, test evaluation and certification system and network.

#### *Finding 6*

There is a great deal of overlap in the homeland defense mission in the Department of Defense, the homeland security mission in the Department of Homeland Security, and the responsibility for defense support of civil authorities that drives the need for interagency interoperability. The 2008 National Defense Strategy recognizes this issue and provides overarching guidance on DOD support to DHS. The focus of this support mission is the partnership between USNORTHCOM, the National Guard Bureau, and DHS. The goal for DOD is a strong working partnership with DHS supporting the mission for homeland defense, homeland security, and defense support of civil authorities.

#### RECOMMENDATION 6 HOMELAND MISSIONS

DOD and DHS should reestablish the current interagency Strategic Advisory Group (SAG) chartered by the National Guard Bureau as a formal DOD and DHS deliberative interagency planning, programming, and resource decision process to ensure interoperability for homeland defense, homeland security, and defense support of civil authorities.

#### *Finding 7*

People are as important as hardware and software, and are truly a part of the net-centric system. The technology and its application often change so fast that the familiarization and training of the people who need to use it suffers. Not all senior U.S. leaders, including users at the network edge, understand the net-centric/cyber issues that the United States faces today. The goal for DOD is to engineer a culture shift, through training, guidance, and collaboration that can develop and

operate the joint DOD and interagency net-centric enterprise as well as defend it against all adversaries.

#### RECOMMENDATION 7 TRAINING

In collaboration with interagency partners, DOD and DHS should develop a training regime for the net-centric enterprise for all levels including planning, acquisition, and operations. The training should include senior military, civilian executives, and users at the network edge.

---

#### *Finding 8*

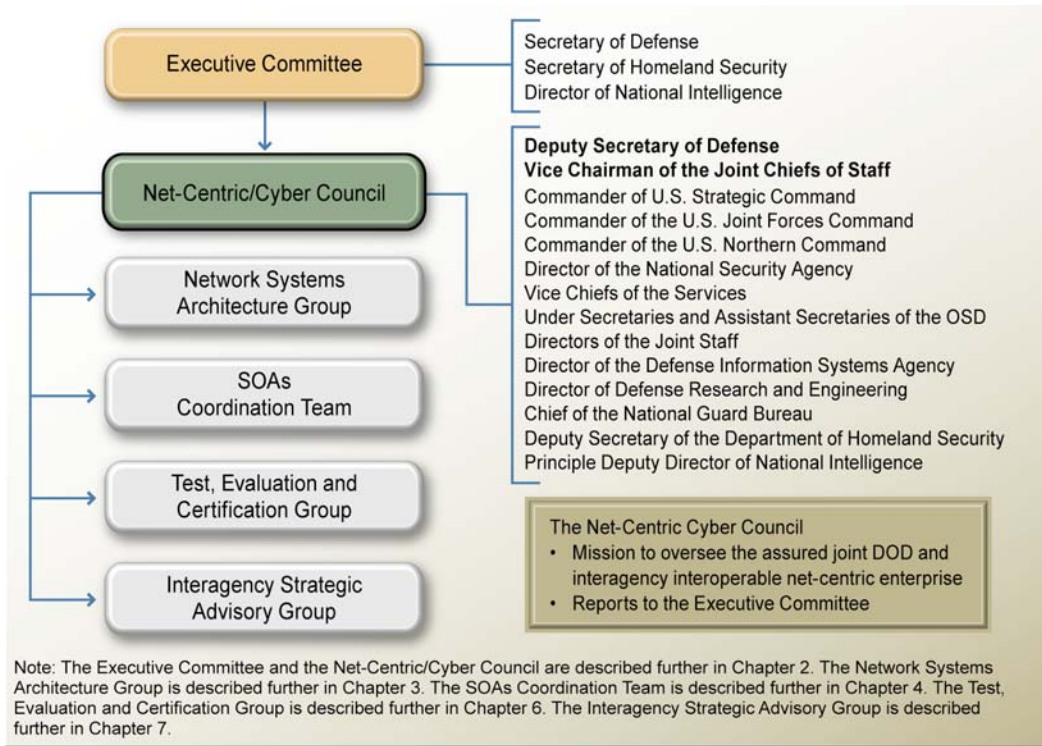
The complexity, criticality, and necessity of a system of systems that meets the criteria for an assured joint DOD and interagency interoperable net-centric enterprise presents a logical and strong imperative for greater cooperation and collaboration between government and industry.

#### RECOMMENDATION 8

Both DOD and DHS chief information officers should guide and exploit such organizations as the Network Centric Operations Industry Consortium and the National Security Telecommunications Advisory Committee to obtain greater cooperation and collaboration between government and industry

---

**The key element of this discussion is that the net-centric enterprise be managed and funded as an enterprise.** Many of the complex issues that have been discussed in the findings of this report would naturally arise, be examined, and be resolved as such an enterprise is developed. To be successful, the enterprise should be managed and funded for the future. One role of the Net-Centric/Cyber Council would be to establish these rules, support the funding, and enforce these actions. Thus many of these recommendations focus on creating essential elements of an effective management structure, as shown in Figure ES-1.



**Figure ES-1.** Organizational chart showing governance oversight for the interoperable net-centric enterprise

True establishment of a net-centric enterprise will require a new culture inside DOD. Current practices to reject solutions because they are “not invented here,” to engage in turf battles, and to protect legacy programs are counterproductive. The United States has entered and may already be engaged in the next generation of warfare—the cyber war. The United States is not yet organized to fight—or win—this war.

# Chapter 1. Introduction

In 1998, Vice Admiral Arthur K. Cebrowski and John J. Garstka presented a concept for net-centric warfare.<sup>7</sup> The importance of net-centric operations in full spectrum dominance has evolved since that time, and now includes conflicts with rogue states and non-state actors such as Al Qaeda, and extends even to small groups of individuals.<sup>8</sup> Today, net-centric technology can allow these adversaries of the United States to attack military operations, and also to target basic economic and social infrastructure in the homeland. At the same time, U.S. military personnel depend on net-centric capabilities for everyday operations.

Transformation in the Department of Defense (DOD) towards net-centricity and interoperability is co-dependent on transformation of traditional military information systems. In the traditional acquisition approach, DOD defines the capability needs and operational requirements of a system, and then provides the needs and requirements to a developer or a group of developers. DOD is responsible for functional requirements analysis and extraction, system architecture, integration, testing, and fielding. When building medium and large systems, DOD has had little success with this approach and has looked to other alternatives.

An alternative is for DOD to provide high-level system requirements to a lead systems integrator. This approach was developed with the intention of providing an effective solution and a single point of accountability to address the difficulties associated with assigning end-to-end systems development and management responsibilities to DOD. An assumption of this approach is that the prime contractor has a better grasp of industry best practices and emerging technologies, relieving DOD of the burden of staying constantly on top of this monumental task.

---

7. A.K. Cebrowski and J.J. Garstka (1998) Network-centric warfare: Its origin and future. *Proceedings of the U.S. Naval Institute*. Available at <http://216.230.103.132/proceedings/Articles98/PROcebrowski.htm>

8. In 1996, Admiral Bill Owens described a defensive concept of operations employing a “system of systems.” W.A. Owens Jr. (1996) The emerging U.S. system-of-systems. *Strategic Forum 63*, Institute for National Strategic Studies. Available at [http://www.ndu.edu/inss/Strforum/SF\\_63/forum63.html](http://www.ndu.edu/inss/Strforum/SF_63/forum63.html)

However, this approach has failed to deliver and has encountered resistance in Congress and elsewhere because of poor performance in some large acquisition programs, and because of perceived lack of DOD visibility and control over the program. Primary concerns with this approach include:

- **Proprietary systems.** This approach often leads to solutions where a single prime contractor owns the intellectual property or is the only organization that can cost-effectively operate and enhance the system. Contracts are also often written in a way that does not incentivize using technologies available from competitive sources. These trends can lock DOD into dealing with a single vendor that has little incentive to capitalize on technology innovations. Requirements do not focus on how the system will interact with the Global Information Grid (GIG) or facilitate interoperability with other similar systems of similar capabilities.
- **Narrow optimization.** System integrators tend to optimize their product to a set of narrow requirements, a practice that limits opportunities to reuse or adapt capabilities for other systems. These same contractors are unwilling to accept risk that comes with adapting or reusing components developed by others. This optimization may make a small system more cost effective, but limits leverage and will result in greater costs to integration and operation of the larger GIG.
- **Closed designs.** With a single integrator or prime contractor responsible for everything from requirements analysis to application development to testing, it is often difficult for DOD to maintain visibility throughout the process. Performance-based contracting relies on the integrator to determine the details of what they are going to build, why they are going to build it, and then how well they built it. Conversely, interoperability requires some level of collaboration and community involvement.
- **Non-standard architectures.** When systems are not built to a standard, development is slower and systems are not scalable.

Traditional approaches have provided some benefits in the past age of large, monolithic systems development. However, these approaches are ill-suited for today's environment of rapid development cycles where smaller modular systems capabilities can be quickly developed and deployed with the expectation that they will interoperate with other modules. Similarly, the program executive officer and program manager roles must also evolve to focus on delivering systems that will operate on appropriately designed and operated networks.



The task force found considerable effort and widely disparate rules for acquisition of services and equipment supporting a net-centric DOD enterprise. It was also concluded that interoperability is needed across the many organizations within DOD and should extend to the larger support community. This community may include homeland security and defense support of civil authorities and extend to international allies and international humanitarian aid. The potential to centralize the requirements generation for all of these systems seems unlikely given the diverse organizations concerned.

The Department of Homeland Security (DHS) has identified five critical success factors as essential elements of interoperable systems. The task force endorses this framework. These five factors have been captured in “the interoperability continuum”<sup>9</sup> and are intended to serve as a tool to improve emergency response communications interoperability.

- governance
- standard operating procedures
- technology
- training and exercises
- usage

## Evolving Definitions

**net-centricity:** The DOD vision of net-centricity—the capability to discover, access, trust, and use information—is a continuously-evolving, complex community of people, devices, information and services interconnected by a communications network to achieve optimal benefit of resources and better synchronization of events and their consequences.

**interoperability:** The ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. Interoperability includes both the technical exchange of information and the end-to-end operational effectiveness.

**cyberspace:** A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

---

9. More information on the interoperability continuum is available at [http://www.safecomprogram.gov/NR/rdonlyres/54F0C2DE-FA70-48DD-A56E-3A72A8F35066/0/Interoperability\\_Continuum\\_Brochure\\_2.pdf](http://www.safecomprogram.gov/NR/rdonlyres/54F0C2DE-FA70-48DD-A56E-3A72A8F35066/0/Interoperability_Continuum_Brochure_2.pdf)

## Addressing the Terms of Reference

The terms of reference (attached to this report) directs the task force to assess different models of achieving interoperability. In doing so, the task force is directed to keep in mind the multiple organizations involved in DOD operations. These include, but are not limited to, the respective military departments, domestic support operations, coalition partners, and non-traditional partners (e.g., non-governmental organizations).

At a minimum, the task force was directed to assess:

- The requirement for military operations in a net-centric environment. To do this, the task force solicited and received major inputs from today's combatant commanders.
- The use of a single, autonomous agency as a mechanism to achieve interoperability (e.g., Army Central Technical Support Facility) established to integrate non-materiel and materiel solution sets for military operations in a net-centric environment.
- A standards-only approach allowing independent development of systems certified to the standards.
- The development of a virtual test, evaluation, and certification capability to assure interoperability of military operations in a net-centric environment.
- The ability of each model to establish and maintain configuration management amongst the multiple organizations involved in DOD operations.
- The potential to use current systems to incrementally evolve to net-centric capability, especially in light of the rapid evolution in the network domain contrasted with the lack of synchronized and comprehensive DOD modernization.

## A Deeper Understanding of Key Concepts

Each of the following chapters will provide a deeper basis for the findings and further development of these major recommendations, as follows:

- The need to define, create, manage, and fund an assured interoperable net-centric enterprise, including specific recommendations on governance and progress toward the vision of such an enterprise (addressed in Chapter 2)

### Part I: Challenges within the Department of Defense

- The need to create an assured integrated heterogeneous network as a critical part of the enterprise (Chapter 3).
- A way ahead for service oriented architectures (SOAs), a key data strategy (Chapter 4).
- A very direct and deep look at the information assurance issues from the point of view of what our adversaries bring to the table both strategically and tactically (Chapter 5).
- Moving test, evaluation, and certification (and experiments and exercises) to a truly joint, federated DOD operation (Chapter 6).

### Part II: Interagency challenges, and beyond

- Furthering the partnership to implement a homeland defense and homeland security enterprise by strengthening the network established by USNORTHCOM, the National Guard Bureau (NGB), and the Department of Homeland Security (DHS). (Chapter 7).
- Raising the human dimension to the same level of importance as technologies and networks, extending the system to include the government and industry workforce (Chapter 8).

### Part III: A 500-day action plan

- A major imperative of the task force was to establish a set of actions needed to implement the recommendations of this report. Toward that end, a 500-day action plan was developed that can be managed and measured. The elements of this plan are detailed in this section (Chapter 9).



## Chapter 2. Governance for the Assured Interoperable Net-Centric Enterprise

The Department of Defense has formally recognized the concept for net-centric warfare for more than a decade. *Joint Vision 2010* and full-spectrum dominance have propelled DOD to define net-centric warfare as a cornerstone to DOD transformation.<sup>10</sup> The terms of reference for this task force state that achieving interoperability in a net-centric environment is recognized as fundamental to addressing the full potential of transformation. Multiple studies, including several Defense Science Board (DSB) reports, have made recommendations on how to move to an effective net-centric environment. While acknowledging these facts, the task force received input—from combatant commanders, the Joint Staff, the Office of the Secretary of Defense (OSD) staff, the defense agencies, and the Services—indicating that the United States is far from achieving the goals of interoperability in a net-centric environment.

### Putting a Value on Interoperability

The Department of Defense is hamstrung by today's disorganized information systems. DOD has consistently failed to optimize efforts to upgrade and insert new technology into systems across a wide range of applications at a time when net-centric operations and networked information exchange is an operational imperative.

It was evident from multiple presentations to the task force that continuous improvement in situational awareness, decision-making, and response to events across all government venues is a national strategic, tactical, and political imperative—and depends strongly on interoperability of net-centric operations.

---

10. Department of Defense. *Joint Vision 2010*. 1996. Available at <http://www.dtic.mil/jv2010/jvpub.htm>

The task force heard a number of examples where interoperability was degraded or lost because of people thinking locally rather than globally. These cases ranged from program managers who had difficult resource choices to make, to unit commanders who spent pre-deployment money to buy software from a local company, to organizations buying their own network servers and laying their own fiber networks in Iraq instead of using those already available. While consistent, the data were not quantitative and the task force did not find a way to tally the value of achieving interoperability, nor could the security penalty for widespread interoperability of information systems be quantified. The task force agreed, however, on the overwhelming value of interoperability for DOD and the nation, and noted that current incentives do not favor interoperability outcomes.

### ***A Vision for Interoperability***

The overarching national security vision determined by the task force is to create an assured joint DOD and interagency interoperable net-centric enterprise as well as critical underpinnings for a cyber strategy that enables U.S. decision superiority—at all levels of decision making, to include out to the tactical edge. This goal envisions a unified enterprise that creates an information advantage for U.S. forces and mission partners by providing a rich data environment in which appropriate information and services are visible, accessible, understandable, and trusted across the enterprise. The enterprise is built on an assured, available, and protected infrastructure out to the tactical edge that enables responsible information-centric operations using dynamic and interoperable communications and computing capabilities.

This goal also envisions a 24/7/365 capability for homeland defense and homeland security. This enterprise allows federal, state, and local systems, units, and forces to provide services and accept services from one another, and to use information and services gained through shared communications, coordination, and collaboration to enable effective operation in homeland defense and homeland security missions. This includes leveraging new institutional processes that enable these organizations to plan, design, build, acquire, test, train, and operate together.

### ***Attaining Interoperability***

Interoperability does not emerge immediately and obviously as a core warfighting need as does firepower, mobility, or command and control. This can result in a lack of guiding oversight and of appropriate incentives resulting in sub-

optimal choices based upon local motivations. An example is buying lightweight commercial radios that work within a unit but won't work across organizational boundaries. The lack of oversight can also mask the implications of some convenient small change to the software on a local machine that may have global consequences for the network. For these and other reasons, decisions at the edge must be guided by the same governance.

A number of factors have slowed DOD's progress toward this goal. Primary is an overall pervasiveness of the net-centric/cyber domain. As the Deputy Secretary of Defense recently observed, "because all combatant commands, military departments, and other defense components need the ability to operate unhindered in cyberspace, the domain does not fall within the purview of any one particular department or component."<sup>11</sup> This has led to the lack of an overall systems architecture and systems engineering organization to design and maintain this enterprise, the lack of a comprehensive risk analysis that considers interoperability and information assurance for net-centric/cyber systems, and the lack of planning and management for bandwidth and frequency allocation. The task force concluded that the situation has been fostered by the persistent institutional culture in DOD that resists change, adheres to historical practice, and rejects new ways of doing business.

Solving the governance issue is most critical to enabling an assured Joint DOD and interagency interoperable net-centric environment.

Several additional factors compound the situation across the Department. First is a lack of joint training programs because there are so few common systems. joint test, certification, and evaluation programs are also late to need. The acquisition system has been unable to provide net-centric/cyber systems to the warfighter in a timely way, leaving a disparate set of current and legacy systems in the field. Finally, there is also a need for greater cooperation and collaboration between government, academia, and industry to address these challenges.

As the United States evolves toward net-centric warfare, the capability for interoperability and information sharing underpins our national decision superiority—both strategic and tactical. This is hampered by the lack of effective governance, which is difficult because the domain does not fall within the

---

11. DOD memorandum defining cyberspace. 12 May 2008.

purview of any single department or component. Attempts to move to a net-centric enterprise, put on a fast track during the deployments for Operation Iraqi Freedom and Operation Enduring Freedom, resulted in the development of multiple stove-piped programs. Overcoming this stove-piped culture will require a major effort in the coming period as defense funding, often provided through supplements today, will likely be greatly reduced.

The task force concluded that solving the governance issue is critical to establishing and maintaining assured and interoperable net-centric/cyber functions. The combatant commanders and DOD staff that briefed the task force stated consistently and clearly that “no one is in charge.” They reported a multibillion-dollar effort that is not managed in an integrated way—each service doing what they need with little consideration of the other services and agencies within DOD.

All recognized the need for an assured joint DOD interoperable network. Presentations to the task force from all levels articulated the need to integrate information from all sources, to quickly access the needed information, and the critical need to improve decision-making based on this information. The task force concluded that the United States faces a clear and present danger in this area, and that these issues should be a high priority for the Secretary of Defense.

## **Interoperability in Support of the Homeland Defense, Homeland Security, and Defense Support of Civil Authorities**

The task force delved deeply into the interoperability needs for net-centric homeland security and homeland defense activities. Multiple inputs from DOD and DHS representatives revealed no existing governance structure for achieving interagency interoperability to support these mission areas. The task force identified several actions and programs in development with promise to provide this necessary governance.

As required in the National Defense Authorization Act for Fiscal Year 2008, the Secretary of Defense has prepared plans for response to natural disasters and terrorist events. In consultation with the Secretary of Homeland Security, the Chairman of the Joint Chiefs of Staff, the Commander of the United States Northern Command, and the Chief of the National Guard Bureau, DOD has prepared a plan for coordinating the use of the National Guard and members of



the Armed Forces on active duty when responding to natural disasters, acts of terrorism, and other man-made disasters as identified in national planning scenarios. This plan recognizes the need for an assured and interoperable communications and information-sharing plan.<sup>12</sup> This plan explicitly points to the need to communicate across disparate networks, with partners small and large, within government and the private sector, and many times with great urgency.<sup>13</sup> This level of planning can benefit from well-designed exercises and experiments with appropriate participation.

The task force confirmed the findings and recommendations from the report of the Defense Science Board 2003 Summer Study on DOD Roles and Missions for Homeland Security. The new findings reinforce the charter for the Strategic Advisory Group (SAG) that was established as a result of that report to address a concept of operations for command, control, communications, and computers (C4). This SAG is envisioned to play a key role in implementing the action items in Part III of this report.

## **A DOD Net-Centric/Cyber Council**

The task force considered a number of potential leadership models. The roles of various agencies were also considered, as well as entirely new organizational strategies. The roles of various offices in OSD, especially the role of chief information officers (CIO), were also discussed. In the end, the task force strongly concluded that this issue was so critical to future success in the next generation of warfare—cyber warfare—that it needs the direct and continuous involvement of the Secretary of Defense.

Considering the many critical issues that demand the attention of the Secretary of Defense, the task force felt a multiservice team would be needed to implement this action. This team should be established by a memorandum from the Secretary of Defense naming a Net-Centric/Cyber Council. The suggested name for the Net-Centric/Cyber Council recognizes that net-centric systems operate within the

---

12. Report to Congress: Plan for Coordinating National Guard and Federal Military Force Disaster Response. August 29, 2008.

13. Department of Defense. 2006. "Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations." Joint Publication 3-08. Available at [http://www.dtic.mil/doctrine/jel/new\\_pubs/jp3\\_08v1.pdf](http://www.dtic.mil/doctrine/jel/new_pubs/jp3_08v1.pdf)

cyber domain and that interoperable net-centric systems must be assured systems. Today, our cyber strategy and our net-centric strategy must be fully interwoven. As the Council works to advance an interoperable, net-centric enterprise, it must always consider the on-going cyber issues affecting national security. Thus, the task force recommends the name of the Council indicate this awareness.

The council would be co-chaired by the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff. The DOD CIO would act as secretariat for the Council, acting to set meeting agendas, provide background on issues for discussion, supply comprehensive network and enterprise expertise, manage compliance, and prepare budgets and program objective memoranda (POM) inputs.

The Council would have the following members:

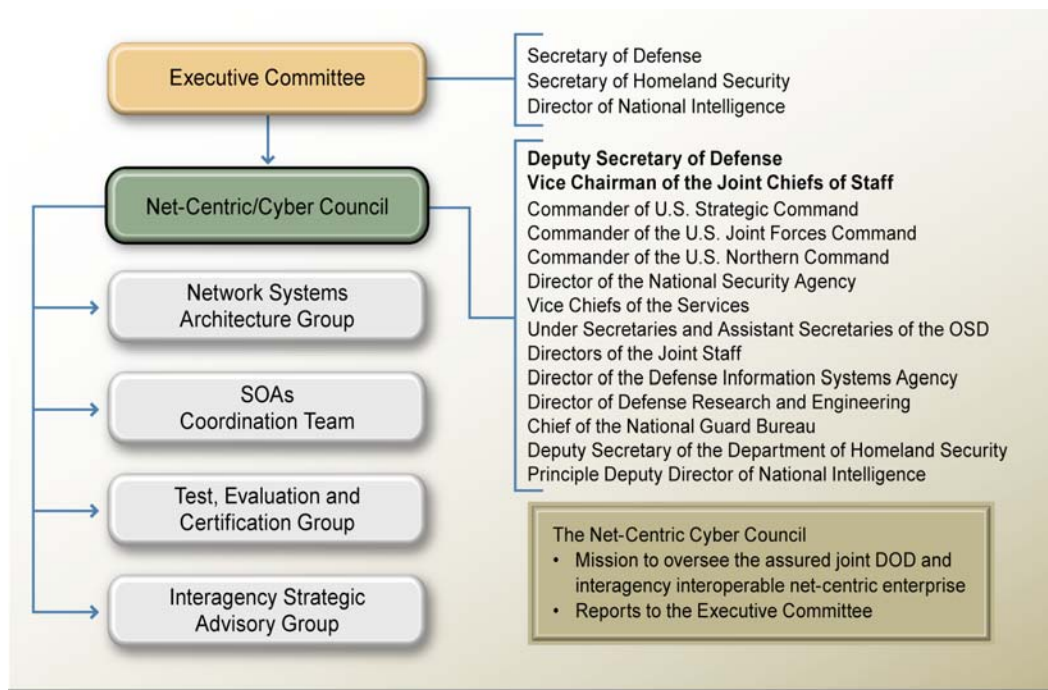
- Commander of U.S. Strategic Command (USSTRATCOM)
- Commander of U.S. Joint Forces Command (USJFCOM)
- Commander of U.S. Northern Command (USNORTHCOM)
- Director of the National Security Agency (NSA)
- Vice Chiefs of the Services
- Under Secretaries and Assistant Secretaries in OSD
- Directors of the Joint Staff
- Director of the Defense Information Systems Agency (DISA)
- Director of Defense Research and Engineering
- Chief of the National Guard Bureau
- Deputy Secretary of the Department of Homeland Security
- Principle Deputy Director of National Intelligence (DNI)

The task force recommends that the Secretary direct the Commander USSTRATCOM, Commander USJFCOM, and the Commander USNORTHCOM to continuously provide requirements of the combatant commands to the Council. To do this effectively, the task force believes the Services should establish or elevate their net-centric/cyber commanders as four-star officers. The task force also recommends that the Secretary of Defense direct the Council to deliver a 500-day plan and a five-year plan delineating clear actions, due dates, and responsible authorities. The 500-day plan should be managed as a program by the Council, reported to the Secretary of Defense quarterly, and updated annually. As

a part of this planning effort, the Services and DOD agencies would be required to develop their budgets for net-centric/cyber integration and interoperability for integration into an overall DOD net-centric/cyber budget element.

In addition, the task force recommends that the Secretary of Defense form an Executive Committee co-chaired by the Secretary of Homeland Security and the Director of National Intelligence. **This executive committee would meet with the Council annually to review work in progress and to guide consensus decisions.**

Figure 1 shows the Council as part of a larger governance plan that addresses specific needs of network architecture, SOAs, test, evaluation and certification, and interagency interoperability.



**Figure 1.** The Net-Centric/Cyber Council as part of the larger governance plan

## Costs and Benefits of Improved Oversight

The task force concludes that if the nation truly recognizes the need to transform now to meet the threats of cyber warfare, that the national leadership will throw out the old book, push the old culture aside, and put a strong governance plan into immediate action. This means the direct involvement of the Secretary of Defense is necessary to form a Net-Centricity/Cyber Council that will demand action on a fast track.

As the enterprise is defined with the help of the recommendations in this report, a full costing and budget program is needed that includes future systems engineering and programmatic analysis of alternatives. The cost of an assured joint DOD and interagency net-centric interoperable enterprise is not trivial. Additional costs may include setting up a network for joint and interagency testing. However, avoiding the cost of multiple networks doing the same thing, the cost of multiple SOA developments, the cost of reinventing systems that were “not invented here,” and the cost of multiple testing of the same systems might be expected to offset this cost.

Estimating these costs—both for taking new actions and continuing old ones—is difficult to assess given the overarching dependence of all systems on net-centricity. In order to fully understand the cost of implementation, responsible agencies and commands should track costs, develop budget data, and insert these actions into their respective POMs. The role of the Net-Centric/Cyber Council is to provide guidance and advocacy and assure compliance with the overall organizational goals.

# **Part I**

---

*Challenges Within the Department of Defense*



## Chapter 3. Defense Communications and Networks

The primary goal of a defense network is to enable users to obtain and share necessary, trusted, and timely information over an integrated heterogeneous dynamic network.<sup>14</sup> It is the opinion of the task force that many of the tough problems associated with achieving an assured, joint DOD and interagency interoperable net-centric enterprise are yet to be fully solved, especially at or near the network edge. This chapter identifies a number of critical problems and some potential paths to solutions. A first priority is to address these problems immediately before they impact large procurement programs.

Success of the defense network rests on the adoption of a carefully designed network architecture. Network architecture may be viewed from three different vantage points: (1) the **user** or operator point of view, (2) the **system** point of view, and (3) the **technology** point of view. The user is only concerned with the service and the quality of service provided by the network. The system point of view is the articulation of a system concept by which the network services can be provided and concerns the selection, sizing, and arrangement of components and links that provide user services. The technology view considers the capability of current and/or future technologies to support a system design and network services. This chapter describes critical constraints and goals on the defense network architecture from the system and technology viewpoints.

**Given that networks evolve at a rapid pace, especially in the commercial sector, no specific system or technology selections are recommended.** It is imperative that the defense network architecture be agile, evolvable, and adaptable over multiple generations of technology and protocols. A traditional DOD rigid specification approach would result in a dinosaur within a decade. Instead, a framework is proposed that enables accommodating the best current technologies and also adaptation to future technology evolution.

---

14. The proposed network must be **integrated** so all the subnetworks can be connected and able to pass information across the entire network, **heterogeneous** because different network types have different characteristics and **dynamic** because both the operational situation and network behavior is constantly changing.

It must be emphasized that DOD does not currently have a clearly stated user architecture for the defense network. There remain gaps—in some cases vast gulfs—between user expectations and wish lists and what reasonable budgets and technology can deliver. The negotiation process to close these gaps must take place before a sensible technology and system architecture can be selected. Understandably, when polled, most users will present a wish list sometimes with little relationship to actual mission requirements or technology capabilities. It is the task of the network architect to understand the concepts of operations and convey to the users what network services might be reasonably expected. Continuous management of user expectations will keep the cost of the network affordable and will also allow the users to exercise and train with the network services they can count on having in real operational scenarios. DOD must establish a process to validate and improve its defense network user requirements, with strong participation by network architects, as part of its network development efforts.

## **Background: Networks and Layers**

Networks are made up of physical communication channels, switches, and routers. To make this hardware work together as a network, algorithms (generally known as network protocols) running on computer processors are used to orchestrate and perform the function of access control, fair allocation of resources, routing, end-to-end reliable delivery of data, and failure detection and recovery of the networks.

Network protocols are generally broken up into “layers” according to the functions they perform. The open system interconnection (OSI) model defines a networking framework for implementing protocols in seven layers, each with their individual functions. They are designed to have minimal interactions so the design of the layer can be largely independent. The top three layers are generally grouped together as the application layer and are responsible for providing end-user services.

This chapter concentrates mostly on the bottom four layers. The bottom two layers, known as the Physical and Data Link Control layers, generally correspond to the communication channel used to carry data from one node to the next. Layer 3, the Routing layer, routes data through intermediate network nodes from the source to the destination. Layer 4, the Transport layer, is responsible for reliable end-to-end delivery of data to the end user.



For more information on individual layers and their functions, the reader should refer to a standard text on data networking and the OSI model.<sup>15</sup>

## Technical Objectives: The Challenge of Defense Networking and Interoperability

To assess the current state of and recommend future directions for the defense network, it is important to characterize the technical objectives of the network as they are generally understood. The following properties of an integrated network of networks are critical or highly desirable. An effective and interoperable DOD network:

- Satisfies a well-documented minimal set of user performance requirements, referred to in this chapter as the hard core network services, at almost any time and any place without interruption. The hard core network services are expected to provide and maintain communication capabilities in tough environments and are selected to be adequate for successful operations.
- Beyond the hard core network services, offers a larger set of network services that can be provided most but not all of the time, where conditions permit, supporting desired but not mission-critical functions.
- Can be deployed in stages and spirally evolved while maintaining support of DOD communications needs.
- Provides assured interoperability across different physical modalities (wired, wireless, and satellite networks) and across different military services and agencies.
- Efficiently supports Internet Protocol (IP) packet switching as well as direct (circuit) connections.
- Supports application quality of service (QoS) requirements by satisfying a set of well-specified service level agreements covering metrics such as throughput minimums, time deadlines, and error/loss probability.
- Maintains a rapid recovery time, for example from link or node failures. Wired and terrestrial wireless networks have recovery times of 50 to 150

---

15. For example, see *Data Networks* by Dimitri P. Bertsekas and Robert G. Gallager, Edition: 2, Prentice Hall, 1992; or *Communication Networks: Fundamental Concepts and Key Architectures* by Alberto Leon-Garcia and Indra Widjaja, Edition: 2, McGraw-Hill Professional, 2004.

milliseconds. Geosynchronous satellite networks and networks in extremely challenged environments have recovery times of approximately 1 second.

- Has application-appropriate end-to-end data transmission delays that do not vary excessively. Delay variation is excessive when it causes higher level transport and application protocols to become inefficient or fail.
- Provides security mechanisms that appropriately mitigate the risks associated with denial of service attacks, traffic analysis, data corruption attacks, and so on.
- Provides multi-level security to enable network sharing among disparate users in joint DOD and coalition operations.
- Uses Service Oriented Architecture (SOA) approaches where appropriate, such as in areas with high bandwidth and low latency service levels.
- Is affordable.

These technical objectives convey the complexity of the interoperability challenge. Interoperability is not simply a matter of assuring that all network elements conform to IP version 6 (IPv6).

## **The Current Defense Network and Directions for Development**

Three communication modalities make up the current defense network: wired, wireless, and satellite communications. While the goal is an integrated network that works seamlessly between users, it is not appropriate to dictate a common homogeneous network architecture across the three modalities, for both technical and cultural reasons. Instead, the networks for each modality should be individually designed and optimized, consistent with an interconnection architecture that makes them interoperable.

In each of the modalities, the current defense network uses largely commercial technologies and protocols at layers 3 and 4. This approach, although good for affordability, faces significant challenges. Commercial solutions are not well-matched to the issues faced by defense networks. The defense network is often highly congested, operates in difficult environments (e.g. wireless networks with poor propagation and lacking fixed infrastructure), and must provide highly reliable service to the most challenged users. These extreme cases, which are particularly prevalent at the defense network edge, are normally not handled by commercial networks. Similarly, commercial solutions that are largely oriented to

a wired network do not interoperate well across heterogeneous modalities. An example of this is the need for proxies to enable the Transport layer protocol to function across satellite communication (SATCOM) links. As a result of challenges like these, the current approach of using largely commercial layer 3 and 4 protocols and network equipment is insufficient to achieve the vision of the future defense network. Substantial DOD research and development is needed to augment or alter commercial solutions; this investment is required before future large systems are procured.

The following sections highlight developments needed in each modality to support a truly integrated network of networks. The time to develop these solutions must be factored into program planning for future network acquisitions.

### ***Wired Networks (Fiber and Copper-based)***

Of the three modalities, wired networks are the most mature. Commercial fiber network technology is in large part directly applicable to defense networks. Few changes to commercial equipment are required for defense applications. The following are areas that will need further development:

- The commercial world is moving toward a hybrid IP packet switching and Layer 2 circuit switching. Hybrid designs are attractive because an all-IP network does not efficiently support applications such as very high data rate virtual private networks (VPNs) for enclaves and very large streaming transactions. To take advantage of these developments, DOD should track and adopt, where appropriate, promising commercial progress in “Carrier-Class” Ethernet at 40 and 100 gigabits per second (Gbps).
- Military applications, more so than commercial applications, will need to send large files between sensors, archives, data processing facilities, and end users. Low cost, agile connections are needed that can handle these large burst transactions. Agile circuit-based transport mechanisms, such as “flow switching,” should be investigated to support these applications and incorporated into the network design if appropriate.
- Fiber networks have demonstrated efficiency and low-cost for high-speed commercial applications, but they have security vulnerabilities that have not been adequately addressed. Research and development of an appropriate security architecture is needed if DOD plans to use these and future generations of fiber networks.

- Access network architectures are evolving quickly, with rapid progress toward higher rates and lower costs. This may have important implications for information management and flow architectures of C4ISR systems (command, control, communications, computers, intelligence, surveillance, and reconnaissance). Investigation is needed on ways to incorporate advanced access networks into C4ISR architectures.
- Internetworking between wired networks and other modalities—wireless and satellite communication—causes significant problems. Research programs to solve these problems are urgently needed. The time to modify wired network designs and equipment in accordance with cross-modality internetworking solutions must be factored into the network development baseline.

### ***Wireless Networks, with and without Infrastructure (Mobile ad hoc Networks—MANETs)***

Despite significant past DOD and commercial investments, and the recent developments of wireless networks by the communication and information theory researchers, particularly those that use multiple antennas for beam forming and to fight multipath fading, wireless network technology is still immature in two critical areas for the envisioned defense network. At Layer 1, the physical communication link, it remains challenging to support a wide range of waveforms and operating frequencies in a single cost-effective power-efficient radio set. At Layers 2 and 3, it is unknown how to build MANETs (mobile ad-hoc networks) that offer the throughput and connectivity guarantees and the efficiency and scalability needed for tactical operations.

#### **Layer 1**

Fundamental research in recent years has led to significant physical layer improvements in radio communications, especially through the use of multiple antennas for beam forming and to fight multipath fading. However, radios and waveforms used in defense networks must continue to improve their ability to maintain connectivity and performance at the physical layer under battlefield conditions, where the wireless channel is highly impaired.

The defense network faces a significant wireless Layer 1 interoperability challenge due to the wide range of waveforms and operating frequencies used by current and planned wireless networks. Supporting multiple waveforms and

operating frequencies in a single radio set (a software defined radio) remains challenging for several reasons. Progress is needed in individual components such as filters and power amplifiers to achieve the necessary combination of performance, power efficiency, and tunability. Antennas have not yet been developed with the required wideband gain characteristics. It is expensive to build sufficient processing capacity and waveform software into a radio to support the desired range of current and future waveforms.

There is an immediate need for innovative network solutions that enable radios operating at different frequencies and with different waveforms to communicate with each other through their respective network connections. Gateways that provide data connectivity between the networks are just the first step. Critical services for interoperability include discovery, naming, authentication, authorization, and similar functions that enable users to effectively exploit data connectivity. Widespread availability of such services would dramatically reduce the cost and development challenges created by high physical layer flexibility and agility requirements.

### **Layers 2 and 3**

In tactical wireless networks, channel conditions and network topology can change rapidly. The network must efficiently manage communications over shared, dynamic, and often unreliable resources. The most extreme version of these challenges arises in MANETs (mobile ad-hoc networks), which lack the cellular base stations and similar infrastructure used in commercial networks to simplify the solution of analogous problems. No comparable commercial counterpart exists to DOD MANETs, which implies that a large development and experimentation task lies ahead. Specific MANET challenges include the following:

- **Assured throughput:** Ad hoc wireless networks provide no assured delivery and service guarantees. They often do not work well, or at all, in difficult environments. The standard approach of nearest-neighbor routing results in diminishing throughput as network population increases and is not scalable. Smart routing schemes are needed to achieve throughput scalability. However, many proposed schemes for sustaining throughput need geolocation information and node trajectory predictions, which are challenging to provide reliably in battlefield conditions.
- **Efficient routing:** Node mobility in MANETs results in rapid changes to the network topology, a situation not encountered in any commercial networks. Frequent link status updates sometimes consume most of the

capacity available. The network may make bad routing decisions or even become unstable due to the inability of the routing layer (Layer 3) to keep up with rapid changes.

- Assured connectivity: Disconnections are likely to occur unless the population of nodes is sufficiently large or their motions dictated to maintain connectivity. Neither of these requirements is acceptable for general defense mission profiles.
- Reliable data delivery: A communicating pair of nodes may be temporarily disconnected due to topology changes; packets may be dropped or channel capacity may be temporarily reduced due to mobility-induced fading. These effects significantly impact the performance of Transmission Control Protocol (TCP). Slow starts, time outs, and session terminations are common. The alternative of using User Datagram Protocol does not provide reliable data delivery. These problems prevent the use of typical IP services end-to-end over MANETs.

An aggressive program will be needed to solve the throughput deficiency, routing, and connectivity problems of MANETs. This will entail reworking the mobile infrastructure-less wireless network architecture, from the Link layer to all higher layers. This new architecture must be able to provide service guarantees for critical hard core network services. Specific areas for development include the following:

- Physical layer: Act proactively to maintain critical connections, through methods such as relay node insertion before disconnection, antenna beam forming, and nulling.
- Routing layer: Distinguish dropouts from congestion and share this information and capacity information with the Transport layer protocols. Share information with physical layer about which links are critical. Route effectively when network links are dynamically random on-off channels. Improve mobile addressing and routing to minimize stress on back-haul capacities (beyond mobile IP), and route effectively over dynamically random on-off channels.
- Transport layer: Provide stable performance and effective congestion control over connections that have dynamically changing capacity.

## *Satellite Communications*

Satellite communication systems can be categorized in terms of their support for IP networking. For example, the proposed Transformational Satellite Communications System (TSAT) and the Infrared Imaging System (IRIS) are IP-based systems while most heritage satellite systems are not. Heritage systems present different challenges from IP-based SATCOM systems when asked to interoperate with other network modalities.

### **Heritage SATCOM Systems**

SATCOM systems that were not originally designed to handle IP include advanced Extremely High Frequency (EHF), Wideband Gapfiller, and many others. These systems have difficulties interconnecting with IP networks. Gateways and protocol encapsulation can be used to patch over the incompatibility, albeit with significant performance degradation. For example, the number of access points is limited to the number of uplink channels in the quasi-statically assigned channelized (circuit) access architecture, which is very limiting. If TSAT or an improved version that is specifically designed to support IP is not deployed, there will be a significant weakness in the SATCOM part of the envisioned defense network, especially in the areas of interoperability and jam resistance.

### **Future Extremely High Frequency Satellite Network**

The task force recognizes a future requirement for protected EHF satellite networks that is a jam-proof and robust transport network (a substrate core network as in a wavelength division multiplexing fiber network) whose primary function is the interconnection of access/tail networks and core-fiber networks. A few SATCOM terminals may reside in end-user platforms but that is not its primary usage. Such a satellite network is analogous to core-fiber networks to which a few high-end users having direct access. However, there is no equivalent system in the commercial sector. The critical role of such an EHF SATCOM system at the center of the global defense network creates specific architectural and feature requirements if the overall network is to achieve its performance, scalability, and security goals. The following are critical challenges facing the design of these systems:

- In some EHF SATCOM system concepts, access to the satellite network is via circuit setup similar to dialup point-to-point protocols, except the rate assignment is dynamically variable depending on channel conditions and capacity demands. Quasi-static (slowly changing) demodulator

assignments are controlled by a dynamic bandwidth resource allocation system, and other design features place hard limits on the total number of connections, typically a few thousand access points. This is a significant constraint on the system architecture and concept of operations of the overall defense network, preventing proliferation of small SATCOM terminals and eventual ubiquitous use of the EHF SATCOM system.

- In any capacity-limited SATCOM system, all traffic flows—except those with the highest priority—experience rapidly changing link capacity due to dynamic bandwidth resource allocation and channel-fading effects, which are especially strong in high-frequency bands such as EHF. Rapidly changing link capacity creates significant problems at layers 3 and 4 that must be addressed both in the EHF SATCOM system and in other network modalities that interoperate with it.
- Layer 3 problems caused by rapidly changing link capacity include routing inefficiency, potential routing instability, and failure of current border gateway protocols (BGPs).
- Layer 4 problems caused by rapidly changing link capacity include poor performance of TCP, a problem exacerbated by rapidly changing and high-link delays of SATCOM connections due to propagation, buffering, and processing.
- Current solutions to the layer 4 problems associated with TCP over SATCOM links rely on installing performance-enhancement proxies (PEPs) at the satellite gateway terminals. Since most application flows are encrypted before they reach the gateway terminals, decryption and re-encryption is required which seriously impacts interoperability, rapid connection setup, and key management. Some significant PEP networking problems remain to be solved, such as Network layer (L3) rerouting upon link failure.

The following are specific areas of investment to help overcome these problems:

- A random multiple-access mode or other contention-based algorithm should be provided to allow EHF SATCOM access by an unlimited number of potential users at proportional rates. Such an access mode would enable the satellite network to give many more users the ability to reliably send critical short burst messages, whose size is of the order of a few IP packets, without increasing the total required SATCOM capacity.



This capability is very attractive given the cost of such a high reliability satellite network.

- Specific protocols for assuring QoS will be needed. QoS in commercial core-fiber networks today is implemented via over-provisioning. Given the projected cost of new satellite networks, such over-provisioning is not affordable. Specific protocols for delivering satellite network QoS should be developed.
- A comprehensive analysis of the vulnerability of a protected EHF SATCOM network to adversarial attacks is needed. This must include a time-statistical model of EHF communication channels under benign operations and under adversarial attacks. Then this model should be used to examine how upper-layer protocols are affected.
- Since the prime function of the required satellite network is interconnection of terrestrial networks, its internetworking architecture must be well designed and articulated. New internetworking protocols are necessary since commercial BGPs do not provide enough state information across network boundaries to deliver the necessary end-to-end QoS.

### **Commercial SATCOM as Augmentation**

DOD augments current military satellite constellations with commercial capabilities, both in peace and at war. Currently, nearly 80 percent of DOD satellite communications on a day-to-day basis are commercial, embedded in intelligence systems such as Trojan Spirit (C Band), command and control ( $K_u$  band), and maritime, “on the move” and command communications (L Band). The Army’s Joint Network Node (JNN, Warfighters Information Network-Tactical (WIN-T) increment 1) is fielded to 85 percent of the Army and the Marine Corps’ Support Wide Area Network and Line-Of-Sight Support Wide Area Network use commercial  $K_u$  band for fighting units for corps, division, brigade, battalion, and in some cases company communications. The capabilities used include voice, data, video, and collaboration.

Unfortunately, the commercial SATCOM systems are vulnerable to a range of disruptive attacks such as jamming, interference, electro-magnetic pulse, direct kinetic attack of ground components, and so on. In addition, the use of commercial grade proxies at satellite gateways can present serious difficulties for secure connections. Fortunately, all current commercial satellite communications operate at  $K_u$  band and below with much smaller channel variations than protected defense

EHF SATCOM systems and thus present fewer problems for IP routing and Transport layer protocols.

Augmentation of DOD SATCOM systems by commercial satellite capability can be expected to continue even as newer, much more robust DOD constellations are fielded and improved. With the exception of future protected EHF SATCOM systems that can hop over a large frequency band, all existing and planned SATCOM systems (commercial or DOD) are inherently vulnerable to jamming attacks. Important missions should not rely entirely on these systems for critical communications. A contingency plan and operational exercises are needed to prepare for the possibility that use of these SATCOM systems may be denied.

### **Space Backbone**

Optical space communication is the key technology that allows the interconnection of communication satellites into a global coverage space network. An optical inter-satellite backbone can operate at a very high rate, commensurate with fiber capacities, and can support both communication traffic and ultra-high rate sensor read outs and relays. The space backbone concept is a powerful architecture that will substantially lower space system costs if proper sharing across missions is achieved. This concept requires that the access and network transport architecture be designed for sharing. While small- and medium-volume communications are best suited for IP based networking, large transactions such as sensor readout will significantly benefit from dynamic circuit-flow switching on-demand. Thus, a space network architecture that is the mirror image of the future ground fiber network architecture is desired.

### ***Issues that Cross All Modalities***

The following are critical areas that need specific attention:

- End-to-end hybrid network: IP packet switching will not be sufficient to support all application and user needs. Proper roles should be determined for IP and Link layer (L2) switching, with the objective to create and adopt a flexible, evolvable hybrid L2-switched and IP network architecture (beyond IPv6). New transport mechanisms such as flow switching should be investigated, as well as architectures that effectively support high-end high-rate users.
- User and application visibility into the network: Unlike current networks, which function largely as a black box, a mechanism should be developed

to appropriately inform users of the rate and quality of their network services and properly manage their expectations. This is particularly important for infrastructure-less wireless networks and SATCOM networks with dynamic bandwidth allocation.

- **Transport protocols:** The effects of rapid-channel bandwidth and latency variations on upper-layer protocols need to be quantified. TCP may need to be supplanted by innovative protocols better suited to the defense network environment. Such innovative protocols may exploit support from endpoints, routers, and network gateways to provide end-to-end reliable data delivery and effective congestion management in a heterogeneous network that combines black core, multihop wireless, and high-delay congested SATCOM links.
- **Black core performance and manageability:** Current end-to-end cryptography solutions such as a High-Assurance Internet Protocol Encryptor (HAIPE) lead to high response times and opaque flows that are challenging to manage. Improved methods are needed that combine necessary security with support for other network requirements.
- **Information assurance:** In the balance between interoperability and information assurance, there is a fulcrum of risk that balances the immediate or time-sensitive need of the warfighter against the information assurance and protection of the network and its associated data. From a warfighter perspective, information assurance risk—like any other operational risk—should not only be accepted, but also expected in order to trade this assurance against the operational benefits of propagation of critical information and communication. Finding an appropriate balance between these needs is essential to success.
- **Technical information about network designs:** DOD should have full technical and operational information about all DOD networks serving critical strategic, tactical, and operational users. This information must include architectures of individual networks and subnetworks and government rights to software including source code where needed. This is key to both interoperability and to information assurance. The current lack of this type of information impedes DOD's ability to interoperate current systems or efficiently acquire future systems. This view may be at odds with some forms of performance-based contracting, but when the value of interoperability is properly weighed, it is likely to dominate the factors that suggest a lower degree of openness.

- Business case for software and IP vendors: DOD should develop new acquisition processes that provide a sustainable business case for suppliers whose primary contribution is expressed as software or intellectual property. A large portion of the innovation required for the envisioned future defense network is of this type. This innovation is hampered by current acquisition processes. Incentives should be structured to encourage innovative solutions, efficiency, interoperability across suppliers, reuse of certified components, and retention of key personnel to support future evolution of acquired software products. A particular challenge is to provide a sustainable business case in situations where government access to source code is required for interoperability, information assurance, or other reasons. Licensing arrangements from commercial industry may provide useful models for solving this problem. Software reuse is also key and will enhance heterogeneous network interoperability.

## Network Management and Internetworking

The heart of the interoperable defense network problem is in its internetworking architecture. There is no analog of this network situation in the commercial sector, primarily due to the dynamic nature of defense edge networks and the requirement for information assurance.

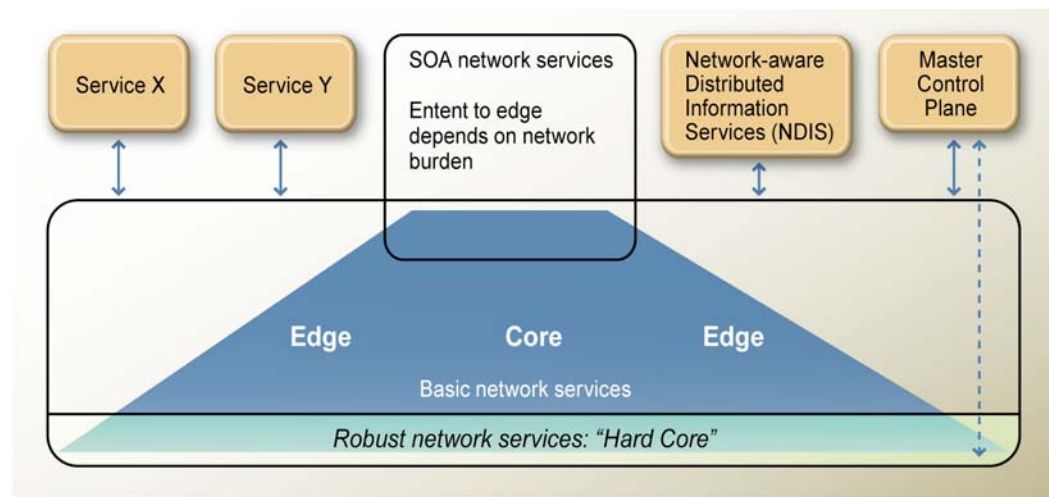
The envisioned defense network will seamlessly integrate multiple disparate modalities—wired, wireless, and satellite communications—with very different system properties and network architectures. The resulting network is dynamic, with critical parameters changing on a time scale of milliseconds to seconds, due to open-air channel fading, mobile users, heavily choked tail links and priority preemptions. Unlike the Internet where some dropped packets or time delays are tolerated, for critical defense missions, a high QoS is required with accurate deadlines and guaranteed delivery. This challenging problem is further exacerbated by often heavily choked tail links in the network.

As a result of the defense network's dynamic nature and high QoS and efficiency requirements, network management is vital for satisfying user requirements. **Effective network management and control may well be the Achilles' heel of the integrated global defense network** and is the most critical technical issue to be addressed for the realization of a high-performance integrated heterogeneous defense network.

Network management can be broken into two functions. Network diagnosis is the sensing of network states, particularly congestion, failures, or impairments. Network control is the assignment of resources to applications, flows, or users and the replacement or bypass of faulty equipment when necessary. The two functions are incorporated into a collection of resources and protocols called a network control plane. The network control plane supports both centralized oversight by a network operations center and distributed automatic control mechanisms.

Each communication modality has unique properties. For each one, a unique control plane architecture and supporting systems has been developed, tuned to its specific dynamics. Replacing these with a common network management architecture for all modalities, while desirable, would result in poor network performance. Moreover, retaining subnetwork-specific network management systems is desirable for reasons of reliability, survivability, scalability, and extensibility.

Nevertheless, providing end-to-end service guarantees and high efficiency will need some form of global coordination. The task force concluded that efficient operation of the overall integrated network will require a powerful master control plane (MCP) to coordinate among the individual network control planes, as shown in Figure 2. The MCP is responsible for internetworking and QoS networking, QoS assurance, and information assurance across multiple network modalities.



**Figure 2.** Proposed network architecture

### ***Role of Commercial Network Management Technologies***

The envisioned defense network cannot rely substantially on commercial network management technologies.

- In commercial networks, overprovisioning is often used to ensure QoS. This is not a viable option in a defense network owing to the high cost of SATCOM and tactical wireless capacity. High congestion and strict QoS requirements make the defense network control plane significantly different and more challenging than commercial control plane solutions.
- In commercial networks, the interconnection of different networks is usually done via BGPs. BGP designs are driven in part by the desire of interconnected commercial operators to shield proprietary usage and performance data from each other. As a result, commercial BGPs provide little knowledge of network states across network administrative domains. The defense network requires much greater information sharing for efficiency and end-to-end QoS.
- Commercial wired networks are much less dynamic than the defense network, which is shaped by open-air channel fading, mobile users, heavily choked tail links, and priority preemptions. As a result, commercial “ready to use” control planes and management approaches do not have the necessary level of sensing and control agility.

Although commercial components should be used where possible, DOD-specific network management architectures and systems will be required.

### ***Master Control Plane***

The defense network MCP coordinates resource allocation across heterogeneous subnetworks to assure the overall integrated network meets operational needs. The following are critical and necessary functions to be performed by the MCP:

- Interface to the control planes of heterogeneous subnetworks, providing appropriate diagnosis and control functions across the integrated network.
- Use the subnetwork control planes to automatically provision and reallocate resources (transmission and storage capacity, QoS guarantees) across users, organizations, applications, and flows as operational conditions change in accordance with policy.

- Enable a commander's intent and network management policies to be expressed at a high level and changed dynamically.
- Exercise admission control for subnetworks, high-capacity circuits, and priority users.
- Sense congestion, anomalies, or unexpected usage patterns; and as necessary, isolate misbehaving, failed, or compromised subnets while adjusting routing to minimize the impact on the rest of the network.
- Provide information about network topology, status, and behavior to network-aware applications and information services enabling them to optimize their network usage.
- Operate in accordance with security requirements and provide the functions required to support detection and response to internal and external attacks. Maintain network security through sensing congestion, anomalies, unexpected network usage patterns, and faults—and if necessary, isolating misbehaving and/or compromised subnets.
- Reroute around problematic or failed subnets.
- Implement robust control messaging over the network to maintain time criticality and security requirements.
- Ensure reliable operation during network upgrades.

To achieve this vision, a first step is to establish a research and development program to explore the architecture for a defense MCP. Interfaces between the control planes for all network modalities need to be defined including observables, controllable parameters, and performance monitoring. **The overall architecture of internetworking satellite, wireless, and fiber networks must also be addressed.** The architectural stress points will be on interoperability of higher-layer protocols (Routing layer and above) and border gateway protocols and proxy service at gateways.

An architecture migration path to support the MCP is needed for all networks—existing and planned. A hybrid approach may be possible where part of the MCP is centralized for the slow processes in the network, such as provisioning, massive failure recovery, admissions of new subnets, and pre-computation of quasi-static circuit setups. For the fast processes, such as fast flow setups and timely diagnosis of the health of network subsystems for integrity, the MCP functions may be distributed. Finally, performance goals and metrics are needed for end-to-end performance tests of the MCP and the integrated network itself.

### *Interconnection Switches, Gateways, and Proxies*

Connection of networks can be done at different layers. If the networks are very similar, such as two Ethernets, interconnections are made at L2 via switches. Usually interconnection at L2 is simple and network performance does not suffer as a result.

Many IP networks are connected at the Routing layer using border gateways with BGP. The problem with BGPs is that usually they do not reveal the internal state of the subnets, owing to commercial competitors not sharing their network loading and business information with others. When a master control plane concept is introduced to the network, this problem can be fixed by having the master control plane negotiate and orchestrate internetwork flows and route optimization.

Performance enhancement proxies are one frequently suggested solution to the internetworking problem, particularly between SATCOM and fiber networks. While this may be the right solution, the following problems need to be addressed:

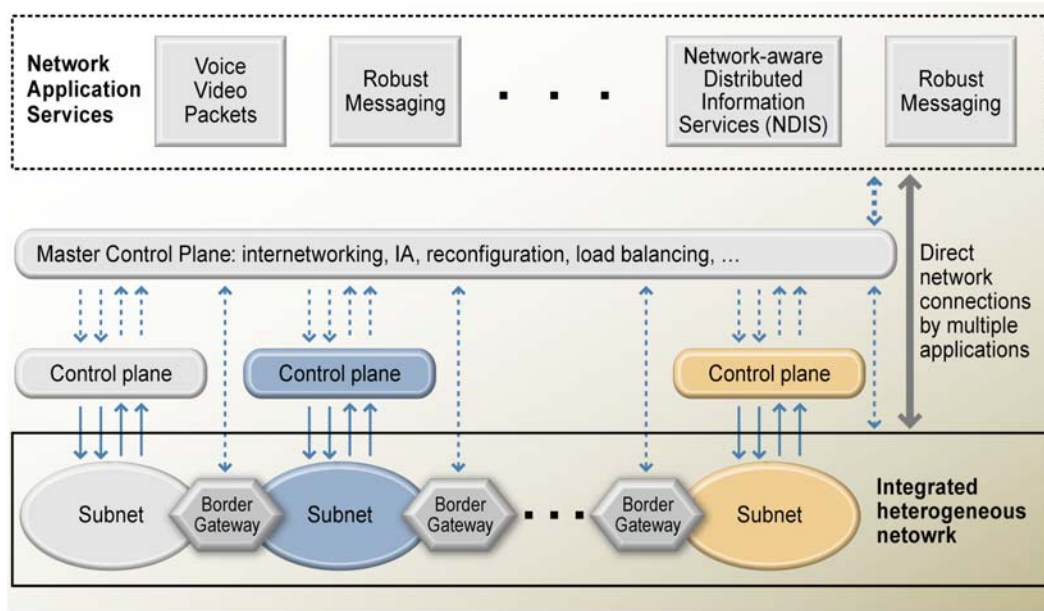
- Interconnection of subnets should be done at the lowest possible network layer whenever possible and efficient. The master control plane should be responsible for sensing the global states of each subnet and orchestrate efficient interconnections. BGPs that are used should be improved to include more visibility into the internal states of each subnet to facilitate efficient routing, load balancing, and congestion control.
- PEPs may require all gateway nodes to possess the crypto-keys of all potential users passing through the gateway and may lead to an unwieldy and large list of keys for look-up and excessive delay at session initiation.
- It is hard to guarantee time deadline delivery passing through a PEP service unless the computation resources at the PEP are over-provisioned.
- PEPs are usually point-to-point processes over links and it is hard for the Routing layer (L3) to reroute in case of failure or congestion. This problem of rerouting must be addressed if PEPs are used in a defense network.

### *Network-aware Distributed Information Services*

In the future, the proliferation of information and data services out to the tactical edge will generate and consume vastly more bandwidth. This bandwidth explosion will saturate the backhaul network, especially if it is via SATCOM. To be successful, current centralized server-based applications will need to evolve into network-aware services that adjust their behavior as the network changes to



maintain critical services (Figure 3). Network-aware distributed information services (NDIS) have a distributed architecture to prevent disconnection and also discover and manage network resources based on proximity.



**Figure 3.** Network-aware distributed information services

There are no commercial analogs for this service. It must be developed by DOD based on the properties of each network modality. Development of a common architecture and protocols for NDIS deployment, support, and management is needed. Co-locating NDIS support platforms with gateways that connect subnetworks is one option for investigation.

At all times, users should be informed of the rate and quality of network services they will be getting and their expectations properly managed. The system may also add the ability to get information from closer, local sources rather than from central nodes. **The manageability and flexibility of the network at the enterprise level will suffer if each application vendor or service develops and deploys their own stove-piped NDIS protocols and distributed application host platforms.** Common protocols and platforms will enable new information services to be developed and deployed much more quickly and cost effectively. For example, new software applications required by changing threats or operational doctrines could be distributed wirelessly to hardware platforms that are already deployed and supported in the field.

When implemented, the master control plane and individual network control planes should expose information about network topology and resource availability to the NDIS software layer. This information is needed so applications can adjust their behavior and therefore optimize services provided to the end-user as network conditions change. A network-aware distributed information service near the network edges can adjust its behavior as the network changes to maintain critical services on the edges of the network. Research is needed on the appropriate abstractions, interfaces, and protocols that will support sophisticated NDIS applications without constraining network evolution or compromising security.

## **Combining Reliability and Affordability**

A critical difference between the envisioned defense network and commercial networks is the high reliability it provides in order to ensure mission success. The commercial sector is motivated by profits and therefore aims to provide good service to their customers only 95 to 99 percent of the time. To provide satisfactory service for the last few percent is very costly—up to 10 or perhaps 100 times more—and is not justified in current business models. In contrast, it is vitally important for the defense network to provide service to all users no matter what the conditions.

The technical objective of high reliability creates a significant affordability challenge for DOD. The following sections describe approaches to mitigate network costs while still providing the necessary level of reliability.

### ***The Two-tier Network***

The future defense network should offer two tiers of service within a single network, as shown in Figure 2. The first tier is a robust minimum “hard core” that meets the minimal requirements necessary for successful defense operations. This tier will have modest rates but solid connectivity at all times with low delays. The second tier is an enhanced network, which is less robust but has higher rates and supports data-intensive functions such as Web browsing and video services.

The two-tier approach mitigates cost pressures by relaxing the requirement to provide enhanced service levels to users and platforms that are in highly challenged situations. Such situations include aggressive jamming, underground operations, and high-threat levels requiring extreme low probability of detection. It is an accepted rule of thumb that supporting the last few percent of users/situations drives a disproportionate share of the network design and build costs.

The two-tier approach has significant benefits for network evolution as well. Networks and network technologies evolve at a very rapid pace, especially in the commercial sector. Given this situation, it is vitally important for the defense network architecture to be crafted in a way that both accommodates the best of current technologies and protocols, and also anticipates and adapts to future technologies and protocols. DOD should be prudent and refrain from predicting future standards and technologies for networks. In the two-tier architecture, the enhanced service tier can be enabled to evolve much more quickly than the hard core, with much higher reuse of commercial components, without compromising the reliability, security, and other necessary attributes of the hard core.

### ***Service Oriented Architectures***

Among its other attributes, service oriented architectures (SOAs) can serve as an application-layer mechanism for improving reliability and reducing network cost.<sup>16</sup> It provides these benefits by dynamically binding service customers to service providers that are nearby in the network. Each service request thereby consumes fewer network resources and is less likely to be affected by link outages or congestion. As an application layer mechanism, SOA's reliability benefits are limited if the underlying network transport has connectivity, physical layer interoperability, congestion, or delay variation problems that interpose between service customer and service provider.

Current implementations of SOA are effective only if the underlying network provides low latency, low bandwidth-delay variation, and high bandwidth, for example in fiber networks. Latency is an important parameter for current SOA implementations due to the number of network round-trips associated with discovery, negotiation, and service binding. Low latency and low bandwidth variation are important due to the use of TCP for data delivery. High bandwidth is important due to the use of Web service and representational state transfer paradigms, which do not seek to minimize the amount of data transferred.

Successful deployment of SOA in more challenging network environments, such as wireless or satellite networks, requires quantifying the network burden of SOA implementations. This is not well understood at present. Critical unknowns include data rate demands, delay tolerance, and the number of roundtrips for service

---

16. SOAs are explored more fully in Chapter 4.

set-up and usage. For example, many current SOA implementations time-out (i.e. sessions dropped) when network delays at levels common in DOD edge networks are encountered. In many cases the binding process takes a many as 12 roundtrips.

Before a full-up SOA paradigm is pushed all the way to the tactical edge, the government should immediately put in place a SOA-network-performance investigation effort to quantify the network burden and network QoS requirements for various SOA implementations. It may be possible that a reduced capability implementation of SOA can be developed to work effectively in defense networks that provide low data rates or high latency. Such a solution may require the presence of an intelligent master control plane and also support from gateways at the interface between the high-rate backbones and the low-rate edge network that act as the network resource and service broker.

### *Survivable Networks*

Network vulnerability to attacks grows with level of integration, interoperability among modalities, and number of users. While good security architectures must be included early in the conception of the network architecture, no network can be assumed to be invulnerable. Thus, the operational decision to use a network for a specific function is a matter of risk-benefit management.

In the balance between interoperability and information assurance, there is a fulcrum of risk that balances the immediate or time-sensitive needs of the warfighter against the information assurance and protection of the network and its associated data. From a warfighter perspective, information assurance risk—like any other operational risk—should not only be accepted, but also expected in order to trade this assurance against the operational benefits of communication and propagation of critical information. Regardless of where the balance lies between these needs, there must be a healthy discussion and understanding that the end user requirements of the warfighter tip the scale in favor of the operational mission. The alternative questions the fundamental value of the network.

While networks cannot be made totally bulletproof, some existing techniques cited here may substantially diminish their vulnerabilities. DOD should pursue these and others that can allow more robust network service over an unreliable

network substrate. For example, the concept of “Byzantine-Robust” networking should be fully investigated.<sup>17</sup>

### **Akamai and Similar Architectures**

One common attack on a network service is to send many session requests to the server providing that service, tying up its resources until it can take no more new sessions. The Akamai architecture and its equivalents defend effectively against this attack.

In this architecture, there are typically many servers providing a given service (over 2000 in commercial Akamai deployments). Each server acts as a surrogate for the important server to be protected. The important server never directly communicates with the outside world, only through the surrogates. When one surrogate server is overloaded, the load-balancing feature of the system allocates new sessions to other surrogates. Thus, the attacker will have to take down all the surrogates (which is very difficult) to be successful in disabling the service. The Akamai implementation of this approach has a “zero time-to-live” feature in the surrogates so that all sessions are terminated when there is no pending transaction. This is not the practice with typical servers today (time to live is usually 5 minutes). The zero time-to-live feature prevents attackers from creating more and more idle sessions to jam the system.

This architecture makes the attackers’ efforts much more difficult by orders of magnitude. However, this technique is only as secure as any one of the surrogates. If one is compromised (electronically or physically), it can be used as a devastating attacker and can bring down the important server it is designated to protect.

This method is appropriate to protect important servers that if brought down will be an inconvenience or an annoyance. Servers in this category may be a brokerage firm’s transaction server, or the Internal Revenue Service server. This method is not sufficient to ensure survivability of life- or mission-critical servers in the defense network.

---

17. Byzantine robust networking is a possible mode of network operations, if designed in, that will allow successful data transfer even though a fair fraction of network elements and resources are denied or broken down.

## Reliable Networking over Unreliable Networks: Diversity Routing and Network Coding

Even using the best available security approaches, the defense network cannot be considered totally bullet-proof. For critical network services, it may be appropriate to treat the network substrate as basically unreliable. Even with such an assumption, reliable data communications can be achieved via the two following techniques:

- Diversity routing spreads information over disjointed delivery paths via error-correction coding. This increases reliability at the expense of increased network resource consumption. Diversity routing can support hard time deadlines. Some network topologies are better for diversity routing than others. This creates a need to optimize network design as a function of protocol choices at the higher layers.
- Network coding is a new technique that uses almost no buffering, no route computations, and no flow control. It exploits all available routes simultaneously. The use of appropriate security on each link, such as hash functions, can provide Byzantine robust networking.<sup>18</sup>

## Summary of Technical Findings and Suggested Future Directions

The findings and conclusions presented here are consistent with the report *Federal Plan for Advanced Networking Research and Development*.<sup>19</sup> While that report mentioned problem areas for research, this report focuses, in addition to research, on the need for an overarching defense network architecture and the problems of internetworking.

While there are many DOD network programs that have substantively achieved their primary goals, such as the GIG-BE (GIG-Bandwidth Expansion), a

---

18. Byzantine robust networking is a possible mode of network operations, if designed in, that will allow successful data transfer even though a fair fraction of network elements and resources are denied or broken down.

19. National Science and Technology Council. *Federal Plan for Advanced Networking Research and Development*. Report of the Interagency Task Force on Advanced Networking, September 2008. Available at: <http://www.nitrd.gov/pubs/ITFAN-FINAL.pdf>

number of critical areas have been identified that need to be addressed. The tables presented in Appendix C summarize these areas for easy reference.

### ***A Heterogeneous Defense Network***

The defense network should be heterogeneous and accommodate multiple types of networks of different generations. Integration into a single interoperable network should be carried out via gateways between disparate subnets and a master control plane.

Before a sensible, integrated heterogeneous defense network can be deployed, many difficult network problems need to be solved, particularly at or near the network edge and at subnet interfaces. There should be a sense of urgency to tackle these tough network problems now. The integrated defense network should support voice, video, data, hybrid IP, and circuit-based services. It should have two-tiered network services, as shown in Figure 2.

- The first tier is a robust minimum “hard core” network service necessary for successful defense operations. This service will have modest rates but solid connectivity at all times with low delays.
- The second tier is a much higher rate “soft” network, which is less robust but has higher rates and supports data-intensive services such as Web browsing.

### ***Technical and Operational Insights***

DOD should have: (1) full technical and operational insights into all DOD networks serving critical strategic, tactical, and all operational users, including architectures of individual (sub)networks; (2) government rights to software, including source code where needed; and (3) performance metrics, estimates, and verification in a variety of key scenarios.

This is key to both interoperability and to information assurance, and its current absence is impeding DOD’s ability to interoperate current systems and efficiently acquire future systems. This may be at odds with some forms of performance-based contracting, but if interoperability is required, this is clearly necessary.

### ***Architecture Developments***

DOD should address the critical outstanding architecture and technology issues of the core fiber network, infrastructure-less MANETs, and SATCOM networks.

Before a sensible integrated heterogeneous defense network can be deployed, many difficult network problems need to be solved, particularly those at or near the network edge and at the interface between subnets and different network modalities. These problems include the following:

- Tracking new network architecture developments in fiber networks and incorporation into the GIG new architectural features in a timely fashion. This entails the following steps:
  - Determine a proper role in a defense setting for IP and L2 switching; create and adopt a flexible, evolvable hybrid L2-switched and IP network architecture (beyond IPv6).
  - Promote research and development (R&D) to finish development of new transport mechanisms (such as flow switching) for large transaction, agile services.
  - Address optical network security architecture immediately.
  - Address network management and control of resilient and dynamic networks in situations not encountered in commercial applications.
  - Study access network architecture for high-end, high-rate users.
  - Address internetworking with SATCOM and wireless networks immediately.
- An aggressive program to solve the MANET throughput deficiency and disconnection problems. This entails the following steps:
  - Completely rework mobile infrastructure-less wireless network architecture, from the Link layer to all higher layers.
  - Pursue architectures that provide service guarantees for critical minimal core services; proactive network approaches such as relay node insertion before disconnection, and antenna beam forming and nulling might be used to maintain critical network connections.
  - Address areas where IP does not work or is deficient; e.g., need to distinguish drop-outs from congestion in the Transport layer (L4); create more stable Transport layer protocols over dynamically changing wireless link capacities; improve mobile addressing and routing to minimize stress on back-haul capacities (beyond mobile IP), and routing over dynamically random on-off channels.



- The critical outstanding architecture and technology issues of infrastructure-less wireless networks and some SATCOM networks. Steps include the following:
  - Determine a way to inform users of the rate and quality of their network services and properly manage their expectations, as depicted in Figure 3.
  - Introduce a random access mode for future EHF satellite networks to help scale the number of end-users with direct access to the system.
  - Generate a dynamic statistical model of the SATCOM channel to aid in the development of a heterogeneous network interconnection architecture.
  - Quantify effects of the rapidly changing channel to upper network layer protocols.
  - Rework all higher layer protocols. IP as used in commercial products should be modified or changed in different layers to enhance network performance.
  - Address difficulties in black/red interfaces and cryptography at network interfaces so networks will be interoperable and/or response time will not be unacceptably long.
  - Develop sensible hybrid IP and circuit on-demand switching architectures for on-board processing in satellites.
  - Develop efficient network-sharing architecture across missions. The stress point here will be the control plane and medium access control protocols

### *Master Control Plane*

**DOD should add to its architecture construct the concept of a master control plane as a key element to facilitate internetworking and information assurance.** An aggressive program for internetworking of disparate networks should be established. There are tremendous technical challenges to deploy an integrated heterogeneous network and make the disparate networks interoperable. The unique dynamic nature of the different defense network modalities and the need for QoS for some critical services make the problem very difficult. The concept of a master control plane to manage network assets, internetworking,

interoperability, priority and policy enforcement, access control, and security, is critical to the successful realization of this network, and should be fully explored.

This master control plane should be responsible for the provision of networked information services (transmission, nodal interfaces, and storage capacity), based on mission needs and externally injected policies. Operating this “information utility” requires a single operator responsible for the development, investment, and operation of the entity. This entails the following steps:

- Immediately establish a research and development program to explore the architecture of the master control plane.
- Define with all network modalities the interfaces between their individual control planes and this master control plane in areas such as observables, controllable parameters, and performance monitoring; and insist on up-front planning of all network modalities to interact with this master control plane.
- Develop performance goals and metrics and subject all elements of the network to end-to-end performance tests.
- Provide an architecture migration path by which all networks under development and evolution can be integrated into this heterogeneous network incrementally without major disruption and wholesale changes in architectures and protocols.
- Address the overall architecture of internetworking of satellite, wireless, and fiber networks. The architectural stress points will be on interoperability of higher layer protocols (Routing layer (L3) and above) and border gateway protocols and proxy service at gateways when necessary.

### *Service Oriented Architecture*

The government should consider carefully the use of SOA, paying particular attention to information assurance (IA) and the underlying network capabilities that are required to support it. Critical services do not have to and should not use SOA for real time command and control services, such as the fire control loop. For example, theater battle management core systems itself could be a SOA for the support, situational awareness, and collaboration piece, but not for real-time applications, reprogramming of sensors and munitions, network sensing and control, and critical messaging with time deadlines. **Due to the very heterogeneous nature of the different modalities that make up the defense network, there is no universal solution to achieving interoperability.** While using a service oriented architecture may assist with some interoperability issues,

many open questions concerning its implementation, especially towards the bandwidth challenged tactical edge, remain. The government should carefully consider the use of SOA, paying particular attention to IA and the underlying network capabilities that are required to support it. Steps include the following:

- Determine the network burden of SOA.
- Determine how far toward the network edge SOA can be supported.
- Develop “lightweight” SOA for the tactical edge.
- Develop SOA with an IA architecture. Proper use of SOA should neither diminish nor improve the security of the underlying network substrate. Critical network functions such as management and control should not use SOA, but use the most robust network mode for transport.

### ***Evolution of Networks***

DOD should be prudent and refrain from predicting future standards and technologies for networks.

Networks are by nature of different types and continually evolving. For example, the commercial sector is leading the charge in the architecting of a hybrid IP and Carrier-Class L2 switching network paradigm for the wired networks. The government should incorporate this change into its future networks and evolve its architecture alongside this and other future developments. The concept of gateways and master control plane when properly executed will allow incremental insertion of new modalities coming on-line into the defense network. Allowing heterogeneity is the key for continual evolution and improvements.

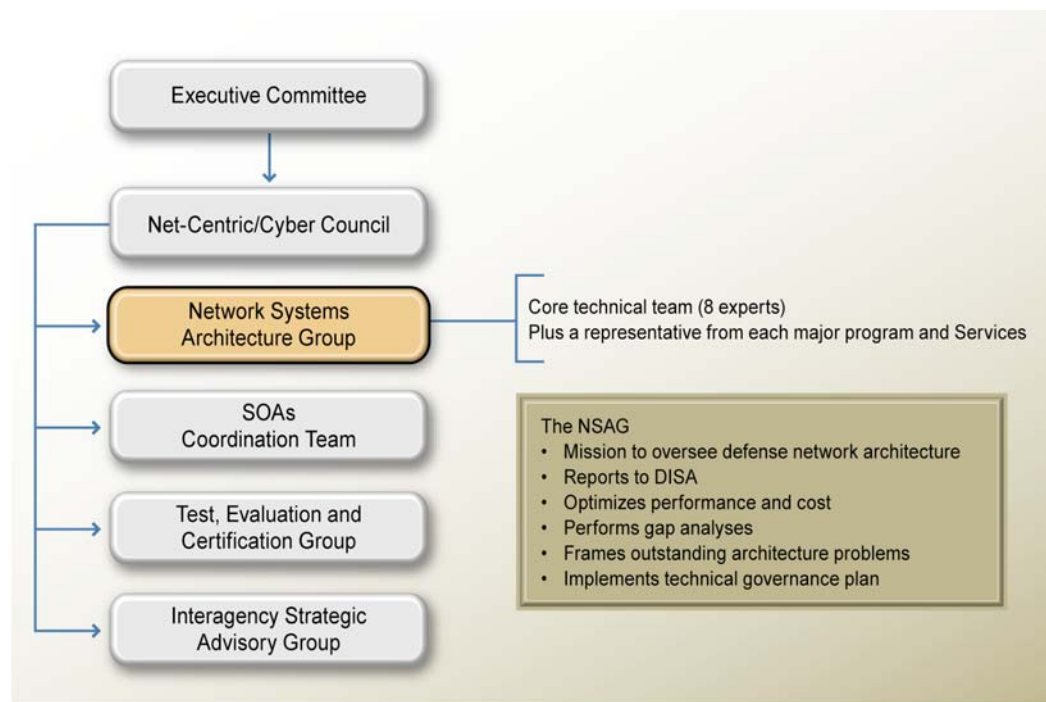
### ***Network-aware Distributed Information Service***

Deploy a network-aware distributed information service (NDIS) near the network edges to adjust middle-user behavior as the network changes to maintain critical services on the edges of the network.

The proliferation of information and data services to the tactical edge will generate and consume vastly more bandwidth in the future and will saturate the backhaul network. At all times, users should be informed of the rate and quality of network services they will be getting and their expectations properly managed, as shown in Figure 3. The system may also add the ability to get information from closer, local sources rather than from central nodes.

## Governance of a Heterogeneous Network

The Net-Centric/Cyber Council should charter a strong Network System Architecture Group (NSAG) to create and oversee an overall defense network architecture that is scalable and evolvable. The group, shown in Figure 4, should be independent of the individual programs and not tied to the industry suppliers. Network governance should be anchored with a technical core of approximately eight members who are augmented by representatives from each service and major programs.



**Figure 4.** Roles and responsibilities of a Network Systems Architecture Group (NSAG)

The major roles of the NSAG will be:

- Create and maintain an integrated heterogeneous defense network architecture, including road-mapping and planned evolution and insertion of new technologies and architecture features.
- Define and mediate interfaces between disparate networks, and in particular the mediation of fair and proper interfaces across different communication modalities and administrative domains.

- Analyze gaps and optimize high-level performance/cost, such as the gap between the state of current technology, architecture and requirements, and user expectations.
- Frame outstanding architecture problems, identify outstanding critical architecture problems, and recommend remedial plans to reduce procurement program risks, including R&D and reduction of requirements and user expectations.
- Recommend to the Net-Centric/Cyber Council a realistic roadmap toward the realization and evolution of the defense network and implement technical network governance plans.

While there are several current groups that perform some of these functions, they are not well coordinated nor are they fully functional and empowered. Members of this new group should have the following technical attributes:

- Deep technical knowledge of communications and networks.
- Prior experience in the conception, design, and implementation of large complex networks.
- Good understanding of the current state and future directions of commercial industry.
- Familiar with the defense community and their concepts of operations and practices.
- Able to project technology and architecture trends.

The NSAG should play a strong role in prioritizing research and development. A number of these areas are discussed in the recent report of an interagency task force on advanced networking. Summary tables of additional research areas for consideration are included in Appendix C.



## Chapter 4. Service Oriented Architectures

While it is a strong step forward, the “tier 2” heterogeneous network described in Chapter 3 cannot be extended to all of these entities. A service oriented architecture (SOA)—a structured way of obtaining services over a network—offers a promising solution. **A SOA is a body of standard design and engineering processes, tools, and best practices that leverage the modularity and composability of services to support mission objectives.**

SOAs offer a fresh perspective on how systems may be constructed, interconnected, and then accessed through a consistent interface. This approach enables organization and utilization of distributed capabilities in a heterogeneous network that is inherently interoperable. The potential benefits of a SOA include improved responsiveness, simplified delivery of mission services, more efficient information sharing, and improved transparency, security, and resilience.

Services in the commercial world are evolving, moving from human-to-human and machine-to-human deliveries of services, to machine-to-machine interactions such as automated check deposit. Business activities and processes once buried deep in the inner organizational structures, some as simple as ordering office supplies or as complex as the command and control of a large sensor network, are now becoming shared services accessible over a ubiquitous network, even to those outside the organization boundary.

With the embracing of Web 2.0 technologies, services are no longer strictly between providers and consumers. Armed with the ability to quickly “mash up” information widgets from disparate sources, users are now creating innovative services themselves and sharing them with others, in unanticipated ways—from concerned citizens tracking sex offenders in Google Earth™ to young soldiers organizing battle plans using Facebook on the front lines of the global war on terror.

A major advantage of a SOA is reusability of services. Instead of buying standalone systems, services can be delivered as reusable modules, thus avoiding redundant development and large-scale re-engineering of capabilities. In an effective SOA, existing functionality can be directly leveraged on a network, improving speed to realize and propagate a capability. Organizations can react

rapidly to changing mission needs by assembling required services rather than purchasing new systems. The use of standard design practices can also eliminate vendor lock-in.

In summary, the task force believes that successful SOA implementation, while not easy, is achievable; and if rigorously implemented will significantly enhance interoperability. While a SOA can significantly enhance interoperability, it is only part of the solution. An assured joint DOD and interagency net-centric enterprise will also require enhanced governance, an effective technical authority or “network architect,” rigorous information assurance, steady funding, properly designed networks and protocols, and sound data strategies.

## Challenges to Implementation of a SOA

The primary risk of a SOA is ad hoc implementation. When its application is not steadily funded and effectively governed, a SOA is no more (and can be less) effective than other approaches. SOAs must be designed into each organization’s enterprise architecture, governance, and policy framework and implemented incrementally with each step tied to delivered mission value.

Some critical strategies and tactics have been demonstrated to facilitate SOA adoption.<sup>20</sup> A general approach is to start with a small system to help de-couple larger mission objectives from the complexity of the technology infrastructure. This should be part of a sequenced approach for service implementation that aligns programs, funding, and resources. This approach should incrementally re-capitalize technology assets against the most critical mission drivers, and encourage reuse of emerging or existing services rather than making redundant investments. The early challenge is to balance the incremental demands on program and project teams to deliver for the immediate customer while also considering the requirements of the broader enterprise. Later on, the objective is to balance the intertwined dependencies—among requirements, service levels, and funding—in a way that results in increased organizational agility and improved mission performance. Throughout, strong leadership and effective governance is required.

---

20. Several former defense chief technology officers and chief information officers informed the task force that *A Practical Guide to Federal Service Oriented Architecture* is a valuable reference and the source of many lessons learned.



**Due to the very heterogeneous nature of the different modalities that make up the defense network, there is no universal solution to achieving interoperability.** Current forms of SOA count on an underlying network infrastructure that can support Web-based, representational state transfer for the discovery, negotiation, and service binding processes. This is generally true for current wired networks, although at the Transport layer (Layer 4), TCP currently has difficulty with low throughputs on overseas long-haul fiber networks, with delays of more than 300 milliseconds over fiber. Further, because most SOA deployments are over wired connections with plenty of capacity compared to satellite and wireless networks, the network burden of SOA in the form of data rate demands, number of roundtrips for set-up and usage, and delay requirements are not well quantified and understood. In fact, many SOA applications sessions are dropped (i.e., are timed out) when excessive network delays are encountered.

For theater operational and tactical echelons, network communications often go over a mix of satellite, wireless, or even line-of-sight networks with low throughputs and unreliable connectivity. While efforts are underway to bring broadband transport to the edge, such as the Warfighters Information Network-Tactical (WIN-T) and GIG-BE programs, the bandwidth-challenged tactical edge will require special considerations. As part of a robust planning process, network architects should use modeling and simulation techniques to consider the network burden of SOAs and determine how far toward the network edge SOA can be supported. A limited form of SOA may also be developed to work with low data rates. In this case, an intelligent master control plane and gateway at the interface between the high-rate backbones and the low-rate edge network could act as the network resource and service broker.

It is important to recognize that SOA will not solve connectivity, physical layer interoperability, capacity limitations, and delay variation issues in the network transport. These capacity and protocol problems must be addressed before any SOA vision can be implemented throughout the network.

Finally, the upfront infrastructure investment for the service oriented infrastructure, development environment, and testing environments must be considered. Also, while widespread use of developed services can lower costs for all, creating a generic and reusable software component may take more resources than creating a specific solution. The task force concluded that the costs of implementation were far outweighed by the projected operational benefit.

## Data Strategies

Historically, data structures were created by and for specific applications; these applications then owned the associated data. In many cases, the data itself was locked up in the applications and it was difficult or impossible to reuse the data in other applications. Modern design recognizes that the value of data sometimes exceeds that of the application, and thus requires that the data be separated from the applications from the start. This should be done immediately; it is not necessary to wait until the original application has completed its processing, as other applications may be able to derive value from the data immediately.

### *Metadata*

Integrating data from multiple sources builds knowledge only if the data can be related in some way—perhaps through a common location, timestamp, or intelligence target. Available information, whether collected from sensors or shared by others, cannot be combined in a meaningful way unless some element of common data can be related in this fashion. Thus the utility of data, especially utility involving purposes beyond the original design intent, requires “data about the data,” called metadata.

Metadata are usually produced at the time the data are created. Metadata can often take up more storage space than a data point itself, but its existence and availability is essential to the use of the data by different systems and services. Recognizing that different systems and services will have different purposes for data and derive different value from it, new metadata should be added or “tagged” with the data on an on-going basis. This tagging process expands the usability of the data. For example, a camera may add metadata to a digital photograph such as date, time, and lens settings. The photographer may add further metadata such as the names of the subjects and the Global Positioning System (GPS) coordinates where the photograph was taken.

The essential metadata elements are often known at the time the data are created, but are not always published with the data itself. A sensor designer may assume that he/she knows all possible uses of the sensor data, and therefore that publication of metadata is not necessary. An analyst or operator may assume that he/she is the final consumer of the data and that spending time on recording conclusions in the form of metadata is not productive. Because the individual or program producing metadata is often not the individual or program receiving the

benefit of metadata, providing guidance and policy may be necessary to ensure essential metadata are available.

Additionally, guidance and policy are critical to ensuring that the data that is made available is trusted and correct. Metadata about the source of the data is critical to make a determination on the reliability of the information. The existence of metadata does not imply that the underlying data will necessarily be shared, but the absence of metadata guarantees the data will be difficult to share. If the attributes about the data are carefully detailed, policy decisions can be more easily applied, resulting in the use of the data where appropriate.

Properly defined SOA data strategies will help alleviate network burdens. For example, the defense network ingests large amounts of data from sensors that can be tagged and processed in such a way that reduces network overload and allows the data to be searched efficiently. A model for this is the “MapReduce” tagging and reduction algorithm used by Google™ for ingesting many petabytes of data per day. By tagging data as it is entered into the network, local processing can reduce the amount of data sent over capacity-challenged network links and also permits automatic binning to facilitate subsequent searches.

### ***Metadata and Common Information Cores in a SOA***

A wide range of applications use an equally wide variety of incompatible data formats as well as incompatible semantics and meanings between applications. The overhead of translation among stove-piped systems and data formats adds unacceptable cost, time, and effectiveness friction that compromises effective operation of the systems of systems in its parts and in the whole.

Coding everything in a single language (e.g. Ada or Java or C++) does not address the problem. Having a standard schema or registry is not enough, although it may help reconcile incompatible data formats. Systems must also overcome incompatible semantics and meanings, which may require semantic modeling for each application domain, and a means of bridging semantic models across domains. As an example, the U.S. Air Force systems and U.S. Air Force logistics may have different frameworks for the same data for the same aircraft—one coming from a flight performance viewpoint, the other from a failure trend-monitoring viewpoint.

A common information core—made up of commonly accessible databases and look-up tables—would overcome these communication failings and facilitate

development focus on the correlation between an application and mission needs. It should be noted that common information cores are required, rather than a single core for all purposes. In complex systems of systems, multiple common information cores are crucial to interoperability of heterogeneous system elements performing disparate tasks reliant on common but diverse information bases. An interoperating, global information core system enables effective future operations—routine, exceptional, and emergency—and helps make sense of the information overload resulting from increasing data collection efficiencies.

It is both reasonable and essential to create an environment where every network user can get the information he/she needs, when he/she needs it, through heterogeneous, integrated network and information cores. Such cores must be trusted, secure, robust, and ubiquitous. Information technology continues to advance at a rapid pace; any common interoperable network-centric information core must be designed to evolve with technology and mission changes. Industry has shown a willingness to partner with DOD in the adoption of current and emerging open standards, prototyping, developing, and instantiating of a common information core in product and services through industry-wide groups such as the Network Centric Operations Industry Consortium (NCOIC). Leveraging this opportunity is a valuable avenue for DOD.

Concepts for a Universal Core, for mission-area common cores (for logistics, battlespace awareness, and so on) and for federated search are maturing. These standards efforts have focused on defining a minimal set of metadata (such as data regarding time and place) that will be included in all collections. Progress has also been made in defining standards for metadata that will facilitate information search and discovery.

### ***Additional Data Considerations***

A number of additional considerations will affect data management in a SOA. Primary is the issue of legacy data previously gathered that must also be made available. A vigorous metadata tagging effort and indexing must be launched to ensure legacy data is discoverable. Development of data quality and data cleansing strategies is needed to ensure the integrity of information. In general, DOD's intent should be to encourage continuous innovation in applications and in data storage and retrieval concepts. While commercial standards addressed and maintained by various consortiums will be used in any SOA, they alone do not

ensure interoperability. DOD and the intelligence community have unique requirements and standards that must be met.

**DOD's data strategy does not call for standardization of data across the entire enterprise; rather, it calls for managing data within communities of interest (COIs).** COIs are knowledgeable communities that are a logical focal point to achieve semantic understanding and to define and govern the use of metadata standards with the scope of a defined user base. This strategy gives those who have the most to gain by effective information management the authority to make the key decisions about semantics and quality of data. The task force concludes that while initial COIs have been a success, relying on COIs for every possible subset of every mission domain would be prohibitively time consuming. For this reason, additional governance is required to ensure that minimal sets of authoritative metadata are appropriately and accurately managed.

## Information Assurance in a SOA

A tremendous benefit of a SOA is the ability for authorized users to access and obtain information that is critical to doing their job from anywhere in the network. This flexibility, however, requires that essential IA be designed into the architecture from the beginning.

The paradigm shift toward service-oriented system collaboration and composition brings fundamental changes to the approach used to define security architectures. Most security solutions that exist today are based on the assumption that both clients and servers are located on the same physical or virtual network. The architectures generally rely heavily on perimeter-based security such as neutral zones, firewalls, and intrusion detection to thwart security threats. Similarly, the security policies that back existing solutions are also to a large extent perimeter-based. For example, obtaining access to an application usually requires creation of a new user account on the machine or network where the application is installed, and includes granting the user physical access to the facility where the machine or network is located. Accordingly, application-level security is usually regarded as not quite so critical and oftentimes is enforced by a simple username and password. Under a SOA, however, such perimeter-based security models are far from adequate.

In a SOA, consumers—that may be services themselves—can dynamically discover services and make use of their data in real-time. Services are inherently

location independent, with their network addresses published in a service registry that can change over time as services are relocated during normal system evolution. Service consumers and providers may belong to different physical networks or even different organizations, and these networks or organizations may be governed by entirely different security policies. For these reasons, in a SOA environment, an information assurance strategy calls for augmenting the traditional perimeter-based security models with a service-level view of security. To support SOA, the security infrastructure and network operations must become service-oriented. The network operations domain manages the assets, incidents, and vulnerabilities of the network infrastructure and is essential to assured network-centric information sharing. Many of the current network operations tasks are accomplished through vendor product-driven solutions and proprietary platforms, which will need to transform to a standards-based SOA.

Proper use of SOA will not diminish or improve the security of the underlying network substrate. Critical network functions such as management and control should not use SOA but instead should use the most robust network mode for transport. It may not be appropriate to use SOA for other critical services, such as real-time command services. For example, theater battle management core systems could be structured as a SOA for the support, situational awareness, and collaboration portions, but not for real-time applications such as reprogramming sensors and munitions, network sensing and control, and critical messaging with time deadlines.

An end-to-end IA solution involves more than just technologies and standards. Traditional security mechanisms should be augmented with security frameworks based on use of authentication, authorization, confidentiality, and integrity mechanisms. More importantly, “to adequately support the needs of the Web services-based applications, effective risk management and appropriate deployment of alternate countermeasures are essential. Defense-in-depth through security engineering, secure software development, and risk management can provide much of the robustness and reliability required by these (Web service) applications.”<sup>21</sup>

The certification and accreditation processes for SOA systems need to be continuously improved to accommodate agile and incremental system development. DOD needs to collaborate with the intelligence community, the homeland security

---

21. NIST Special Publication 800-95, *Guide to Secure Web Services*.

community, and other federal agencies on defining the standards and specifications for interoperable enterprise security services. These standards should be endorsed with enterprise policies so they can be materialized through capability acquisitions. A current effort between DOD and the Director of National Intelligence (DNI) on defining the security service specifications is a great first step in defining these enterprise security services. These services are based on industry SOA security standards that have matured over the years, such as Web service security and security assertions markup language. Moving toward specification-driven security architecture allows for the commoditization of security solutions with implementations tailored to local environments, and ensures that vendors compete on price, reliability, and speed, rather than features.

The current IA policies such as DIACAP (which replaces DITSCAP),<sup>22</sup> though very effective, usually require a lengthy compliance process that hinders the rapid development and deployment of software systems—a key tenet for SOA. DOD should include SOA considerations into IA processes so that agile and incremental system development can be supported without compromising overall system security, which is a critical challenge to be addressed.

## Governance of Network Architectures

The task force found that the current governance processes required to rapidly execute DOD's data strategies and network architecture standards are not sufficient. Actions in this area that could have been quickly accomplished are taking years to address. Currently, each Service, agency, and combatant command is able to interpret these directives in different ways and the Assistant Secretary of Defense for Networks and Information Integration (ASD (NII)) is not empowered to ensure compliance.

A key factor in the success of a SOA is the speed of implementation. Implementing a new architecture over a typical five-year system acquisition cycle means that commercial technology will have turned over at least three times. For these reasons, DOD must establish a sustainable infrastructure—leadership, people, and funding—to support a rapid SOA implementation.

---

22. The DOD Information Assurance Certification and Accreditation Process (DIACAP) replaced the DOD Information Technology Security Certification and Accreditation Process (DITSCAP) in 2007.

The technical challenges involved in transforming DOD networks have caused delays on a number of fronts. It is unclear whether it is possible to appropriately execute the current data strategies and network architecture standards. Additional challenges include the need for agreement to the standards and implementation profiles among DOD acquisition agents; Web services and other SOA standards are still maturing and leave room for ambiguity with multiple disparate implementations. In addition, compliance testing should be integrated as a critical element of the system engineering processes.

**The Net-Centric/Cyber Council should direct DISA to establish senior-level technical and management-level leadership with a strong technical engineering team to address a common SOA across DOD** (Figure 5). A sound methodology is needed to plan for future capabilities, conduct capability assessments, and evaluate and establish SOA governance processes. Leadership, spearheaded by CIOs, must ensure that a formalized, structured approach is incorporated into SOA implementation and evaluated through assessment frameworks. High-level, four-star leaders that are knowledgeable on net-centric issues are needed in each Service's applicable net-centric billet.

This team should coordinate with the Network System Architecture Group to determine the appropriate level of implementation of SOA on a heterogeneous defense network. The group's charter should include determining the appropriate level of implementation of SOAs on DOD networks. The group should immediately draft a roadmap to establish direction, identify contributing organizations, and determine the specific steps to undertake within each area.

Moving from the disconnected and non-standard systems in use today to an effective SOA will require increased oversight at the enterprise level. The use of an enterprise-wide service portfolio management construct will be critical to maintain service development standards and reduce redundant SOA efforts. An enterprise or COI architectural and acquisition oversight for SOA development is needed to coordinate the development of services to reduce duplication of effort. If a service is supposed to be used as a common component in a series of programs or projects, contract language and incentives must be explicitly organized around that goal.<sup>23</sup>

---

23. MITRE Corporation. 2008. *Leveraging Federal IT Investment using Service Oriented Architecture (SOA)*.



Acquisition standards and frameworks may also need to be modified to address the acquisition of smaller services versus major systems.



**Figure 5.** Role of the SOAs Coordination Team in the larger governance structure

To reap the full benefit of SOA and lower development costs, there should be as much sharing as possible. However, there is the question of how fine a granularity of services can be sensibly shared among many different types of usages and with what level of efficiency. For example, fast Fourier transforms (FFTs) are used in a variety of applications and perhaps should be a basic service that can be shared by many. Other very specific services, such as a tailored graph-matching algorithm, will not suit general purposes. Thus, it behooves the SOA coordination team to understand and trade off the level of granularity of service modules that can be effectively shared in a SOA architecture and optimize the cost-benefit of future deployments.

Adopting a SOA requires a new way of looking at operational processes. Some of the key challenges that DOD faces in moving toward the SOA paradigm include the underlying resistance to change and the requirement to trust that a service developed and delivered elsewhere is reliable and secure. Because users in a SOA

must expose their data and publish it to the enterprise, they must let go of the concept of “owning” data and using it only for their own needs. The paradigm needs to shift from ownership to stewardship of data, and from building systems to building services. Training of both military and civilian personnel is essential to successfully acquiring, building, securing, operating, and defending government networks and applications.

**Overcoming these challenges in DOD will require some major cultural shifting that can only occur under strong leadership.** DOD needs to move beyond traditional hardware boxes and packaged applications to embrace a more loosely coupled, reusable, and standards-based network of services.

Technology advances of the past thirty years have laid the foundation on which an interoperable network centric core can be built: the Internet, service oriented architectures, and inexpensive but powerful distributed computing capability. The technology is in hand for such an information core. It now must be brought to bear. Much of the infrastructure required already exists. What is lacking is decision, discipline, and culture adjustment.

## Chapter 5. Interoperability and Information Assurance

In this age of network-centric warfare—where a global networked environment enables information superiority—it is inevitable that an era of cyber-based warfare also emerges. Just as the United States has recognized the enormous potential for strategic and tactical military advantage offered by a global network of interconnected information systems, so too have adversaries realized the need to seek out and exploit vulnerabilities in the global information grid. As reliance on automated information systems for command, control, communications, and operations increases, it is essential that defenses of these information systems also increase—systems now critical to our military strategy and success.

Today's military missions are intimately tied to information and information systems—from strategy development to operational execution; from doctrine formulation to training and force readiness; and from materiel acquisition and provision to warrior transportation and deployment. For these systems to be effective they must interoperate; that is, they must be interconnected to share information and support the integration of our force projection toward a coordinated goal. Yet with each improvement in interoperability comes an increase in the scope, magnitude, and potential impact of a strategic cyber attack upon those systems.

Attacks on information systems can take many forms, from outright kinetic attacks on the physical devices to clandestine information attacks on the data they contain. The attacks may be immediately evident (e.g., loss of a network node or a system “crash”) or less readily apparent (e.g., subtle modification of critical data values or exfiltration of sensitive data through a hidden data channel). An attack may result in immediate damage when it strikes its intended target, or it may have a delayed result such as lying in wait to enable some future attack. Or it may result in no apparent damage at all, merely playing a reconnaissance role in surveying our networked information environment to prepare the cyber battle space for future conflict. The primary concerns apply to our core networks as well as peripheral microelectronic mini-networks that service such functions as intelligence, surveillance, and reconnaissance, navigation, and meteorology.

Just as information systems must interoperate to achieve mission assurance, so too must information systems serve to ensure the availability, integrity, and confidentiality of the information they contain and the functions they perform. No matter how accurate precision weapons are, targets will be missed if the targeting data are corrupted or inaccessible. Today, the typical operational plan cannot be executed if communications are blocked, choked, or misdelivered. Further, the forces projected into battle cannot be commanded effectively if blue force tracking and positioning data are not reliable or the situation assessments they report cannot be trusted.

Cyber attacks can result in a commander's loss of confidence in information systems, the loss of classified information, or even the loss of critical operational capabilities. To be effective, an attack does not have to bring down the entire network, nor does it have to last a long time to have a lasting effect. Cyber-based attacks can be effective when used in concert with other forms of military operations (e.g., to temporarily "blind" our forces or to delay our response), or they can be used to isolate one unit from another or from national support systems—just long enough to enable a conventional attack or to facilitate an evasive maneuver. They can even support hidden and prolonged espionage of national security information. Information assurance today is the greatest challenge to warfare with a competent near-peer and perhaps others.

## **Interoperability Poses Risks to Information Assurance**

As found previously by the Defense Science Board Task Force on Mission Impact of Foreign Influence on DOD Software, "information assurance is typically treated as if it were a network security and confidentiality matter. Yet it actually entails several additional issues, including integrity of the system, availability, quality of service, authentication, and attribution ... With the addition of each new module of capability, a degree of vulnerability is added."<sup>24</sup> No network is absolutely secure or 100 percent assured after it is made interoperable; the entire issue is about risk management. Connection to the GIG or the Internet introduces benefits and

---

24. Defense Science Board. (2007) Mission Impact of Foreign Influence on DOD Software. Available at [http://www.acq.osd.mil/dsb/reports/2007-09-Mission\\_Impact\\_of\\_Foreign\\_Influence\\_on\\_DoD\\_Software.pdf](http://www.acq.osd.mil/dsb/reports/2007-09-Mission_Impact_of_Foreign_Influence_on_DoD_Software.pdf)

risks that must be understood and accounted for. The following are several factors that must be considered in this analysis.

### ***Increasing Complexity and Interconnectedness***

Modern information systems are incredibly—sometimes incomprehensibly—complex. Today’s systems of systems, interconnected and interoperating, almost seem to evolve more than proceed from a monolithic, overarching design. Extensions to system deployments are achieved by building “bridges” between existing systems and networks, allowing new access to information resources for a burgeoning population of system users, operators, and components. With this almost exponential growth in connectivity comes a skyrocketing challenge of managing the system resources and protecting them against failure as well as deliberate attack.

When sharing more and more information, however, the noise may increase faster than the signal and the resultant babble may erode expected gains in efficiency or effectiveness. “Drowning in data” is no idle expression.

“Software has become the central ingredient of the information age, increasing productivity, facilitating the storage and transfer of information, and enabling functionality in almost every realm of human endeavor. However, as it improves the Department of Defense’s (DOD) capability, it increases DOD’s dependency... this growing dependency is a source of weakness exacerbated by the mounting size, complexity, and interconnectedness of its software programs. It is only a matter of time before an adversary exploits this weakness at a critical moment in history... The combination of DOD’s profound and growing dependence upon software and the expanding opportunity for adversaries to introduce malicious code into this software has led to a growing risk to the Nation’s defense... The U.S. is protected neither by technological secrets nor a high barrier of economic cost. Moreover, the consequences to U.S. defense capabilities could be even more severe than realized. Because of the high degree of interconnectedness of defense systems, penetration of one application could compromise many others.”<sup>25</sup>

---

25. *ibid.*

### ***Incentives and Disincentives for Information Sharing***

Information is a rare commodity because its value increases as it is shared. For this reason, interoperability enables the system to be greater than the sum of its parts. On the battlefield, effective information sharing and interoperability can make the difference between winning and losing. Fundamental to interoperability is control over access to information. Interoperability and information sharing are in tension with assuring the confidentiality, integrity, and availability of that information. As the interoperability extends and the “circle of trust” expands, the likelihood of a malicious insider grows, as does the vulnerability to external attack.

Providing technical interoperability hardly ensures that information will be shared. Protecting information may mean limiting access to those with a need to know. In other cases, cultural barriers cause information to be withheld. Incentives for members of an organization to protect information often conflict with the organization’s sharing policies. There is a critical need to fairly assess the costs and values—perceived by the doers—of sharing, or not, in cases where the sharing was either desirable or undesirable. And, in the event that the incentives are in conflict, they should be resolved, perceptions re-measured, and performance re-evaluated until sharing practice aligns with sharing policy.

### ***Global Information Infrastructures***

The extensive nature of the global information infrastructure means an adversary does not need to attack a component or device located on U.S. territory to have an impact on DOD information systems. In today’s global system, even a simple message from one military base to another may be fragmented and take a largely circuitous route (across the country or around the globe) before it is reassembled and presented at its intended destination. Redundancies in the communication system may make an attack on a single node ineffective, but global rapid rerouting systems may also enable easier access to tamper with the message traffic—to copy, misroute, delay, or even change the content of the message.

Further, attacks do not have to be made directly on live message traffic to have a significant effect. Attacks can render computers inoperable, perhaps at random, or perhaps as part of a larger coordinated strategic attack. Such attacks may not be delivered via the Web such as with common e-mail viruses, but can be launched through deliberate tampering with the commercial supply chain of information technology. Such tampering—for example, inserting so-called

“malware” in software or malicious circuitry in hardware—can occur at the point of manufacturing, during product shipment, or as systems are assembled or upgraded from multiple sources.

As the information technology industry has become increasingly globalized, more and more of the commercial supply chain is being developed off-shore and out of direct U.S. control. Just as economics has driven the U.S. government to build systems largely from commercial components, economics has also driven formerly U.S.-based companies to seek more cost-effective manufacturing capabilities overseas. These trends toward commercialization and globalization are largely viewed as irreversible, yet they contribute to increasing vulnerability to attacks on our information systems. Indeed, much of the groundwork for a future strategic cyber attack may have already been put in place—undetected and perhaps even undetectable with today’s inspection capabilities.

### ***Increasing Use of Commercial Products and Services***

Increasing use of commercial information technology products and services can introduce system risk in a number of ways. A primary issue—both a concern and a benefit—is that both partners and adversaries have access to the same products and services that are used by DOD and DHS. Dependencies on commercial products and services can enable adversaries to target our information in many ways. The target of cyber attacks is not exclusively military systems, but also includes critical infrastructure systems that support the military, the economy, and society.

Most of the military information infrastructure rides upon a common base of commercial hardware, software, and networking. Even if military information assets could be robustly defended, underlying commercial resources may offer vulnerabilities that adversaries can exploit. Why attack a fortified military base when attacking the commercial communications and switching network can have the same result? Further, why attack the military at all when a potentially more devastating blow can be dealt directly to the homeland? Why try to steal official state secrets when industrial trade secrets can be readily siphoned off to advance an adversary’s national or commercial interests?

## Case Studies

New thinking needs to be applied to testing, certification, exercising, red-teaming, and use of ranges and demonstration environments. A long-standing recommendation has been for unfettered exercises against red teams acting as top-tier cyber adversaries. With notable exceptions, few such exercises have occurred because of their cost and potential interference with other exercise objectives. Further, they would embarrass many players, from DOD commanders to operators to system developers. In addition, even if such exercises motivated participants to confront these problems, convenient solutions are not available. Any near-term influence strategy must affect both motivation and ability and should serve as a tipping point to catalyze broad action.

**The task force recommends that DOD charter teams to examine a few critical systems to identify what top-tier cyber adversaries might do against them, and assess the resulting likely mission impacts.** Several mission-critical systems that have been recently penetrated should be included within this study. Recommendations would then follow on specific changes to the design, implementation, or processes that might best mitigate the threats.

The mission impacts resulting from loss of interoperability will show the value proposition for interoperability and allow focus on near-term tipping points. After initial teams complete their work, follow-on teams should select several acquisitions, analyze their requirements and recommend changes, and recommend more general protection requirements for other acquisitions. For the recommendations to be effective, these teams must consist of top national authorities and the terms must be “no fault,” with no attempt to place blame for the problems. The desired outcome is to provide motivation to change as well as the specific technical guidance in how to accomplish it.

An example case study is on trusted microelectronics for sensors, high-speed data processing, and communication technology. These are central to the U.S. military’s ability to maintain technological advantage over its adversaries, enabling superior sources of information, the most advanced algorithms, and network supremacy. Opportunities for U.S. adversaries to infiltrate and attack critical DOD systems during their lifetime through compromised microelectronic components is real and dramatically increasing as the U.S. military dependence on foreign suppliers rises. Avoiding the risk entirely would be cost prohibitive, but several key defensive elements are necessary as part of an overall information



assurance risk mitigation strategy. As concluded previously by a Defense Science Board task force, “if real and potential adversaries’ ability to subvert U.S. microelectronics components is not reversed or technically mitigated, our adversaries will gain enormous asymmetric advantages that could possibly put U.S. force projection at risk. In the end, the U.S. strategy must be one of risk management, not risk avoidance.”<sup>26</sup>

The following is proposed as an examination of one system for vulnerabilities to both information assurance and interoperability.

### ***Supply Chains for Trusted Microelectronics***

Understanding and protecting the chain of custody of a microchip is the first step in creating trustworthy hardware. Today, DOD does not ensure a chain of custody for commercially purchased integrated circuit components. Existing procurement procedures provide multiple paths of access and would not allow for significant traceability to the origin of a microchip attack. Current exceptions to this occur for highly sensitive parts or obsolete parts purchased through the Trusted Foundry Program. In addition, once the original system has been deployed, replacement parts are usually obtained through open markets. Authentication of supplier and traceability of component provenance should be an integral part of closing trust gaps in the microchip supply chain.

A primary need is for authentication of suppliers and traceability of chip provenance. One way to ensure the chain of custody is to design, fabricate, and package all military microchips in a secure domestic semiconductor facility. However, the cost of keeping a domestic captive fab near the state-of-the-art is considered prohibitive and unsustainable. In addition, very few U.S. circuit manufacturers are capable or willing to meet DOD performance, variety, volume, and classified chip needs. A near-term and long-term supply strategy is needed. The Trusted Foundry Program, administered by the Trusted Access Program Office, effectively addresses short-term trusted microchip needs by validating trusted suppliers capable of providing secure and quality-certified facilities. A long-term strategy and tactical plan guaranteeing reliable access to trusted microelectronics components is still needed. In response to the 2005 Defense

---

26. Defense Science Board. (2005) High Performance Microchip Supply. Available at [http://www.acq.osd.mil/dsb/reports/2005-02-HPMS\\_Report\\_Final.pdf](http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf)

Science Board report on the microchip supply, the Defense Advanced Research Projects Agency (DARPA) initiated a program to define revolutionary methodologies for detecting malicious or rogue circuits inserted in different parts of the microchip supply chain. The enduring strategy should also include legacy parts and special needs such as radiation-hardened electronics and classified components.

The Trusted Foundry Program could allow legacy parts designed at historically larger linewidths to be fabricated and qualified in a domestic foundry. Even parts that should be redesigned for military specifications could be manufactured onshore and in a less than state-of-the-art facility. A low volume, high-product mix microchip fab would be ideal for fabricating a new generation of parts meeting more aggressive operational requirements, while maintaining identical functionality. Sharing of microchip testing, device modeling, and qualification resources could help to reduce costs of a trusted foundry. **Anonymity in commercial off-the-shelf (COTS) hardware procurement is another policy strategy that can protect supply chains.**

### *Chip Design*

Policy changes may include securing design data and hiding end-to-end design information. Beginning with the design phase, there is little ability to validate the trustworthiness of an integrated circuit design; designers are typically the only ones with intimate knowledge of the circuit and its function. For overseas foundries, the design libraries include logic blocks as part of their cell library with strict controls disallowing access to the inner workings. Such complex functionality is followed by many errata (fixes) post-production release, which is another opportunity for compromise. By establishing a trusted design research and development center for U.S. government agencies with a focus on system assurance, risk could be reduced via anti-tamper techniques, hidden functionality (obfuscation), secured public key information, design for evaluation, and design for trust methodologies.

Once a chip has been designed and verified, it is sent to the mask house or to the foundry first for process-specific layout modifications prior to shipping to the mask vendor. In state-of-the-art semiconductor manufacturing, layouts are often tweaked in proprietary ways to improve product yield and manufacturability and to reduce critical lithographic linewidth variations. There seems to be ample opportunity in this portion of the chain for devilry. Maintaining a trusted supplier mask house can reduce risk, but most mask houses are either offshore or foreign-

owned, making it difficult to achieve trusted supplier accreditation. The long-term solution is unclear, but there appears to be some efforts afoot with maskless chip fabrication using ion beam lithography and processing techniques.

Field programmable gate arrays (FPGAs) are a chip design of interest. These devices are extensively used in military systems and commercial markets and continue to gain even greater applicability and acceptance as the technology improves. FPGAs can be considered relatively more secure than custom application specific integrated circuits (ASICs). Because they have a much larger user base, any generic tampering would have a higher likelihood of being discovered. Because 80 percent of FPGAs are manufactured in Taiwan, they are generally co-processed with commercial chips. This can increase the trustworthiness of FPGAs where the chain of custody could not be verified.

Another potentially attractive defense to subversion of integrated circuits is the structured ASIC (sASIC) microchip. The sASIC is a programmable device not unlike an FPGA, except the sASIC is programmed during processing at one of the via levels. In the sASIC, programming leads to changes in functionality based on the particular layer data and not just memory code as in the FPGA. The entire functionality of the chip is determined at only one layer. That one layer would be designed and processed entirely in-house with no mask house involvement—the programming data never leaves home. The sASIC concept fits well into the co-processing model by allowing leading-edge fabrication of sASIC frontends to be processed anywhere in the world, while the less demanding backend metal layers are processed in a domestic-trusted foundry at reduced capital costs. The sASIC, which has a very repeatable regular fabric of logic blocks, would allow more efficient reverse engineering techniques for identifying rogue elements within the die.

### ***Process Control***

Irrespective of the future microelectronic manufacturing and R&D global scenario, the threat of tampering with malicious intent is and will be omnipresent throughout the entire system lifecycle. As a result, risk of a compromised supply chain must be mitigated and managed continuously and aggressively now and in the future.

During chip production, access to intellectual property or the ability to modify just a layer or two increases significantly and is of serious concern. DOD and its contractors need a methodology for ensuring the trust of leading-edge parts

fabricated overseas; completing the metal interconnect on wafers in a domestic foundry could greatly reduce their risk. Some process models have the potential for alleviating the threat of fabrication sabotage. Fabrication tampering is prevented by wiring circuits in an onshore foundry; tampering is detected prior to metal deposition steps; dies are uniquely identified via “signatures” added during interconnect fabrication; and critical algorithms and encryption are protected based upon a chip’s unique characteristics, which may employ physical unclonable functions (PUFs) as watermarks.

Various specifications require the hermetic protection of fabrication tools and dies. While this process provides environmental protection to the chip, it also provides concealment of any mischief during fabrication. Today, as packaging options become more complex and incorporates multiple dies per layer and multiple layers in three-dimensional packaging, the ability to add malicious functionality is even greater. This type of complex packaging can also increase trust by hiding the overall design scheme and allowing completion of final interconnects through layers of packaging at a single accredited trusted supplier.

### ***Test and Certification***

Over 65 percent of chip packaging is done in Asia and U.S. military chip suppliers routinely test and package their chips abroad. Trusted suppliers are needed onshore to reduce this substantial threat and continued R&D in leading-edge packaging solutions enabling higher performing microelectronics must be supported.

Failure analysis, reverse engineering, and vulnerability assessment capabilities are invaluable in the fight against adversaries tampering with the microchip supply chain. Though difficult and time consuming, reverse engineering is a key factor in determining that what is designed is what is received. Completely vetting a complex chip for malicious circuitry through exhaustive testing is costly and fallible—typically chips are tested for proper functionality not for backdoors or hidden agendas. Even though failure analysis and reverse engineering are long and expensive processes, being able to assign attribution through forensic analysis is of critical importance when national security is concerned. Through attribution, deterrence is bolstered and asymmetric threats are reduced. Vulnerability assessments are used to determine the security of a component. These assessments are critical in components where knowledge of the design of the component (e.g., cryptographic keys) would result in an adversary gaining significant advantage.

Although research is in progress on techniques that could cut costs and time significantly (e.g., super-resolution infrared imaging, scanning confocal transmission electron microscopy, X-ray tomography), successful application of the fruits of research into these techniques is, at best, several years off.

## Readiness

While the tide of commercialization and globalization cannot be reversed, the means to defend our information systems and the information they contain is needed. Information assurance and the emerging activity of mission assurance entail making systems more resistant to attack, more resilient while under attack, and more able to be reconstituted after attack. Active defense mechanisms are needed to detect and deflect intrusions from external sources, to monitor and isolate insider-enabled sabotage and espionage, and to inspect and encapsulate malfeasant hardware and software. Contingency plans are also needed for continuing operations when information systems are down by preparing in advance alternative (perhaps isolated) systems and methods for achieving mission effectiveness even while operating in a degraded mode. Training and preparation are needed to quickly reconfigure and restart critical systems to recover from any loss of capability.

### *Assessment Capability*

**The task force recommends that DOD establish a cyber- or information-readiness assessment capability to include situational awareness of a cyber attack, up-to-date mechanisms for defending against known and novel attacks, contingency planning for fighting through a cyber outage, and extensive training for system users and administrators on how to restore operations as quickly and orderly as possible.** Establishing such a capability is no small feat. It will require an extensive awareness campaign to keep the need for better information assurance foremost in the minds of warriors, planners, and resource managers alike. It will also require the research and development of better methods for recognizing and analyzing cyber attacks, properly attributing cyber attacks to those responsible and understanding their intended purpose, and responding to the comprehensive cyber threat both before and after an attack. It will also require an effective partnership with the entire federal government, with other nations, and with the private sector. Because of the interdependency of global information systems and technologies, DOD cannot ensure mission

assurance by only defending its own systems; a much broader defensive strategy is required.

### ***Battle-mode Protection Requirements***

As systems have been developed, deployed, and modified over the last decade, system-of-systems complexities and interdependencies have evolved and tactics, techniques, and procedures have been established and refined. The result has been increased use of and reliance upon information services. Systems users and operators may not promptly recognize degradation or loss of critical assets and may not be proficient in using alternative mechanisms, even when they exist. Further, there are cases where military capabilities rely on assets with no adequate current alternative. As a better assessment of cyber readiness becomes available, the need emerges to invest in a set of high-assurance systems and techniques that can provide essential mission capability during times of high information operations intensity. Introducing realistic, sophisticated threats in current and future exercises will help us identify mission-critical functionality. It is imperative that we employ mechanisms to ensure the integrity of this functionality.

National security systems have long been treated with great care and rigor. Intelligence collection and analysis are performed to thoroughly understand the threat environment and mechanisms that may be used to defeat or deny the weapon system. Countermeasures are conceived and employed to ensure that these systems are capable of surviving military-grade threat conditions. These systems are tested thoroughly in realistic environments to ensure that weapons system integrity is not compromised. Critical information systems should be treated with no less rigor.

Battle-mode protection requirements are needed for specific net-centric mission-essential functions. This could entail identifying thin-line critical paths, minimal interoperability threads, capabilities for resilience and reconstitution, and a characterization of battle-mode identity and access management. USJFCOM and the National Security Agency (NSA) should jointly formulate a set of risk management assumptions about the presumed security state of systems and networks and the presumed capabilities and intent of adversaries. This information should be made available (at increasing classification levels and with appropriate controls) to planners, warfighters, designers, and system accreditors.

A long-term strategy and tactical plan are needed to guarantee reliable access to trusted mission-critical components. DOD must prioritize resources on mission-critical network elements, systems, and information repositories. It is often not until

crisis occurs that appropriate resources are directed to these components. Technology assets and interoperability must fully consider requirements for safety, availability, reliability, and sustainability. Resiliency must be designed into systems, networks, and processes. A long-term strategy is to investigate the feasibility of a minimum essential information infrastructure to support mission-critical functionality, to be determined through realistic exercises.

## **Awareness of Threats to Information Assurance**

The future of the United States (and its national military strategy) is irreversibly tied to leveraging information technology. Even as information technology enables military superiority, vulnerability to cyber-based attack and exploitation is concurrently increased. Despite best efforts to bolster cyber defenses, information systems (and the information they maintain) remain at risk—and with them the potential to fight and win the next war. A broad awareness campaign is needed across DOD to raise the level of understanding and appreciation of the cyber threat and what is needed to counter it.

This awareness is needed across acquisition staff, testers, and certifiers, who too often are unaware of specific threats. The ability to recognize cyber vulnerabilities must be improved, including indicators for novel surreptitious attacks, insider-enabled exploits, and attacks to the supply chain in hardware and software. The ability to attribute an attack or exploit must be improved, including the ability to identify the responsible perpetrator (not some unwitting “bot”) and to recognize when an attack is stand-alone or part of a larger strategic effort. The complex issue of authorities and responsibilities for passive and active defensive measures must also be addressed, including legal and policy issues concerning appropriate deterrents and responses.

For improved understanding, the security and counterintelligence and counterespionage organizations in the Services need new tools and technical competencies. DOD programs are incorporating more and more commercial off-the-shelf components, even for information assurance. At the same time, the NSA, which has the most sophisticated competencies in information assurance, has had its mission expand beyond its budget. As a result, the NSA has insufficient resources to service all of DOD, especially as DOD strives to coordinate with the defense industrial base and the homeland security mission.

Further advancement of interoperability policy is needed, including focus on complex deterrence and dissuasion notions, as well as asymmetric action-response

in the warfare context. Perhaps most importantly, many issues of trust across both the public and private sectors must be resolved, including issues of offensive and defensive equities; issues of classification and compartmentation; issues of competence, competition, and cooperation; and issues of legal authorities for privacy and security. Cybersecurity is a national problem deserving of a national-level response, a response that in its own way must highlight the need for interoperability in our cyber defense and response mechanisms. DOD needs to transform its policy and practices regarding mission assurance, especially regarding capabilities to assess, reallocate, and reconstitute critical missions after attack.

### ***Awareness Needed: Suite B***

A comprehensive set of trusted cryptographic algorithms is vital to system security. The “Suite B” family of cryptographic algorithms provides hashing, digital signatures, and key exchange functions. As Suite B become available for both classified and unclassified applications, the ability to design and implement cryptographic systems across military, federal, state, and local domains with Suite B should significantly enhance the interoperability characteristics of such an architecture. With the intertwining of military and civilian systems, the military system’s cryptographic infrastructure must be extensible to civilian systems. Therefore, to maximize DOD’s ability to utilize commercial technology, all commercial vendors should consider the incorporation of Suite B (including the use of extensible markup language (XML) standards) in their products.

The sustained and rapid advance of information technology in the 21st century dictates the adoption of a flexible and adaptable cryptographic strategy for protecting national security information. Several years ago, the Committee for National Security Systems issued a policy stating that the Advanced Encryption Standard (AES) could be used to protect both classified and unclassified national security information. However, because a single encryption algorithm could not satisfy all of the needs of the national security community, NSA created a larger set of cryptographic algorithms that could be used in conjunction with AES to support DOD and other national security user’s cryptographic requirements.

Suite B includes, in addition to the AES, cryptographic algorithms for hashing, digital signatures, and key exchange. The entire suite of cryptographic algorithms is intended to protect both classified and unclassified national security systems and information. Because Suite B is also a subset of the cryptographic algorithms approved by the National Institute of Standards and Technology, Suite B is also suitable for use throughout the U.S. government. NSA’s goal in presenting Suite B is to provide industry with a common set of cryptographic



algorithms that they can use to create products that meet the needs of the widest range of U.S. government needs. Additionally, for exceptionally sensitive applications, Suite A algorithms continue to be available.

It is important to note that Suite B only specifies the cryptographic algorithms to be used. Many other factors need to be addressed in determining whether a particular device implementing a particular set of cryptographic algorithms should be used to satisfy a particular security requirement. The improper integration of secure algorithms may indeed be insecure.

The original policy on AES use states that AES with either 128- or 256-bit keys are sufficient to protect classified information up to the SECRET level. For Suite B, protecting TOP SECRET information would require the use of 256-bit AES keys, as well as numerous other controls on manufacture, handling, and keying. These same key sizes are suitable for protecting both national security and non-national security related information throughout the government.

Consistent with this policy, elliptic curve public key cryptography using the 256-bit prime modulus elliptic curve as specified in FIPS-186-2 and SHA-256 are appropriate for protecting classified information up to the SECRET level. Use of both the 384-bit prime modulus elliptic curve and SHA-384 is necessary for the protection of TOP SECRET information. Another key aspect of Suite B is its use of elliptic curve technology instead of classical public key technology. Rather than increase key sizes beyond 1024-bits, a switch to elliptic curve technology provides more security, more effectively.

Today SUITE B includes:

- Encryption via the Advanced Encryption Standard (with key sizes of 128 and 256 bits)<sup>27</sup>
- Digital Signature via the Elliptic Curve Digital Signature Algorithm (using the curves with 256 and 384-bit prime moduli)<sup>28</sup>
- Key Exchange via the Elliptic Curve Diffie-Hellman (using the curves with 256 and 384-bit prime moduli)<sup>29</sup>

---

27. Federal Information Processing Standard 197, available at <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

28. Federal Information Processing Standard 186-2, available at <http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf>

- Hashing via the Secure Hash Algorithm (using SHA-256 and SHA-384)<sup>30</sup>

In order to facilitate adoption of Suite B by industry, NSA has licensed the rights to 26 patents held by Certicom, Inc., covering a variety of elliptic curve technology. Under the license, NSA has a right to sublicense vendors building equipment or components in support of U.S. national security interests. While NSA offers vendors royalty-free licenses for the use of these patents, NSA is not suggesting that licensing any of these patents or any other patents is necessary for implementing Suite B.

To master the information battlespace, warfighters and intelligence analysts in DOD and the intelligence community need to be able to share, analyze, and secure vast amounts of information. Interoperable standards are critical to prevent all of the information in DOD networks from becoming meaningless. As the requirements for security, information sharing, and interoperability for DOD and critical infrastructure networks increase, the widespread adoption of Suite B cryptography could be instrumental in meeting these needs.

---

29. Special Publication NIST-800-56A, available at [http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A\\_Revision1\\_Mar08-2007.pdf](http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf)

30 Federal Information Processing Standard 180-2, available at <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf>

## Chapter 6. Joint DOD Test, Evaluation, and Certification

In the late 1990s, the Army began a serious program to move into the net-centric world of battlefield operations. The Army Battle Command System (ABCS) brought digitized operations, intelligence, logistics, personnel, fire support, and air defense capability into a battlefield tactical operations center. The ABCS system of systems provided a common operating picture to all facets of command, and began the transformation of the Army Divisions to the net-centric divisions of today.

To ensure interoperability in this newly formed net-centric environment, the Army established an integrated Central Technical Support Facility (CTSF), bringing together as one team the project managers of individual systems along with engineers from both government and industry. The CTSF was sited at Fort Hood, Texas, home of one Army corps and two Army divisions, in order to gain user inputs from the beginning. The brigade that was to be the first equipped with ABCS was co-located with the developers. The results after ten years have demonstrated that this decision was critical to the Army's success in transforming to a net-centric organization.

As the requirements for networks and communications in Operation Iraqi Freedom (OIF) increased, a need evolved for a quick response capability to introduce new technology to the theater and the battlefield. Implementation of programs emerging from longer development cycles was needed in the battlefield in both Iraq and Afghanistan. One such program was Blue Force Tracking. In order to introduce this capability quickly and ensure it could operate across the Force, the system went to the CTSF where systems in use in theater could be tested and adjusted to interoperate with the Blue Force Tracking System. The concept was a success—Blue Force Tracking went to the OIF theater, and interoperated successfully with systems already in use. As greater net-centric capability was then needed in the tactical operations center and the ABCS prepared for the next generation, the Command Post of the Future program was initiated at DARPA. To transition this system to the OIF battlefield, it would need to interoperate with the other net-centric systems in use. To accomplish this, the hardware was sent to the CTSF, where it was successfully modified and adapted.

A similar fast track was used to integrate the Joint Network Node (JNN) for homeland security applications.

The task force understood that a network of CTSF-like operations—potentially including the Navy SPAWAR system and the Air Force Electronic Systems Command—could lead to a network for joint test, evaluation, and certification. A system that was organized jointly would be able to provide results that were accepted jointly.

As the task force further explored the interagency issues with DHS. A high-priority DHS issue was identified as the desire to evaluate DOD technologies and systems that could support DHS missions in a timely manner and could also interoperate with DOD technology and systems.

The terms of reference for the task force were specifically directed to assess this area, including:

- The requirements for military operations in a net-centric environment.
- The use of a single autonomous agency as a mechanism to address interoperability, e.g., the Army's CTSF was established to integrate non-materiel and materiel solution sets for military operations in a net-centric environment.
- A standards-only approach to allowing independent development of systems certified to the standard.
- The development of a virtual test, integration, and certification capability to assess capability and ensure interoperability of military operations in a net-centric environment.
- The ability of each model to establish and maintain configuration management among multiple organizations involved in DOD operations.
- The potential to use current systems to incrementally evolve to net-centric capability, especially in light of the rapid evolution in the network domain contrasted with the lack of synchronized and comprehensive DOD modernization.

## Issues in Achieving Interoperability

There are some general approaches to the technology for interoperability. One is to buy two different systems, and then customize one or both ends of the misconnection. A translating intermediate component or subsystem may also be

used. While this method has been proven at the CTSF, it incurs costs for each new combination and must be updated as either incompatible system is updated.

Another approach is to buy the same equipment (e.g., hardware, firmware, and software) from the same manufacturer or from vendors who advertise and deliver cross-brand compatibility. This method has also been proven over time, but flies in the face of competition and is eventually more expensive than a standards-based approach.

### ***Standards***

Improved standards can be a challenging and effective approach. In the past, DOD established government standards, military specifications, interface control documents, qualified suppliers, and so on, and bought only compliant products. Policy tends to embrace this standards approach to interoperability but this is not an unalloyed good. In many instances, hard standards are the enemies of progress and hold back technical innovation. In addition, the standards approach is not without cost although the costs may not be direct or explicit—costs may be borne initially by the manufacturer or vendor and then indirectly passed on to the buyer.

A more flexible approach is to rely on industry standards. There are two distinct opinions on this subject—from the “haves” and the “have-nots.” According to the “haves” (i.e., the market leaders), de facto standards are set by products that ship in volume. According to the “have-nots” (i.e., the rest of the pack), standards should be set by public/private consortia. Consortia bodies are often political, and their standards may be designed to unseat the market leader’s de facto standard or to increase market access in a closed economy. The negotiation of standards in international bodies can be especially troublesome for information assurance efforts.

The political nature of the process frequently results in inclusive and flexible standards. Flexible standards often include legacy provisions, which can propagate previous bad decisions. Such standards may also carry implementation-dependent definitions, platform-specific options and exceptions, and a number of open-ended decisions that are put off for future deliberation. Such standards do not support effective interoperability and are antithetical to best information assurance practices.

Ambiguity, imprecision, and variability in hardware and software behavior, protocols, and interface control documents are the quintessential elements of

inefficiency and vulnerability. Without defined standards, for example, a system interface or defensive mechanism would have to be continually consulting a look-up table, which is generally not specified within the standard.

Effective standards must be precise, fully defined, and provide no functionality beyond that which is immediately required. This may mean that a standard does not have room for growth. It might have to be revised. And it might not be able to satisfy everyone.

### ***Synchronicity***

Standards are important, but are also insufficient when synchronicity is involved. It is not uncommon for three or more generations of a system to cohabit the field: the new/incoming; the old/legacy/outgoing; and the current. Getting a new system on the ground, working with other legacy systems directly or through simulations, with soldiers using the systems, is necessary and critical for success.

From a “system of systems” perspective, interoperability may be introduced with, and be limited to, new and future systems. This means legacy systems may need to be abandoned sooner. Legacy interoperability can also be required of all new systems—adding cost to the new systems, and potentially limiting functionality. Also at a higher cost, interoperability may be retrofitted to current and legacy systems. Forfeiting interoperability in some cases may be prudent, depending on the circumstances.

## **Approaches for Improved Interoperable Systems**

Approaches beyond standards are necessary and critical for success. These include soldiers with operational experience evaluating the systems in real conditions and interfacing with legacy systems directly or through simulations. Through such an implementation, the CTSF was able to establish and maintain configuration control during test, evaluation, and certification, and also on a continuing basis by placing engineering teams in the units and in theater to make and record adjustments as needed. Additionally, the CTSF met their requirement to interoperate with current systems and incrementally evolve to a higher capability.

As the CTSF evolved, it expanded from Army to joint DOD systems, principally with the introduction of the Joint Network Node (JNN). This progress led to one of the questions before the task force—to assess the concept of the



## *Testing Methodologies*

Many test, evaluation, and certification processes and methodologies are well documented across DOD, the federal government, industry, and academia. The U.S. spends billions of dollars a year on testing laboratories and redundant systems testing. While some efforts, such as the Army-led Federated Net-Centric Sites, have been initiated to connect these labs in methodology and infrastructure, the lack of the common test methodology and infrastructure standards at the federal level often makes interoperability testing itself, not interoperable. However, inconsistent processes, methodologies, and infrastructure, coupled with the lack of governance has allowed only a few stove-piped interoperability successes

Multiple certification processes and inconsistent retest processes exist, often resulting in the delivery of obsolete products or products that are no longer supported. Current test, evaluation, and certification (TE&C) processes take months and often years. In a wartime environment where information and technical capability is becoming more and more critical to the warfighter, a delay of months or years for redundant testing to deliver a new capability is unacceptable.

Many DOD-wide interoperability TE&C efforts are currently coordinated by DISA. In most cases, these efforts do not include all of the cross-organizational stakeholders required to achieve the interoperability necessary in today's environment. The task force concludes that DISA should continue to lead the accreditation of test centers and the definition of certifications for test processes, methodologies, and infrastructures. The JITC has the technical know-how to be the central hub for these efforts.

An integrated task force led by DISA and JITC should define a consistent set of certification test processes, methodologies, and infrastructures that are approved by a cross-service technical advisory board. Once agreement is achieved, a "test by one, accept by all" construct should be instituted based on the common test processes, methodologies, and infrastructures. Today, test and certifications performed by one federal organization are most often not accepted by other organizations. In some extreme cases, results are not accepted within different components of the same organization.

To be successful, TE&C standards and metrics must be included earlier in the acquisition process. This enables programs and developers to build interoperable



technology during the first iteration and avoid costly revisions and reengineering. **The acquisition cycle should include interoperability certification testing starting early in the system development and demonstration process and interoperability requirements should be included as a standard set of requirements for any acquisition of a net-centric system.**

### *Governance and Infrastructure*

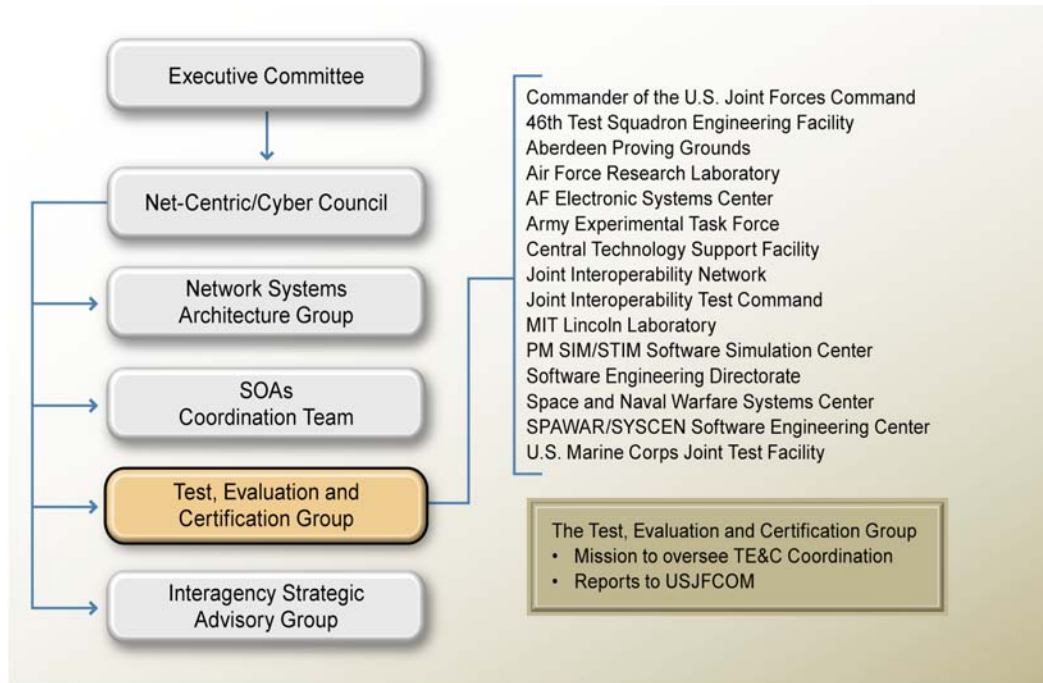
Multiple efforts to establish joint DOD interoperability testing and approved products lists are causing confusion about processes, policies, and governance. The lack of a governing organization in the federal government chartered to lead interoperability testing, interoperability processes, and enforcement policies, results in conflicting structures and standards. Further, organizations across the federal government establish approved product lists for their specific efforts resulting in multiple lists that are often in conflict.

At the root of the issues is a lack of definition of the processes and methods for designing and executing tests of the system of systems in the joint DOD mission and/or non-DOD environment. A clear understanding is also needed to assess system performance as it pertains to capabilities supporting joint DOD missions.

The task force recognizes that DOD and DHS are critical stakeholders in interoperability and information sharing. TE&C governance processes and methodologies that will be enforced by DOD must also be agreed to by DHS and must be enforced at all levels of the organizations. Formal agreements are needed between DOD and DHS organizations.

DOD needs a lead organization for joint DOD and interagency TE&C of net-centric systems. The task force recommends that USJFCOM be designated as the central authority for joint DOD interoperability testing to lead and manage this joint DOD capability and to establish funding priorities.

**The task force recommends that USJFCOM support a “cross service technical advisory board” to ensure joint DOD coordination** (Figure 7). In addition, because COTS capabilities continue to be an extremely important component of DOD’s technical architecture, the task force recommends a coordinated industry advisory council to ensure that that industry understands DOD’s interoperability requirements as they build and deliver COTS products.



**Figure 7.** Test, evaluation, and certification coordination in the larger governance structure

### *Exercises and Experiments*

Operational scenarios are most often being conducted in stovepipes and, in the rare cases where multiple organizations are brought together for interoperability testing, TE&C governance processes, methodologies, and technologies are different and result in poor performance. Few governance processes truly encompass DOD, intelligence community, and state and local first responders, all of which are critical organizations in real-life operational scenarios.

**The task force recommends that USJFCOM be designated as the responsible organization to identify test scenarios, test exercises, experiments, and demonstrations.** USJFCOM's current critical role in the joint DOD environment will enable the organization to establish test scenarios that enable better TE&C planning and preparedness for today's environment of rapid deployments with coalition partners. TE&C today includes joint DOD, multinational, interagency, and industry organizations. Establishing priorities for experiments and exercises should be done by the organization that is also responsible for joint DOD capabilities development.

# **Part II**

---

## *Interagency Challenges*



## Chapter 7. Interagency Interoperability: Redefining “Jointness”

The task force was briefed on a variety of interoperability issues associated with the homeland defense, homeland security, and defense support of civil authorities (HD/HS/DSCA) mission. Many presentations discussed the difficulties of applying U.S. military assets and capabilities to fulfill interagency support requirements. These difficulties were especially pronounced when dealing with the wide array of regional, state, tribal, and local first responders who support the homeland security mission. Breakdowns in communication, coordination, and collaboration in support of HD/HS/DSCA were also reported within DOD, e.g., between the military Services and the National Guard.

A common theme was evidenced in after-action reports from Hurricane Katrina, 9/11, and California wildfires, and heard in several presentations to the task force—the lack of appropriate situational awareness throughout levels of response. In times of national emergencies, this has resulted in faulty decision making and poor resource allocation at federal, state, and local levels. Coordination, collaboration, and interoperability of communications are critical issues in the successful execution of the mission to defend the homeland.

The vision for interagency interoperability is the consistent ability of all federal, state, and local systems, units, and forces to provide services and information and accept services and information from one another in order to ensure mission success for HD/HS/DSCA. These organizations should also leverage improved institutional processes as they plan, design, build, acquire, test, train, and operate together.

Successes in bridging the interoperability gap were reported in cooperation within the intelligence community involved in the HD/HS/DSCA mission. As a federation of 15 executive branch agencies, the intelligence community works jointly and individually to conduct intelligence activities to protect the national security of the United States. In the instances when they have been successful in HD/HS/DSCA, that success was attributed to frequent cross-agency interactions. The task force observed that exposure, training, and experience in the interagency environment breeds understanding and awareness of the broader community's interoperability capabilities and challenges.

The task force believes that DOD should expand their transformation planning for a joint force to include the ability to work effectively as part of an interagency force in the same way the Goldwater-Nichols Act of 1986 altered the command structure of the U.S. military. Because there is no such mandate for interagency interoperability, it will require significant leadership to take these steps beyond their current levels.

## Governance

The Department of Defense and the Department of Homeland Security share an important mission for HD/HS/DSCA, as shown in Figure 8. Several elements inside DOD, as well as elements in a number of other federal agencies also play a role in this mission. It is important to recognize that the regime for HD/HS/DSCA includes more than federal agencies—it includes the relationships with the state, local, and tribal governments, with certain non-governmental and private sector organizations, and with foreign governments and their associated interagency structures.

*We will continue to work to improve understanding and harmonize best practices amongst interagency partners. This must happen at every level from Washington DC-based headquarters to the field. DOD, in partnership with DHS, also will continue to develop habitual relationships with state and local authorities to insure we are positioned to respond when necessary and support civil authorities in times of emergency, where allowable by law. Through these efforts we will significantly increase our collective abilities to defend the homeland.*

### **2008 National Defense Strategy**

*Whether responding to a disaster of natural or man-made origins, collaboration among interagency partners at all levels of government are built upon the cornerstone of communication. More than five years after the attacks of 9/11, our nation continues to struggle with two distinct communications issues: interoperability and survivability.*

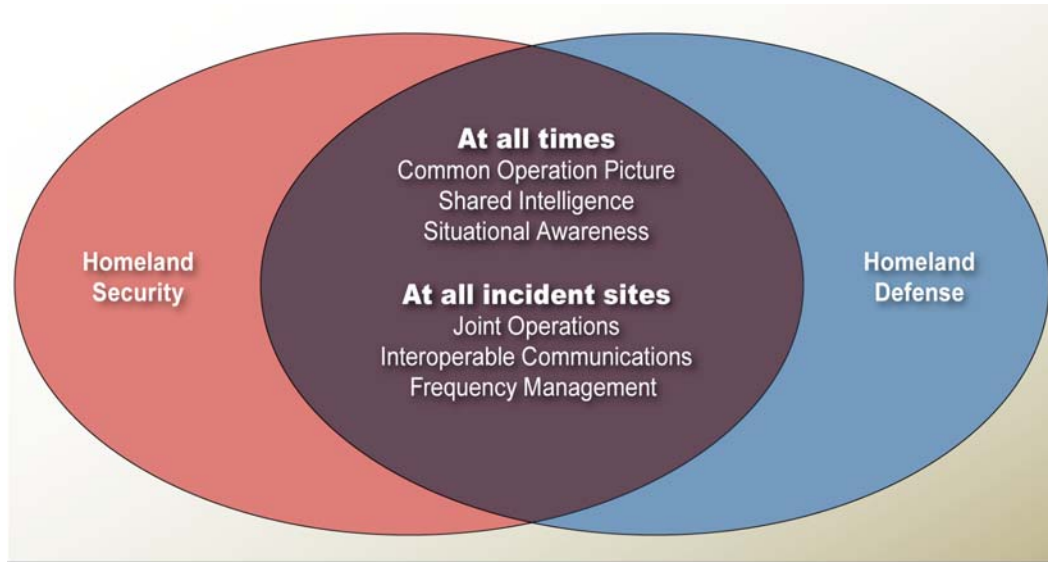
**General Victor E. Renuart, Jr., USAF  
Commander NORAD and US Northern  
Command**

*Continue to promote coordinated development of governance, technology and protocols necessary to enhance minimal capabilities for interoperable communications (voice, video and data) among all levels of government and the private sector.*

**Protecting Americans in the 21st Century:  
Imperatives for the Homeland  
DHS Homeland Security Consortium**

*The Department must have the ability to transfer information to and obtain information from external partners overcoming situations where these partners may have disparate processes and capabilities and whose role and nature may not be known prior to an event.*

**DOD Information Sharing Strategy**



**Figure 8.** Overlapping agency responsibilities for homeland security and homeland defense drive the need for interoperability

### ***The DOD Mission for Homeland Defense***

The 2008 National Defense Strategy states that defending the homeland is the core responsibility of the Department of Defense. This strategy recognizes that globalization presents new opportunities and challenges, and acknowledges the ability of adversaries to attack via cyberspace to disrupt commerce and daily life in the United States.<sup>31</sup> The task force strongly agrees that “DOD should expect and plan to play a key supporting role in an interagency effort to combat these threats and to help develop new capacities and capabilities, while protecting its own vulnerabilities.” This guidance also contains a new emphasis in the area of DSCA during natural and man-made disasters, noting that this support will rely heavily on vertical and horizontal interoperable interagency communication, coordination, and collaboration. Additional policy documents support information

---

31. National Defense Strategy. 2008. Available at <http://www.defenselink.mil/pubs/2008NationalDefenseStrategy.pdf> (Accessed November 2008)

sharing across joint DOD, intergovernment, interagency, and multinational efforts during events of national significance.<sup>32,33</sup>

The 2008 National Defense Authorization Act established a requirement for the Secretary of Defense to prepare a plan for response to natural disasters and terrorist events in the homeland. The Secretary of Defense, in consultation with the Secretary of Homeland Security, the Chairman of the Joint Chiefs of Staff, the Commander of the United States Northern Command, and the Chief of the National Guard Bureau, prepared a plan for coordinating the use of the National Guard and members of the Armed Forces on active duty when responding to natural disasters, acts of terrorism, and other man-made disasters as identified in national planning scenarios. This plan recognizes the need for an assured and interoperable communications and information-sharing plan.<sup>34</sup> This plan explicitly points to the need to communicate across disparate networks, with partners small and large, within government and the private sector, and many times with great urgency.<sup>35</sup> The planning for homeland defense can benefit from well-designed exercises and experiments with appropriate participation.

### ***DOD Organizations for Homeland Defense***

The U.S. Northern Command (USNORTHCOM) was established in 2002 to consolidate command and control of DOD homeland defense efforts and to coordinate defense support of civil authorities. Its area of responsibility encompasses the continental United States and Alaska. The defense of Hawaii and U.S. territories and possessions in the Pacific is the responsibility of U.S. Pacific Command (USPACOM). The commander of USNORTHCOM also commands the North American Aerospace Defense Command (NORAD), a bi-national command jointly operated with Canada. While USNORTHCOM plans, organizes, and executes missions, it has only a small permanent staff and is assigned

---

32. Department of Defense. Defense and National Leadership Command Capability. DOD Directive S-5100.44. July 9, 2008.

33. Department of Defense 2008. *Department of Defense Information Management and Information Technology Strategic Plan, 2008-2009*. Available at [http://www.defenselink.mil/cio-nii/docs/DoDCIO\\_Strat\\_Plan.pdf](http://www.defenselink.mil/cio-nii/docs/DoDCIO_Strat_Plan.pdf)

34. Report to Congress: *Plan for Coordinating National Guard and Federal Military Force Disaster Response*. August 29, 2008.

35. Department of Defense. 2006. *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations*. Joint Publication 3-08. Available at [http://www.dtic.mil/doctrine/jel/new\\_pubs/jp3\\_08v1.pdf](http://www.dtic.mil/doctrine/jel/new_pubs/jp3_08v1.pdf)



mission-specific forces as necessary. Mission responsibilities include natural disaster and terrorist event relief operations and counter-drug operations.

The National Guard and Reserve also plays an important role in DOD's HD/HS/DSCA mission. The emerging importance of the National Guard was evidenced when the Chief of the National Guard Bureau was elevated to a four-star officer in 2008. The National Guard serves a dual role, both as a state militia and a federal reserve force. In regular service, National Guard soldiers and airmen serve under the command and control of each state governor, but when mobilized for federal active service, they are under the command and control of the President. In its state role, a state governor can employ the National Guard for many tasks subject to the laws of the state.

This multiplicity of roles is a special challenge to interoperability both within the National Guard, and for any organization working with Guard personnel.<sup>36</sup> In 2003, a comprehensive reorganization of the National Guard structure enhanced unity of effort through the establishment of a Joint Force Headquarters-State (JFHQ-S) in each of 54 states and territories. A complementary restructuring of information technology support for the multiple activities and forms of National Guard participation in national homeland security and defense is still ongoing.

Interagency interoperability remains a challenge in support of the HD/HS/DSCA mission. While this is a primary mission for some organizations in the Department of Defense, this is not true across the Department. Entities with this focus include the National Guard Bureau, the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (OASD (HD&ASA)), the North American Aerospace Defense Command, and the U.S. Northern Command. The U.S. Pacific Command and U.S. Southern Command also protect relevant portions of the homeland.

---

36. This status can change under Title 32 of the U.S. Code, generally invoked in cases of national disaster, where the National Guard remains under the command and control of the state governor but personnel costs are paid by the federal government. A third status is under Title 10 of the U.S. Code, which takes effect when National Guard units are ordered into federal service under the command and control of the President. These status options afford quick and flexible response in times of need, but also add complexity. For example, the National Guard can carry out law enforcement tasks when under the command and control of the governor, but not when operating under Title 10 due to restrictions in the Posse Comitatus Act of 1878.

While homeland defense remains a federal mission, federal funding is typically not commensurate with the task and states are generally expected to maintain operational readiness. For example, in the U.S. Northern Command's Strategic Operations Information Sharing (SOIS) Plan of Action, all command and control nodes are funded for continuous (24/7/365) operation with the exception of the National Guard JFHQ-S Joint Operations Centers (JOCs). These JOCs are the DOD's first responders to incidents and situational awareness throughout the 54 states and territories, but all are currently only staffed during business hours (8/5/261). The task force feels this decision carries significant risk that should be carefully evaluated.

### ***Interagency Coordination***

In 2003, the Defense Science Board task force on Roles and Missions of the Department of Defense in Homeland Security completed their analysis and report just as the U.S. Northern Command and the Department of Homeland Security were established.<sup>37</sup> The report recognized the need for interagency processes to support an integrated security strategy, planning functions, and operational capabilities. It also recognized the need for processes to engage state and local governments, interoperable communications for command and control, and the need to develop solutions that reduce vulnerability to cyber attacks.

*DOD's ability to fulfill its missions—most notably force protection—is dependent on an intricate infrastructure in the United States. The majority of this infrastructure is not owned or controlled by DOD or the federal government, but by the private sector or state and local governments... Both physical and cyber attacks on the infrastructure are of concern.*

#### **DOD Roles and Missions in Homeland Security, 2003**

*Sound risk management and mitigation considers threat (capability and intent), vulnerabilities, consequences, and mitigation options. The task force discovered that the Department is far from practicing a risk-based approach...DOD further complicates the situation by implementing programs in response to specific threats, events, or concerns...each of which generates its own assessments, focuses on compliance rather than performance, and deals with current threats.*

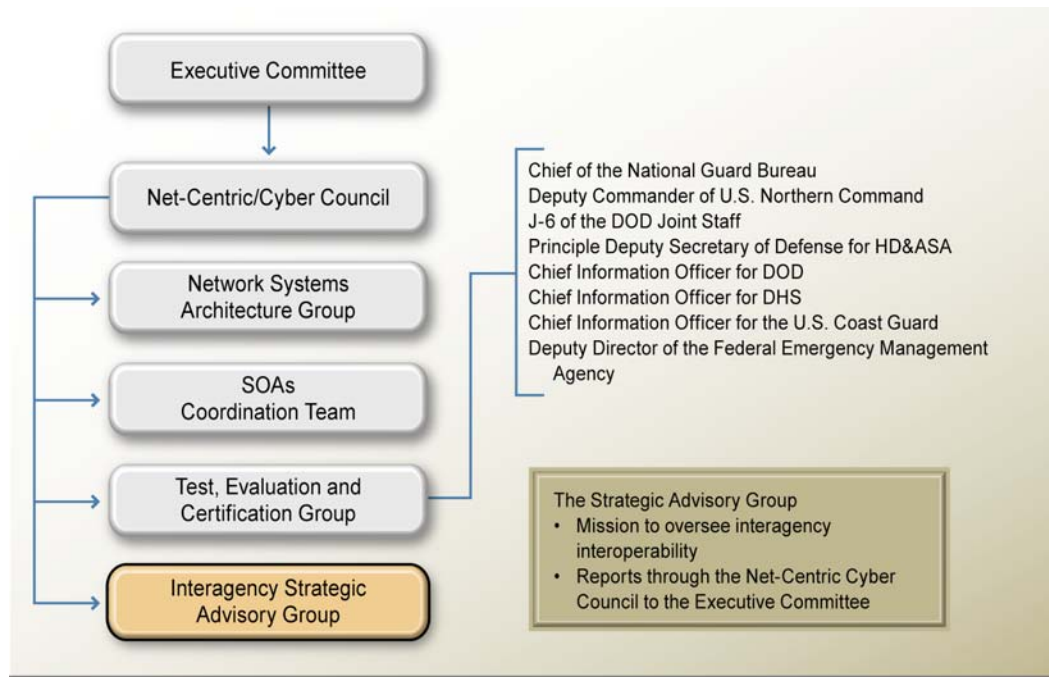
*...a much bigger issue lies outside the protection of DOD critical facilities alone. A starting focus should be in the area of protection of the country and its military national security mission capability...This study has recommended reasonable beliefs in protecting critical military facilities, including the defense industrial base. A second view would consider policies and strategies for making facilities less critical rather than just protecting critical facilities.*

#### **Critical Homeland Infrastructure Protection, 2007**

---

37. Defense Science Board. DOD Roles and Mission in Homeland Security. 2004. Available at <http://www.acq.osd.mil/dsb/reports/homelandss.pdf>

As a result of these recommendations, a Strategic Advisory Group (SAG) was established and chartered through 2010 by the Chief of the National Guard Bureau. Members of the SAG include key leadership from DOD and DHS, including the Chief of the National Guard Bureau, the director for command, control, communications, and computer systems (J-6) of the Joint Staff, the Deputy Commander of USNORTHCOM, the Principal Deputy Secretary of Defense for HD&ASA, the CIO of the DOD, the CIO of the Department of Homeland Security (DHS), the CIO of the U.S. Coast Guard, and the Deputy Director of the Federal Emergency Management Agency (FEMA). **The task force identified the SAG as an appropriate group to lead the execution of recommendations in this report** (Figure 9). A principal need is for DOD and DHS to synchronize their planning, programming, budgeting, and execution process to leverage common equipment, organization, and personnel requirements.



**Figure 9.** Role of the Interagency Strategic Advisory Group in the larger governance structure

## **Establishing a *Common and Constant* Communication, Coordination, and Collaboration Environment**

Ideally, if an incident were to occur, anyone with information to share could easily upload facts and analyses and, if they had a need, could download situation reports and analysis surrounding an incident from others with equal ease. All of this information would be tagged with times and locations that can be automatically correlated against other data. This would form the basis of a common operating picture (COP) that enables effective decision-making in a collaborative environment. Characteristics of the required COP include the following:

- Provides for immediate and continuous situational awareness for leadership at all levels of government.
- Shares tactics, technologies, and procedures at appropriate levels.
- Geolocates and time stamps information.
- Operates 24/7/365.
- Available in all JFHQ-S JOCs in all 54 states and territories.
- Available at incident sites.
- Able to quickly transition from routine operations to crisis operations.

### ***The Need for Constancy***

Because the HD/HS/DSCA mission exists 24 hours a day, 7 days a week, 365 days a year, the need for homeland defense collaborative environment staffing and funding for comprehensive, round-the-clock support in all 54 states and territories should be periodically re-examined. Today, the military Services fund this mission at the NGB Joint Communication Coordination Center (JCCC) and at each JFHQ-State Joint Operations Center (JOC). None of the JOCs are currently staffed for 24/7/365 operation.

### ***Barriers***

A number of barriers exist to implementing such a complex, interagency system. Some are technical, others cultural, and others are mired in policy that does not reflect shifts in either technology or culture. These barriers include the following:

- **Lack of common network access.** This access may be via cables, wireless, or satellite communications and coordinated centrally. While the distributed Internet is widely available, its reliability in times of crisis is not guaranteed. The need for dedicated network access for HD/HS/DSCA must be considered.
- **Lack of a common intranet.** Portal software such as Microsoft Sharepoint is used for various intranets across the HD/HS/DSCA community, including the Homeland Security Information Network (HSIN), Joint Information Exchange Environment (JIEE), Regional Information Sharing System Network, Law Enforcement Online, and others. However, there is no common portal (or interoperable arrangement of these existing intranets) that serves the entire community.
- **Lack of effective processes for information assurance** for classified, sensitive but unclassified (SBU) or controlled unclassified information (CUI), and unclassified information.

Most important may be the lack of standard operating procedures for appropriate interagency communication and information sharing that takes each of these factors into consideration. Addressing all of these barriers is necessary for success in the HD/HS/DSCA mission.

### ***Information Access and Assurance***

Different stove-piped information streams contribute to the COP result in many access points at the tactical edge—at JFHQ-S JOCs and incident sites—and introduce unneeded complexity in maintaining common communication, coordination, and collaboration among disparate users. Today, multiple unique networks and security domains drive a need for many servers, systems, keyboards, and display screens at the tactical edge, and also drive excessive supporting infrastructure requirements. The cost of such systems is elevated throughout the purchase, sustainment, and replacement life cycle.

Information pertinent to homeland defense comes from many sources, and can be from open sources, SBU/CUI, or classified information. The need by all parties concerned with HD/HS/DSCA—federal, state, tribal, local, and non-governmental organizations—to access this information is complex. To be useful, access needs to be on a daily basis rather than granted only when an emergency occurs. A number of portals exist that access parts of this information funded by various federal and state entities. On a positive note, information exchange

between the JIEE and the HSIN has been initiated.<sup>38</sup> The interoperability of existing federated portals and networks for this purpose must be considered.

Expansion of the DOD Common Access Card (CAC) credential to other federal agencies is an excellent step.<sup>39</sup> Further expansion to state, local, tribal, and non-governmental personnel should also be considered.

Currently, some important Secret-level information remains unavailable to cleared state and local personnel. Access is available through the National Counterterrorism Center under the DNI and the DHS Office of Intelligence and Analysis Web site on Intelink-S, but some sites are not accessible even to eligible personnel. Many sources of information hosted on SIPRNET, for example, are currently unavailable to most cleared regional, state, and local partners. The task force recommends the use of red teams to routinely test information assurance and identify system vulnerabilities in all interagency communication, coordination, and collaboration environments.

### ***A Common Intranet, and Standards for Interoperability***

Secure portals can provide common access to share information across different user platforms. A successful implementation is the Joint Continental United States Communications Support Environment (JCCSE). JCCSE provides situational awareness and information sharing capabilities on site at 54 state and territory JFHQ-S JOCs, including a common operational picture of Army and Air National Guards' information technology assets, and can link an incident site anywhere in the United States to state and national headquarters. The system directly supports National Guard soldiers and airmen engaged in HD/HS/DSCA missions. The three sub-components of JCCSE are the Joint Incident Site Communications Capability (JISCC), the Joint Communications Control Center (JCCC), and the Joint Information Exchange Environment (JIEE).

The Joint Communications Coordination Center is currently operated and managed by the Army Guard's 261st Theater Signal Brigade and the Air National Guard's 281st Combat Communications Squadron. Both organizations came

---

38. Colonel (Ret.) Scott Forster and Professor Bert Tussing. 2008. Reexamining the Role of the Guard and Reserves in Support to Civilian Authorities. Available at [http://www.csl.army.mil/usacsl/publications/IP\\_7\\_08\\_Reserve\\_Component\\_Symposium\\_Gp\\_1.pdf](http://www.csl.army.mil/usacsl/publications/IP_7_08_Reserve_Component_Symposium_Gp_1.pdf)

39. Deputy Secretary of Defense Directive-Type Memorandum 08-006, November 2008.

together to provide resources and capabilities after Hurricanes Katrina, Rita, and Wilma and provided the impetus to identify the requirements needed in a disaster situation and work together. **Lessons learned from Hurricanes Gustav and Ike showed the JCCC is now a proven capability and should be institutionalized to support the HD/HS/DSCA mission.** The Army CIO G-6 and the Air Force CIO A-6 should collaborate to institutionalize this function.

### *Developing a Reliable Network*

**A major impediment to fully implementing a HD/HS/DSCA collaboration environment is the lack of a reliable network.** The key role of the National Guard in homeland defense, homeland security, and defense support of civil authorities requires reliable and interoperable access to information sharing services. The National Guard has nearly 3,300 installations in over 2,700 communities; this wide physical deployment of the National Guard has made it particularly vulnerable to poor network connectivity, which has impacted assured information sharing and collaboration capabilities in support of domestic operations. Options for meeting this need for reliability exist and should be analyzed in order to establish the required HD/HS/DSCA network. This analysis should balance the costs and benefits of reliability and interoperability, and should also include a sound, practiced concepts of operations (CONOPS) for “fighting through” and operating successfully with intermittent connectivity, constrained bandwidth, and incomplete information.

Two network infrastructures—the Army GuardNet, and the Air Force Air National Guard Network—currently support National Guard activities at state and national levels. Neither network was designed to support the command, control, coordination, and collaboration central to the operational space of National Guard assets. The network capacity, security, and architecture are inadequate to meet current mission needs. Neither is funded as an operational network, and increased reliance on these as the National Guard’s joint operational network results in substantial risks in reliability, responsiveness, capacity, scalability, and security related to both current and emerging domestic operational mission requirements.

In order to rectify this situation, a number of options should be considered. One option is to extend the GIG-BE for the National Guard. A second option is to expand Defense Information System Network (DISN) Core Network Services to provide a National Guard backbone. Exploration of these concepts was recommended in the 2003 DSB Summer Study on DOD Roles and Mission

in Homeland Security, but no action has been taken toward implementation of either path.

A third option is to establish a joint network based on the existing assets in the Air National Guard network and the Army's GuardNet. The Army GuardNet is currently not compliant with the DOD Global Information Grid architecture. The Air Force is currently planning a major upgrade of their network to include support for the Air National Guard mission. A fourth option is to appoint one of the military Services as the executive agent to take responsibility for this network. **The task force does not recommend which of these to pursue, but definitely believes that the SAG should take action toward the selection, funding, and implementation of an option that supports these mission requirements.**

## Implementing the Vision

### *Communication, Coordination, and Collaboration*

Many interagency information sharing initiatives in support of HS/HS/DSCA were found by the task force to be tactically focused on near-term needs. Several specific efforts show promise toward the goal of unity of effort. One example of a successful effort is the development of the NORAD and USNORTHCOM (N-NC) Situational Awareness Geospatial Enterprise. The requirement for improved information sharing was identified by N-NC in late 2003. The intent was to develop both an unclassified enterprise architecture with a Web portal that provided real-time, geospatial, and live tracking of blue force data to any mission partner within or outside the federal government. The homeland defense Coalition Warfare Interoperability Demonstration in 2004 was a proof-of-concept for HD COP, a homeland defense common operating picture. Development continued with various funding initiatives until the approach was advocated by the Joint Staff J-3 as the DOD standard. The impediments were not centered on the requirement, but instead on obtaining joint advocacy and technical maturity. The initial requirement for an unclassified COP has now become an approved DOD CONOPS, is fully funded by N-NC, and is included as part of Increment 1 of the Net Enabled Command Capability.

The task force also endorses full implementation of the Joint CONUS Communications Support Environment (JCCSE) initiative in the National Guard Bureau (NGB). JCCSE is supported by senior leadership, and the construct of leveraging the National Guard for information exchange is highlighted in the U.S.



Northern Command CONOPS. In 2007, the Joint Requirements Oversight Council requested that the Army and Air Force provide sustainment funding for the JCCSE, with recognition that the final amount required would be finalized in the Service POMs. In this instance, the Air Force elected to comply with the Council's request, but the Army has not. Congress provided supplemental procurement funding that the NGB used to procure capabilities that were validated by the Council and are vital to filling near-term gaps. Currently without sustainment funds, this promising effort remains at risk.

The Strategic Operations Information Sharing Plan of Action (SOIS POA) sponsored by the U.S. Northern Command is commended as a way to move beyond documentation of roles and missions to a full governance plan for DHS, OSD, Joint Chiefs of Staff, N-NC, and NGB operations and command center information sharing processes during normal operations, significant events, incidents, crises, and exercises. This plan supports the national vision to create a situational awareness, collaboration, coordination, planning, decision-making, and execution environment.<sup>40</sup> The intent of this plan is to support active evolution of a broad framework for information management through the use of enterprise-wide, net-centric capabilities and shared standards among mission partners across the homeland security and homeland defense mission environment. Further, this plan will enable a process for continuous monitoring and reporting of relevant and critical elements of information to facilitate timely, risk-mitigated decisions by senior decision makers.

Another promising effort is the Task Force for Emergency Readiness (TFER) program led by FEMA. This is on the near-term horizon to establish a federally supported interface with state emergency management offices. Currently implemented in five pilot regions, it is focused on aiding states by integrating federal, state, and local planners and, as appropriate, non-governmental organizations into a state planning body. The TFER mission is strongly supported by the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (HD&ASA) and is designed to integrate national planning for communication, coordination, and collaboration and to build planning processes to identify and resolve information sharing and communication plans. The

---

40. National Command Capability Functional Requirements and Implementation Plan, July 2006

program also includes requirements for assessment and analysis and for testing and improving plans through exercises.

### ***National Telecommunications System***

After some serious failures in telecommunications interoperability during the Cuban missile crisis, the Department of Defense became a partner in commercial telecommunications in support of national security and emergency preparedness. In 1963, the Director of the Defense Communications Agency, with responsibility for communications for DOD's overseas missions supported by the Armed Services, also assumed responsibility for the National Communications System (NCS).<sup>41</sup> The NCS assumed coordination of the planning for and provisioning of national security and emergency preparedness communications for the federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution throughout the 54 states and territories.

Currently, 24 U.S. government organizations are represented on the NCS through a Committee of Principals. Each of these 24 NCS member organizations is represented on the Committee of Principals. The Committee provides advice and recommendations to the NCS and the National Security Council. The NCS also participates in joint industry-government planning through coordination with the President's National Security Telecommunications Advisory Committee (NSTAC). The NSTAC was established in 1982 to advise the President on appropriate assistance from the U.S. telecommunications industry for national security.

In 2003, after nearly 40 years with the Secretary of Defense serving as its executive agent, the NCS became part of the newly-formed Department of Homeland Security. Prior to this change, the Committee of Principals was co-chaired by the Director of DISA and the Assistant Secretary of Commerce for the National Telecommunications Information Agency. The Director of DISA was also the manager of the NCS and acted as secretariat to organize meetings for the Committee of Principals and the NSTAC and track actions.

The National Communications System has been a critical part of HD/HS/DCSA for decades, and is certain to continue in this important role. The U.S. telecommunications industry has demonstrated critical support to both homeland

---

41 The National Communication System website is available at <http://www.ncs.gov/about.html>

security and the global war on terror. In the homeland security mission, the NCS and commercial communications industry partnership play key roles in response to natural disasters and to terror attacks in the homeland.

Lessons learned from Hurricanes Katrina, Rita, Wilma, Gustav, and Ike and findings in the 9/11 Commission Report, reveal a number of interoperability challenges that must be addressed in an integrated manner. First responders—police, firefighters, and emergency medical technicians—could not communicate with other first responders or with the National Guard and other federal agencies. Frequency management and assignment was different in different locales and coordination of government agencies and commercial providers was poor in most instances. These delays had dramatic effects on disaster response. These findings reinforced those in the 2003 Defense Science Board Summer Study on DOD Roles and Missions in Homeland Security. A strong partnership between commercial telecommunication providers and the federal government is needed to resolve these issues. The NCS and the NSTAC team provides the U.S. government with critical telecommunications support.

DOD has long relied on the NCS to support homeland defense and provides substantial resources for protection and support of the NCS in times of crisis. While all 24 members of the Committee of Principals share this same dependence on reliable telecommunication, only DOD carries the responsibility to defend the infrastructure. Protection of this critical infrastructure must be done in close coordination with DHS and with the telecommunications industry. **For these reasons, the task force believes the Director of DISA can serve an important role as the co-chair of the Committee of Principals.**

An additional opportunity for collaboration is the recent DHS Office of Emergency Communications National Emergency Communications Plan with a need for coordination with existing and planned DOD infrastructure.<sup>42</sup>

---

42. National Emergency Communications Plan. July 31, 2008. Information at [http://www.dhs.gov/xnews/releases/pr\\_1217534334567.shtm](http://www.dhs.gov/xnews/releases/pr_1217534334567.shtm)

### ***Federated Interagency Test, Certification, and Technology Evaluation***

As discussed in Chapter 6, a federated interagency system to test, evaluate, and certify homeland defense and homeland security capabilities is needed. The military and the defense industry have developed many technologies that have clear usefulness for HD/HS/DSCA. What is unknown is how these work with existing homeland security networks.

The ability to test for interoperability before acquisition could greatly expand the applicability of all C4 systems to both the warfighter mission and the HD/HS/DSCA mission. When Service capabilities are developed without consideration of domestic mission communication and coordination requirements, interoperability challenges are created as well as the inability to fully leverage potential economies of scale. As the Services move closer to shared enterprise and thin client approaches, the opportunity for dual benefit is even greater. The communications industry is moving increasingly toward national standards and open architectures. If DOD could test, evaluate, certify, build, and field capabilities in coordination with interagency needs, real national cost savings would be realized.

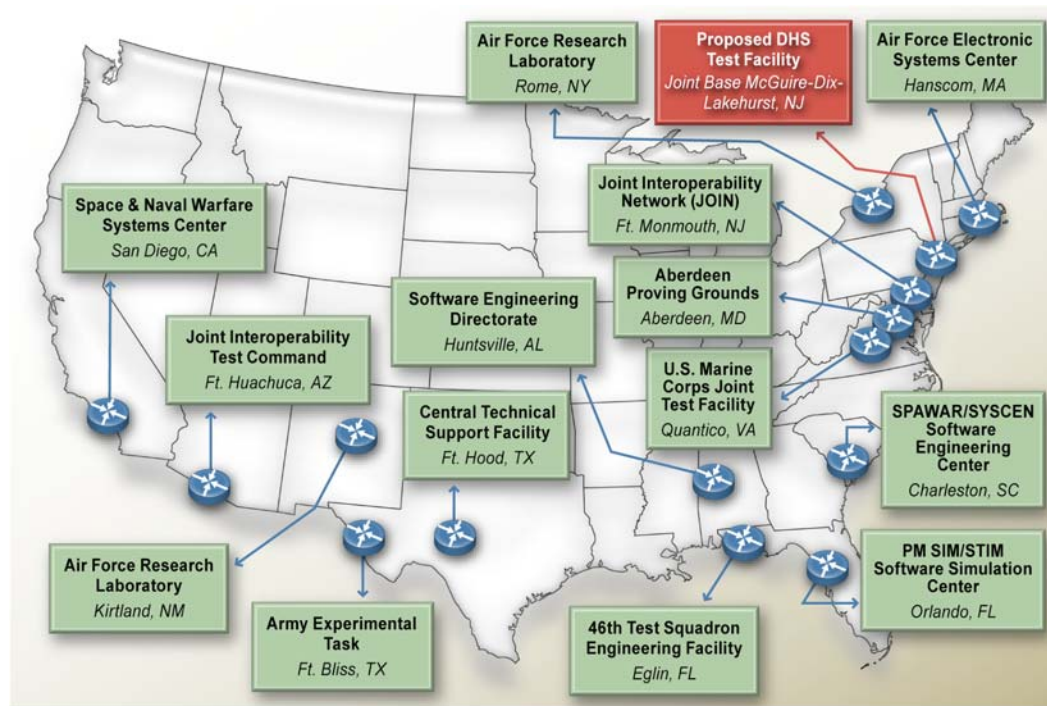
Standard procedures and communication elements should include messaging interface standards to enable emergency information sharing and data exchange. An interagency standards compliance assessment program should include the full range of public safety communications standards for both voice and data communications to ensure compatibility.

All secure communication processes and capabilities across the interagency continuum, including state and local entities, should be tested regularly. In all areas of network connectivity, radio interoperability, telecommunications capability, and data sharing, establishing and improving tactics, techniques, procedures, and the ability to coordinate and collaborate under pressure is paramount. Without regular testing, the risk of changes to components or connections that lead to failure is high.

An important focus is the leveraging of commercial capability and common communications at the tactical edge for unified interoperability. A primary example is radio-over-IP mobile capability that connects data and voice communication even in low-bandwidth conditions through universal gateways. This has the potential to connect disparate current and legacy communication

systems—cellular, 3G, land mobile radio, mobile data, paging, satellite, broadcast, and wireless networks—without the prohibitive cost of driving all users to a single platform solution. Without adequate testing, however, failure of interoperability is likely.

**New technologies are expected to be introduced both by the DHS Science and Technology (S&T) Directorate and by the military Services and the capability to evaluate them will need to continue and evolve.** The proposed DHS center at the Joint Mega Base (combining McGuire Air Force Base, Lakehurst Naval Engineering Center, and Fort Dix) may address many of these goals. This proposed DHS test facility is shown in Figure 10. The task force identified the ASD(HD&ASA) as the appropriate liaison for this activity within DOD.



**Figure 10.** Participants in a proposed federated test, evaluation, and certification network—including the proposed DHS facility at the Joint Base McGuire-Dix-Lakehurst

Such a shared environment is needed to discover and design, build, test, and certify communication, coordination, and collaboration interagency technologies from the start of programs at individual agencies. In the future, this federated capability should be expanded to include additional federal laboratories and federally funded research and development centers, such as those operated for

DOD and DOE. Leveraging the national research laboratory system, as well as the defense Service laboratories, is expected to contribute new testing and evaluation methods and new interoperability capabilities.

### *Joint Exercises and Experiments*

**Interagency exercises and experiments are a very useful tool to identify and resolve homeland defense, homeland security, and civil support interoperability issues.** Practice before an actual situation occurs is a long-recognized method to ensure future success. Such exercises are critically important to establish interoperability awareness and identify gaps in technology and tactics, techniques, and procedures among military responders, public health and other agencies, non-governmental organizations, industry partners, and state and local first responders.

Numerous councils, committees, and task forces are focused on domestic operations planning, populated by personnel from DOD, DHS, and other interagency partners. The National Exercise Program, established in 2007 by the Department of Homeland Security provides a framework for prioritizing and coordinating federal, regional, and state exercise activities without replacing any individual department or agency exercises. The program enables alignment of federal, state, and local departments and agencies on a five-year schedule of tiered exercises, and includes issuing annual exercise planning guidance derived from a strategic review of risks including threats, hazards, and operational vulnerabilities.

A recent opportunity to improve interoperability in HD/HS/DSCA was Noble Resolve, a USJFCOM experimentation campaign plan to enhance homeland defense and improve defense support of civil authorities in advance of and following natural and man-made disasters. In 2008, USJFCOM, USNORTHCOM, and USPACOM partnered with organizations from across the government including the Department of Homeland Security, the National Guard Bureau and National Guard, emergency management organizations from several states, and nongovernmental aid organizations. Together, they worked to integrate and synchronize joint experimentation in the areas of homeland defense and defense support of civil authorities and provided information sharing and synchronization solutions.

In June 2008, USJFCOM announced that DOD no longer plans to execute an overarching Noble Resolve 09 campaign.<sup>43</sup> Instead, their homeland defense experiments will be executed as smaller, discrete venues.

DOD participation and leadership in such experiments and exercises is clearly needed, especially concerning areas affecting DOD bases. There is no doubt that DOD will be a major contributor during an actual crisis situation, and their full participation during regular and comprehensive interagency exercises and experiments is critical for success. These focused exercises and experiments drive resource and operation decisions for interoperable communication, coordination, and collaboration. They deliberately probe the mission responsibilities and interoperability of communications of DOD partners. Red teams used in such exercises also test and identify system vulnerabilities for information assurance, especially around interagency seams.

Independent military exercises, however well planned and executed, will not necessarily reveal DOD's mission responsibilities as part of an interagency response. To ensure relevance of these exercises and experiments, HD/HS/DSCA readiness indicators should be included in DOD operational readiness assessments and leadership evaluations.

## The Role of Advocacy

While Service advocacy was appropriate to resolve these issues prior to 2001, the changed national landscape that coalesced organizational response for HD/HS/DSCA missions, points to the need for an equivalent change in DOD advocacy for a joint communications environment. This task force has identified lack of appropriate advocacy as a key impediment to accomplishing the necessary enhancements to the National Guard's network infrastructure and for supporting the JCCSE.

The Department's experience with the national counter narcotic mission provides an appropriate model for advocacy and implementation. ADNET, a

---

43. Col Gene Taylor, U.S. Air Force, USJFCOM Noble Resolve Campaign Lead. "Noble Resolve FPC/CDC Schedule Change" dated June 9, 2008. The Final Planning Conference/Cross-Domain Collaborative (FPC/CDC) was planned for June 24-25, and the Initial Planning Conference (IPC) for Noble Resolve 2009 was scheduled for June 26. The time set aside for the IPC was repurposed in this memorandum.

SECRET-level enclave of the DOD SIPRNET, provides connectivity for the national counter narcotics mission. Advocacy from the Assistant Secretary of Defense for Counter Narcotics led to the establishment of requirements and funding for ADNET. Program support for ADNET is currently executed by DISA. **The ASD (HD&ASA) is the appropriate advocate for the JCCSE.**

To support this advocacy, the task force also observed the need for effective assessments of Service POM investments against strategic guidance in the National Defense Strategy related to HD/HS/DSCA. The Office of the Assistant Secretary of Defense for Program Analysis and Evaluation (ASD (PA&E)) has the responsibility to assess service POMs. The requirements of DOD support to HD/HS/DSCA requirements needs additional attention in this area.



## Chapter 8. The Human Dimension

Ultimately, people are the end users of information. This includes how people learn what information is available, how people interpret information, how people use the information, and finally, how human behavior can enable or undermine interoperability.

If the purpose of a net-centric/cyber enterprise is to share information, then it becomes important that information is easy to find and share. Often, end users are unaware of the kinds of information that are available and encounter difficulty in accessing it. Considering the human dimension from the beginning—during system concept planning—addresses the tradeoffs that are possible among hardware, operability, and interoperability. If this aspect is left any later, there is no opportunity to integrate usability into the system. If usability is left as training development at the end of a program, there is inevitably no funding left for it, and little chance of real improvement in interoperability.

### Cultural Drivers for Decision Making

Net-centric interoperability and information security are entrusted to the same people. While anecdotes and horror stories may help convince users to choose wisely, the Net-Centric/Cyber Council and the SAG need data on the value of interoperability to support decisions that will inevitably raise the cost of a system. Without data, reasoned, global decisions, whether to pay for interoperability or not, are unlikely. Changing individual behaviors and attitudes is a major challenge, but if the user's motivations don't change, no amount of governance from the top will succeed.

Users dislike systems that impose a degree of global control over their personal desktops. Users complain that they can't do things they want or need to do within these constraints. However, the users generally have little notion of the value that having common software delivers or what they, or the government, might pay for more local control. It is impossible for a local user to understand all of the global effects of a few innocent changes on their personal device. Part of the problem is that humans notice exceptions that annoy but not routine behavior that works. Security and interoperability are not visible when they are working, and thus users and managers must understand what is gained by security and interoperability and what is lost if they fail.

Although current information systems and networking technology can address many defense and DSCA operational needs, technology is evolving at a rate that continues to leave behind those government and industry organizations that lack the agility to embrace it at an equal rate. The military has many unique applications, but the underlying systems that enable their operation have many similarities with processing, distribution, and usage in other government, academic, industrial, and personal information systems. It has been amply illustrated that satisfaction of operational military needs has not kept up with technology capabilities. Several reasons exist for this failure to map capability improvement velocity to the increasing pace of technology advancement. One challenge is an embedded institutional culture; another challenge is a regulatory and acquisition environment that was developed with platforms and analog services as its basis. Achieving the designed agility will require institutionalizing a culture of risk taking and risk management.

Training at all levels is key to success. **The first priority is to educate the Council and the SAG, next to educate senior leadership, and then flow all of this down to the acquisition and logistics core, operations, and ultimately to the tactical edge.**

## A Hierarchy of Training

Today's training on net-centric/cyber interoperability does not adequately address the reality of the situation today. In DOD there is the need for a major education and training program at all levels. This program will need continuous, real-time updating in order to keep up with, and adequately address, the current training requirements. Each Service, as well as DOD, should have net-centric/cyber training and education in all of their schools, and should provide required programs on a continuous basis for personnel in leadership roles.

Training is needed at the tactical edge for users under pressure and for local users whose innocent actions can impair interoperability. It is also needed for the technicians who can disrupt interoperability by inappropriate installation, configuration, or maintenance actions. The broad class of managers who can undermine interoperability by programmatic and purchasing decisions also need training.

### *Senior Leadership Training*

In 1998, a two-day course on Digital Information Systems and Technology was implemented to give senior officers a general technical background and a forum for discussion. Over 100 general officers took advantage of the course between 1998 to 2004, including the Chief of Staff of the Army and the Chairman of the Joint Chiefs of Staff. In August 2005, a finely tuned, more operationally oriented version of the course was made mandatory for all general officers in the Army. This course provides an opportunity for the attendees to get a quick review of network technologies and a more in-depth understanding of its true power. To date, over 500 senior Army personnel have attended the course. The potential to expand similar training across DOD and the federal government should be considered.

### *Using the Network*

It seems only fitting to use the latest in information technology to create and enrich training for all levels—top, middle, and edge. However, a balance is needed in skill sets between cyber and traditional communication capabilities (i.e., computers, phones, radios, wires, and infrastructure). Communication solutions are not exclusively data and cyber—hard-wired fiber, voice, and spectrum continue to play an important role.

A desirable training and education program could include readily available desktop-based training systems that contain digital tutors that interact with students in the same way that human tutors do, posing problems, remediating gaps in an individual student's knowledge, and challenging them to learn more. These systems mimic the interaction between human tutors and learners and, at small scale, have proven to be as good and fast as human tutors. Use of such tools for the technical as well as the non-technical training in network use, security, and maintenance would go a long way toward ensuring that people at all levels would make informed choices affecting interoperability, security, and information assurance.

Truly interactive training tools are needed that can customize the training to the individual. Human tutors are very difficult to train and costly to reproduce. Good tutors are even harder. Digital tutors, if effective, should change the equation. **DARPA's Education Dominance digital tutor program shows promise for improved training effectiveness and reduced cost.** The Net-Centric/Cyber Council and the Strategic Advisory Group should evaluate this program and incorporate it into their planning as it becomes viable.

All Services and agencies should develop a training and training resource plan. As recommended in earlier reports on training, developers of net-centric/cyber programs going forward should design and implement a training and training resource program as a part of their overall system development process.<sup>44,45</sup> These plans should be submitted for coordination to the Net-Centric/Cyber Council. Of course, such training should be interoperable among the Services. Further, DOD and DHS should form a study team that will lay out a training and training resource program for this critical homeland defense, homeland security, and defense support of civil authorities mission area.

## Responsibilities for Information Sharing

Like technology transfer, the concept of sharing information will not happen by delivery of directives and documents, but by movement of people. The process can be seeded by creating a cadre of people for whom interoperability of knowledge is a direct, everyday mandate. This group should consist of senior-level people who discover organizational information holdings, know the anthropology of information and its distribution, and reveal its value to those who otherwise would not know of its existence. Substantial information interoperability could be enabled within and beyond DOD with minimal hardware or software cost in this way.

If the concept of sharing information among organizations becomes a full-time function rather than a collateral duty to be addressed in a staff officer's spare time, then new ways to make data available will emerge. Establishing billets for this purpose makes sense within a number of organizations and agencies. The DOD CIO will also need to foster the growth of professionals in this new field of endeavor by supporting interagency conferences and journals.

In the HD/HS/DSCA area, difficulties in information interoperability require good interpersonal skills. Beyond operational and technological savvy, an additional characteristic an information broker should possess in this context is skill in outreach and a degree of tact in working with others who may be suspicious of outsiders. Personnel charged with this mission not only need to

---

44. Defense Science Board. 2001. Training Superiority and Training Surprise. Available at <http://www.acq.osd.mil/dsb/reports/trainingsuperiority.pdf>

45. Defense Science Board. 2003. Training for Future Conflicts. Available at <http://www.acq.osd.mil/dsb/reports/tfc.pdf>

know how their own organization works, but how prospective users of their data operate, and how they might utilize an unfamiliar source of information.

Today, the U.S. Northern Command has two full-time positions and has trained a number of others for this duty. USNORTHCOM reported that these positions were exercised with some success during the 2007 California wild fires. That operation exposed the need for those charged with sharing knowledge to be senior-level with operational savvy and the capability to understand the human dimension of information needs and distribution. This need also raises the larger issue that interoperability is in essence a parallel rather than hierarchical business. At its core, net-centricity is intended to avoid bottlenecks where one organization feels it must control and restrict the flow of information. Individuals charged to break such bottlenecks are needed at all echelons.

The task force believes there is value in expanding the concept of an information exchange broker or command knowledge-sharing officer for military commands and federal agencies.

## **The Essential Industry Contribution to Interoperability**

At their core, government operational needs are seldom unique. It is the ability to address those needs in their highly demanding operational contexts that differentiates them from the needs of any other enterprise. Examples of such requirements and descriptors are found in programs of record like Army Future Combat Systems, the Joint Tactical Radio System, the DHS One-Net, and others. The underlying information technology, networks, and communication schemes for all of these, however, are commercial components and designs.

The implementation of government and military systems involving information technology is done today by industry. While government operational requirements were once based solely on government standards, they are now more frequently stated in terms of commercial products and industrial knowledge services. Information technology increasingly defines platforms and systems of all types—sensors, decision option producers, and effectors—as collections of nodes that operate within and provide the fabric of modern networks. In turn, these collections of nodes depend upon information technology to gain the upper hand throughout the operational spectrum of every domain.

The speed of acquisition and integration of technology, however, has been vastly different between government and industry. Commercial technology advances at increasing rates in response to global market demands. Government systems are far slower to change, leading to conflicts on a number of levels. A recent Defense Science Board Task Force on Defense Industrial Structure for Transformation examined the defense industrial base's effectiveness at addressing many of these issues.<sup>46</sup> Key recommendations from that report that relate to interoperability included the recommendations to rebuild and reshape the government and industry workforce and that DOD should focus on interoperable, net-centric systems of systems with independent architects and enhanced government management and systems engineering capability.

The report also proposed a renewed effort to build a true partnership between government and industry. In the area of interoperability, organizations focused on this goal include the Network Centric Operations Industry Consortium (NCOIC) and the National Security Telecommunications Advisory Committee (NSTAC). **The task force recommends exploration of the NCOIC and the NSTAC as forums for improved communication, cooperation, and collaboration between government and industry.**

---

46. Defense Science Board. 2008. Creating an Effective National Security Industrial Base for the 21st Century: An Action Plan to Address the Coming Crisis. Available at <http://www.acq.osd.mil/dsb/reports/2008-07-DIST.pdf>

# **Part III**

---

*Actions for the First 500 Days*





## Chapter 9. Actions for the First 500 Days

A major recommendation to the Department of Defense (DOD) is the publication and implementation of a 500-day action plan. Such a plan is key to putting governance into action and achieving the goals of assured joint DOD and interagency interoperable net-centric enterprise described in this report.

These changes will come at a cost, and so the cost and associated benefits must be addressed within the programmatic context of DOD operations planning. The following actions are included as those that can and should be accomplished within the first 500 days within budgetary constraints.

The actions listed here are presented for input to the Secretary of Defense and the Net-Centric/Cyber Council as a starting point for moving DOD to a rapid transition to a prepared force to address and win the battles that now face us as a nation. The Council is charged with delineating clear actions, due dates, and responsible authorities based on these suggestions.

### **Strategic Goal 1:**

*Establish a governance system to create and manage an assured joint DOD and interagency interoperable net-centric enterprise*

#### **ACTION ITEM 1**

The Secretary of Defense should issue a directive memorandum to rapidly establish the governance system to create an assured joint DOD and interagency interoperable net-centric enterprise. This memorandum establishes a Net-Centric/Cyber Council co-chaired by the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff. The DOD Chief Information Officer (CIO) should be designated as the secretariat for the Council.

---

### ACTION ITEM 2

The DOD CIO should develop a DOD 500-day action plan for implementation by the Net-Centric/Cyber Council based on the actions in Part III of this report. The 500-day plan should encompass budget and program execution.

---

## Strategic Goal 2:

*Establish a heterogeneous network for defense communication*

### ACTION ITEM 3

The Net-Centric/Cyber Council should charter a strong Network System Architecture Group (NSAG) assigned to the Defense Information Systems Agency (DISA) which will be made up of core technical staff with extensive technical experience in networking, independent of the individual network portfolios, and augmented by technical representatives from all services and major programs. The NSAG will also develop supporting cost, budget, and program objective memorandum (POM) data for DOD.

---

### ACTION ITEM 4

The Network System Architecture Group should assess shortcomings in current network hardware and architectures and perform a gap analysis. The group should publish an architecture and execution roadmap to provide architectural oversight of acquisition programs. This is an immediate need for many programs on the verge of or starting final procurements.

---

### ACTION ITEM 5

The Network System Architecture Group should frame outstanding architecture problems and directions for further research and development (R&D) to reduce risks. Several network visions within DOD lack firm technical foundations and it is imperative that R&D programs be initiated to address these problems.

---

#### ACTION ITEM 6

The Network System Architecture Group should establish standards for services and quality of service that users on the network should expect. Users need an accessible understanding of the realistic level of core and enhanced network service to support future operations to allow operations planning according to these capabilities.

---

#### ACTION ITEM 7

The Net-Centric/Cyber Council should direct DISA to establish a senior-level technical and management-level leadership with a strong technical engineering team to address a common service oriented architecture (SOA) across DOD. This team should coordinate with the Network System Architecture Group to determine the appropriate level of implementation of SOA on a heterogeneous defense network.

---

#### ACTION ITEM 8

The U.S. Strategic Command (USSTRATCOM), acting as a member of the Council, should establish leadership in implementing recommendations of the Network System Architecture Group for a DOD heterogeneous network and SOAs.

---

### **Strategic Goal 3:**

***Integrate information assurance as part of interoperability in a net-centric environment***

#### ACTION ITEM 9

The Net-Centric/Cyber Council should direct USSTRATCOM to examine a few selected systems (e.g., command and control, weapons platform) to identify what top-tier cyber adversaries might do and the resulting likely mission impacts, and to recommend specific changes to the design, implementation, or processes that might best mitigate the threats.

---

**ACTION ITEM 10**

The Net-Centric/Cyber Council should direct USSTRATCOM to establish information readiness assessment capability to include situational awareness of a cyber attack, up-to-date mechanisms for defending against known and novel attacks, contingency planning for fighting through an information outage, methods for achieving mission effectiveness while operating in a degraded mode, and extensive training for system users and administrators on how to restore operations as quickly and orderly as possible.

**ACTION ITEM 11**

USSTRATCOM and the National Security Agency (NSA), acting as a members of the Council, should develop battle mode protection requirements for specific net-centric mission essential functions. This should entail identifying thin line functions, minimal interoperability threads, capabilities for resilience and reconstruction, and a characterization of battle mode identity and access management.

**ACTION ITEM 12**

The Net-Centric/Cyber Council should direct USSTRATCOM to develop a DOD awareness campaign to raise the level of understanding and appreciation of the cyber threat and what is needed to counter it.

**Strategic Goal 4:**

***Develop a joint DOD and interagency test, evaluation, and certification policy and practice***

**ACTION ITEM 13**

The U.S. Joint Forces Command (USJFCOM), acting as a member of the Council, supported by DISA and the Services, should establish a federated, virtual, joint DOD, integrated, test, evaluation, and certification system and network and should establish leadership in identifying joint DOD and interagency test scenarios, test exercises, and demonstrations.

**ACTION ITEM 14**

The Net-Centric/Cyber Council should designate DISA to define certification test processes, methodologies, and infrastructures, and to accredit test centers of excellence to provide a basis to enforce “test by one, accept by all” practices within a federated system.

---

**ACTION ITEM 15**

The Net-Centric/Cyber Council should direct DISA to establish interoperability standards and metrics to be included as part of the requirements acquisition processes.

---

**ACTION ITEM 16**

The Net-Centric/Cyber Council should direct the DOD staff to develop the policies and implementation strategies that will require interoperability testing during the system development phases.

---

**Strategic Goal 5:**

***Establish interoperable net-centric systems between the Department of Homeland Security (DHS) and DOD***

**ACTION ITEM 17**

DOD and DHS should reestablish the interagency Strategic Advisory Group (SAG) chartered by the National Guard Bureau (NGB) as a formal DOD and DHS deliberative interagency, planning, programming, and resource decision process for homeland defense, homeland security, and defense support of civil authorities.

---

**ACTION ITEM 18**

The Strategic Advisory Group should monitor and ensure implementation of the U.S. Northern Command (USNORTHCOM) sponsored Strategic Operations Information Sharing Plan of Action initiative and should analyze results of the five current pilot programs of the Task Force for Emergency Readiness and provide input for a nationwide capability.

---

**ACTION ITEM 19**

The Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD (HD&ASA)) working with DHS Science and Technology Directorate should create a federated interagency test, evaluation, and certification system for homeland defense and homeland security capabilities. Integrate a center for this purpose to be located at the Joint Base McGuire-Dix-Lakehurst. This center should seek to leverage the national research laboratory system to expand and improve this network.

---

**ACTION ITEM 20**

USJFCOM should ensure full DOD participation in interagency exercises and experimentation to identify and resolve interoperability issues before an actual situation occurs for homeland defense, homeland security, and defense support of civil authorities.

---

**ACTION ITEM 21**

DOD and DHS should reestablish the DOD co-chair role on the Committee of Principals supporting the National Communications System and support and participate in the implementation of the DHS Office of Emergency Communications National Emergency Communications Plan.

---

**ACTION ITEM 22**

The ASD (HD&ASA) should assume primary responsibility for advocating on behalf of NGB and for the National Guard enterprise information technology requirements. In conjunction with the DOD CIO and the J-6 of the Joint Staff, the ASD (HS&ASA) should conduct an immediate analysis of the National Guard network support requirements and the shortfalls in order to develop, select, fund, and implement appropriate courses of action.

---

**ACTION ITEM 23**

The ASD (HD&ASA), working with DISA and NGB, should ensure access to a consistent and constant (24/7/365) ability for USNORTHCOM, NGB and National Guard Joint Forces Headquarters-State, and DHS to share information relevant to homeland defense and defense support of civil authorities. The Strategic Advisory Group should evaluate the risk and cost issues surrounding this support in order to develop the inputs for the POM going forward.

---

**ACTION ITEM 24**

The Army CIO G-6 and the Air Force CIO A-6 should collaborate to institutionalize and align the Joint Communications Coordination Center (JCCC) to NGB in support of both NGB and USNORTHCOM requirements. The JCCC is operated and managed by the Army Guard's 261st Theater Signal Brigade and the Air Guard's 281st Combat Communications Squadron.

---

**ACTION ITEM 25**

The Strategic Advisory Group should evaluate the sources of sensitive but unclassified (SBU) or controlled unclassified information (CUI) and classified information and the need by all parties concerned with homeland defense—federal, state, tribal, local, and non-governmental organizations—to access this information on a daily basis in preparation for emergency situations. The Strategic Advisory Group should consider the interoperability of existing federated portals and networks for this purpose.

---

## Strategic Goal 6:

*Focus on the human dimension and training for interoperable net-centric systems*

### ACTION ITEM 26

All DOD leadership schools should implement curriculum elements for leadership training on netcentricity and cyber defense. The Army education program on netcentricity and cyber defense for senior military and civilian personnel should be considered as a possible model for such training across DOD and the federal government.

### ACTION ITEM 27

The ASD (HD&ASA), working with DHS, should collaborate in the design for a joint interagency training and training resource program for the mission for homeland defense, homeland security, and defense support of civil authorities.

### ACTION ITEM 28

The Net-Centric/Cyber Council should mandate that established training standards and metrics be included as part of the requirements acquisition processes, and be co-equal with other subsystems funded within the acquisition.

### ACTION ITEM 29

The DOD CIO and the DHS CIO should explore the Network Centric Operations Industry Consortium (NCOIC) and the National Security Telecommunications Advisory Committee (NSTAC) to obtain greater cooperation and collaboration between government and industry.



## Appendix A. Relevant Government Directives, Letters, and Memoranda

Name of Document	Date	Author
Capability Portfolio Management	25 Sept 2008	Deputy Secretary of Defense
Transferring DOD Technology to Protect the Homeland	22 Apr 2008	Assistant Secretary of Defense, Homeland Defense
DOD and Intelligence Community (IC) Commitment to Converge Authorization and Attribute Services Initiatives	21 Apr 2008	DOD Chief Information Officer
The Definition of "Cyberspace"	12 May 2008	Deputy Secretary of Defense
Terms of Reference for Defense Science Board (DSB) Task Force on the Department of Defense Policies and Procedures for the Acquisition of Information Technology	1 May 2008	Under Secretary of Defense, Acquisition, Technology, and Logistics
Memo: Transformation Effort	16 Apr 2008	Vice Chairman, Joint Chiefs of Staff
DHS Secretary Chertoff Letter to the Defense Science Board	25 Feb 2008	Secretary of Homeland Security
Interoperability & Supportability of Information Technology and National Security Systems	May 5, 2004	DOD Chief Information Officer
Procedures for Interoperability and Supportability of Information Technology and National Security Systems	June 30 2004	DOD Chief Information Officer



## Appendix B. Draft Directive

The following is draft language for consideration by the Secretary of Defense to support the findings and recommendations in this report.

---

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS  
 CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
 COMMANDER, U.S. STRATEGIC COMMAND  
 COMMANDER, U.S. JOINT FORCES COMMAND  
 COMMANDER, USNORTHCOM  
 COMMANDER, USPACOM  
 UNDER SECRETARIES OF DEFENSE  
 ASSISTANT SECRETARIES OF DEFENSE  
 GENERAL COUNSEL OF THE DEPARTMENTS OF  
 DEFENSE  
 DIRECTOR, NATIONAL SECURITY AGENCY  
 DIRECTOR, OPERATIONAL TEST AND EVALUATION  
 INSPECTOR GENERAL OF THE DEPARTMENT OF  
 DEFENSE  
 ASSISTANTS TO THE SECRETARY OF DEFENSE  
 DIRECTOR, ADMINISTRATION AND MANAGEMENT  
 DIRECTOR, PROGRAM ANALYSIS AND  
 EVALUATION  
 DIRECTOR, NET ASSESSMENT  
 DIRECTORS OF THE DEFENSE AGENCIES  
 DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Creating an Assured Joint DOD and Interagency Interoperable Net-Centric Enterprise

Achieving interoperability in an assured net-centric environment is recognized as fundamental to achieving the full potential of transformation. While interoperable forces demonstrate superior performance in combat environments, in defense support of civilian authorities, and in all other functions of the Department, the Defense Science Board recently concluded that the Department of Defense is far from achieving the goals of assured interoperability in the evolving net-centric/cyber environment.

To meet these challenges, I am establishing a Net-Centric/Cyber Council to act as a governing body for this enterprise within the Department of Defense. The Council will be co-chaired by the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff. The Department of Defense CIO will act as Secretariat to the Council.

This Council will have the following members:

- Commander of U.S. Strategic Command
- Commander of the U.S. Joint Forces Command
- Commander of the U.S. Northern Command
- Director of the National Security Agency
- Vice Chiefs of the Services
- Under Secretaries and Assistant Secretaries in OSD
- Directors of the Joint Staff
- Director of the Defense Information Systems Agency
- Director of Defense Research and Engineering
- Chief of the National Guard Bureau
- Deputy Secretary of the Department of Homeland Security
- Principle Deputy Director of National Intelligence

I invite the Secretary of Homeland Security and the Director of National Intelligence to join me as members of an Executive Committee to oversee these activities.

I am further directing the Council to address the major recommendations described in the Defense Science Board report on *Creating an Assured Joint DOD and Interagency Interoperable Net-Centric Enterprise* and to further develop the issues and actions in the report with the goal of implementing a DOD-approved 500-day plan delineating clear actions, due dates, and responsible authorities. The Council should assure resource support for the approved actions in the plan, update the plan each year, and report to me quarterly.

## Appendix C. Challenges for Network Technologies

Tables 1 through 6 present a thorough list of the technical challenges for network technologies. Table 1 gives an outline overview of the problem areas of the different major components of the network architecture. Tables 2 through 5 expand on each of these components and provide more details on each area. In the tables, problem areas are labeled “yellow” (caution) and “red” (serious). Not listed here are numerous well addressed and executed areas that would be “green” Many of the concepts listed here are covered more fully in Chapter 3.

Table 1. Critical network areas of concern

Modality	Critical problem area	Commercial analog	Status of government directions
Wired	Support mixed traffic - packet and fast and slow ckt	Carrier-class ethernet and IP services	IP vision only, ckt not explicitly addressed
	Bursty large file transactions	Flow-switching	IP or long term ckt
	Security	Have not addressed sophisticated attacks	Deficient IA architecture
	High speed dynamic access	PON, flow and fast ckt switching	All static electronic connections as in current
	Internetworking with other modalities	Static connections at POP	Issues interfacing with mobility and changing channels
	Management and control of dynamic networks	Quasi-static	Some future dynamics too fast for commercial algorithms
	Interoperability of many wireless radios and networks	At most Quad-band	Cannot meet reasonable w/power/\$ goals
	Routing in MANET	Static and peer to peer	Hard to deal with changing topology and scaling
	Assured delivery with deadline	Ad hoc services, static	Ad hoc services, no guarantees
	Rapidly changing link rates due to motion and fading	Accept drop-outs and re-initiation	Faster dynamics and unstable routing and low thruputs
Wireless	Maintain connections with mobility	static	Disconnections, no beam forming and relays
	Scalable multiple access	ckts	Ckts U/L, no random access - not scalable
	Link delays effect on TCP	Much shorter delays, wired lines with long delays has problems with thruput	Not addressed properly, problem with internetworking and low thruputs
	Rapidly changing link capacities affect TCP	No analog	TSAT's effects on higher layer protocols likely to be bad but not quantified
	Must have a time statistical model of channel	Lower frequency satellites with less fades	Not adequately addressed
	Efficient Internetworking	Gateways and BGP's	Current gateway solutions too static, does not re-route and have serious issue with security and crypto.
	Internetworking at physical layer	Static and quasi-static capacities	Dynamic and fast changing capacities
	Control plane	Tuned control planes to media, quasi-static IP based	No Master Control Plane and IA protection
	Robust messaging for control	Over provisioning	No robust messaging mode
	Time deadline	SOA network burden	Hard to provide QoS over current gateways
Inter-network	SOA network burden	Assume fiber and high speed connections	Rate constrained tail link cannot use SOA
	Overall architecture must survive multiple generation of technologies and protocol changes	Survival of the fittest voted by \$	Static Government standards resistant to change
	Need coherent network architecture	Big service providers and equipment manufacturers lead architecture	No overall architecture group
	Must work over difficult environments	Business case for 95-99% environments	Defense applications often works in harsh environments
Architecture	Overall architecture must survive multiple generation of technologies and protocol changes	Survival of the fittest voted by \$	Static Government standards resistant to change
	Need coherent network architecture	Big service providers and equipment manufacturers lead architecture	No overall architecture group
Architecture	Must work over difficult environments	Business case for 95-99% environments	Defense applications often works in harsh environments

Table 2. Critical areas of concern for wired networks

Modality	Critical problem area	Commercial analog	Status of government directions
Wired	Support mixed traffic - packet and fast and slow ckt	Carrier-class ethernet and IP services -Next horizon will take care of VPN between enclaves @40-100Gbps quasi-static ckt switched -Most video broadcast continue not to be IP, e.g. FIOS	IP vision only, ckt not explicitly addressed -Must evolve with industry and incorporate "Carrier-class" Ethernet into the architecture -The important issue is not the specifics but the notion of carrying both IP and Ckts. -TCP will work much better with new transports
	Bursty large file transactions	Flow-switching -Emerging transport mechanism -Large transactions will be more efficient, cost-effective and less delay with flow switching -Probably wait for DoD first	IP or long term ckts -Efficient large transaction transfer critical -Being developed -Will be very useful for "enterprise-bus" plus network service architecture to be used by many high end network usage agencies.
	Security	Have not addressed sophisticated attacks -Network architectures and components barely works with co-user interference and natural fiber impairments	Deficient IA architecture -Vulnerabilities in Physical, MAC, Routing and Transport Layers -Physical and PON Mac Layers are different from traditional electronic networks
	High speed dynamic access	PON, flow and fast ckt switching -Dynamic service on demand will eventually come in play	All static electronic connections as in current commercial -Must anticipate new services in the commercial sector not just standardize on
	Internetworking with other modalities	Static connections at POP -Must come up to the Application Layer with delays and Proxies have vulnerabilities -Many current proxies cannot re-route quickly around problems -Only have to internet with rather static networks with predictable and slow changing capacities	Issues interfacing with mobility and changing channels -Issue with delays and crypto-key storage and re-keying when come up to Proxies at Application Layers -Dynamic defense networks needs fast re-routing around network failures and changing capacities -IA issues
	Management and control of dynamic networks	Quasi-static -Other than restoration (50ms) mostly done by human and quasi-static -No immediate needs for massive fast reconfiguration of networks	Some future dynamics too fast for commercial algorithms -Need for agile large bursty large transactions -Dynamically changing tail networks needs fast automated management -Need for more traffic monitoring and decisions for managing network against attacks and isolation of compromised subnets; IA

Table 3. Critical areas of concern for wireless networks

Modality	Critical problem area	Commercial analog	Status of government directions
Wireless	Interoperability of many wireless radios and networks	At most Quad-band <ul style="list-style-type: none"> <li>-Commercial systems more homogeneous and only a few are grouped together</li> <li>-Handsets only service subset of formats, e.g. either GSM or CDMA but not both</li> </ul>	Cannot meet reasonable w/power/\$ goals <ul style="list-style-type: none"> <li>-JTRS cannot deliver at targeted goals</li> <li>-Many more formats and frequencies to deal with</li> </ul>
	Routing in MANET	Static and peer to peer <ul style="list-style-type: none"> <li>-Rudimentary applications such as peer to peer and user to hub</li> </ul>	Hard to deal with changing topology and scaling <ul style="list-style-type: none"> <li>-Outstanding problem with user discovery, topology formation, routing and thruput scaling</li> <li>-Very hard to perform congestion and rate control on dynamically changing networks, routing algorithms may become unstable</li> <li>-Link State Protocols will have to operate frequently and consume large fraction of capacities to manage dynamic configurations</li> </ul>
	Assured delivery with deadline	Ad hoc services, static <ul style="list-style-type: none"> <li>-Mostly static connections have predictable QoS, still no guarantees</li> <li>-Very small population</li> </ul>	Ad hoc services, no guarantees <ul style="list-style-type: none"> <li>-Not possible to guarantee QoS due to unpredictable movements and propagation environment.</li> <li>-User rate highly dependent on other traffic and load of relay function, hard to guarantee rates</li> <li>-Disconnection due to mobility and propagation effects prevent QoS guarantees</li> </ul>
	Rapidly changing link rates due to motion and fading	Accept drop-outs and re-initiation <ul style="list-style-type: none"> <li>-Static situation present acceptable occasional drop-outs due to reflections and interference</li> </ul>	Faster dynamics and unstable routing and low thruputs <ul style="list-style-type: none"> <li>-Rapid dynamics present much more frequent drop-outs. TCP will have serious reactions and low thruputs</li> <li>-Drop-outs will cause rapid Routing Layer instabilities that may drive the network to instabilities.</li> </ul>
	Maintain connections with mobility	Static <ul style="list-style-type: none"> <li>-No commercial mobile MANET deployed</li> </ul>	Disconnections, no beam forming and relays <ul style="list-style-type: none"> <li>-Disconnections will require beam forming, and relay insertion to maintain network connections; not yet developed in current architectures.</li> </ul>



**Table 4. Critical areas of concern for SATCOM networks**

Modality	Critical problem area	Commercial analog	Status of government directions
Satcom	Scalable multiple access	<p>Ckts</p> <ul style="list-style-type: none"> <li>-Ckt services</li> <li>-Some future systems will use IP with random access modes</li> <li>-Split protocols via proxies and encapsulation of IP packets</li> <li>-Jammable</li> </ul>	<p>Ckts U/L, no random access - not scalable</p> <ul style="list-style-type: none"> <li>-Limited number of users served by TSAT</li> <li>-Need random access mode to be scalable in number of users</li> <li>-Due to long link distances, MAC protocol design are different from wireless systems</li> </ul>
	Link delays effect on TCP	<p>Much shorter delays, wired lines with long delays has problems with thruout</p> <ul style="list-style-type: none"> <li>-Work around using proxies and encapsulations</li> </ul>	<p>Not addressed properly, problem with internetworking and low thruputs</p> <ul style="list-style-type: none"> <li>-TCP over high rate satellite channels will suffer window closing and slow starts due to drop-outs resulting in low thruputs</li> <li>-Long outages will cause time-outs and require re-establishment of connections</li> </ul>
	Rapidly changing link capacities affect TCP	<p>No analog</p> <ul style="list-style-type: none"> <li>-All current satellite systems do not have dynamic rate adjustments, only suffers small efficiency loss due to lower frequency of operations and less drop-outs</li> </ul>	<p>TSAT's effects on higher layer protocols likely to be bad but not quantified</p> <ul style="list-style-type: none"> <li>-Fast channel rate adjustment not compatible with current routing layer algorithms; may lead to unstable routing</li> <li>-Hard to deal with congestion/rate control and buffer management in Network Layer</li> <li>-Large queuing delay variances may lead to Transport layer time-out of sessions.</li> </ul>
	Must have a time statistical model of channel	<p>Lower frequency satellites with less fades</p>	<p>Not adequately addressed</p> <ul style="list-style-type: none"> <li>-No dynamic model of TSAT channel behavior in turbulence and weather</li> <li>-Unable to quantify effects of channel effects on Routing and Transport Layers protocols</li> <li>-Will adversely impair inter-networking with other networks such as fiber and wireless networks</li> </ul>
	Efficient internetworking	<p>Gateways and BCP's</p> <ul style="list-style-type: none"> <li>-All scenarios quasi-static</li> </ul>	<p>Current gateway solutions too static, does not re-route and have serious issue with security and crypto.</p> <ul style="list-style-type: none"> <li>-Dynamic channel changes will have problem when interfaced with wired and wireless networks</li> <li>-Severity hard to quantify for lack of models</li> </ul>

**Table 5. Critical areas of concern for internetworking**

Modality	Critical problem area	Commercial analog	Status of government directions
Inter-network	Internetworking at physical layer	Static and quasi-static capacities –Currently both IP and ckt based –Ethernet will be an important format at Layers 1 and 2. –Capacities of subnets are typically rather static	Dynamic and fast changing capacities –Changing capacities can be as fast as 1s –Rate of change never encountered in commercial sector today nor anticipated –Will present serious problem to Routing and Transport Layers –Rapid changes may cause Routing Layer instabilities –Causes low thruputs in Transport Layer using TCP
	Control plane	Tuned control planes to media, quasi-static –Specialized control planes for each modalities even when they use IP. –Typically do not fully interact autonomously	No Master Control Plane and IA protection –Dynamic environment and policy driven networking needs coordination of resources –Rapid changes cannot wait for L-3 and L-4 reactions to congestions and user rate demands –Need for an overseer for IA monitoring and reaction
	Robust messaging for control	IP based –Not especially robust to attacks –Commercial grade authentication	No robust messaging mode –Robust messaging mode needed for critical control messages and monitoring of important parameters –Robust mode needed for critical messages essential for operations
	Time deadline	Over provisioning –Over-provisioning (~x5) used for guaranteeing time deadlines	Hard to provide QoS over current gateways –Tail links too expensive and capacities too scarce to use over-provisioning –Gateways and proxies present complex and sometimes unpredictable delays –Approach with resource aware networking needed to be effective (e.g. NDIS)
	SOA network burden	Assume fiber and high speed connections –Assumes web-based applications will work using TCP and high speed network with many roundtrips for discovery, negotiation, binding and operation	Rate constrained tail link cannot use SOA –Highly constrained user rates will not support applications with large network burden –Delay over satcom will create slow response of SOA applications due to the many roundtrips currently necessary –SOA must go through significant developments for extension beyond wired networks to open air tail links

Table 6. Critical areas of concern for network architecture

Modality	Critical problem area	Commercial analog	Status of government directions
Architecture	Overall architecture must survive multiple generation of technologies and protocol changes	Survival of the fittest voted by \$ -PSTN designed by MaBell over many years -Continued development of network management and control -Many standards, only a few with good properties survive	Static Government standards resistant to change -Should not standardize without thorough analysis, simulation and prototyping. -Choosing single standard is usually picked before survival of the fittest takes its course. may pick the wrong standard -Single standard prevents innovation and future radical changes -Will be out of step with the commercial sector in a few years with significant financial and technical implications
	Need coherent network architecture	Big service providers and equipment manufacturers lead architecture -Market place will be the ultimate decider -IETF although political have contributions from many excellent network architects	No overall architecture group -Many DoD networks are unique with no commercial counter parts -Stove pipe programs do not deal with interface to other networks well (no explicit budget) and often ignore this critical problem -Survival of the fittest not applicable to current DoD practices and thus an architect is needed for coherency
	Must work over difficult environments	Business case for 95-99% environments -Commercial systems are not designed to work in difficult environments -Technologies are well developed	Defense applications often works in harsh environments -Significant fraction of DoD applications must work in difficult environments – architecture must extend to these situations -Likely need significant modification, augmentation and even new architecture innovations to provide robust services for tall networks -IA



# Terms of Reference





ACQUISITION,  
TECHNOLOGY  
AND LOGISTICS

## THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3010

FEB 13 2008

### MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board (DSB) Task Force on  
Achieving Interoperability in a Net-Centric Environment

Achieving interoperability in a net-centric environment is recognized as fundamental to achieving the full potential of Transformation. Interoperable forces demonstrate superior performance in every operational environment. This is true in both combat environments and in the civilian sector where net-enabled devices are transforming the way people live and work. However, numerous impediments exist that have significantly delayed the achievement of the desired end state despite the demonstrated benefits of fully interoperable forces.

You are requested to establish a DSB Task Force on Interoperability in a Net-Centric Environment. The Task Force should assess different models of achieving interoperability. In assessing the different mechanisms to achieve interoperability, the Task Force must keep in mind the multiple organizations involved in DoD operations. These include, but are not limited to, the respective Military Departments, domestic support operations, coalition partners, and non-traditional partners (e.g., NGOs).

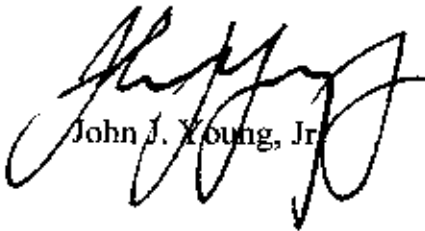
At a minimum, the Task Force should assess:

- The requirement for military operations in a net-centric environment;
- The use of a single autonomous agency as one mechanism to achieving interoperability (e.g., Army Central Technical Support Facility) established to integrate non-materiel and materiel solution sets for military operations in a net-centric environment;
- A standards-only approach allowing independent development of systems certified to the standards;
- The development of a virtual test, integration, and certification capability to assure interoperability of military operations in a net-centric environment;
- The ability of each model to establish and maintain configuration management amongst the multiple organizations involved in DoD operations;
- The potential to use current systems to incrementally evolve to net-centric capability, especially in light of the rapid evolution in the network domain contrasted with the lack of synchronized and comprehensive DoD modernization.



The Under Secretary of Defense for Acquisition, Technology and Logistics, the Under Secretary of Defense for Intelligence, the Assistant Secretary of Defense (Networks, and Information Integration), and the Commander, U.S. Strategic Command, will sponsor this study. The Honorable Art Money and Lieutenant General Bill Hilsman, USA (Ret.), will co-Chair the Task Force. Mr. David Jakubek of OUSD(AT&L), Mr. R.C. Porter of OUSD(I), and Mr. Jack Zavin of OASD(NII), will serve as co-Executive Secretaries. Commander Cliff Phillips, USN, will serve as the DSB Secretariat representative.

The Task Force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DOD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of title 18, U.S. Code, section 208, nor will it cause any member to be placed in the position of acting as a procurement official.



John J. Young, Jr.



# Task Force Membership

## CHAIRS

Name	Affiliation
LTG Bill Hilsman USA (Ret.)	Institute for Defense Analyses
Hon. Arthur Money	Private Consultant

## TASK FORCE MEMBERS

Mr. Michael Bayer	Private Consultant
LTG Steven Boutelle, USA (Ret.)	Private Consultant
Ms. Dale Brazale	Institute for Defense Analyses
LTG William Campbell USA (Ret.)	BAE Systems
Gen Michael Carns USAF (Ret.)	Private Consultant
Dr. Vincent Chan	Massachusetts Institute of Technology
Dr. Ralph Chatham	Private Consultant
ADM Archie Clemins USN (Ret.)	Caribou Technologies
Dr. Donald Duncan	Johns Hopkins University
Mr. Victor Ferlise	Private Consultant
Dr. Craig Fields	Private Consultant
Dr. Ted Gold	Private Consultant
Mr. James Gosler	Sandia National Laboratories
Mr. Al Grasso	MITRE
Dr. George Heilmeier	Private Consultant
Dr. Robert Hermann	Private Consultant
Dr. William Howard	Private Consultant
Lt Gen Ronald Kadish USAF (Ret.)	Booz Allen Hamilton
Dr. Paul Kaminski	Technovation, Inc.
Dr. Joe Markowitz	Private Consultant
Gen Jim McCarthy USAF (Ret.)	U.S. Air Force Academy
Lt Gen Carl O'Berry USAF (Ret.)	Private Consultant

MG Conrad Ponder USA (Ret.)	Booz Allen Hamilton
Lt Gen Harry Raduege USAF (Ret.)	Deloitte & Touche LLP
GEN Dennis Reimer USA (Ret)	Private Consultant
LTG Robert Shea USMC (Ret.)	Smartertronix, Inc.
RADM Ken Slaght USN (Ret.)	General Dynamics
Mr. John Stenbit	Private Consultant
ADM William Studeman USN (Ret.)	Private Consultant
Mr. Alan Wade	Private Consultant
Mr. Joe Wright	Scientific Games Corporation/ Member NSTAC

**EXECUTIVE SECRETARIES**

Mr. David Jakubek	AT&L
Mr. R.C. Porter	OUSD(I)
Mr. Jack Zavin	ASD (NII) DOD CIO

**DSB REPRESENTATIVE**

LTC Karen Walters	DSB Office, U.S. Army
-------------------	-----------------------

**GOVERNMENT ADVISORS**

Mr. Jeremy Armon	Army G6
Mr. Paul Blatch	U.S. Navy
Mr. Mark DallaBetta	USNORTHCOM
Mr. John Johnson	U.S. General Services Administration
Mr. Daniel Judy	USJFCOM
Brig Gen Allison Hickey	U.S. Air Force
LTC Mark Holloway	USNORTHCOM
Dr. Steven Hutchison	Defense Information Systems Agency
Ms. Rosanne Hynes	ASD Homeland Defense
MajGen Timothy Lowenberg	Washington Army and Air National Guard
Mr. Slade MacTaggart	Army G-6
Maj Gen Dale Meyerrose (Ret.)	Office of the Director of National Intelligence
Dr. Carter Morris	Department of Homeland Security

Mr. Michael Nicholson	Department of Homeland Security
Ms. Cecilia Phan	Joint Staff J-6CTO
LtCol Daniel Russ	Washington Air National Guard
Ms. Joan Smith	Army G6
COL Kent Woods	CECOM LCMC

**STAFF**

Joe Maniaci	Strategic Analysis, Inc.
Toni Maréchaux	Strategic Analysis, Inc.
Adam Savery	Strategic Analysis, Inc.



# Presentations to the Task Force

Name	Topic
<b>SEPTEMBER 18–19, 2007</b>	
HON Larry Burgess Deputy Undersecretary of Defense for Intelligence, Collection & Analysis Mission Management	Discussion of USD(I)
LTG Peter Chiarelli, USA Senior military advisor to the Secretary of Defense	Discussion of the state of interoperability in the U.S. Army
HON John Grimes Assistant Secretary of Defense for Networks and Information Integration & Department of Defense Chief Information Officer	ASD(NII) discussion
VADM Nancy Brown Director, Command, Control, Communications and Computer Systems (C4 Systems), Joint Staff (J-6)	J-6 discussion
HON Peter F. Verga Principal Deputy Assistant Secretary of Defense for Homeland Defense	Interoperability? Information Sharing? The Challenges
LtGen Charles Croom, USAF Director, DISA, & Commander, Joint Task Force–Global Network Operations	DISA discussion
GEN James E. Cartwright, USMC Vice Chairman of the Joint Chiefs of Staff	Discussion
<b>OCTOBER 22–23, 2007</b>	
Mr. Vernon Bettencourt CIO G6 (acting)	Opening Remarks & Army's Vision for Interoperability
BG(P) David Halverson, Deputy Chief of Staff, G3/5/7 Director of Operations	Interoperability in Support of the Warfighter
LTC Ross Osborne Mr. Bob Pace, CW5 (ret)	Warfighter's Perspective on Interoperability
Mr. Claude Bolton Assistant Secretary of the Army (Acquisition, Logistic & Technology)	Regulations, Policies, and the Need for Change to Allow for Responsiveness to Acquisition
Mr. Ronald Bechtold Director of Architecture, Army G6	Networks and Architectures; including transport, applications data modeling and standards
Mr. Terry Edwards Army Material Command, G6	Interoperability and what the DSB can do for the Army

**NOVEMBER 27–29, 2007**

Mr. Jack Zavin Associate Director, Architecture & Interoperability, NII/DOD-CIO	Beyond Technical Interoperability
Mr. David E. Green Chief Technology Advisor, C4, HQ USMC	USMC
Mr. Paul Blatch RDML (Sel) Dave Simpson CAPT Scott Krambeck Mr. Charlie Suggs, PEO C4I CDR Stu Warren LCDR Luis Reinoso Mr. Pete Blackledge	Panel discussion on Navy issues in interoperability Panel Chair: Vice Admiral Mark J. Edwards OPNAV(N6), DCNO Network Communications
LTG John R. Wood, USA Deputy Commander, U.S. Joint Forces Command	Joint Forces Command
Col Elizabeth Bierden, Director of Interoperability, Joint Staff (J-6I)	Joint Staff
HON John Grimes, ASD(NII)/DOD CIO Mr. David Wennergren, Deputy DOD CIO and Deputy Assistant Secretary of Defense for Information Management/Integration & Technology Mr. Robert Lentz, Deputy Assistant Secretary of Defense for Information and Identity Assurance Mr. Donald Diggs, Deputy to the ASD(NII)/DOD CIO for National Leadership Command Capabilities	Networks & Information Integration (NII) Seniors Roundtable
LtGen Charles E. Croom Jr., USAF Director, DISA Ms. Diane McCoy Dr. Edwards Siomacco, Vice Principal Director, Global Information Grid Enterprise	Discussion of the Defense Information Systems Agency

**JANUARY 7–8, 2008**

Dr. Ronald Jost Deputy Assistant Secretary of Defense for Command, Control, Communications, Space and Spectrum	Joint Net Centric Operations
Mr. John B. Foulkes Director, DOD Test Resource Management Center	Testing in a Joint Environment
Mr. Mike D. Crisp Deputy Director, Air Warfare Operational Test & Evaluation, OSD	Joint Test and Evaluation Program
LTG William G. Webster USA Deputy Commander, USNORTHCOM	Northern Command
Captain John Dzinowicz USN JS-J-6X Assured Information Sharing	Assured Information Sharing
Ms. Jennifer Johnso LTC Andrew Petrett COL Barry Hensley	Joint Task Force on Global National Operations: Threat Brief (Secret)

**FEBRUARY 12–13, 2008**

MG Timothy J. Lowenberg, Adjutant General of the State of Washington	Homeland Security / Homeland Defense
RADM Jay M. Cohen (USN Ret) Under Secretary, Science & Technology VADM Roger T. Rufe, Jr. (USCG Ret) Director, Operations Coordination Mr. Scott Charbo, Deputy Under Secretary, National protection & Programs Director Mr. Craig Kaucher Deputy Director, Information Sharing & Knowledge Mgmt.	Department of Homeland Security- Roundtable
Mr. James W. Clark Chief Information Officer and Director, Center for Networks and Communications U.S. Special Operations Command	U.S. Special Operations Command
RADM Dave Glenn Assistant Commandant for C4 and Information Technology / Chief Information Officer U.S. Coast Guard	U.S. Coast Guard
Mr. Dennis R. Schrader Deputy Administrator for National Preparedness Federal Emergency Management Agency	National Response Framework
Ms. Lorraine Wilson OUSD(I) Acquisition Resources and Technology	Distributed Common Ground Station (DCGS) Integrated Backbone
Mr. William McCarthy DOT&E	IA Assessments
Mr. Doug Schultz USJFCOM	Concept Development and Experimentation
COL Michael A DeMarco Chief, Joint Exercises Division NORAD-USNORTHCOM J-71	Ardent Sentry
Mr. Jim Kish DHS	Top Off and National Level Exercise

**MARCH 18–19, 2008**

Department of Homeland Security	Office of Emergency Communications
National Communication System	Briefing the Defense Science Board
National Command and Coordination Capability Overview Briefing	Cyber Security and Infrastructure
Network Centric Operations Industry Consortium	
Special Projects Office/ Northeast Regional Response Center	SPO Mission

<p>LTG Steven H. Blum Chief, National Guard Bureau</p> <p>Mr. Larry W. Guderjohn Chief of Staff (J-3), National Guard Bureau</p> <p>COL Timothy Keasling, Deputy (J-2), National Guard Bureau</p> <p>Maj Gen Alan L. Cowles Director Command, Control, Communications, and Computer Systems Division (J-6), National Guard Bureau</p> <p>Maj Gen William H. Etter, Director, Joint Staff, National Guard Bureau</p>	Panel on National Guard Issues
<p>Dr Linton Wells, Transformation Chair Distinguished Research Professor, National Defense University Center for Technology and National Security Policy</p>	Defense Transformation
<p>Dr Peter Fonash, Acting Chief of Staff for the Office of Cybersecurity and Communications</p> <p>Mr Chris Essid, Director of the Office of Emergency Communications</p> <p>Mr Lawrence Hale, Acting Director of the National Communications System</p>	Panel on Cyber Security and Infrastructure at the Department of Homeland Security
<p>LtGen Carl O'Berry, USAF(ret)</p> <p>LtGen Harry Raduege, USAF (ret)</p> <p>Mr John Osterholtz</p>	Network Centric Operations Industry Consortium
<p>Ms Debra Filippi Federal Information Sharing Executive OSD(NII)/DCIO</p> <p>Mr Paul Grant Deputy, Information Sharing Executive, Information Sharing Office</p> <p>Ms Janice Haith Information Sharing Executive for Intelligence and Homeland Defense</p> <p>Mr Anthony Simon</p>	Overview of the Draft DOD Information Sharing Implementation Plan

**APRIL 15–16, 2008**

<p>Mr. Michael Krieger, Director, Information Policy OASD(NI)/DOD CIO</p>	Data Sharing and Service Oriented Architecture Strategy and Implementation
<p>Lt. Gen. Ted F. Bowlds, USAF Commander, Electronic Systems Command</p>	IT Acquisition
<p>LTG William G. Webster, Deputy Commander, USNORTHCOM</p>	USNORTHCOM: Interoperability and Information



**MAY 13–14, 2008**

Brigadier General Susan Lawrence, Commanding General U.S. Army Network Enterprise Technology Command/ 9th Signal Command (Army) (Former USCENTCOM J-6)	Net-Centricity: The View of the issues from the Combatant Command Perspective (SECRET)
--	--

**JUNE 10–11, 2008**

Dr John Chapin Chief Scientist, Vanu, Inc Dr Cynthia Dion-Schwarz Information Systems Director for DUSD(S&T), Department of Defense	Panel discussion on Network Technologies, Architectures and SOA
Mr. Victor A. Meyer Global Head of Corporate Security and Business Continuity, Deutsche Bank	Discussion of Industry Approaches to Protect IT

**JULY 15–16, 2008**

LTG William Hilsman (ret) Mr Joe Wright, Intelsat (ret)	National Communications System
--	--------------------------------



# Glossary

A-6	command and control, communications and computers systems staff office in the Air Force
ABCS	Army Battle Command System
AES	Advanced Encryption Standard
ASD	Assistant Secretary of Defense
ASIC	application specific integrated circuit
AT&L	acquisition, technology and logistics
BGP	border gateway protocols
C4	command and control, communications and computers
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CAC	common access card
CIO	chief information officer
COI	community of interest
CONOPS	concept of operations
CONUS	continental United States
COP	common operating picture
COTS	commercial off-the-shelf
CTSF	Central Technical Support Facility
CUI	controlled unclassified information
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DIACAP	DOD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DNI	Office of the Director of National Intelligence
DOD	Department of Defense
DSB	Defense Science Board
DSCA	defense support of civil authorities
EHF	extremely high frequency
FEMA	Federal Emergency Management Agency

FPGA	field programmable gate arrays
G-6	command and control, communications and computers systems staff office in the Army or Marine Corps
GIG	Global Information Grid
GIG-BE	Global Information Grid-Bandwidth Expansion
HD&ASA	Homeland Defense and Americas' Security Affairs
HSIN	Homeland Security Information Network
IA	information assurance
IP	Internet Protocol
IPv6	Internet Protocol version 6
IRIS	infrared imaging system
IT	information technology
J-3	operations directorate of a joint staff
J-6	command, control, communications, and computer systems directorate of a joint staff
J-7	engineering staff section; operational plans and joint force development
JCCC	Joint Communications Control Center
JCCSE	Joint CONUS Communications Support Environment
JFHQ-S	Joint Force Headquarters-State
JISCC	Joint Incident Site Communications Capability
JITC	Joint Interoperability Test Command
JNN	Joint Network Node
JOC	Joint Operations Center
MANET	mobile ad hoc wireless network
MCP	master control plane
NCOIC	Network Centric Operations Industry Consortium
NCS	National Communications System
NCTC	National Counter Terrorism Center
NDIS	network-aware distributed information services
NGB	National Guard Bureau
NII	Networks and Information Integration
N-NC	NORAD and USNORTHCOM
NSA	National Security Agency
NSAG	Network Systems Architecture Group
NSTAC	National Security Telecommunications Advisory Committee
OIF	Operation Iraqi Freedom
OSD	Office of the Secretary of Defense

OSI	open systems interconnection
PA&E	Program Analysis and Evaluation
PEP	performance enhancement proxy
POM	program objective memorandum
PUF	physical unclonable functions
QoS	quality of service
R&D	research and development
SAG	Strategic Advisory Group
sASIC	structured application specific integrated circuit
SATCOM	satellite communications
SBU	sensitive but unclassified (information)
SIPRNET	secret internet protocol router network
SOA	service oriented architecture
SOIS	strategic operations information sharing
TCP	transmission control protocol
TE&C	test, evaluation and certification
TFER	Task Force for Emergency Readiness
TOC	tactical operations center
TOR	terms of reference
TSAT	Transformational Communications Satellite
USA	United States Army
USCENTCOM	United States Central Command
USJFCOM	United States Joint Forces Command
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
USSTRATCOM	United States Strategic Command
VPN	virtual private network
WIN-T	Warfighters Information Network-Tactical
XML	extensible markup language

