Department of Defense
Information Sharing Implementation Plan

April 2009

**The Office of the Assistant Secretary of Defense
for
Networks and Information Integration / DoD Chief Information Officer**

As stated in the 2008 National Defense Strategy, "Intelligence and information sharing have always been a vital component of national security. Reliable information analysis, quickly available, is an enduring challenge…

Concepts such as "net-centricity" can help guide DoD, linking components of the Department together and connecting organizations with complementary core competencies, forging the Total Force into more than the sum of its parts. The goal is to break down barriers and transform industrial-era organizational structures into an information and knowledge-based enterprise. These concepts are not a panacea, and will require investments in people as much as in technology to realize the full potential of these initiatives."

EXECUTIVE SUMMARY

The 2006 *Quadrennial Defense Review* report called for the Department of Defense (DoD) to improve "information sharing with other agencies and with international allies and partners" and to "develop an information sharing strategy" that guides "operations with Federal, State, local, and coalition partners." Accordingly, the Office of the DoD Chief Information Officer (CIO) developed and signed the DoD Information Sharing Strategy on May 4, 2007. It established DoD's vision for achieving effective information sharing across the extended enterprise (i.e., all internal and external participants required to ensure mission success). The Strategy highlighted five implementation considerations to improve DoD's ability to share information: culture, policy, governance, economics and resources, and technology and infrastructure. This plan, the DoD Information Sharing Implementation Plan, addresses those considerations through an initial set of near-term tasks intended to move DoD toward implementing information sharing as envisioned in the Strategy. Additionally, this plan provides amplifying guidance on achieving Goal 2, Information as a Strategic Asset, of the DoD Information Management (IM)/Information Technology (IT) Strategic Plan.

The DoD Information Sharing Implementation Plan was developed in coordination with the combatant commands, military departments, and defense agencies. A senior leadership group and its action officers, representing a cross-section of DoD, brought these organizations together through interviews and a workshop to collect their information sharing requirements and concerns. The DoD Information Sharing Implementation Plan represents the results of those efforts. It identifies focus areas and tasks with associated offices of primary responsibility to achieve key information sharing improvements, targeting current and future operations and technologies, within a 36-month timeframe.

To make tangible and cost-effective improvements, this plan leverages the successes of existing capabilities and ongoing initiatives that are internal and external to DoD. For example, DoD made substantial progress in developing the infrastructure required for information sharing. This foundation included the physical infrastructure, as well as the associated policies, processes, and personnel for meeting the information demands of DoD missions. The implementation of the DoD Net-Centric Data and Net-Centric Services Strategies, through efforts such as the Maritime Domain Awareness Community of Interest and the Joint Functional Component Command for Global Strike and Integration, resulted in a number of successes in which relevant information was made visible, accessible, and understandable to all authorized users.
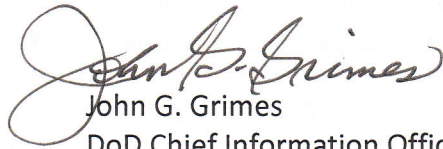
The DoD Information Sharing Implementation Plan recognizes that organizations' cultures play a significant role in any successful information sharing environment. This plan identifies tasks to drive cultural transformation as needed to better promote the practice of information sharing. Recognizing that cultural shift alone is not sufficient, the DoD Information Sharing Implementation Plan also addresses management, operations, classification and marking processes, identity and access management, technical infrastructure, and federal government-wide information sharing initiatives.

DoD recognizes its responsibility to support its own missions and its role in the broader national information sharing landscape. Accordingly, this plan supports the National Strategy for Information Sharing and other federal initiatives that include areas of cooperation with the Director of National Intelligence, activities from the Federal Information Sharing Environment

Implementation Plan, and development of the National Command and Coordination Capability in conjunction with the Department of Homeland Security.

DoD-wide support in implementing the tasks outlined in this plan will enable the Department to create an environment that encourages the secure sharing of information to better defend our nation and protect its citizens against the threat of ever-changing adversaries at home and abroad. Together, we will achieve an information advantage for our people and mission partners.

John G. Grimes
DoD Chief Information Officer

TABLE OF CONTENTS

INTRODUCTION

The Department of Defense (DoD) Information Sharing Implementation Plan is DoD's plan for implementing the vision and goals of the DoD Information Sharing Strategy (Appendix A), as well as Goal 2, Information as a Strategic Asset, of the DoD Information Management (IM)/Information Technology (IT) Strategic Plan. The tasks identified in this plan focus on enhancing DoD's ability to share information in a timely and protected manner with appropriate internal and external participants as required to ensure mission success. These internal and external participants are hereafter referred to as mission partners or the *extended enterprise*.[1] For the purposes of this document, *information sharing* is defined as it is in the DoD Information Sharing Strategy: "making information available to participants (people, process, or systems)," which "includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant."

> "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**
> **May 4, 2007**

Multiple events highlighted the need to share information with the extended enterprise. The most notable were the September 11 terrorist attacks and Hurricane Katrina. As noted in *The 9/11 Commission Report*, "Much of the public commentary about the 9/11 attacks has dealt with 'lost opportunities'…, often characterized as problems of 'watchlisting,' of 'information sharing,' or of 'connecting the dots.'" The report revealed several instances in which the inability to share information with external partners resulted in slow reporting and poor response due not only to technical barriers, but procedural and cultural barriers as well. A congressional report on Hurricane Katrina stated that "many of the problems… identified can be categorized as 'information gaps.'"

> "No one agency can do it alone."
> **The 9/11 Commission Report, p. 418**
>
> "One would think we could share information by now. But Katrina again proved we cannot."
> **Congressional Reports:**
> **H. Rpt. 109-377**

Since these events, DoD has made progress in developing its information sharing infrastructure, which includes the physical infrastructure as well as the associated policies, processes, and personnel for meeting the information demands of DoD missions. Notably, the implementation of the DoD Net-Centric Data and Net-Centric Services Strategies, together with enterprise information environment enablers (i.e., communications, core services, computing infrastructure, and information assurance), resulted in numerous successes in which information and services were visible, accessible, and understandable to authorized users.

> The Maritime Domain Awareness Community of Interest (MDA COI) implemented the DoD Net-Centric Data Strategy and demonstrated a capability that successfully enabled the sharing of information among intelligence, defense, homeland security, and law enforcement maritime data producers.

---

[1] Extended enterprise includes Federal, State, local, tribal, coalition partners, foreign governments and security forces, international organizations, non-governmental organizations, and the private sector.

The DoD Information Sharing Implementation Plan recognizes this progress and seeks to expand these capabilities and leverage successes to enhance information sharing with the extended enterprise. Along with the technology needed to extend information sharing, the plan addresses management and cultural barriers that hinder DoD from fully realizing the value of the current and future information sharing infrastructure.

In addition, the DoD Information Sharing Implementation Plan furthers key initiatives, including the National Strategy for Information Sharing, *Successes and Challenges in Improving Terrorism-Related Information Sharing* (October 2007), the 2006 National Military Strategy for Cyberspace Operations, and the DoD IM/IT Strategic Plan. The plan advances solutions from the information sharing findings and recommendations of the Defense Intelligence/Joint Intelligence Operations Center (JIOC) Staff Assistance Visit Report (December 2007) and the Multinational Information Sharing (MNIS) program.

Information sharing is a key mission enabler. The Department's Joint Capability Areas (JCA) are drivers for the evolution of the information sharing landscape and provide a common lexicon and taxonomy for the development of DoD's future required capabilities. The DoD Information Sharing Implementation Plan furthers the goals of the Tier I Net-Centric JCA and its subordinate Enterprise Services and Network Management concepts. It also supports the Command and Control, Battlespace Awareness, Building Partnerships, and Corporate Management and Support capability areas. These JCAs are integral to evolving the capabilities-based planning process and are reference points for measuring success in the execution of this plan.

PURPOSE AND SCOPE

The purpose of the DoD Information Sharing Implementation Plan is to identify a set of tasks that work toward **achieving the goals and vision of the DoD Information Sharing Strategy** in accordance with existing laws, policies, and agreements, while taking into account the commander's need to maintain operations security.

To achieve this, the plan is organized as follows—

> ➢ **Focus Areas.** Related tasks are grouped into focus areas for improved readability and understanding. Each focus area provides background and context for related tasks. Collectively, the focus areas address all DoD Information Sharing Strategy goals. The order of the focus areas does not indicate priority.

> ➢ **Tasks.** The tasks identified in this plan address information sharing priorities as determined by the Office of the Secretary of Defense, the combatant commands, military services, and defense agencies (CC/S/A). Determination of priority is based on CC/S/A need and the level of direct relevance to the goals of the DoD Information Sharing Strategy. Accordingly, Appendix B maps each task to its associated Strategy goals and implementation considerations.

> Each task describes a specific action or set of actions that need to be accomplished to address concerns in each focus area. The tasks identified in this plan address information sharing issues with broad, Department-wide impact.

> ➢ **Offices of Primary Responsibility (OPRs).** One or more OPRs are assigned to each task. The OPRs will lead and work the task with the support of other organizations

as necessary. OPRs will report progress to the plan oversight body and will be required to provide a Plan of Action and Milestones (POA&M) for each assigned task as appropriate.

➢ **Offices of Collateral Responsibility (OCRs).** OCRs are assigned to a number of tasks. The OCRs will support the OPRs in activities necessary to accomplish each task. OCR roles will be specified in the POA&Ms developed by the OPRs with OCR support.

DEVELOPMENT APPROACH

Upon release of the DoD Information Sharing Strategy on May 4, 2007, work began on the DoD Information Sharing Implementation Plan. Action officers, representing a cross section of DoD, led this effort with oversight from senior leadership.[2] The action officers gathered information using the following approaches:

➢ **Informal Data Collection.** The action officers collected initial data on information sharing barriers and current efforts from subject matter experts within their organizations.

➢ **Formal Interviews with the CC/S/As.** The action officers formally interviewed the CC/S/As to solicit their information sharing requirements and concerns. Use of the DoD Information Sharing Strategy implementation considerations (culture, policy, governance, economics and resources, and technology and infrastructure) guided discussions and ensured that all aspects of information sharing were addressed.

➢ **DoD Information Sharing Workshop, July 25–26, 2007.** The action officers conducted a workshop with the CC/S/As to collect additional inputs on the key concerns gathered from the initial interviews.

IMPLEMENTING THE TASKS OF THIS PLAN

In his memorandum dated August 29, 2007, the Deputy Secretary of Defense designated the DoD Chief Information Officer (CIO) as "lead for the Information Sharing Strategy and its implementation." Pursuant to this direction, the Office of the DoD CIO will establish a cross-functional oversight body to guide and monitor the execution of the DoD Information Sharing Implementation Plan.

Within 45 days of the publication of the DoD Information Sharing Implementation Plan, the DoD CIO will lead a working group to establish and publish a formal charter for an oversight body that will manage the execution of the plan and the actions of the tasked OPRs. The working group and the eventual plan oversight body will include representation from the offices of the DoD CIO, Under Secretary of Defense for Intelligence (USD(I)), Under Secretary of Defense for

---

[2] Senior leadership consisted of the Joint Staff J5, Joint Staff J6, the Under Secretary of Defense for Intelligence (USD(I)), the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (ASD(HD&ASA)), and the DoD CIO.

Policy (USD(P)), Joint Staff (J2, J3, J5, and J6), and Military Services (Army, Navy, Marine Corps, and Air Force).

Within 60 days of the formal release of the plan, the DoD CIO will hold a kickoff meeting with the OPRs. During this meeting, the oversight body will coordinate with the OPRs on the execution of their assigned tasks.

OPRs will be required to—

> ➢ Submit a POA&M for each of their tasks within 90 days from the date of the kickoff meeting that includes major milestones, resource activities, and a 36-month target

> ➢ Identify means of incorporating task requirements into appropriate budgetary processes if applicable

> ➢ Specify performance metrics

> ➢ Report progress to the DoD Information Sharing Implementation Plan oversight body on a periodic basis.

POA&Ms will map out the activities, responsibilities, and timeline necessary to complete assigned tasks, staying within a 36-month timeframe. The oversight body will track the progress of each task against submitted POA&Ms and the Office of the DoD CIO will convey the progress of the plan in its annual report to Congress.

Changes in technology, policy, and priorities make information sharing a dynamic activity. Therefore, the plan oversight body will continually monitor the information sharing landscape and evaluate the plan every 18 months to ensure that DoD continues to proceed in the appropriate direction.

Focus Area 1

Managing Information Sharing in the DoD

In addition to the traditional warfighting information requirements, in today's environment DoD must share information in a timely and protected manner with multiple U.S. and international partners in a variety of situations that include intelligence, counterterrorism, multinational and stability operations, humanitarian assistance, disaster relief, and homeland defense. Recognizing the complexity of sharing information across organizational boundaries and in support of a broad range of missions, CC/S/As took steps to implement policies, processes, and technologies for sharing and protecting their information. Although CC/S/As were successful in addressing the complexities within their specific mission areas, DoD as a whole needed improved coordination and management across these individual and localized efforts.

The Deputy Secretary of Defense recognized the need to formally align and leverage independent efforts across DoD to improve information integration, transparency, and agility. In his March 15, 2007, memorandum, *Institutional Reform and Governance Actions to Critical Path (ACP)*, he stated: "Improving governance within the Department of Defense is essential. The Department needs to move toward a general management framework that provides clear and executable strategic direction for the current, mid and far term." Such a management framework for information sharing activities in DoD will streamline the resolution of issues, enable the coordination of independent efforts, and ensure consideration of information sharing in key decisions.

The tasks in this focus area seek to align Departmental guidance, avoid duplicative efforts, and enhance mission effectiveness. They lay out initial steps for establishing a governance structure for information sharing activities across the Department.

Tasks and Responsibilities

Task 1.1	Establish an overarching governance structure for DoD enterprise information sharing.
Details	▪ Analyze existing DoD governance structures and processes to determine if they can be adapted to meet information sharing governance goals and objectives
	▪ If no adequate structure exists, develop a plan for establishing an appropriate structure
	▪ Identify appropriate interfaces between DoD and its mission partners
	▪ Prescribe the governance structure through an appropriate DoD issuance

Responsibilities	OPR: USD(P), Joint Staff J5
	OCR: USD(I), DoD CIO, Joint Staff J6

Task 1.2	Develop and manage information sharing situational awareness to ensure synchronization among activities.
Details	▪ Track information sharing best practices/lessons learned, barriers, and activities across the Department
	▪ Manage dependencies and enable the coordination of information sharing initiatives
Responsibilities	OPR: USD(P), Joint Staff J5
	OCR: USD(I), DoD CIO, Joint Staff J6

Task 1.3	Integrate information sharing considerations into key DoD decision support processes.
Details	▪ Assess and incorporate, as appropriate, information sharing requirements into the key DoD decision support systems (Joint Capabilities Integration and Development System (JCIDS); Defense Acquisition System (DAS); Planning, Programming, Budgeting, and Execution Process (PPBE))
	▪ Assess and incorporate, as appropriate, information sharing requirements into the capability portfolio management process
Responsibilities	OPR: JCIDS—Joint Staff J8
	DAS—Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))
	PPBE— Director of Program Analysis and Evaluation (PA&E)
	Capability Portfolio Management—Capability Portfolio Managers

Focus Area 2

Instilling an Information Sharing Culture

Culture plays a key role in successful information sharing. Changing the values and behaviors of an institution's culture must start with leadership. Leaders at all levels must convey the importance of developing and maintaining trust between mission partners and the significance of cultural change ushered in by advances in technology and a new generation.

Many organizations took steps to transform their culture into one that promotes information sharing.

> ➢ The Federal Government, in response to the recommendations of *The 9/11 Commission Report* and the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), is addressing the cultural gap between agencies and State, local, and tribal governments. Through training, incentives, and performance measurements, the Federal Government seeks to convey the importance of sharing and fusing information from various domains for a more accurate and complete awareness of today's threat environment.

> ➢ The Intelligence Community developed "a strategy to establish a new culture and to share information better, both among those whose job it is to provide intelligence and with those who need intelligence to perform their missions – i.e., policy makers, warfighters, defenders of the homeland, and the officials who enforce our laws."[3]

> ➢ DoD is moving from parochial system ownership to collaborative development through various initiatives. For example, the United States Northern Command (USNORTHCOM) is working with the National Guard Bureau (NGB) and Department of Homeland Security (DHS) National Operations Center to improve information sharing by ensuring that operators are familiar with the processes, policies, and systems of both organizations. Additionally, the Maritime Domain Awareness (MDA) Community of Interest (COI) demonstrated the capability to share maritime vessel tracking data across multiple federal departments (DoD, DHS, and Department of Transportation (DOT)).

> ➢ The North American Aerospace Defense Command (NORAD) and USNORTHCOM are using Information Exchange Brokers (IEBs) to address the information sharing and knowledge management needs of their operational elements. The IEB is the human element embedded in the process of information sharing. IEBs identify impediments to information sharing, leverage collaborative tools, and train the force.

These and similar efforts are contributing to the necessary evolution of DoD culture. Cultural change is critical to organizational transformation and is an organization's most difficult challenge. While leadership is beginning to convey the importance of an information sharing

---

[3] Office of the Director of National Intelligence, *United States Intelligence Community Information Sharing Strategy*, February 22, 2008.

culture, the need still remains to institutionalize information sharing behaviors while maintaining information assurance and operations security. Incentives must be in place to advance information sharing, policies must be revised to remove information sharing impediments or disincentives, people must be educated and trained to understand the value of sharing information, and processes must be in place to promote and enforce the appropriate sharing of information.

Tasks and Responsibilities

Task 2.1	Develop incentives to promote information sharing practices and procedures.
Details	▪ Develop incentives to encourage program managers to address information sharing when building or acquiring capabilities ▪ Ensure incentives account for control measures to promote trust and to maintain the integrity and protection of information
Responsibilities	OPR: DoD Components
Task 2.2	Identify and revise the policies and processes that create impediments or disincentives to sharing information while ensuring the Department's continued compliance with laws, policies, and agreements.
Details	▪ Resolve conflicting policies and processes ▪ Remove or update outdated policies ▪ Resolve legal issues associated with information sharing across communities (e.g., Intelligence Community versus law enforcement) and clearly identify the legal bounds for the sharing of information and its use
Responsibilities	OPR: USD(P) OCR: USD(I), USD(AT&L), DoD General Counsel (DoD GC)
Task 2.3	Educate and train personnel on their roles in information sharing.
Details	▪ Leverage ongoing and planned training activities and initiatives within DoD and across the Federal Government and Intelligence Community ▪ Emphasize individual and organizational responsibility to manage risks associated with information sharing
Responsibilities	OPR: DoD Components
Task 2.4	Determine the applicability of and expand if validated, the NORAD/ USNORTHCOM IEB concept to other CC/S/As to enhance organizational information exchange processes and procedures.

Details
- Enable the "responsibility to share" construct by expanding the human dimension of information sharing captured by operational IEBs, who are system and process experts that shape efforts to synchronize DoD; Federal, State, local, and tribal government; and non-government information sharing processes and procedures
- Ensure that IEBs look across a broad field of operational information and that they coordinate with key organizations to share and synchronize all critical and relevant information among agencies

Responsibilities

OPR: United States Joint Forces Command (USJFCOM)

OCR: NORAD/USNORTHCOM, Joint Staff J3, Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)), Combatant Commands

Focus Area 3

Leveraging the Power of Social Networks

The Internet provides the unprecedented ability to communicate and collaborate electronically across the globe. Online capabilities such as message boards, wikis,[4] and instant messaging are staples for communicating and sharing ideas. Social networks also are becoming increasingly popular. Users of such networks not only exchange information in a variety of forms, but also maintain a virtual link to others in the network. These capabilities, along with new "Web 2.0" technologies, result in a powerful information sharing environment.

DoD implemented information sharing and collaboration capabilities to support its users. These tools proved vital in executing missions and evolved over time to support new requirements for improved performance. Some recent examples include the newly established Defense Knowledge Online (DKO). DKO enables users throughout the DoD community to access a number of valuable online tools, including group messaging, shared spaces for accessing information, real-time virtual meetings and group collaboration, and instant messaging. In addition to DKO, other modern information sharing capabilities populate the Global Information Grid (GIG). The Intelligence Community and other national security related organizations share classified information on Intellipedia, which consists of three wikis running on the Joint Worldwide Intelligence Communications System (JWICS), the SECRET Internet Protocol Router Network (SIPRNet), and Intelink-U.

Although some advances are being made, other information sharing capabilities—particularly those that are increasingly popular with the latest generation of people entering the workforce—are not equally embraced. For example, DoD is wary when it comes to allowing its workforce to use social networking websites. A key concern is the obvious security and information assurance challenges that arise from exchanging information in a largely uncontrolled public forum. If used appropriately, however, these websites enable the user to build a valuable social network in which he/she can collaborate using the most modern technologies.

Today's generation is accustomed to social networking and leverages this capability to communicate and collaborate among friends, colleagues, and globally dispersed groups to share ideas and information freely. As this generation continues to enter the workforce, DoD needs to position itself to benefit from such information sharing practices. DoD needs a partnership between information assurance, operations security, and information sharing—a partnership in which capabilities are not discarded because their baseline implementation inserts risk into missions, but rather are embraced with risks appropriately assessed and managed to enable the full benefit of technology within the DoD mission space.

---

[4] A collaborative website whose content can be edited by anyone who has access to it.

Tasks and Responsibilities

Task 3.1	Develop a plan to leverage modern social networking capabilities appropriately within DoD.
Details	▪ Identify modern information sharing and social networking capabilities commonly used on the Internet and within other large information sharing communities
	▪ Perform a risk/benefit analysis on social networking to determine its relative value to DoD and U.S. Government missions
	▪ Identify and categorize concerns and risks for inserting this capability into the DoD information sharing environment
	▪ Develop an information assurance, operations security, and information sharing partnership initiative to develop action plans for enabling social networking within DoD
Responsibilities	OPR: DoD CIO
	OCR: Under Secretary of Defense for Personnel and Readiness (USD(P&R)), Defense Information Systems Agency (DISA), USJFCOM

Focus Area 4

Operationalizing Information Sharing

DoD must coordinate internally and with multiple mission partners in a variety of scenarios and situations that require immediate response. The ability to share information during such times is critical to operational success. Accordingly, the incorporation of information sharing in joint exercises, demonstrations, and experiments enables the practice, testing, and improved performance of information sharing policies, processes, and technologies in operational settings.

Past and planned demonstrations and exercises incorporated information sharing into their objectives.

> ➢ The Coalition Warrior Interoperability Demonstration (CWID) is a Joint Staff-sponsored demonstration of evolving interoperability solutions key to enabling an information sharing infrastructure. It is an annual event with rotating combatant command hosts and emphasis areas. The USNORTHCOM-hosted CWID focused on identifying gaps in homeland defense that prevented DoD and the extended enterprise from realizing the potential of a shared trusted exchange environment. The United States European Command (USEUCOM) is currently hosting a CWID with focus on the North Atlantic Treaty Organization (NATO). USJFCOM is scheduled to host the CWID in 2009. Participants will include traditional military allies, as well as non-DoD government agencies, national and international law enforcement organizations, and the first responder community.

> ➢ Winter Fox, a 1-day exercise that took place in 2006, demonstrated the success of an identity management solution compliant with the Federal Information Processing Standard-201 (FIPS-201), *Personal Identity Verification of Federal Employees and Contractors*, across various organizational locations. It focused on first responders and proved the effectiveness of Homeland Security Presidential Directive-12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*.

> ➢ In 2007, an exercise called Winter Storm expanded the Winter Fox demonstration to include DHS, DoD, and other public and private sector participants.

> ➢ Noble Resolve, a USJFCOM experimentation campaign plan, sought to enhance homeland defense and to improve military support to civil authorities through solutions that included a reliable collaborative environment and tool sets that encompassed shared operations, shared information, and shared situational awareness. Participants included multiple commands, various non-DoD agencies, State governments, academic institutions, and multinational partners.

Information sharing success requires the continuous operational practice and testing of enabling policies, processes, and technologies. Including information sharing objectives in joint exercises,

demonstrations, and experimentations ensures the operational effectiveness of information sharing in an environment that requires agility.

Tasks and Responsibilities

Task 4.1   Develop an approach that ensures information sharing activities (policies, procedures, and technologies) are integrated into appropriate joint experiments, demonstrations, and exercises.

Details
- Assess the operational effectiveness of information sharing activities
- Capture and apply any lessons learned from joint experiments, demonstrations, and exercises

Responsibilities   OPR: USJFCOM

OCR: USD(AT&L), Combatant Commands, Secretaries of the Military Departments

Focus Area 5

Removing Sharing Barriers Created by Improper Classification

Classification of national security information under Executive Order 12958, as amended, "Classified National Security Information," (E.O. 12958) is a critical tool in protecting national security. However, improper and over-classification of information undermine the nation's safety and security by impeding the timely sharing of perishable information with relevant stakeholders, including Federal, State, local, and coalition partners. In addition, improper and over-classification may unduly restrict the public's access to important information.

The National Commission on Terrorist Attacks upon the United States—known as the 9/11 Commission—recommended limiting the unnecessary classification of information and providing incentives for information sharing. The IRTPA also called for reducing disincentives that impede information sharing including over-classification. Nonetheless, improper and over-classification remain barriers to information sharing.

DoD, in coordination with the Director of National Intelligence, has taken steps to overcome the barriers, including issuance of the following guidance:

➢ The May 17, 2005, USD(I) memorandum, Use of the "Not Releasable to Foreign Nationals" (NOFORN) Caveat on Department of Defense (DoD) Information, to clarify the appropriate use of the NOFORN caveat;

➢ The Office of the Director of National Intelligence (ODNI) Community Policy Memorandum Number 2007-500-1, Unevaluated Domestic Threat Tearline Reports, to clarify the appropriate use of threat tearline reports; and

➢ The January 26, 2007, Director of the Joint Staff memorandum, Information Sharing with United Kingdom, Australia, and Canada, to amplify ODNI instructions to improve understanding of handling and marking to facilitate information sharing with U.S. allies.

While these efforts above, along with automated tools, greatly facilitate the use of appropriate classification markings, improper and over-classification remain barriers to information sharing throughout the Federal Government. According to the National Archives' Information Security Oversight Office, which oversees the national security classification programs for both the Federal Government and industry, improper and over-classification deficiencies were found in fiscal year 2007 at multiple federal agencies. These deficiencies related to basic requirements concerning implementing regulations, security education and training, self-inspections, classification, and document markings. Training on the proper classification and marking of information is essential for the consistent and appropriate application of classification markings and caveats which, in turn, improves the sharing of vital information with the relevant stakeholders.

Tasks and Responsibilities

Task 5.1 Coordinate with ODNI to update "write-for-customer relevance" guidance and "write-for-customer relevance" and "tearline" information sharing training for all intelligence producers.

Details
- Revise DoD intelligence sharing policies, as applicable
- Emphasize component responsibility to train intelligence personnel
- Oversee component implementation of updated issuances
- Report intelligence sharing or training impediments to the offices of the DoD CIO and USD(I)

Responsibilities OPR: USD(I)

OCR: Joint Staff J2

Task 5.2 Coordinate with ODNI and the Information Security Oversight Office to update information security policy, guidance, and training materials.

Details
- Revise DoD information security policies, as applicable
- Emphasize component responsibility to adhere to classification guidance with regard to proper use of NOFORN, Originator Control (ORCON), and other caveats
- Oversee component implementation of updated issuances

Responsibilities OPR: USD(I)

OCR: USD(P), USD(P&R), Defense Intelligence Agency (DIA), National Geospatial-Intelligence Agency (NGA), National Security Agency (NSA), National Reconnaissance Office (NRO)

Focus Area 6

Sharing Unclassified Information for Civil Support and SSTR Operations

One of DoD's missions is to provide support to a wide range of U.S. and foreign civilian authority-led operations. This includes assistance in times of natural disaster and health epidemics worldwide and other emergencies at the Federal, State, local, and tribal levels within the U.S. and its territories. Recently, this included the DoD response to Hurricane Katrina, in which several DoD Components provided critical support functions, including pre-landfall alerts and notifications and post-landfall rescue and relief operations. In addition to civilian aid and relief, DoD also plays an important role in U.S. and foreign stability, security, transition, and reconstruction (SSTR) operations. SSTR operations are conducted to help establish order that advances U.S. interests and values. The immediate goal often is to provide the local populace with security, restore essential services, and meet humanitarian needs. The long-term goal is to help develop indigenous capacity for securing essential services, a viable market economy, rule of law, democratic institutions, and a robust civil society.

Both civil support and SSTR operations necessitate interaction and information sharing with many external organizations, including other U.S. departments and agencies, foreign governments and security forces, international organizations, non-government organizations, and members of the private sector. Because of technical limitations, security concerns, and political sensitivities, the sharing of unclassified information to support these operations is over non-military networks (e.g., Internet, other). DoD established numerous, useful portals and other tools to facilitate the sharing of information among the wide range of external partners. Many of the U.S. combatant commands established unclassified online portals to help coordinate their operations with external partners within their areas of responsibility (AOR). Examples include USNORTHCOM's Collaborative Information Environment (CIE), United States Pacific Command's (USPACOM) Asia Pacific Area Network (APAN), USEUCOM's Multi-National Collaboration Environment (MNCE), USJFCOM's Harmonieweb, and United States Southern Command's (USSOUTHCOM) Shape. Each portal of the combatant commands operates independently of each other using individual internal funding and operational support.

These information sharing capabilities are used extensively and provide benefit to both DoD and external partners in jointly executing support and relief missions. The various AOR portals and tools typically provide a common suite of capabilities such as real- and non-real-time collaboration, common operational pictures (COP), message boards, shared workspaces, and document repositories. Many of the portals are tailored to support requirements specific to an AOR and/or to meet the requirements of specific external partners.

Because these portals were designed to meet the specific needs of an AOR mission space, they each have a unique look-and-feel and are built on differing technical architectures (i.e., different solutions for access control, data storage, data standards, and portal components). They were developed with a range of external partners in mind, not taking into account an increasingly

common need to share information with new, unanticipated partners and between the various portals and tools.

The uncoordinated development of DoD's various civil support and SSTR unclassified information sharing initiatives resulted in capabilities that are useful within their respective AORs, but are stovepiped and not federated for use across DoD or combatant command geographic boundaries. Specifically, the lack of a federated SSTR architecture hinders combatant commands and mission partners from efficiently and effectively sharing information in civil support and SSTR operations.

Tasks and Responsibilities

Task 6.1

Develop an enterprise approach, informed by the USJFCOM-led MNIS Analysis of Alternatives (AoA), that enables the federation of existing CC/S/A unclassified information sharing systems in support of civil support and SSTR operations.

Details

- Establish a set of web-service specifications to drive the net-centric development of functionality common to civil support and SSTR operations built on DoD Core Enterprise Service (CES) standards
- Establish various authentication and access standards/mechanisms to allow DoD and its external mission partners, both planned and unanticipated, to achieve an appropriate level of access to information concerning civil support and SSTR operations
- Develop standards for control measures to ensure the integrity and protection of information
- Establish data exchange standards to facilitate the sharing and integrating of information from across the various portal instantiations
- Develop a common look-and-feel among civil support/SSTR portals to facilitate ease of use and to reduce training requirements
- Leverage solutions developed by the combatant commands

Responsibilities

OPR: ASD(NII), Joint Staff J6

OCR: Combatant Commands, DISA, Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (ASD(HD&ASA))

Focus Area 7

Sharing Information for Enhanced Operations

Most of the regional combatant commands identified mission partner information sharing as the number one information sharing requirement. Currently, fielded technologies and organizational processes and policies are not fully meeting this requirement. Often, combatant commands individually pursue development of various infrastructures to meet their needs, resulting in a proliferation of networks that are not always interoperable nor linked so appropriate data is discoverable. Although individual combatant command mission partner efforts at the secret collateral level (e.g., the USPACOM fielding of an NSA-approved capability in fiscal year (FY) 2008) demonstrate progress, an overarching effort is needed to leverage the best of these efforts to provide a foundation for a unified, efficient DoD mission partner information sharing environment. In obtaining solutions, it is imperative that initiatives leverage current efforts, advance capability development, use demonstrations (e.g., CWID and Joint Capability Technology Demonstrations) to validate the operational benefits of newly certified and accredited capabilities, and orchestrate the fielding of information sharing capabilities across the combatant commands.

Migrating U.S. users and mission planning and execution capabilities to a converged mission partner network for coalition operations reduces the associated risk model to U.S. national systems/networks and improves the quality and timeliness of information on the mission partner network. The consolidation will allow fielding of currently certified technologies without the need for drastic changes to information sharing policy. It will lead to a reduction in the overall need for cross-domain solutions (CDS), the usage of CDS for U.S. user reach back, and the usage of CDS by trusted mission partners to their similarly classified and protected national networks. The converged enclave also will have the flexibility to allow mission leads to limit access appropriately for less trusted mission partners to areas within the mission partner environment. It also will provide an environment in which to prove prior to deployment that service-oriented architecture (SOA)-enabled GIG information assurance capabilities between our national networks and those of U.S. coalition mission partners can be effectively operated and maintained by our soldiers, sailors, airmen, and marines.

The current patchwork of both physically and cryptographically separated classified mission partner networks restricts the ability to share appropriate information with mission partners and limits opportunities to ensure positive mission outcomes based on efficient collaboration. This patchwork of individual infrastructures is a result of working around the capabilities of currently certified and fielded technologies, policies that are difficult to implement, and inflexible organizational processes. Accordingly, in March 2007, the Joint Staff's Net-Centric Functional Capabilities Board (NC-FCB) validated the combatant command requirement to converge the multiple secret-level multilateral and bilateral coalition networks into a single environment and infrastructure architecture. It was submitted in accordance with the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6285.01 as an enhancement to the current operational Combined Enterprise Regional Information Exchange System (CENTRIXS) Networks.

DISA received the requirement to engineer, test, and certify the reference architecture and implement the technical solution beginning in FY 2008. The solution must be in line with the 2006 QDR report, the Program Objective Memorandum 2010 (POM-10) Program Decision Memorandum I (PDM-I), the Program Review 2009 (PR-09) PDM-II, and the NC-FCB April 2007 and August 2008 memoranda to consolidate and standardize the current MNIS operational systems. It must support the vision for GIG net-centric operations and the transition to the objective MNIS capability. Implementation beyond FY 2008 is envisioned to integrate the combatant command CENTRIXS convergence efforts and be informed by the USJFCOM-led MNIS AoA. The CENTRIXS Cross Enclave Requirement (CCER) is currently identified as the first step in converging the physically separated mission partner networks and lays the foundational infrastructure to integrate certified and accredited capabilities iteratively to achieve the objective net-centric, classified, information sharing environment.

The Department needs to expedite and re-emphasize its efforts to drive toward a single, net-centric, information sharing capability with coalition mission partners. It must leverage ongoing efforts (e.g., MNIS, net-centric enterprise services (NCES), Net-Enabled Command Capability (NECC), Defense Information Systems Network (DISN), DKO, and CCER) to advance the goals of the DoD's Information Sharing Strategy in coordination with complementary documents (e.g., Data Strategy, Security Strategy, Cyberspace Operations). This technical effort will be done in conjunction with appropriate changes to culture, policy, processes, and technology and within the framework of formal legal agreements among U.S. agencies and various countries' bilateral networks.

Tasks and Responsibilities

Task 7.1
Develop an architecture to converge the multiple secret-level coalition networks into a single mission partner assured information sharing environment, providing a common suite of information services to all mission partners, along with controlled access to command and control, as well as intelligence applications in support of mission planning and execution based on the trust level and duties of the individual user.

Details
- Designate a combatant command as the MNIS Operational Sponsor who will act as advocate for the warfighter, oversee MNIS requirements, and help guide the efforts of the acquisition community
- Converge appropriate physically separate multilateral and bilateral classified mission partner networks onto a single, virtually separated network environment that will provide a single wire solution, single client workstation, increased information sharing and collaboration, and the ability to rapidly share information with mission partners
- Implement technical security protection measures to ensure users (e.g., combatant commands, the Intelligence Community, close allies) are sufficiently confident in the ability of the new environment's security capabilities to protect their sensitive secret-level releasable information—enabling usage and sharing equal to or greater than the legacy, physically separated network environment

20

- Provide a fully integrated and secure data storage capability
- Ensure virtual separation is consistent with all legal agreements and modify agreements as appropriate to execute this task

Responsibilities   OPR: DISA, Joint Staff J6, USJFCOM

OCR: NSA, ASD(NII), United States Strategic Command (USSTRATCOM)

Focus Area 8

Extending Identity and Access Management

The ability to verify the identity of individuals who request access to DoD data and services is central to establishing a trusted and agile information sharing environment. Knowing that a user is who he or she claims to be helps break down one barrier to information sharing: the risk that information may be inadvertently shared with someone who should not be trusted with it. There are a number of policies, processes, and technologies in place and under development for verifying an individual's identity within DoD, across the Federal Government, and within external mission partner organizations at the State, local, tribal, private sector, and foreign national levels. One challenge in verifying a user's identity is in trusting other organizations' identity verification processes and procedures. Addressing identity authentication and authorization across the Federal Government and beyond requires using a federated approach across the individual efforts of each of the organizations involved.

Once an individual's identity is verified through a trusted means, there remains a need to determine whether the individual is authorized to access particular types of information. Unfettered access to information is only possible for unclassified, publicly releasable information. Other types of information, at various levels of classification and controlled unclassified information (CUI), continue to require business rules that prescribe who is authorized to access what types of information and when. Access control is an essential service in the information sharing infrastructure that enables an identified and authorized user to gain access to a data source or use a service.

DoD successfully implemented an authentication solution within DoD to address identity management (strong identity proofing and credentialing with public key infrastructure (PKI) and common access cards (CACs)). HSPD-12/FIPS-201 set the stage to extend this solution to federal partners and contractors. While progress is being made, work still remains to complete implementation across the extended enterprise in alignment with other initiatives. These other initiatives include the development of an identity management strategic plan by the Identity Protection and Management Senior Coordinating Group that seeks to, among other things, integrate CAC, PKI, and biometrics capabilities, extend operations across tactical and austere environments, and establish a common security and identity management services tiger team to develop an architectural framework to facilitate assured information exchange across DoD and the Intelligence Community.

DoD and DNI are moving toward a security implementation that will exploit attributes to support information sharing, whether implemented through attribute-based access control (ABAC) as it matures or role-based access control (RBAC) in its current commercial-off-the-shelf (COTS) instantiation. In the ABAC approach, access control rules are defined based on a number of attributes, including the classification or CUI marking of the information, an individual's organization and position within it, and many other factors. This approach requires clear definitions of the policies, attributes, and circumstances under which information may be shared. Through implementation of ABAC, DoD obtains the ability to grant access to information

to those who need it in an agile manner in accordance with existing laws, policies, and agreements.

Tasks and Responsibilities

Task 8.1	Complete implementation and DoD-wide issuance of DoD's HSPD-12/FIPS-201 compliant credential.
Details	■ Work with the Federal Identity Credentialing Committee to establish an identity credential standard for non-Federal Government entities ■ Develop a roadmap that outlines the necessary steps to complete implementation ■ Capture lessons learned
Responsibilities	OPR: USD(P&R) OCR: USD(I), DoD CIO, USD(AT&L), DoD GC

Task 8.2	Conduct ABAC pilots to test the effectiveness of the ABAC approach in operational settings, as well as to confirm that the attribute set is robust.
Details	■ Include operational concepts for using enterprise-wide directory services to support access control services ■ Include enterprise-wide processes or capabilities for the establishment and management of attributes, especially role and COI attributes ■ Identify lessons learned for further evolution ■ Ensure ABAC effectiveness for all user scenarios
Responsibilities	OPR: DoD CIO OCR: Joint Staff J6, DISA, Secretaries of the Military Departments

Focus Area 9

Advancing Information Sharing Enablers

The DoD Net-Centric Data Strategy emphasizes the need to make data visible, accessible, and understandable to all anticipated and unanticipated users, both within and external to DoD, and promotes the secure posting of information on networks to make it accessible to participants. It also promotes moving the Department beyond the "point-to-point" exchanges of information and strict interoperability across systems to the broader need to share information on the "many-to-many" front regardless of systems and organizational boundaries. The DoD Net-Centric Services Strategy focuses on DoD's vision of providing a net-centric environment (within the DoD Information Enterprise) of shared services in an SOA using common standards and infrastructure. Continued implementation of the Data and Services Strategy is necessary to achieve technical and data interoperability. Various enablers are required to continue making progress in implementing these strategies and to ensure effective information sharing at large.

The Data Strategy identifies COIs as an enabler for reaching agreement on the format (structure) and meaning (semantics) of information. Wide acceptance of the Data Strategy resulted in a growing number of COIs. Facilitating the success of COIs is an important aspect of implementing the Data Strategy. To help ensure continued success, DoD needs to assess the current COI environment to determine areas of improvement, as well as to identify capability gaps that are necessary for COIs to continue playing a vital role in the Department's operations and missions.

Although many COIs are formed to address the information sharing needs of specific communities, other initiatives are established to enable enterprise-wide data and information sharing needs. One example of such an effort is the Universal Core (U-Core) initiative. This initiative is standardizing a small, universal set of data elements and is leveraging COIs to develop data elements applicable to their mission area and discipline needs. The definition of these information exchanges are stored and shared in DoD's Metadata Registry. Efforts such as the U-Core initiative are important and their continued development and testing is critical to information sharing.

The DoD Net-Centric Services Strategy places emphasis on the use of shared services as an enabler for providing access to the myriad DoD data and data-related capabilities. DoD's technology infrastructure for establishing a service-oriented environment is maturing rapidly and includes a suite of capabilities being offered through DoD's enterprise service initiatives. In addition to the technical challenges, the Department must establish the business processes, funding models, and incentive programs to encourage the widespread use of shared services within a service-oriented environment.

Tasks and Responsibilities

Task 9.1   Assess and provide recommendations for evolving/enhancing the COI construct in support of information and data sharing.

Details	▪ Assess and provide a recommendation for integrating COI activities and products within Programs of Record management and development efforts
	▪ Provide a recommendation for integrating the COI construct within DoD decision support processes
	▪ Assess and provide a recommendation for improving the integration of the COI construct within net-centric enterprise tools and capabilities, including service and metadata registries and collaboration services
Responsibilities	OPR: DoD CIO
	OCR: Secretaries of the Military Departments, USJFCOM, USD(AT&L)

Task 9.2	Continue to develop and improve data standards for the exchange of basic information elements across the DoD enterprise.
Details	▪ Align the DoD U-Core and National Information Exchange Model (NIEM) efforts to meet cross-boundary/cross-organizational mission needs
	▪ Leverage efforts by the Common Terrorism Information Sharing Standards (CTISS) Committee
Responsibilities	OPR: DoD CIO
	OCR: DISA, Secretaries of the Military Departments, USJFCOM, USD(AT&L)

Task 9.3	Establish the business processes and funding models for implementing the Net-Centric Services Strategy goals.
Details	▪ Establish the processes for funding, acquiring, developing, managing, and operating shared services
	▪ Integrate requisite shared service processes and governance constructs into existing DoD decision support systems
	▪ Include an incentive strategy to encourage the provisioning and use of shared services throughout the enterprise
Responsibilities	OPR: DoD CIO
	OCR: DISA, Secretaries of the Military Departments, USJFCOM, USD(AT&L)

Focus Area 10

Supporting DoD's Mission Needs Across Federal Information Sharing Initiatives

As DoD implements its information sharing strategy across the Department, it also actively supports cross-cutting federal information sharing initiatives to ensure unity of effort and a uniform DoD response across those initiatives. Federal initiatives include but are not limited to the following: the Federal Information Sharing Environment (ISE), Maritime Security, Aviation Security, the National Command and Coordination Capability (NCCC), the Joint Continental U.S. Communications Support Environment (JCCSE), and the Next Generation Air Transportation System (NextGen).

Each of these interagency initiatives developed a strategy and/or plan for improving information sharing within its own mandated mission scope:

➢ The IRTPA and EO 13388 mandated the establishment of the Federal ISE to improve the sharing of terrorism and weapons of mass destruction (WMD) information across the Federal Government and with external mission partners. The Federal ISE activities are driven by the November 2006 Federal ISE Implementation Plan and priority implementation areas.

➢ Maritime Security policy and guidelines to enhance national security and homeland security in the maritime domain were established by National Security Presidential Directive 41 (NSPD-41), also issued as HSPD-13. Maritime Security efforts are driven by actions prescribed in these directives and the National Maritime Security Strategy. The Maritime Security initiative is led by the Maritime Security Policy Coordinating Committee, which is co-chaired by members from the National Security Council (NSC) and Homeland Security Council (HSC).

➢ The classified NSPD-47/HSPD-16 directed the development of a National Aviation Security Strategy and supporting plans to integrate and coordinate public and private sector aviation security activities to address national/homeland security threats and vulnerabilities in the air domain. DHS leads the Aviation Security initiative.

➢ NCCC is a White House directed program that provides crisis management for the President. The NCCC is the means to provide the President and Vice President with the ability to respond deliberately and appropriately to any crisis. It includes responsive, reliable, survivable, and robust processes and systems to command, control, and coordinate operations among Federal, State, tribal, insular, and local governments, as required. DHS is the executive agent.

➢ The JCCSE Concept for Joint Command, Control, Communications, and Computers (C4) defines the approach for improving information sharing to support DoD missions of Homeland Defense and Defense Support for Civil Authorities. JCCSE is

initially focused on NGB/USNORTHCOM collaboration but is also scoped to address NGB collaboration with USSTRATCOM, USPACOM, and others.

➢ Public Law (P.L.) 108-176 established the NextGen program to transform the national airspace system across federal agencies and with the private sector. The Joint Planning and Development Office (JPDO), chaired by the Secretary of Transportation, oversees NextGen.

These initiatives are integral in implementing the DoD information sharing vision.

Tasks and Responsibilities

Task 10.1 Support, as appropriate, the FY 2010–2014 priorities for development of the Federal ISE (Appendix C)[5].

Details
- Coordinate transition to the CUI framework as the standard for markings, safeguards, and dissemination for unclassified information in the information sharing environment[6]
- Determine the level of DoD engagement and support the Interagency Threat Assessment Coordination Group (ITACG) priority, as appropriate
- Determine the level of DoD engagement and support the State and Major Urban Area Fusion Centers priority, as appropriate
- Determine the level of DoD engagement and support the Suspicious Activity Reporting priority, as appropriate
- Develop DoD's portion of the Federal ISE Shared Space
- Determine the level of DoD engagement and support the Alerts, Warnings, and Notifications priority, as appropriate

Responsibilities OPR: CUI—DoD CIO

ITACG—ASD(HD&ASA)

State and Major Urban Area Fusion Centers— ASD(HD&ASA)

Suspicious Activity Reporting—ASD(HD&ASA)

Shared Space—DoD CIO

Alerts, Warning, and Notifications—ASD(HD&ASA)

Task 10.2 When appropriate, support Federal information sharing initiatives through consistent coordination and integration.

Details
- Support cross-cutting issues and themes for improving information sharing across the Federal Government and with external mission partners

---

[5] Priorities are in accordance with the Office of Management and Budget (OMB) Memorandum, *Budget Guidance for Justification of Fiscal Year 2010 to 2014 Investments Supporting the Information Sharing Environment (ISE) Priorities*, dated February 14, 2008.

[6] Presidential Memorandum for the Heads of Executive Departments and Agencies, *Designation and Sharing of Controlled Unclassified Information (CUI)*, May 8, 2008.

Responsibilities

OPR: Federal information sharing activities—DoD CIO

Program Manager (PM)-ISE activities—DoD CIO with support from PM-ISE responsibility area OPRs identified in Appendix C

Maritime Security—Department of the Navy

Aviation Security—Department of the Air Force

NCCC—ASD(HD&ASA)

JCCSE—USNORTHCOM

NextGen—Department of the Air Force

Task 10.3

Develop a phased strategic level Homeland Defense/Civil Support Information Sharing Plan that captures information sharing processes, procedures, products, and critical information sharing requirements among key operation centers.

Details

- Capture and expand upon the information sharing processes and procedures developed among the National Military Command Center, Global Situational Awareness Facility, Department of Homeland Security National Operations Center, NGB Joint Coordination Center, and the NORAD and USNORTHCOM Command Center

- Integrate other key agencies and operations centers in the Federal Government in a synchronized information exchange plan

- Leverage the information sharing efforts among U.S. centers to develop a Bi-Lateral, Bi-National Information Sharing Plan between Canadian and United States operations centers, including the Public Safety Canada Operations Center, Royal Mounted Police Operations Center, and the Canada Command Operations Center to capture information sharing processes, procedures, products, and critical information sharing requirements in cross border operations

Responsibilities

OPR: USNORTHOM

OCR: ASD(HD&ASA), ASD(NII), NGB, Joint Staff J3

APPENDIX A—DoD Information Sharing Strategy

In May 2007, the Department of Defense (DoD) Chief Information Officer (CIO) signed the DoD Information Sharing Strategy. The Strategy was developed in direct response to the 2006 Quadrennial Defense Review (QDR) and establishes the vision and goals for information sharing across the Department.

Improving the Department's ability to share information helps DoD realize the power of information as a strategic asset. Benefits include: (1) achieving unity of effort across mission and coalition operations; (2) improving the speed and execution of decisions; (3) achieving rapid adaptability across mission and coalition operations; and (4) improving the ability to anticipate events and resource needs, providing an initial situational advantage, and setting the conditions for success.

The DoD Information Sharing Strategy establishes the following vision for information sharing:

Deliver the power of information to ensure mission success through an agile enterprise with freedom of maneuverability across the information environment.

This vision describes a future state in which transparent, open, agile, timely, and relevant information sharing occurs to promote freedom of maneuverability across a trusted information environment. To achieve this vision, the Strategy describes four goals that, when met, form the requisite DoD information sharing environment. These goals are listed below.

Goal	Description
Promote, encourage, and incentivize sharing.	Successful information sharing necessitates a mindset where information is continually shared as a normal course of work. Leaders shall align individuals to the common information sharing vision and encourage the adoption of the new mindset and culture.
Achieve an extended enterprise.	The extended enterprise refers to all internal and external participants required to ensure mission success. This facilitates collaborative and coordinated decision making, shared situational awareness, and improved knowledge at every level.
Strengthen agility, in order to accommodate unanticipated partners and events.	To accomplish information sharing in diverse and disadvantaged situations, the DoD shall enact and implement adaptive policies, guidance, practices, protections, and technologies.
Ensure trust across organizations.	A cornerstone of information sharing is trust - trust in the partner organizations including, but not limited to, their policies, procedures, systems, networks, and data. The DoD shall develop methods to promote and establish trust.

APPENDIX B—Mapping to the Goals and Touchstones

The following table maps each task to its associated Department of Defense Information Sharing Strategy goal and implementation consideration, also referred to as touchstone. In some cases, a single task may map to more than one goal or touchstone.

Goals / Touchstones	Promote, encourage, and incentivize sharing.	Achieve an extended enterprise.	Strengthen agility, in order to accommodate unanticipated partners and events.	Ensure trust across organizations.
Culture	2.1, 2.3	2.4, 3.1	2.4, 3.1, 4.1	2.3, 2.4, 5.1, 5.2
Policy	1.3, 2.2	3.1, 5.1, 5.2, 10.3	3.1	10.3
Governance	1.1, 1.2, 10.2	1.2, 9.1	9.1	1.2
Economics and Resources	1.3, 9.1	10.1, 10.2		
Technology and Infrastructure		4.1, 6.1, 7.1, 9.2, 9.3	4.1, 6.1, 7.1, 8.1, 8.2, 9.2, 9.3	8.1

The following table groups tasks by Office of Primary Responsibility (OPR):

OPR	Task numbers
ASD(NII)	6.1
ASD(HD&ASA)	10.1, 10.2
Capability Portfolio Managers	1.3
Department of the Air Force	10.2
Department of the Navy	10.2
DISA	7.1
DoD CIO	3.1, 8.2, 9.1, 9.2, 9.3, 10.1, 10.2
DoD Components	2.1, 2.3
Joint Staff J5	1.1, 1.2
Joint Staff J6	6.1, 7.1
Joint Staff J8	1.3
PA&E	1.3
USD(AT&L)	1.3
USD(I)	5.1, 5.2
USD(P&R)	8.1
USD(P)	1.1, 1.2, 2.2
USJFCOM	2.4, 4.1, 7.1
USNORTHCOM	10.2, 10.3

APPENDIX C—Federal ISE Responsibilities

A major focus area of the Federal Government is to improve the sharing of information concerning terrorism and weapons of mass destruction. Section 1016(g) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) required the establishment of an Information Sharing Council to assist the President and the terrorism Information Sharing Environment (ISE) Program Manager in this endeavor. In support of the IRTPA requirements, the President directed in the December 16, 2005, memorandum, "Guidelines and Requirements in Support of the Information Sharing Environment" that the heads of the executive departments and agencies shall, to the extent permitted by law and subject to the availability of appropriations, provide assistance and information to the Director of National Intelligence (DNI) and the Program Manager (PM)-ISE in the implementation of the guidelines and requirements listed in the memorandum.

The Under Secretary of Defense for Intelligence (USD(I)) was initially assigned as the Department of Defense (DoD) lead in support of this effort, but this role was subsequently transferred to the DoD Chief Information Officer (CIO) on December 16, 2005, by DoD Executive Secretary action.

The PM-ISE Implementation Plan, issued November 2006, includes actions that are to be performed in two phases through 2009 to establish the foundational elements of the ISE. The Office of the DNI, PM-ISE memorandum, *Fiscal Years 2010-2014 Programmatic Guidance for the Information Sharing Environment (ISE)* dated February 14, 2008, highlighted the Federal ISE priorities for FY 2010–2014. These priorities are further discussed in the following table:

Controlled Unclassified Information (CUI) Framework Transition	CUI is unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, but still requires protection from unauthorized disclosure. If approved by the President, the recommended CUI Framework for the ISE will establish policies and standards for the designation, marking, safeguarding, and dissemination of sensitive information throughout Federal Government organizations, regardless of the medium used for its display, storage, or transmittal.
State and Major Urban Area Fusion Centers	State and Major Urban Area Fusion Centers are vital assets that are critical to sharing information related to terrorism. The President has directed that federal departments and agencies will provide terrorism-related information to State, local, and tribal authorities primarily through these fusion centers. Unless specifically prohibited by law or subject to security classification restrictions, these fusion centers may further customize such information for dissemination to satisfy intra- or inter-state needs.
Interagency Threat Assessment Coordination Group	The Interagency Threat Assessment and Coordination Group (ITACG) supports the efforts of the National Counter Terrorism Center (NCTC) to produce "federally coordinated" terrorism-related information products intended for dissemination to State, local, and tribal officials and private sector partners through existing channels established by federal departments and agencies. The ITACG Detail is composed of State, local, and tribal homeland security and law enforcement officers and intelligence analysts detailed to work with federal intelligence analysts

	within the NCTC to assist in the development and production of federally coordinated information products regarding terrorist threats and events that are intended for dissemination to and use by State, local, and tribal officials and the private sector. The ITACG Advisory Council sets policies and develops processes for the ITACG Detail to facilitate the integration, analysis, and dissemination of federally coordinated information within the scope of the ISE, including homeland security information, terrorism information, and weapons of mass destruction information.
Suspicious Activity Reporting	Suspicious activity reporting (SAR) is documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention. An ISE-SAR is a SAR that has been determined to have a potential terrorism nexus in accordance with a two-step process set forth in the ISE-SAR Functional Standard. The objective of the ISE-SAR effort is to implement an improved business process that better manages the collection, review, integration, and sharing across the ISE. This process develops an ISE-wide capability for reporting, tracking, and accessing terrorist-related suspicious incidents in accordance with direction in the National Strategy for Information Sharing (October 2007).
Shared Space	The ISE Shared Space enables uniformity in the information exchange of terrorism-related information. It is built in accordance with the ISE Enterprise Architecture Framework (ISE EAF) and is the IT infrastructure for information sharing. The ISE Shared Space enables each ISE participant to make terrorism-related information, applications, and services accessible to ISE users in each of the three security domains (TS/SCI, Secret/Collateral, and SBU/CUI). More specifically, the Shared Space is where the ISE elements are standardized through the implementation of common terrorism information sharing standards (CTISS). Physically, the Shared Space is a set of hardware and software on a protected/secure network (technically referred to as demilitarized zone or DMZ) that is exposed at the boundary of an ISE participant's internal network—intranet. Alternatively, it may be hosted by a third party (e.g., another ISE participant), while remaining under the participant's funding, management, and control.
Alerts, Warnings, and Notifications	Alerts and warnings within the ISE are advisory messages among Federal, State, local, tribal, and foreign governments and the private sector that provide immediate or urgent information on threats or situations. Notifications within the ISE are specific or general advisory messages among federal communities and among the Federal, State, local, and tribal governments that provide information or advice of a less urgent nature. The ISE alerts, warnings and notifications (AWN) effort focuses on establishing an ISE-wide framework for the improved sharing of terrorism-related alerts, warnings, and notifications among ISE participants, within each security domain (TS/SCI, Secret/Collateral, and SBU/CUI).

To leverage inherent DoD component roles and responsibilities as well as specific responsibilities identified by DoD for these federal initiatives, PM-ISE OPR responsibilities are categorized into responsibility areas. The following table provides a description of the

responsibility areas necessary for supporting these Federal information sharing initiatives and the DoD component organization(s) responsible as OPR for each. The DoD CIO has the overarching responsibility for coordinating across Federal information sharing initiatives.

PM-ISE OPR Responsibility Area	DoD OPR for PM-ISE Responsibility Area	PM-ISE OPR Responsibility Description
Overall within DoD	DoD CIO	Acts as the single DoD voice to PM-ISE and its participants; coordinates, integrates, and monitors activities across DoD component organizations involved in supporting DoD's role in the initiative; and establishes DoD's overall position to the initiative. Represents DoD in the Information Sharing Council.
Policy	USD(P)	Determines the impact of federal mandates and legislation on DoD policies and establishes DoD positions on policy associated with the Federal ISE.
Mission Requirements and Associated JROC-Approved Processes	Joint Staff	Represents DoD mission area requirements and business processes that are applicable to the ISE. Establishes DoD mission performance parameters associated with ISE and across Federal information sharing initiatives. Represents DoD in the Business Process Working Group.
Performance and Related Processes	USD(AT&L)	Reviews and coordinates performance metrics and management measures applicable to ISE. Represents DoD Performance Improvement Officer executive order roles with respect to ISE.
Architecture	DoD CIO	Determines any impact of ISE needs on DoD's overarching architecture efforts and establishes DoD's positions on proposed architectural elements. Represents DoD in the Chief Architects Roundtable.
Standards	DoD CIO	Leverages existing DoD and industry standards in Federal ISE efforts. Determines any impact of ISE standards needs on DoD's ongoing standards efforts and establishes DoD's positions on proposed standards. Represents DoD on the CTISS Committee. Designation of DISA as Office of Collateral Responsibility indicates the strong DISA influence and related responsibilities on standards evolving beyond CTISS.
Disclosure and Information Sharing Agreements	USD(P)	Develops procedures and approval mechanisms for disclosure and release of information to parties involved in the ISE, including the structure, development, negotiation, and monitoring of information sharing agreements.
Marking and Classification Policy and Training	USD(I)	Establishes requirements and procedures for marking information, including both national security classified information and controlled unclassified information, as required by ISE.
Marking and	DoD CIO	Ensures use of net-centric information sharing concepts for

Classification Technical Implementation		marking information, including both national security classified information and controlled unclassified information, as required by ISE.
Interagency IT Services and Shared Space	DoD CIO	Leverages the results of implementing DoD's Data Strategy and Services Strategy in ISE efforts. Identifies DoD IT services to support a DoD mission need in conjunction with the ISE and also the potential impact of additional ISE requirements on DoD's Net-Centric Enterprise Services. Also determines how DoD should participate in any "shared spaces" for sharing information among mission partners.
Information Assurance	DoD CIO	Defines information assurance policy, requirements, risks, and trust relationships associated with information sharing needs of the ISE. Leverages existing and ongoing DoD and Federal IA efforts and establishes DoD's positions for using or linking DoD IA capabilities with those of other federal agencies and external mission partners.
Privacy and Civil Liberties Protection	USD(P)	Represents DoD in ISE efforts involving the protection of privacy and civil liberties when sharing information.
Training and Exercises	Joint Staff	Coordinates DoD's planning and participation in training and exercises conducted within the scope of ISE and across federal information sharing initiatives.
State/Local/ Tribal/Private Sector Coordination	USD(P)	Represents DoD's authorized role in sharing information with State, local, and tribal governments within the purview of the ISE.

APPENDIX D—References

a. DoD. *National Defense Strategy*. June 2008.
    <http://www.defenselink.mil/news/2008%20national%20defense%20strategy.pdf>

b. Department of Defense. *Quadrennial Defense Review Report*. February 6, 2006.
    <http://www.au.af.mil/au/awc/awcgate/DoD/qdr2006feb03.pdf>

c. DoD Chief Information Office. *DoD Information Sharing Strategy*. May 4, 2007.
    <http://www.defenselink.mil/cio-nii/docs/InfoSharingStrategy.pdf>

d. DoD Chief Information Office. *Department of Defense Information Management & Information Technology Strategic Plan 2008 – 2009*. August 2008.
    <http://www.defenselink.mil/cio-nii/docs/DoDCIO_Strat_Plan.pdf>

e. DoD Chief Information Office. *Department of Defense Net-Centric Data Strategy*. May 9, 2003.
    <http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf>

f. DoD Chief Information Office. *Department of Defense Net-Centric Services Strategy*. May 4, 2007. <http://www.defenselink.mil/cio-nii/docs/Services_Strategy.pdf>

g. The White House. *National Strategy for Information Sharing, Successes and Challenges in Improving Terrorism-Related Information Sharing*. October 2007.
    <http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf>

h. Office of the Director of National Intelligence, Program Manager, Information Sharing Environment. *Information Sharing Environment Implementation Plan*. November 2006.
    <http://www.ise.gov/docs/ise-impplan-200611.pdf>

i. National Commission on Terrorist Attacks. *The 9/11 Commission Report*.
    <http://www.9-11commission.gov/report/911Report.pdf>

j. Congressional Report: H. Rpt. 109-377. *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*.
    <http://www.gpoaccess.gov/serialset/creports/katrina.html>

k. Chairman of the Joint Chiefs of Staff. *The National Military Strategy for Cyberspace Operations*. 2006.

l. Under Secretary of Defense for Intelligence. *JIOC Staff Assistance Visit Report*. December 5, 2007.

m. Deputy Secretary of Defense Memo. *Implementation of the Department of Defense Information Sharing Strategy Deputy Secretary*. August 29, 2007.
    <http://www.defenselink.mil/cio-nii/docs/DSD_DoD_IS_Strategy.pdf>

n. Deputy Secretary of Defense Memo. *Institutional Reform and Governance Actions to Critical Path (ACP)*. March 15, 2007.

o. United States Public Law. *Intelligence Reform and Terrorism Prevention Act of 2004*. December 17, 2004. <http://www.nctc.gov/docs/pl108_458.pdf>

p. United States Intelligence Community. *Information Sharing Strategy*. February 22, 2008.
    <http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf>

q. National Institute of Standards and Technology. *FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors*. March 2006.
    <http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>

r.   Homeland Security Presidential Directive. *HSPD-12 Policy for Common Identification Standard for Federal Employees and Contractors*. August 27, 2004.
<http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>

s.   Executive Order 12356. *National Security Information*. April 2, 1982.

t.   Executive Order 13292. *Further Amendment to Executive Order 12958, As Amended, Classified National Security Information*. March 25, 2003.
<http://www.whitehouse.gov/news/releases/2003/03/20030325-11.html>

u.   Under Secretary of Defense for Intelligence. *Use of the "Not Releasable to Foreign Nationals" (NOFORN) Caveat on Department of Defense (DoD) Information*. May 17, 2005.
<http://www.dtic.mil/whs/directives/corres/pdf/int050517norforn.pdf>

v.   Office of the Director of National Intelligence Community Policy Memorandum Number 2007-500-1. *Unevaluated Domestic Threat Tearline Reports*. November 19, 2007.

w.   Director of the Joint Staff Memorandum. *Information Sharing with United Kingdom, Australia and Canada*. January 26, 2007.

x.   Chairman of the Joint Chiefs of Staff Instruction. *CJCSI 6285.01 Multinational Information Sharing (MNIS) Current Operational Systems Requirements Management Process*. August 1, 2006. http://www.dtic.mil/cjcs_directives/cdata/unlimit/6285_01.pdf

y.   Executive Order 13388. *Further Strengthening the Sharing of Terrorism Information to Protect Americans*. October 25, 2005.
<http://www.whitehouse.gov/news/releases/2005/10/20051025-5.html>

z.   National Security Presidential Directive. *NSPD-41 Maritime Security Policy*. December 21, 2004.

aa.   Homeland Security Presidential Directive. *HSPD-13 Maritime Security Policy*. December 21, 2004.

bb.   The White House. *The National Strategy for Maritime Security*. September 2005.
<http://www.whitehouse.gov/homeland/4844-nsms.pdf>

cc.   National Security Presidential Directive. *NSPD-47 [on aviation security and threats to commercial aircraft]*. June 22, 2006.

dd.   Homeland Security Presidential Directive. *HSPD-16 Aviation Security Policy Released*. March 26, 2007.

ee.   The White House. *The National Strategy for Aviation Security*. March 26, 2007.
<http://www.whitehouse.gov/homeland/nstrategy_asecurity.pdf>

ff.   Joint Staff. *Joint CONUS Communications Support Environment (JCCSE) Concept for Joint C4*. October 15, 2005.

gg.   United States Public Law. *P.L. 108-176 VISION 100 – Century of Aviation Reauthorization Act*. December 12, 2003.
<http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ176.108.pdf>

hh.   Office of Management and Budget (OMB) Memorandum. *Budget Guidance for Justification of Fiscal Year 2010 to 2014 Investments Supporting the Information Sharing Environment (ISE) Priorities*. February 14, 2008.

ii.   President Memorandum. *Guidelines and Requirements in Support of the Information Sharing Environment*. December 16, 2005.

jj.   Office of the Director of National Intelligence, PM-ISE Memorandum. *Fiscal Years 2010-2014 Programmatic Guidance for the Information Sharing Environment (ISE)*. February 14, 2008.

APPENDIX E—Acronyms

Acronym	Description
ABAC	Attribute-Based Access Control
ACP	Actions to Critical Path
AoA	Analysis of Alternatives
AOR	Area of Responsibility
APAN	Asia Pacific Area Network
ASD(HD&ASA)	Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
ASD(NII)	Office of the Assistant Secretary of Defense for Networks and Information Integration
AWN	Alerts, Warnings and Notifications
C4	Command, Control, Communications, and Computers
CAC	Common Access Card
CC/S/A	Combatant Command/Military Services/Defense Agencies
CCER	CENTRIXS Cross Enclave Requirement
CDS	Cross Domain Solution
CENTRIXS	Combined Enterprise Regional Information Exchange System
CES	Core Enterprise Services
CIE	Collaborative Information Environment
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
COIs	Communities of Interest
COP	Common Operational Picture
COTS	Commercial Off-the-Shelf
CTISS	Common Terrorism Information Sharing Standards
CUI	Controlled Unclassified Information
CWID	Coalition Warrior Interoperability Demonstration
DAS	Defense Acquisition System
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DKO	Defense Knowledge Online
DMZ	Demilitarized Zone
DNI	Director of National Intelligence
DoD	Department of Defense
DoD CIO	Department of Defense Chief Information Officer
DoD GC	General Counsel
DOT	Department of Transportation
EO	Executive Order
FIPS	Federal Information Processing Standards

FY	Fiscal Year
GIG	Global Information Grid
HSC	Homeland Security Council
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IEB	Information Exchange Broker
IM	Information Management
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISE	Information Sharing Environment
IT	Information Technology
ITACG	Interagency Threat Assessment Coordination Group
JCA	Joint Capability Area
JCCSE	Joint Continental U.S. Communications Support Environnent
JCIDS	Joint Capabilities Integration and Development System
JIOC	Joint Intelligence Operations Center
JPDO	Joint Planning and Development Office
JROC	Joint Requirements Oversight Council
JWICS	Joint Worldwide Intelligence Communications System
MDA	Maritime Domain Awareness
MNCE	Multi-National Collaboration Environment
MNIS	Multinational Information Sharing
NATO	North Atlantic Treaty Organization
NCCC	National Command and Coordination Capability
NCES	Net-Centric Enterprise Services
NC-FCB	Net-Centric Functional Capabilities Board
NCTC	National Counter Terrorism Center
NECC	Net-Enabled Command Capability
NextGen	Next Generation Air Transportation System
NGA	National Geospatial-Intelligence Agency
NGB	National Guard Bureau
NIEM	National Information Exchange Model
NOFORN	Not Releasable to Foreign Nationals
NORAD	North American Aerospace Defense Command
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council
NSPD	National Security Presidential Directive
OCR	Office of Collateral Responsibility
OMB	Office of Management and Budget
OPR	Office of Primary Responsibility
ORCON	Originator Control
P.L.	Public Law

PA&E	Program Analysis and Evaluation
PDM	Program Decision Memorandum
PKI	Public Key Infrastructure
PM	Program Manager
PM-ISE	Program Manager, Information Sharing Environment
POA&M	Plan of Actions and Milestones
POM	Program Objective Memorandum
PPBE	Planning, Programming, Budgeting, and Execution
PR-09	Program Review 2009
QDR	Quadrennial Defense Review
RBAC	Role-Based Access Control
SAR	Suspicious Activity Reporting
SBU	Sensitive But Unclassified
SIPRNet	SECRET Internet Protocol Router Network
SOA	Service Oriented Architecture
SSTR	Stability, Security, Transition, and Reconstruction
TS/SCI	Top Secret/Sensitive Compartmented Information
U.S.	United States
U-Core	Universal Core
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USD(P)	Under Secretary of Defense for Policy
USEUCOM	United States European Command
USJFCOM	United States Joint Forces Command
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
USSOUTHCOM	United States Southern Command
USSTRATCOM	United States Strategic Command
WMD	Weapons of Mass Destruction

APPENDIX F—Glossary

Term	Definition
Capability	The ability to execute a specified course of action. (A capability may or may not be accompanied by an intention.)The ability to achieve a desired effect under specified standards and conditions through combinations of ways and means to perform a set of tasks.
Community of Interest (COI)	The inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes, and who therefore must have shared vocabulary for the information they exchange.
Extended Enterprise	All internal and external participants required to ensure mission success.
Global Information Grid (GIG)	The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, defense policymakers, and support personnel.
Information Assurance	The ability to provide the measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.
Information Management	The function of managing an organization's information resources by the handling of knowledge acquired by one or many different individuals and organizations in a way that optimizes access by all who have a share in that knowledge or a right to that knowledge. The planning, budgeting, manipulating, and controlling of information throughout its life cycle.
Information Sharing	Making information available to participants (people, processes, or systems). Information sharing includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a DoD Component directly, or used by a contractor under a contract with the DoD Component, which requires the use of such equipment, or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term also includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term does not include any equipment that

is acquired by a federal contractor incidental to a federal contract. The term includes National Security Systems (NSS).

Joint Net-Centric Operation	The ability to exploit all human and technical elements of the Joint Force and its mission partners by fully integrating collected information, awareness, knowledge, experience, and decision-making, enabled by secure access and distribution, to achieve a high level of agility and effectiveness in a dispersed, decentralized, dynamic, and/or uncertain operational environment.
Mission Partners	External partners as defined in the DoD Information Sharing Strategy: Federal, State, local, tribal, coalition partners, foreign governments and security forces, international organizations, non-governmental organizations, and the private sector.
Net-Centric Environment	The framework for full human and technical connectivity and interoperability that allows all DoD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence and protects information from those who should not have it.
Net-Centric Joint Capability Area	The ability to provide a framework for full human and technical connectivity and interoperability that allows all DoD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and protects information from those who should not have it.
Net-Centric Operations	The exploitation of the human and technical networking of all elements of an appropriately trained Joint Force by fully integrating collective capabilities, awareness, knowledge, experience, and superior decision making to achieve a high level of agility and effectiveness in dispersed, decentralized, dynamic, and uncertain operational environments.
Net-Centricity	The realization of a networked environment (including infrastructure, systems, processes, and people) that enables a completely different approach to warfighting and business operations.
Portfolio Management	The management of selected groupings of IT investments using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability.
Social Networking	A social structure made of nodes (generally individuals or organizations) that are tied by one or more specific types of interdependency.