DEPARTMENT OF DEFENSE

INFORMATION MANAGEMENT & INFORMATION TECHNOLOGY

STRATEGIC PLAN

2008-2009

CREATING AN INFORMATION ADVANTAGE FOR OUR PEOPLE AND MISSION PARTNERS

FROM THE DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER (DoD CIO)

Defense transformation hinges on the recognition that information is a critical enabler for ensuring mission success. Accordingly, the DoD is initiating a strategy to ***"Lead the DoD enterprise to achieve an information advantage for our people and mission partners."*** As stated in the National Defense Strategy, March 2005, "Transforming to a network centric force requires fundamental changes in processes, policy, and culture. Change in these areas will provide the necessary speed, accuracy, and quality of decision-making critical to future success. Beyond battlefield applications, a network centric force can increase efficiency and effectiveness across defense operations, intelligence functions, and business processes by giving all users access to the latest, most relevant and accurate information."

This DoD Information Management / Information Technology (IM / IT) Strategic Plan was developed collaboratively with the CIOs of the Military Departments (MILDEPs), Defense Information Systems Agency (DISA), National Security Agency, United States Strategic Command and Joint Chiefs of Staff to provide a common understanding of our shared vision, mission and governing principles for IM / IT. The plan identifies specific goals and objectives to guide the net-centric transformation of the DoD during the period 2008 - 2009. It also defines key performance indicators for assessing progress toward meeting the goals and objectives that will move the Department's transformation to net-centric information sharing from concept to reality. Success stories are provided to illustrate progress being made. Progress will be reviewed and this plan will be updated every two years. Together we can lead the DoD in achieving an information advantage for our people and mission partners.

John G. Grimes
Department of Defense
Chief Information Officer

This document supersedes the 2006 ***Department of Defense Chief Information Officer Strategic Plan Version 1*** and the June 2004 ***DoD Chief Information Officer Strategic Plan for Information Resources Management (IRM)***.

VISION

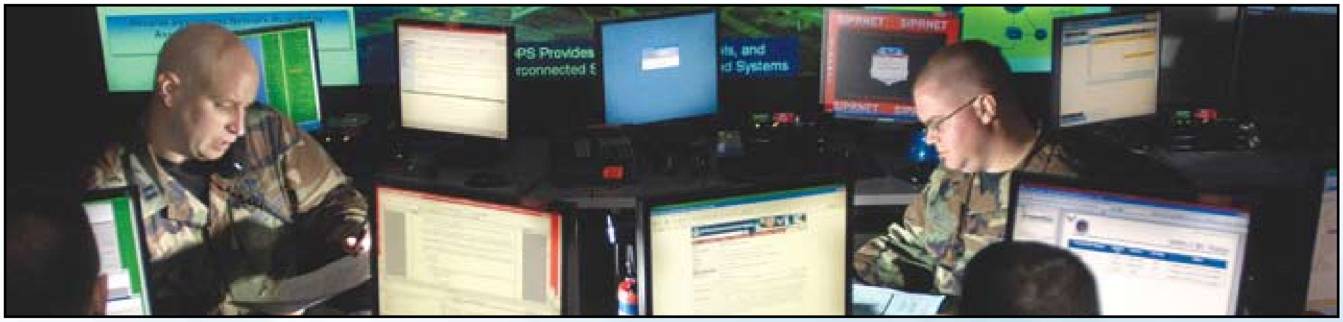
DELIVER THE POWER OF INFORMATION

An agile enterprise empowered by access to and sharing of timely and trusted information.

MISSION

ENABLE NET-CENTRIC OPERATIONS

Lead the information age transformation to enhance the Department of Defense's effectiveness and efficiency.

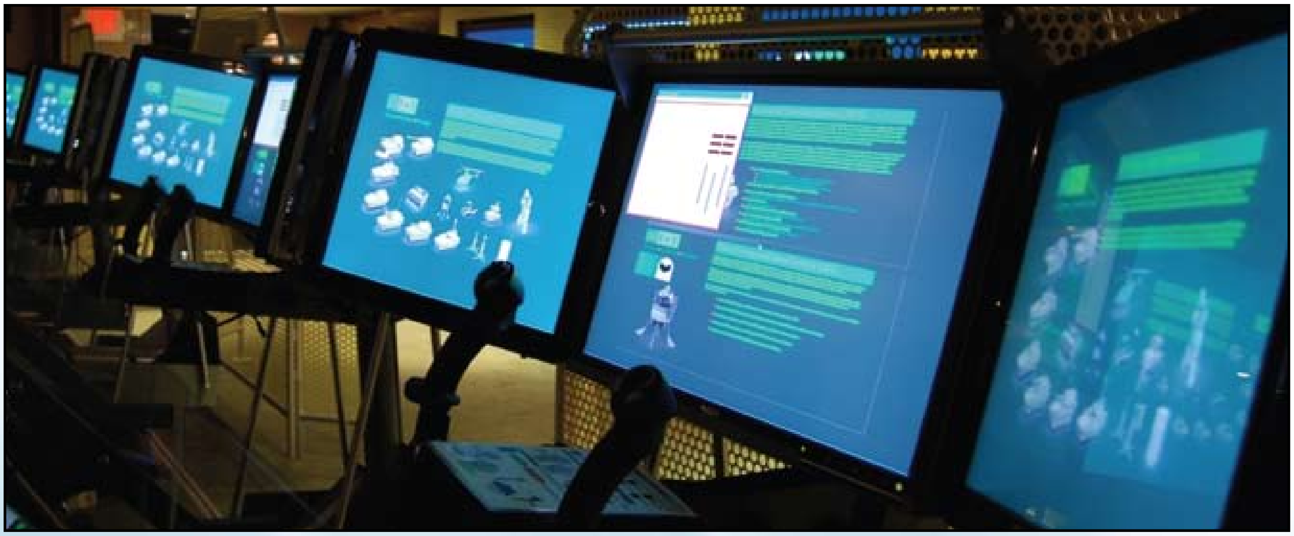


IM / IT
GOVERNING PRINCIPLES

- *Ensure mission effectiveness through the transformation to net-centric information sharing.*

- *Ensure IM / IT investments and mandates meet mission needs.*

- *Identify, leverage and share best practices from industry, government and academia.*



IM / IT GOALS:

1. NET-CENTRIC TRANSFORMATION

Accelerate DoD's net-centric transformation to facilitate effective and efficient warfighting, intelligence and business processes and other national security activities.

2. INFORMATION AS A STRATEGIC ASSET

Use information sharing to enable effective and agile decision making through visible, accessible, understandable and trusted data and services – when and where needed.

3. INTEROPERABLE INFRASTRUCTURE

Ensure robust and reliable world-wide connectivity and infrastructure within DoD and with external mission partners.

CURRENT VIEW:

- *Stove-Piped Information*
- *Centralized Control*
- *Unique Software Solutions*
- *Data Not Shared*
- *Inefficiency*

JOURNEY OF

4. ASSURED INFORMATION ACCESS

Protect and defend DoD systems, networks and information to maximize mission assurance.

5. RETURN ON INVESTMENT

Maximize the contribution of IT investments to national security and defense outcomes.

6. IT WORKFORCE DEVELOPMENT

Maintain an agile IT workforce with the skills to build, extend, exploit and defend a net-centric DoD.

FUTURE VIEW:

- ***Net-Centricity***
- ***Decentralized Control***
- ***Enterprise Services***
- ***Shared Data***
- ***Autonomous Agent***
- ***Enterprise Architecture***
- ***Web 2.0***

1 NET-CENTRIC TRANSFORMATION

Accelerate DoD's Net-centric Transformation to Facilitate Effective and Efficient Warfighting, Intelligence and Business Processes and other National Security Activities. «««««««««««««««««««««««

DESCRIPTION

DoD must implement the organization, culture and technologies to continually transform to a net-centric information sharing environment. Military commanders must understand the potential of sharing information to enable battlefield decision-making superiority. It is the Department's responsibility to hasten the delivery of net-centric information sharing. Socializing the new net-centric information sharing concepts and their advantages Department-wide will help accelerate development of joint and service-specific operational concepts that exploit the benefits of an information environment that unleashes the information advantage.

The effort to accelerate DoD's net-centric information sharing transformation is dependent upon adoption of technologies that support two overarching concepts: Service-Oriented Architecture (SOA) and Web 2.0. Nevertheless, these concepts can be implemented with a variety of complex technologies and are not inherently interoperable. To focus the net-centric information sharing vision while solving this and similar challenges, DoD has established the DoD Information Enterprise Architecture (IEA) to guide the investment into tools, technologies and approaches that will enable the information sharing transformation.

DoD's knowledge sharing capabilities must be implemented using service-oriented development and operational approaches. SOA is an emerging net-centric enabling approach with significant potential for operational, fiscal and engineering benefits to DoD.

Using loosely coupled web-services, DoD users can find and use information without prior knowledge of its existence. Since reuse of software components is central to SOA, DoD could reduce development cost by the elimination of duplicate work. Additionally, improved change management and process improvement is a byproduct of a SOA approach since it requires buy-in from the entire user and development community. A related concept known as Web 2.0 focuses on the ability of people to work collaboratively. Web 2.0 framework includes: development of services vice packaged software; data sources that get richer with use; harnessing collective intelligence; and use of customer self-service.[1] Understanding and leveraging the benefits of the SOA and Web 2.0 concepts is critical to unleashing the information advantage for our people and mission partners.

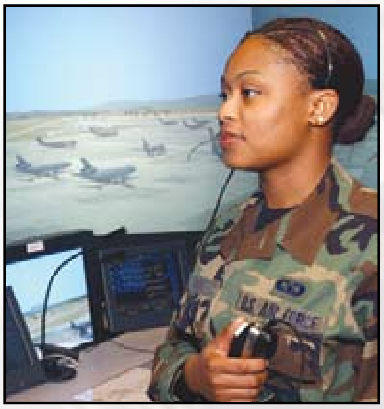
Additionally, successful transformation will require commanders to understand and effectively employ defensive elements of information operations (IO) to ensure mission effectiveness. Managing the life-cycle aspects of IO will increase our ability to perform threat detection, prevention and response to ensure that we maintain the information advantage.

OBJECTIVES

1.1. Warfighting, intelligence and business processes exploit net-centric capabilities.

1.1.1. Incorporate collaboratively developed net-centric information sharing methodologies (e.g., SOA, Web 2.0) into the warfighting, intelligence and business processes supported by DoD acquisition programs.

1.1.2. Ensure DoD components use continuous process improvement initiatives, to include Lean Six Sigma, to enhance the effectiveness and efficiency of their missions.



[1] *O'Reilly, Tim, What is Web 2.0, Design Patterns and Business Models for the Next Generation of Software, 2007 O'Reilly Media, Inc.*

1.1.3. Incorporate net-centric cross-component information sharing into mission planning aspects of major training exercises.

1.2. Use of information technologies enables development of more agile and collaborative cross-component warfighting, intelligence and business processes.

1.2.1. Partner with commercial and educational communities to develop, prototype and implement innovative net-centric capabilities that improve effectiveness and efficiency of DoD processes.

1.2.2. Incorporate emerging commercial technologies that improve mission effectiveness and efficiency and enable use of common services.

1.3. Warfighting, intelligence and business communities understand and effectively employ the defensive elements of IO.

1.3.1. Enhance DoD's IO training capabilities with emphasis upon improving threat detection, prevention and response.

KEY PERFORMANCE INDICATORS

- Percentage of DoD processes that utilize net-centric capabilities as shown in acquisition program documentation.
- Percentage of DoD IT investments that comply with the IEA as shown in acquisition program documentation.
- Percentage of joint experiments, pilots and demonstrations that employ net-centric capabilities (i.e., Community of Interest (COI) pilots).
- Percentage of DoD supported commercial and educational initiatives that have been successfully implemented.

Success Story I: Marine Corps Center for Lessons Learned (MCCLL)

The MCCLL has standardized and improved information delivery to all authorized DoD users conducting a federated search of Marine Corps lessons learned. The MCCLL serves as a single fusion center to collect, analyze, manage and disseminate knowledge gained through operational experiences, exercises and supporting activities. MCCLL enables marines to achieve higher levels of performance and provides information and analysis on emerging issues and trends in support of operational commanders and the Commandant of the Marine Corps. It uses the Lesson Management System (LMS) to manage the Marine Corps lesson collection, tracking, data-mining and dissemination requirements. The Joint Staff has selected the LMS as the DoD lessons learned input support tool. The LMS has been adopted as the Joint Lessons Learned Information System (JLLIS) with the associated Joint Lessons Learned Repository (JLLR). The JLLIS / JLLR affords the user with access, via the web, to federated data from the military services, combatant commands and combat support agencies. It also provides the capability to extract trends, conduct pattern analysis and cross-map solutions to identified shortfalls.

Additionally, knowledge and experience related to systems, tactics, techniques and procedures to remedy deficiencies and reinforce successes are made available.

Success Story II: United States Air Force (USAF) Personnel Management Process Improvement

The USAF is improving the efficiency of its personnel management processes by using the Personnel Service Delivery transformation initiative to move from direct on-base support to web-based and service center-based personnel services. As a result the Air Force has currently centralized 94 personnel processes from its major commands to the Air Force Personnel Center. These on-going business process design efforts have already resulted in a workload cost avoidance of 729 full time equivalents.

Success Story III: Naval Air Systems Command Process Improvement

The Naval Air Systems Command has developed a paperless, fully automated IT process that has saved the Department of the Navy millions of dollars through enhanced efficiency. Prior to this initiative, airworthiness and flight safety instructions for weapons systems were provided in paper-based flight clearance documents. Generating these paper documents could take as long as 45 days, resulting in forces using older technologies to engage threats while waiting for new capabilities to be certified.

To reduce the turnaround time, a process permitting parallel reviews was introduced. This capability permits the engineers to perform a timely and secure review of flight clearances from anywhere in the world. Review of flight clearances has been reduced to less than two days for deployed forces using the fully automated process. In some cases, deployed forces have received new capabilities in response to a changing threat in less than two hours. The process is saving the lives of front-line forces because they quickly receive the most effective weapons systems available.

2 Information as a Strategic Asset

Use Information Sharing to Enable Effective and Agile Decision Making Through Visible, Accessible, Understandable and Trusted Data and Services – When and Where Needed.

Description

Information is a great source of power. Ensuring timely and trusted information is available where it is needed, when it is needed, and to those who need it most is essential to achieving an information advantage. Sharing information greatly enhances joint situational awareness. All data assets, services and applications, to include enterprise resource planning solutions, will be visible, accessible, understandable and trusted by all authorized users, both known and unanticipated, except where limited by law, policy or security classification.

Knowledge Management (KM), the systematic process of discovering, selecting, organizing, distilling, sharing, developing and using information, will provide the basis from which decisions are made and actions are taken. A KM capability can further advance information sharing, however, no central KM effort is currently underway within the Department to refine and standardize the military application of this function.[2]

In addition to improving its internal information sharing processes, the DoD is taking an active role in establishing an effective information sharing environment within the Department and with its external partners. Additionally, the DoD is improving its coalition information sharing capabilities as well as how it shares information in support of the broader Federal mission. Most recently the DoD has placed emphasis on supporting

[2] *Joint Chiefs of Staff, Joint Net-Centric Operations Campaign Plan, Washington D.C., October 2006*

the overarching National Strategy for Information Sharing and its subordinate activities such as the Federal Information Sharing Environment effort and closer alignment with Federal intelligence missions through partnership with the Director for National Intelligence (DNI).

OBJECTIVES

2.1. Timely access to authoritative, relevant, trusted and actionable information is provided to all authorized users.

2.1.1. Ensure data, information and capabilities are visible and accessible to all users except where limited by law, policy or security classification.

2.1.2. Ensure all data, information and capabilities are made available as registered services on the network and are described using the DoD enterprise standard (i.e., DoD Discovery Metadata Specification) for discovery metadata.

2.1.3. Ensure all semantic vocabularies, taxonomies and ontologies are developed through COIs, utilize the Universal Core, and are registered with the enterprise for visibility, re-use and understandability in the DoD Metadata Registry.

2.1.4. Ensure enterprise resource planning solutions make their data and services available to unanticipated users throughout the DoD.

2.2. KM enables effective and agile decision making.

2.2.1. Create a knowledge sharing environment that enables more effective action by DoD and its mission partners (i.e., joint, multinational, non-governmental organizations (NGOs), interagency, state, local and tribal).

2.2.2. Apply knowledge sharing (e.g., lessons learned) during the planning of joint experiments, operational concept development, combat operations and other missions.

2.3. Information sharing within and between DoD and external partners supports accomplishment of national security missions.

2.3.1 Develop an information sharing implementation plan that establishes key outcomes and associated tasks to guide improvements in information sharing within and between DoD and external partners (e.g., allies, coalition forces, federal, state, local, tribal, NGOs, commercial).

2.3.2. Streamline and standardize policy for information classification markings within DoD and for interfaces with external partners.

2.3.3. Work with the Program Manager, Information Sharing Environment, to improve information sharing across the Federal Government.

2.3.4. Leverage key information sharing enablers developed through partnership between DoD and DNI.

KEY PERFORMANCE INDICATORS

- Percentage of IT and National Security Systems (NSS) in DoD IT Portfolio Repository (DITPR) whose data and services are discoverable.

- Percentage of IT and NSS in DITPR whose data format / structure (including vocabulary) is based on COI-defined specifications and is registered in the DoD Metadata Registry.

- Number of formal information sharing agreements in place with members of the extended enterprise, to include sharing of unclassified, controlled unclassified information, sensitive but unclassified, secret and higher information.

- Percentage of the Information Sharing Implementation Plan tasks completed.

Success Story I: The Maritime Domain Awareness Data Sharing (MDA DS) COI

The MDA DS COI pilot was initiated as a first step to provide law enforcement, defense, homeland security and intelligence officials improved awareness of global threats to national and maritime security through sharing of maritime vessel identification and tracking data. The pilot addresses the cultural and technical challenges that impede the ability of the Federal Departments to secure our coasts, ports and waterways by providing a shared awareness of potential threats from maritime vessels, cargo or crews. The 8-month pilot successfully proved the DoD Net-Centric Data Strategy by implementing an enterprise service-based architecture that enabled discovery and access to data from the existing information sources of four functionally and geographically separate data producers. The community is exploring additional data sharing priorities to further improve global maritime situation awareness supporting the national defense and homeland security missions of the Departments of Defense, Homeland Security and Transportation and the DNI.

Success Story II: 1st Cavalry Information Sharing

CavNet was designed as a web-based interactive community to help officers in the 1st Cavalry Division in Iraq trade information at the tactical level about insurgent tactics, gear and even advice on running effective civil affairs operations. In one case, it was learned that insurgents were booby-trapping posters of Moqtada al-Sadr— the Shiite cleric. When the posters were ripped down, an Improvised Explosive Device (IED) would detonate. This information was posted to CavNet. Another officer, operating in another sector of Baghdad, read about this new tactic on CavNet and briefed his men about this new technique. Later that day, using this information, soldiers were able to spot these booby traps and disarm the IEDs without any casualties. Without CavNet there was no way that this type of tactical information could be disseminated quickly and efficiently.

Success Story III: North American Aerospace Defense Command (NORAD) and United States Northern Command (USNORTHCOM) Information Exchange Brokers

NORAD and USNORTHCOM have created a community of practice that uses information exchange brokers to address the information sharing and knowledge management needs of their operational elements. These information exchange brokers are functional area experts knowledgeable in communications, ground, aviation, chemical-biological-radiological-nuclear, foreign area, and logistics operations, and in tactical, operational and strategic planning. They monitor the command's information flow and synchronization system to aid all command elements in the discovery of required information. So that the supported operator can focus on the primary task, the information exchange broker remains alert to clues found in related or fringe efforts. As the system process experts, information exchange brokers are qualified to train others to use these collaborative information processes and tools. They have led information sharing mobile training teams that have deployed to other mission partners' locations including the Canadian National Defense Headquarters and Canada Command. They have also provided short notice response to natural or manmade disasters and serviced many other requests for assistance from other mission partners.

3 INTEROPERABLE INFRASTRUCTURE

ENSURE ROBUST AND RELIABLE WORLD-WIDE CONNECTIVITY AND INFRASTRUCTURE WITHIN DOD AND WITH EXTERNAL MISSION PARTNERS.««

DESCRIPTION

Today's missions are increasingly joint and combined, requiring a dynamic infrastructure that provides world-wide connectivity and enables more effective information sharing among DoD entities and between DoD and its external partners. The DoD is committed to building an integrated IT infrastructure capability across the Department founded in the Net-Centric and Corporate Management & Support portfolios, as defined in the Department's new enterprise portfolio management structure.

DoD IEA establishes the capabilities, services, standards, implementing guidance and best practices that enable IT operations across all missions of the Department. Using a federated enterprise architecture development approach, DoD will identify and incrementally deliver Information Enterprise capabilities that address the information sharing needs of all DoD missions. To achieve the goals of net-centric operations, all DoD IT solutions must adhere to the DoD IEA rules and principles.

The Net-Centric Capability Portfolio oversees core IT infrastructure programs in the areas of Information Transport, Information Assurance, Enterprise Services and Network Management. The Net-Centric Capability Portfolio will provide a timely, synchronized, integrated and cost-effective enabling functionality driven by the needs of warfighters and their associated user applications and the efficient use of the electromagnetic spectrum. For example, this portfolio could use "autonomous agents" which act as mediators between users or devices and network resources to support information sharing within distributed warfighting or business communities. Communicating with each other, agents in the network make decisions about whether a certain user or device, either known or unanticipated, can be given access to a requested resource, by performing authentication, authorization and maintenance of user credentials.[3]

A critical enabler of DoD's net-centric vision is the transition from internet protocol (IP) version 4 (IPv4) to IPv6. IPv6 will greatly improve network ubiquity, increase the address space, enhance quality of service capability, enable mobile ad hoc networking, strengthen end-to-end security and a host of other functionality. The transition to IPv6 will require careful coordination within and across the DoD components as well as external partners.

To assure that the infrastructure supports mission needs, DoD must establish a means to test and evaluate (T&E) all aspects of net-centric operations. This capability must assess gained efficiencies, effectiveness and suitability of net-centric operations to a particular military mission. The assessment must consider human interactions, elements of reach, agility and decision-making under conditions of stress, uncertainty and failure.

[3] Seleznyov, A.; Hailes, S., An access control model based on distributed knowledge management, Advanced Information Networking and Applications, 2004. AINA 2004. 18th International Conference on Volume 2, Issue, 29-31 March 2004 Page(s): 403 - 406 Vol.2

OBJECTIVES

3.1. A set of synchronized capabilities and systems that support DoD warfighting, intelligence and business processes and other national security related activities.

3.1.1. Develop a time-phased, capabilities-based, federated DoD IEA and transition plan which determine and align the common infrastructure components needed to deliver net-centric capability (e.g., data and services deployment, secured availability / information assurance, computing infrastructure, NetOps and Communications).

3.1.2. Ensure the Net-Centric Capability Portfolio and associated methodology supports accomplishment of the DoD objectives and meets the needs of the warfighters and other DoD decision makers.

3.1.3. Enable information sharing between DoD and external partners through federated infrastructure approaches that leverage commercial best practices and enforce commercial standards.

3.1.4. Manage the IPv6 transition through implementation planning, pilot demonstrations, T&E activities and by leveraging commercial standards and products.

3.1.5. Employ access control agents that perform user or device authentication, authorization and maintenance of user credentials.

3.2. A set of coherent, integrated, comprehensive DoD-wide guidance and policies exist, which govern DoD development and operations.

3.2.1. Develop and maintain a DoD IEA transition plan that reflects commercial best practices to enable agile and collaborative net-centric operations.

3.2.2. Implement a configuration management policy and procedures that unify DoD operations and defense.

3.2.3. Implement a comprehensive NetOps policy and procedures that support operations and defense of the DoD.

3.2.4. Align DoD spectrum policies with operational needs and the National Initiatives on Spectrum.

3.3. A scalable joint test and evaluation capability supports assessment of emerging net-centric operations and the enabling infrastructure.

3.3.1. Define the criteria and methods needed to test and evaluate distributed net-centric infrastructures (e.g., IPv6 transition), metadata environments and assured dynamic service composition by leveraging commercial best practices.

3.3.2. Establish a methodology to assess aspects of net-centric operations including: human interactions, elements of reach, elements of agility, elements of decision-making under conditions of stress, uncertainty and failure; gained effectiveness and efficiencies; system survivability and suitability to a particular military mission.

3.3.3. Use interface and operational testing between DoD and external partners to ensure robust and reliable performance of the infrastructure.

3.4. Portfolio funding supports the installation and integration of infrastructure elements needed to achieve net-centric capabilities and lower total ownership costs.

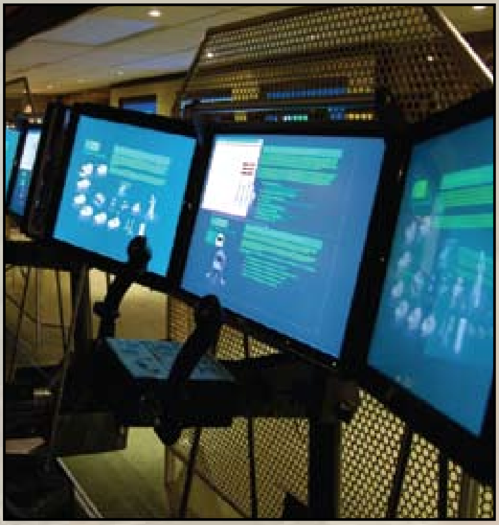
3.4.1. Collaborate with Combatant Commands, Services and Agencies to ensure they adequately fund for incremental installation and integration of necessary infrastructure elements.

3.4.2. Align architectures with the specific needs of the portfolio managers, delivering infrastructure details germane to infrastructure decision making.

KEY PERFORMANCE INDICATORS

- Percentage of Net-Centric Capability Portfolio programs that comply with the DoD IEA and are on-schedule.
- Number of successful IPv6 deployments and T&E events.
- Percentage of successful interface tests between DoD and external partners.

Success Story I: Marine Corps Information Infrastructure



Operation Iraqi Freedom highlighted the need for improved on-the-move and beyond-line-of-sight data capabilities for maneuver units. Command and Control (C2) On-the-Move Network Digital Over-the-Horizon Relay (CONDOR) provides these capabilities throughout the Marine Air Ground Task Force. CONDOR enables the use of C2 applications and tactical data radios to feed the Common Operational Picture (COP), while on-the-move and over-the-horizon. Building the COP increases situational awareness of friendly units and disseminates intelligence products on enemy locations, significantly enhancing the information available for the leader's decision cycle.

The CONDOR capability set bridges the gap between today's radio inventory and the future transformational communication architecture. CONDOR's fundamental premise is to make the tactical network accessible to the warfighter, using organic Marine Corps assets. This architectural approach is based on open standards that provide encrypted connectivity to the forward edge of the battlefield and will readily accept Joint Tactical

Radio System terminals as they are fielded. The CONDOR capability sets are meeting the needs of the operational forces to have C2 on-the-move while conducting operations in Iraq.

Success Story II: United States Joint Forces Command (USJFCOM) Coalition Interoperability

USJFCOM's Multi-National Turnkey C2 Project addresses the need for coalition interoperability in the Joint Task Force (JTF) environment. Leveraging USJFCOM's existing JTF Headquarters (HQ) C2 Baseline Templates and Architectures, the Multi-National Turnkey C2 Project provides an architecture framework with derived organizational, manning and equipping checklists. Using a repeatable C2 equipping process that streamlines the formation of a JTF HQs, the C2 project supports the rapid establishment and improved performance of JTFs for varying missions. When completed, this project will result in an interoperable C2 infrastructure for the North Atlantic Treaty Organization (NATO) led security and development mission in Afghanistan called the International Security Assistance Force.

4 ASSURED INFORMATION ACCESS

PROTECT AND DEFEND DOD SYSTEMS, NETWORKS AND INFORMATION TO MAXIMIZE MISSION ASSURANCE.

DESCRIPTION

Critical DoD and IC systems, networks, platforms and sensors must be developed and deployed with the necessary security and interoperability capabilities. The essential tenets of mission assurance include protecting all information, defending and keeping networks operational, identifying and differentiating between friendly and hostile forces in a cyber environment, partnering with other members of the security community (i.e., physical security, personnel security, critical infrastructure protection, and defense industrial base (DIB)), providing trusted software, providing access to integrated situational awareness, innovating and enabling Information Assurance (IA) capabilities, and creating an IA-empowered workforce. DoD and DNI must promulgate standardized strategies for assured information sharing. Additionally, due to DoD's reliance on commercial communications partners the national security risks arising from the increasing globalization of the Information and Communications Technologies infrastructure must be addressed.

Due to the magnitude and complexity of the net-centric vision, IA will be a phased implementation. The network security approach will address the entire life-cycle using "defense-in-breadth". Common standards-based evaluation and validation of IA and IA-enabled products, plus rapid turn-around, net-centric certification and accreditation of systems and networks will speed transition to the envisioned net-centric capabilities needed to achieve an information advantage.

OBJECTIVES

4.1. Assured information sharing across all domains and COIs.

4.1.1. Implement mechanisms to improve ability to discover and retrieve information based on access rights, metadata standards (e.g., classification, marking and labeling), cataloguing techniques and standardized cross domain solutions.

4.1.2. Leverage the Net-Centric Data Strategy, commercial partnerships and high assurance products to improve the ability to establish trustworthiness of data.

4.1.3. Implement strategies to improve ability to obtain information at mission tempo such as improving the Department's capability to rapidly establish secure information exchange environments with external partners (e.g., allies, coalition forces, federal, state, local, tribal, NGO and commercial), and transition from physical to net-centric electronic keying.

4.2. Protected identity information across the spectrum of military operations and DoD business functions.

4.2.1. Establish DoD policy, guidance and governance for the ownership and utilization of personal identity information while ensuring the security and privacy of personal data.

4.2.2. Leverage the evolution and convergence of robust capabilities associated with biometrics, smart card, Public Key Infrastructure (PKI) and other next generation identity-based technologies to provide attribute-based identification and authentication.

4.2.3. Establish federated identity management systems and processes to manage users' (people, systems and services) identities, credentials and access rights.

4.2.4. Establish federation agreements for identity and access management with external organizations including other U.S. Government agencies and the private sector.

4.3. IA portfolio of capabilities supports the IA needs of the net-centric vision.

4.3.1. Promulgate enterprise capabilities such as de-militarized zones and host based security systems to prevent unauthorized access to networks at enclave boundaries or hosts.

4.3.2. Expand capabilities and implement Federal standards (e.g., data at rest (DAR) protection tools and Homeland Security Presidential Directive 12) to prevent unauthorized access to data at rest or in transit for both austere and tactical environments.

4.3.3. Deploy automated monitoring, detection and forensic tools, and forge external (e.g., federal and international) partnerships to enhance situational awareness and diagnosis of suspicious activity as an attack / event.

4.3.4. Establish automated enterprise capabilities to enable fast and effective execution of required configuration, policy, privilege and network resources adjustments in response to attack / events.

4.3.5. Establish a robust network defense capability by integrating the IA C2 architecture into the overall NetOps construct and employing certified and accredited computer network defense service providers that can respond quickly and effectively to defend the DoD from actual or anticipated malicious cyber attacks.

4.4. Enhanced mission assurance increases DoD resilience, survivability and reconstitution capabilities in the face of cyberspace and physical threats.

4.4.1. Create a partnership with the DIB through clear policy, consistent oversight and streamlined processes to secure U.S. Government sensitive information.

4.4.2. Conduct joint exercises to help identify DoD critical infrastructures that if denied, degraded or untrustworthy would degrade warfighter effectiveness.

4.4.3. Improve IA architectures by redesigning DoD networks for resiliency and diversity to operate through and recover from sophisticated attack.

4.4.4. Develop and implement a multi-pronged, comprehensive and long-term strategy for influencing the evolution of the Internet ensuring DoD equities are addressed.

4.5. Foundational IA processes are streamlined and unified across the DoD and IC enterprises.

4.5.1. Implement a multi-tier strategy to ensure policy alignment to net-centric IA priorities, improve IA policy compliance and bolster component accountability.

4.5.2. Develop new or refine existing methods, such as certification and accreditation and system assurance, to expedite delivery of capabilities and insertion of new technologies without compromising the integrity of the DoD.

4.5.3. Coordinate with both traditional (e.g., research and development) and non-traditional sources (e.g., Defense Venture Catalyst Initiative) to identify and incorporate emerging IA technologies and standards into new capabilities from their inception.

4.5.4. Implement a workforce improvement program to empower the workforce through IA position identification, personnel qualification tracking, certification, training and outreach to operational leadership.

KEY PERFORMANCE INDICATORS

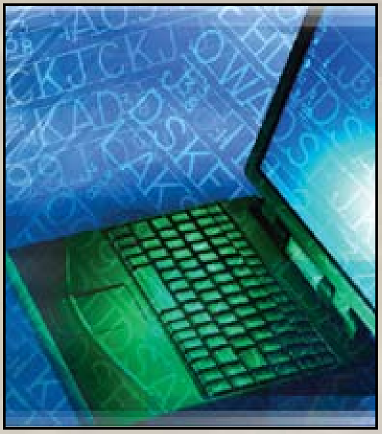
- Percentage of compliant Non-secure Internet Protocol Router / Secure Internet Protocol Router connections to industry, coalition partners and other entities.
- Percentage compliance to JTF-Global Network Operations (GNO) Communications Tasking Order (CTO) 06-02 PKI Implementation Order.
- Percentage compliance to JTF-GNO CTO Data at Rest Encryption order.
- Percentage of mandated enterprise IA capabilities implemented.
- Percentage of IA-related incidents by category.
- Average response time to react and respond to detected attacks.
- Percentage of DoD information systems that are certified and accredited.

Success Story I: Host Based Security Service (HBSS)

The persistent cyber attacks on the DoD infrastructure resulted in DoD needing to implement stronger protection - in depth - for its computing baseline. DoD also needed a capability to implement baseline configuration management and infocon processes. These two needs drove the development of the HBSS capability.

To date, the Department has conducted detailed review and identification of requirements, coordinated a pilot with 22 separate Component elements that extended to 23,000 computers across DoD, awarded the overall contract based on the pilot results, performed security testing and will soon release a corresponding JTF-GNO CTO. HBSS will eventually provide host based security for all DoD host computers - starting with Microsoft Windows platforms.

Success Story II: DAR Encryption Policy



Sensitive government information or personally identifiable information (PII) stored on devices such as laptops, removable media (thumb drives, compact disks, etc.) and Personal Digital Assistants is often unaccounted for and unprotected, and can pose a problem if these devices are compromised. As a direct result of the Afghan Bazaar incident (thumb drives) and the Department of Veteran Affairs' laptop theft and loss of data, the DoD CIO-Command, Control, Communications and Computers Principals formed the Data At Rest Tiger Team (DARTT) in August 2006 to come up with a solution to protect mobile data from compromise. The DARTT was also tasked to implement Office of Management and Budget (OMB) and Office of the Secretary of Defense (OSD) policies concerning protection of PII data and to coordinate various MILDEP's DAR encryption initiatives into one enterprise solution (in other words to stop the MILDEPs from developing "stove-piped" DAR solutions).

Through OSD's leadership of DARTT (eventually comprising 20 DoD components, 18 civilian agencies, NATO) policy was developed, technical solutions were evaluated and standardized, an acquisition vehicle was established and compliance will occur via JTF-GNO CTO (Warning Order 07-047 came out October 2007). The DAR efforts have strengthened security and improved DoD's efforts to safeguard sensitive and personal information across the board.

Success Story III: ***DoD Common Access Card (CAC) PKI Implementation***

In order to make remote exploits of Department computers more difficult by ensuring that only authorized users gain access, the DoD distributed PKI-enabled CACs requiring that every eligible user of its networks and computer systems possess a CAC with multiple PKI credentials (identity, signing and encryption) plus know a personal identification number (PIN) to unlock the PKI credentials. Requiring two factors of authentication – "something you know" such as a PIN and "something you have" such as a PKI-enabled CAC – is called two-factor authentication. Two-factor authentication is a proven method for decreasing intrusions and other types of security breaches by ensuring that stolen user names and passwords are insufficient to gain access to networks. As of March 2007, DoD issued more than 12.5 million CACs and 30 million PKI credentials while the military services deployed CAC readers and the associated middleware which resulted in 92% of logons to unclassified computers in the Department being done using this method. The latest DISA estimates hold that successful intrusions have also declined 46 percent in the past year due to the JTF-GNO CTO 06-02 requiring that all logons to unclassified DoD computers be done via the PKI credential on a CAC.

DoD successes with this initiative led OMB to issue Homeland Security Presidential Directive 12 (HSPD-12), requiring all federal agencies to implement two-factor authentication. Large-scale CAC procurement by DoD and emerging procurements by other federal agencies under HSPD-12 has already reduced the cost of deployment from over $100 to less than $50 per card.

5 RETURN ON INVESTMENT

MAXIMIZE THE CONTRIBUTION OF IT INVESTMENTS TO NATIONAL SECURITY AND DEFENSE OUTCOMES.«««««««««««««««

DESCRIPTION

Achieving the goals of the DoD requires a fundamental change in the way IT is managed in the Department. Historically, IT resources have been managed and acquired as stand-alone systems rather than as integral parts of the Department's core processes. This has had the effect of allowing duplicative investment in systems or platforms that deliver the same or similar capabilities, limiting the ability to share information. Portfolio management is a disciplined approach that provides a framework to assist senior managers in achieving their goal of providing support to the DoD missions. Institutionalizing any initiative is an evolutionary process; it begins with awareness of the initiative, moves to understanding it, evolves to its adoption and implementation, and with commitment and sustained execution eventually the initiative becomes practice that routinely interfaces with other processes in the organization. Portfolio management is following this path.

A sound foundation has been established increasing awareness, understanding and adoption of portfolio management for IT investments. It includes the following guidance:

- Title 40, *Chapter 113*
- OMB Circular A-130, *Management of Federal Information Resources*
- DoD Instruction 8115.02, *Information Technology Portfolio Management Implementation*

The foundation will be further strengthened as the Department rolls out portfolio management more broadly for all investments. The challenge now is to build upon this foundation, and effectively execute the principles and processes espoused in the above guidance. To best leverage portfolio management and capability-based acquisition for IT investments, the DoD is developing an Enterprise Architecture (EA) using a federated approach. The federated EA content makes a vital contribution to the Department's major decision processes by providing a means of tracing required capabilities to investments. Recognizing the vital contribution of the EAs to mission performance, Congress has codified in public law the requirement to develop, maintain and implement EA. Consequently, DoD is incorporating EA into its portfolio management policies.

OBJECTIVES

5.1. All IT investments are aligned with DoD's overall outcome goals and priorities, and warfighter requirements.

5.1.1. Ensure that the DoD's portfolio management processes have the capability to analyze, select, control and evaluate investment proposals (i.e., develop portfolio IT investment plans).

5.1.2. Align IT investments to the DoD Capability Portfolios as they develop.

5.1.3. Establish an IT Asset Management process to track and manage DoD's IT hardware and software inventory.

5.2. Processes systematically maximize the value of IT investments, and assess and manage the risks of IT acquisitions.

5.2.1. Establish and document repeatable IT investment governance processes.

5.2.2. Document and use mechanisms for risk identification, evaluation, management and mitigation.

5.2.3. Establish the federated enterprise architecture as a mechanism for identifying and eliminating duplication of capabilities across each portfolio.

5.2.4. Expand use of the DoD Enterprise Software Initiative (ESI) to lower total ownership cost of IT systems and services.

5.2.5. Align DoD funding for IM / IT resources that support business, warfighter and (people, systems and services) identities, credentials and access rights, intelligence missions and develop funding strategies that are based on integrated IM / IT capability requirements and architectures.

5.3. The IT investment environment is performance- and results-based.

5.3.1. Expose authoritative data to support portfolio-based investment decisions.

5.3.2. Conduct oversight management reviews to gauge maturity of the Department's portfolio management processes.

5.3.3. Conduct post-implementation review of IT, including National Security Systems (NSS), as an integral part of assessing portfolio outcomes.

5.4. A federated DoD EA facilitates management and planning of IT investments to achieve improved mission performance.

5.4.1. Develop DoD Architecture Framework v2.0 to support the Department's net-centric strategies and satisfy the information requirements of major decision processes.

5.4.2. Establish information models, data exchange standards and enterprise taxonomies that enable discovery and sharing of architectures across the Department.

5.4.3. Align the DoD EA Reference Model taxonomies with the federal business, services, performance, data and technical taxonomies.

5.4.4. Develop and maintain a federated EA, which is consistent with the Net-Centric Data Strategy and the Net-Centric Services Strategy, to support IT investment decisions.

KEY PERFORMANCE INDICATORS

- Percentage of IT investments in DITPR aligned to DoD mission capabilities.
- Percentage of portfolios that include IT investment plans.
- Amount of cost avoidance through use of ESI.
- Governance processes in place to manage IT investments as portfolios.
- Activities (e.g., courses, communities of practice, on the job training) executed to educate and train personnel on portfolio management principles, practices and benefits.
- Percentage of IT and NSS acquisition programs performing post-implementation reviews.
- Improvement in Exhibit 300 scores for the DoD EA.
- Percentage of annual increase in the number of architectures registered in the DoD Architecture Registry System.

Success Story I: DoD Business Architecture

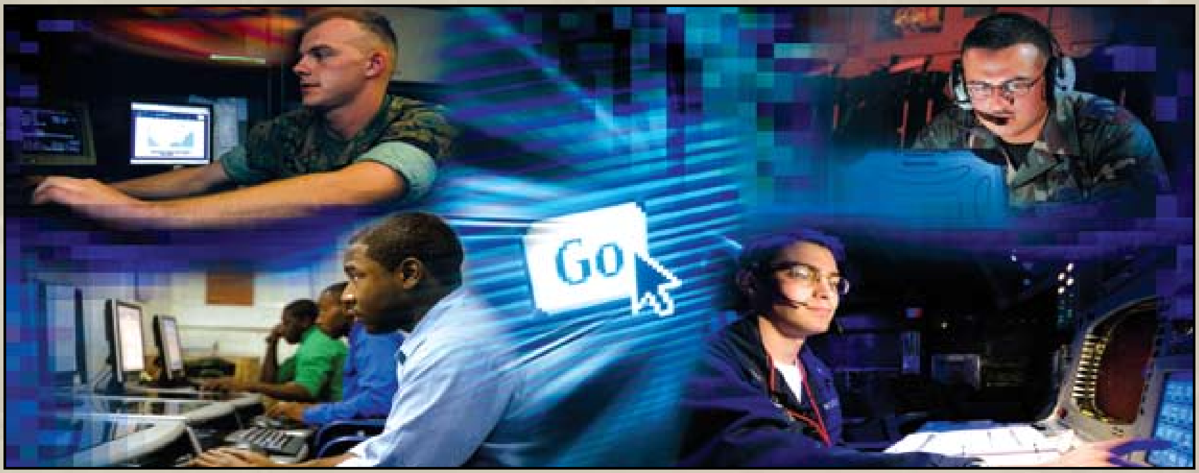
DoD's business transformation effort has made significant progress in the implementation of portfolio management policy through alignment with the Department's overall vision, mission, goals, priorities and outcomes and development of an enterprise architecture and transition strategy.

Specifically, DoD has developed a Business Enterprise Architecture (BEA) that provides the overarching layer of common business services required for interoperability.

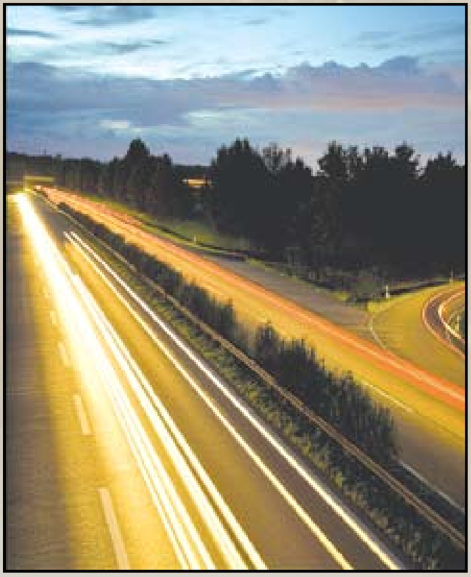
By leveraging the BEA's already defined and vetted architecture artifacts, programs can save both time and cost. As a case in point, the BMA's Defense Agencies Initiative (DAI) demonstrated the utility of the BEA to reduce development time and cost by using the BEA as the foundation for common business processes and data standards. The DAI effort will provide users with access to data shared by the 28 participating agencies.

Success Story II: DoD Enterprise Software Initiative

The DoD ESI partners with strategic commercial information technology vendors to fulfill enterprise-wide DoD IT needs by using Enterprise Software Agreements (ESA) that offer advantageous prices, terms and conditions. Over 90 ESAs are now in place, and more than $2.7B in cost avoidance has been realized through purchases made by DoD ESI customers. The federal General Services Administration (GSA) SmartBUY Program is a direct outgrowth of early DoD ESI successes. DoD ESI maintains close working relations with OMB and GSA to implement and actively support SmartBUY within DoD. Of 23 GSA SmartBUY agreements now in place, 21 are "co-branded" with the DoD ESI. Consequently, DoD Software Product Managers negotiate and administer the agreements for the benefit of all federal and in some cases, state and local government customers.



Success Story III: ***United States Transportation Command (USTRANSCOM) Distribution Portfolio Management (DPFM)***



Commander USTRANSCOM, as the Distribution Portfolio Manager uses DPfM as a method to identify capability gaps and unnecessary overlaps in IT systems that support distribution to the warfighter. DPfM provides the Distribution Process Owner with effective and efficient materiel and non-materiel options to support distribution solutions that enhance strategic support to worldwide customers. DPfM provides the Distribution Portfolio Manager with justification for IT investment decisions in support of the Department's missions. Of 270 systems deemed to be of distribution interest by OSD, over 200 have been analyzed for consideration as DPfM candidates. In the last year, 71 of these systems were eliminated, consolidated or targeted for future migration, significantly reducing duplication and costs within the Distribution Portfolio.

6 IT WORKFORCE DEVELOPMENT

Maintain an Agile IT Workforce with the Skills to Build, Extend, Exploit and Defend a Net-Centric DoD.«««««««««««««««««««

DESCRIPTION

A corps of highly skilled, trained and experienced IT professionals is critical to ensuring information dominance across the range of military operations. The IT workforce architects, designs and operates the infrastructure supporting the collection, processing and dissemination of an uninterrupted flow of information while protecting the infrastructure and information against modern day cyber attacks. DoD has over 163,000 IT professionals serving around the world, meeting its IT needs. Management of the DoD IT community is a dynamic process, given the increasing importance of IT to all missions and the rate of change in IT. Workforce challenges include the evolution of career fields to meet new demands; attracting, training and retaining innovative personnel; and managing the intertwined performance of highly skilled military, DoD civilian and contractor forces.

The DoD IT human capital objectives provide the direction for the Department to identify and capture the skill sets of the IT / IM / IA workforce; to leverage workforce information for better human resources management; to promote continuous skill development and lifelong learning; and to recruit, reward and retain a quality, diverse and multi-generational workforce. DoD must be positioned with the right mix of high performing military and civilian IT personnel with the skills necessary to meet both current and future mission requirements in support of the DoD.

OBJECTIVES

6.1. Recruitment and retention of a dynamic, diverse and highly skilled IT workforce through flexible workforce life-cycle management.

6.1.1. Implement recruitment activities that support multi-dimensional hiring requirements (e.g. education, experience, qualifications and diversity).

6.1.2. Implement retention initiatives (e.g. work-life quality, scholarships and bonuses) to maintain DoD as an IT employer of choice for all generations.

6.2. Opportunities exist for competency-focused training and education.

6.2.1. Provide targeted professional development opportunities to meet individual career and organizational mission requirements.

6.2.2. Implement IT / IM / IA workforce training, education and certification initiatives to provide continuous professional development to the workforce.

6.3. Comprehensive workforce identification, assessment and reporting capabilities support and improve strategic human capital management.

6.3.1. Populate DoD-wide personnel systems and management tools with required IT / IM / IA occupational skill identifiers.

6.3.2. Conduct workforce assessments to validate requirements.

6.4. Attract and retain innovative employees.

6.4.1. Encourage employees to release their creativity by providing an environment that encourages and rewards innovation.

KEY PERFORMANCE INDICATORS

- Demographic distribution of the IT workforce (e.g., diversity, geographic location, grade-levels and skills).
- Retention or turnover rates for IT / IM / IA professionals.
- Percentage of IA workforce positions filled with certified personnel.

Success Story I: ***DoD-Wide Information Assurance Scholarship Program (IASP)***

The IASP was instituted in 2001 and has been continually enhanced to meet DoD's requirements for flexible, multifaceted recruiting and retention tools for its IT / IM / IA workforce. Since its inception, the IASP has awarded 182 recruitment and 95 retention scholarships to undergraduate and graduate program applicants from prestigious colleges and universities designated as centers of academic excellence in information assurance education (CAE / IAEs). The IASP recruitment program allows Components to identify their IT / IM / IA skill requirements and personally select students from among the 86 CAE / IAEs located throughout the United States, to serve as future defense employees in support of diverse mission requirements. Under the IASP retention program, current DoD employees may be nominated to complete a master's or PhD at the Air Force Institute of Technology or Naval Postgraduate School, or through the Information Resources Management College and its partner university program. This program ensures DoD maintains a cadre of experienced professionals with the critical IT / IM / IA skill sets required to support the DoD enterprise.

Success Story II: DISA Career Intern Program

DISA has an aggressive entry level hiring program designed to create more balanced personnel demographics and meet its long range workforce goals, particularly in the engineering / scientist fields. They factor a 2 percent target for new interns into their annual workforce plans and have created an extensive, 3-year training and development plan for the participants in their entry-level Career Intern Program. Additionally, DISA extensively uses their Student Career Experience Program to offer baccalaureate students the opportunity to gain valuable work experience in their chosen, post-academic career field, as well as potential conversion to DISA's intern program. The retention rate for DISA interns is over 60 percent, a significant achievement.

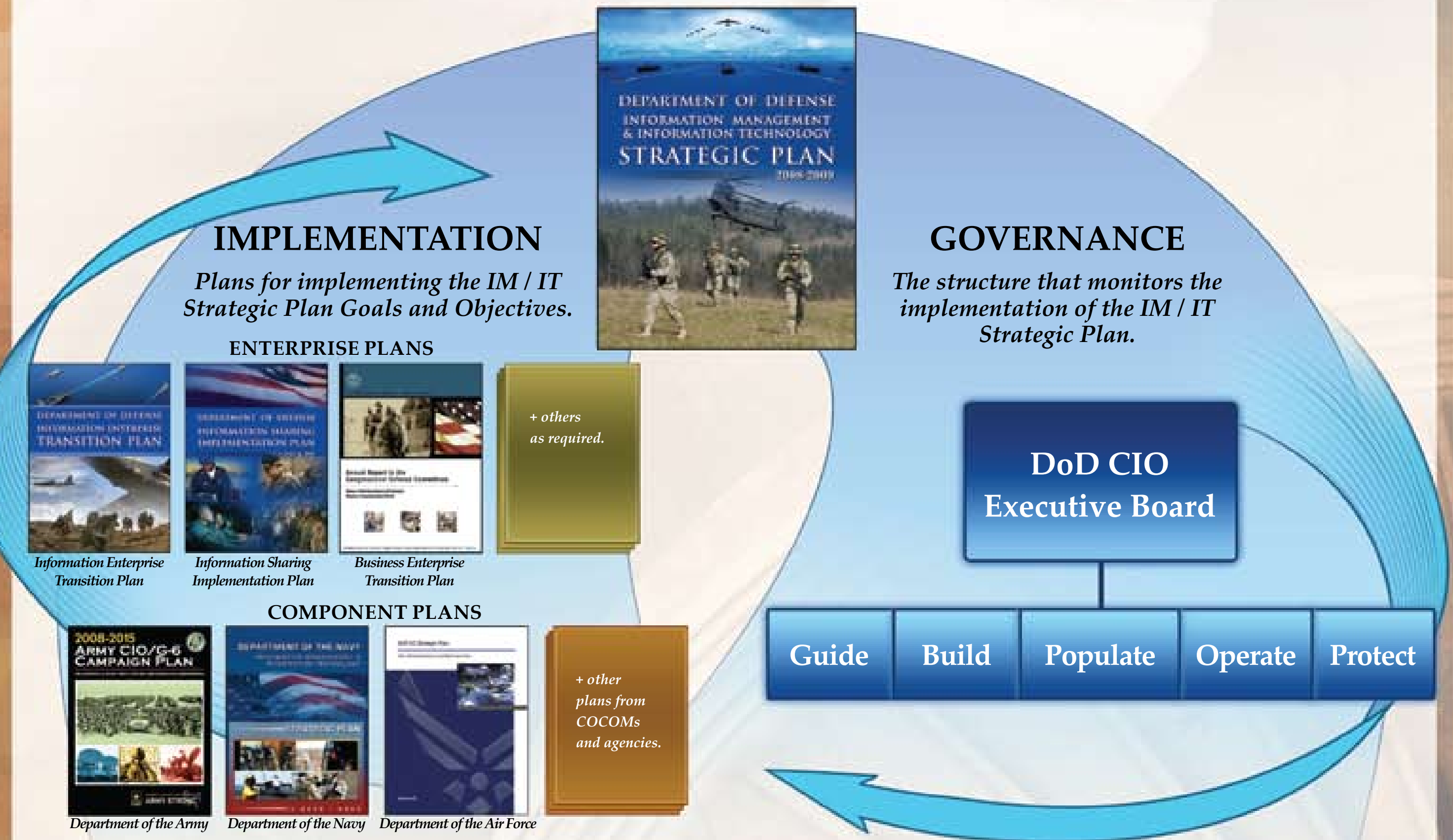
Success Story III: Defense Contract Management Agency's (DCMA) Teleworking

The DCMA CIO Office has been at the vanguard both within its own agency, and within DoD at large, in implementing telework capabilities for its workforce. Currently more than 400 IT personnel, largely at DCMA headquarters, are engaged in teleworking. Participation includes both civilian and contractor personnel, with individual participation ranging from ad hoc to full-time program usage. This valuable work-life flexibility has enhanced both workforce productivity and retention within the CIO organization.

IMPLEMENTATION & GOVERNANCE

Net-centric information sharing increases efficiency and effectiveness across defense operations, intelligence functions, and business processes by providing users access to the latest, most relevant and accurate information. The DoD has developed this DoD IM / IT Strategic Plan to guide that effort. Implementation activities and governance across the Department, coordinated with this plan, will help ensure mission success and further the DoD mission to "achieve an information advantage for our people and mission partners."

The DoD CIO will lead the implementation of this plan through both formal governance and by leveraging collaborative relationships with stakeholders across the Department. The governance structure, capped by the DoD CIO Executive Board, provides forums to monitor progress in achieving the plan and allows stakeholders to discuss and resolve the many issues related to guiding, building, populating, operating, and protecting the resources that comprise the DoD Information Enterprise. IM / IT governance is reinforced by the many portfolio management processes at both the Enterprise and Component levels of the Department.



IMPLEMENTATION

Plans for implementing the IM / IT Strategic Plan Goals and Objectives.

ENTERPRISE PLANS

Information Enterprise Transition Plan

Information Sharing Implementation Plan

Business Enterprise Transition Plan

+ others as required.

COMPONENT PLANS

Department of the Army

Department of the Navy

Department of the Air Force

+ other plans from COCOMs and agencies.

GOVERNANCE

The structure that monitors the implementation of the IM / IT Strategic Plan.

DoD CIO Executive Board

Guide | Build | Populate | Operate | Protect

DEPARTMENT OF DEFENSE
INFORMATION MANAGEMENT & INFORMATION TECHNOLOGY
STRATEGIC PLAN
2008-2009
DEPARTMENT OF DEFENSE INFORMATION ENTERPRISE TRANSITION PLAN
DEPARTMENT OF DEFENSE INFORMATION SHARING IMPLEMENTATION PLAN
2008-2015
ARMY CIO/G-6
CAMPAIGN PLAN

The intra-Departmental collaboration generated through the DoD IM / IT governance structure, and the Department's other decision-making processes, will lead to numerous implementation activities across the Department that detail how DoD will achieve the goals of this plan. At the Enterprise level, the Department is developing the DoD Information Enterprise Transition Plan (DoD IETP) as a direct follow-on to this plan and the DoD Information Enterprise Architecture (DoD IEA) 1.0. The DoD IETP provides a sequencing plan that fosters alignment of net-centric information sharing efforts by identifying and aligning the development of enabling policies, programs, and initiatives. The initial version of the DoD IETP will establish a baseline for measuring the Department's performance in achieving the goals and objectives of the DoD IM / IT Strategic Plan and the priorities of the DoD IEA 1.0. The DoD IETP will also show how organizations are leveraging net-centric information sharing capabilities to improve the effectiveness and efficiency of processes across the Department. Additionally, the DoD Information Sharing Implementation Plan (ISIP) will provide additional details on how the Department is achieving Goal 2 of the IM / IT Strategic Plan. Strategic Implementation Plans developed by multiple DoD Components and portfolios will also be aligned to the goals of the IM / IT Strategic Plan.

Achieving the DoD net-centric information sharing vision requires participation of the entire DoD community in planning, implementation, and governance activities tied to the goals and objectives identified in this IM / IT Strategic Plan. The DoD IM / IT Strategic Plan will thereby help stakeholders across DoD and its mission partners align their information sharing efforts to ensure mission success.

DoD INFORMATION ENTERPRISE ARCHITECTURE VERSION 1.0

The DoD Information Enterprise Architecture (IEA) provides a common foundation to support accelerated DoD transformation to net-centric operations and establishes priorities to address critical barriers to its realization. The DoD comprises the information, information resources, assets, and processes required to achieve an information advantage and share information across the Department and with mission partners. IEA describes the integrated DoD and the rules for the information assets and resources that enable it.

IEA 1.0 unifies the concepts embedded in the many DoD net-centric strategies into a common vision, providing relevance and context to existing policy. IEA 1.0 highlights the key principles, rules, constraints and best practices drawn from collective policy to which applicable DoD programs, regardless of Component or portfolio, must adhere in order to enable agile, collaborative net-centric operations. In today's information environment, the IEA rules clearly apply within the persistently-connected Internet Protocol (IP) boundaries of the Global Information Grid (GIG). Outside of these boundaries, the principles still should be considered, but the rules of the IEA must yield to the state of technology, and the needs and imperatives of the Department's missions. Core principles and rules (summarized in Appendix A) are organized around five key priorities where increased attention and investment will bring the most dramatic and immediate progress towards realizing net-centric goals.

The principles and rules outlined in IEA 1.0 are few, but powerful. When institutionally embedded in decision processes across DoD, and applied appropriately to IT investments, they will drive dramatic change. Our biggest challenge ahead is not deciding what will be in the next IEA release, but rather how to institutionalize the principles and rules established in this one. By reflecting existing IM / IT guidance, policy, and frameworks into a more cohesive vision and informing decision makers across the Department, IEA 1.0 will play a key role in transforming the DoD to net-centric operations.

The DoD CIO / ASD (NII) Contact List can be found at:
www.dod.mil/cio-nii/org/index.shtml

DoD CHIEF INFORMATION OFFICER
6000 Defense Pentagon
Room 3E172
Washington, DC 20301-6000
www.dod.mil/cio-nii