Department of Defense Information Enterprise Strategic Plan 2010-2012

FOREWORD

"Intelligence and information sharing have always been a vital component of national security. Reliable information and analysis, quickly available, is an enduring challenge… The goal is to break down barriers and transform industrial-era organizational structures into an information and knowledge-based enterprise. These concepts… will require investments in people as much as in technology to realize the full potential of these initiatives." -National Defense Strategy, June 2008

The National Defense Strategy of June 2008 highlighted the importance of information sharing to national security. The strategy noted that providing secure, assured, and reliable information requires not only technological changes, but also changes that break down cultural barriers impeding progress. With this in mind, the aim of the Assistant Secretary of Defense (Networks and Information Integration)/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO) is to achieve an information advantage for our people and mission partners (including multinational partners) by leveraging net-centric information sharing. The ASD(NII)/DoD CIO's vision is that: *We are about mission success.* The mission accompanying this vision is based on the understanding that: *Information is one of our nation's greatest sources of power. Our first and greatest goal, therefore, is to bring that power to the achievement of mission success in all operations of the Department.*

Delivering this vision means treating information as a strategic asset; establishing a robust, reliable, rapidly scalable and interoperable infrastructure; and achieving synchronized and responsive operation of the DoD Information Enterprise (IE); all while protecting and defending information and information systems against adverse events. To realize this vision, the Department must optimize Information Technology (IT) investments and more rapidly deploy IT capabilities, drawing on a highly skilled, innovative workforce shaped to meet these emerging and expanding mission requirements. While each of these goals is important in its own right, all six goals in this plan are co-dependent and therefore must work together to attain the vision.

This DoD Information Enterprise Strategic Plan (which supersedes the 2008-2009 DoD Information Management (IM)/IT Strategic Plan) establishes goals, objectives and strategies that reinforce the goals and objectives of related portfolio strategic plans, including Command and Control (C2) and Net-Centric Capabilities. Developing this plan in itself embodies a key aspect of DoD's vision—leveraging the power of mass collaboration. Specifically, this plan was developed using Intellipedia, the Intelligence Community (IC)-hosted social networking wiki toolset. Success stories in this plan represent a small set of the many initiatives leading to the achievement of each goal. The implementation of the DoD IE Strategic Plan's goals will be managed in a roadmap using the same wiki functionality. Consequently, DoD leaders will be better able to assess progress, discover gaps and overlaps, locate information for decision support, and contribute information regarding relevant policies, programs, and initiatives.

This wiki approach enables a dynamic, continuous strategic planning process encouraging unprecedented levels of participation in crafting the DoD IE Strategic Plan's goals, objectives, and strategy elements. This approach enabled a core team encompassing CIO representatives from all Military Departments (MILDEPs), the Defense Information Systems Agency (DISA), and the Joint Staff, as well as elements from across the ASD(NII)/DoD CIO staff to develop the plan collaboratively.

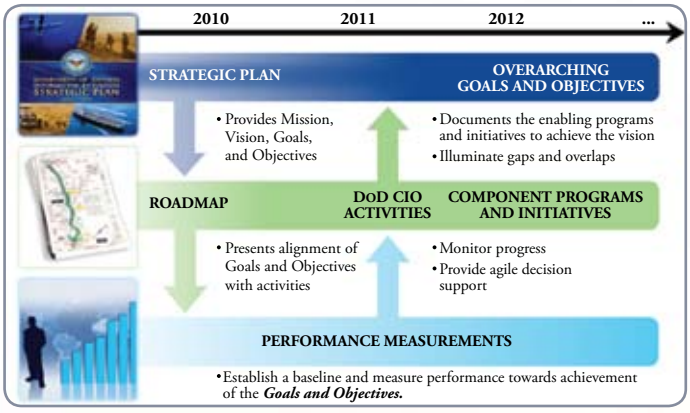
The explosion of Intellipedia usage and other information sharing efforts vividly demonstrate how DoD is beginning to apply information sharing capabilities in innovative and highly effective ways. This plan builds on those successes and adds momentum to our efforts to achieve an information advantage for our people and mission partners.

ACHIEVING THE DoD INFORMATION ENTERPRISE

The DoD Information Enterprise, which enables a new, net-centric[1] way of working, is constructed from the information itself, as well as a set of standards, services and procedures that enable information to be widely available to authorized users. The delivered set of services and tools will provide information and capabilities that enable end-user communities to more effectively and efficiently support mission operations. Finally, the DoD Information Enterprise includes the networks over which information travels and the security protocols that protect it.

The DoD IE Strategic Plan forms the basis for a broad approach to achieving the DoD Information Enterprise, which is collectively termed the DoD IE Strategic Plan & Roadmap (IE SP&R). Together, the Strategic Plan and Roadmap meet the requirements of the Government Performance Results Act, as described in Office of Management and Budget (OMB) Circular A-11. Over time, the DoD IE SP&R will deliver the DoD Information Enterprise envisioned by the National Defense Strategy, the National Military Strategy, the Quadrennial Defense Review, and the Department's Global Information Grid (GIG) 2.0 Concept of Operations (CONOPS) and Implementation Plan. Additional guidance is provided by the principles, rules, constraints, and best practices contained in DoD Information Enterprise Architecture v1.1 (DoD IEA).

The DoD IE SP&R establishes goals and associated objectives that form the basis for a plan to guide the transformation of DoD from a stove-piped information approach to achieving the Department's net-centric information sharing vision. The DoD IE SP&R fosters alignment of the Department's net-centric information sharing efforts, particularly those specified in the GIG 2.0 Implementation Plan, by identifying, relating and measuring the development and implementation of specific net-centric information sharing policies, programs, and initiatives.



The Roadmap portion of the DoD IE SP&R establishes a baseline for measuring the Department's performance in achieving the goals and objectives of the DoD IE Strategic Plan. The DoD IE SP&R also highlights how organizations are leveraging net-centric information sharing capabilities to improve the effectiveness and efficiency of processes across the Department. Strategic planning is one of five levers (policy, planning, governance, performance measurement, and portfolio management) used by the ASD(NII)/DoD CIO to understand and influence what DoD is doing to improve information sharing. The wiki approach provides an opportunity to gain synergy across these levers through the power of collaboration.

DEFINITION OF THE DoD INFORMATION ENTERPRISE

The DoD information resources, assets, and processes required to achieve an information advantage and share information across DoD and with mission partners. It includes: **(a)** the information itself, and the Department's management over the information life cycle; **(b)** the processes, including risk management, associated with managing information to accomplish the DoD mission and functions; **(c)** activities related to designing, building, populating, acquiring, managing, operating, protecting and defending the information enterprise; and **(d)** related information resources such as personnel, funds, equipment, and information technology, including national security systems.

[1] The definition of "net-centric" and other key terms in the DoD IE Strategic Plan can be found in the associated Roadmap's Glossary on Intellipedia.

CULTURE CHANGE

Culture change—taking new perspectives that lead to changed behavior on sharing information—is critical to our ability to achieve the vision laid out in this strategic plan. The principles of need-to-share, breaking down silos, and developing reusable, accessible services must become hallmarks of how we approach information. Addressing this culture change permeates this plan, influencing all goals and objectives and how we measure progress.

To improve net-centric information sharing, DoD must increase trust in the quality and availability of shared information and services, particularly through greater assurance that others will maintain the integrity and security of shared information. Similarly, to achieve interoperable infrastructure and synchronized operations, DoD must persuasively demonstrate that these strategies will improve computing and communication, and especially provide the capacity to meet surge demand. Implementing an operationally effective identity and information assurance model will require buy-in to the perspective that more flexible approaches to risk management are preferable to organizationally-stovepiped network enclaves that avoid risk by limiting interoperability and accessibility. The Department must also gain wider acceptance of rapid acquisition methods for fielding new IT capabilities that demonstrably improve operational performance. Supporting all this change requires that DoD consider innovative approaches in its Analysis of Alternatives, and develop the workforce correspondingly.

To successfully change the culture, DoD must embrace the new mindsets described above and apply new thinking to break down information sharing barriers and more rapidly field critical information sharing solutions. The following story about two online professional development communities, CompanyCommand.mil and PlatoonLeader.mil, described by Dan Baum in a January 2005 *New Yorker* article, shows how two grassroots efforts demonstrated tremendous value to young officers, and as a result were institutionalized by the U.S. Army.

The story below is drawn from that *New Yorker* article and a related article by Dr. Nancy M. Dixon in NASA's *ASK Magazine*:

> *CompanyCommand.mil and PlatoonLeader.mil are two community forums launched by two young Army officers in the late 1990's as unofficial public websites open to registered users. The founders saw an opportunity to leverage the power of the Internet to create a virtual network for sharing and growing professional knowledge.*
>
> *The virtual communities provided valuable information to other young officers who were on the ground in the Iraq and Afghanistan wars, facing leadership situations they had not experienced before. Even at the most remote bases in Iraq, many captains would find at least ten or fifteen minutes every day to check the site. They'd post tricks they had learned or ask questions that in some cases set off months of responses in the form of lively discussion threads. For example, a discussion*

on convoy training offered contradictory views on whether to lay sandbags on the floors of vehicles (they provide potential protection from mines, but wear out Humvees), admonitions to look upward as well as to the sides (guerrillas may shoot from rooftops and overpasses), and suggestions for replacing vehicles' canvas doors with 8-mm. steel (to stop AK-47 and most frag). By 2004, CompanyCommand's membership reached ten thousand, or more than a third of all captains in the Army; those members went to the site sixty-seven thousand times and looked at more than a million pages.

Recognizing the value that these sites were providing, Army senior leadership decided to officially recognize the sites and host them on Army-operated servers. Even after being brought behind the Army firewall, CompanyCommand and PlatoonLeader have retained their grassroots spirit and governance, remaining a community of young officers exchanging knowledge based on the daily struggles of fellow frontline professionals. These online communities have been heralded by the Army as its premier professional forum.[2]

The story above illustrates how shifting the culture requires accepting the premise that rapidly sharing knowledge of people and organizations at all levels provides a vital augmentation to traditional, rigid, centrally-approved knowledge sharing approaches. Additionally, the adoption and widespread application of mass collaboration among organizations and people, via social networking tools, helps those organizations and people work together more seamlessly to create more effective solutions than those developed under *go-it-alone* approaches. Such collaboration enables a broader, more geographically diverse group of people to participate in those processes that will benefit from wider involvement, such as planning, coordination, and analytical activities—to name only a few.

The success of DoD's information sharing environment is predicated upon achieving ***secure information sharing*** within the context of a highly contested information environment. Therefore, a critical aspect of the culture change for DoD is to embrace the notion that in order to maximize the potential of the information sharing enterprise, proper solutions (like cross domain solutions) must enable both sharing information widely and stringent protection mechanisms. Solutions cannot optimize one at the expense of the other. Consequently, the Department aims to change the current information sharing culture to one that understands, embraces and continuously seeks to improve the secure net-centric information enterprise and its enabling processes. These changes should produce more efficient and effective national security processes and aid in increasing the public's trust.

[2] Dan Baum, "Battle Lessons," *The New Yorker,* January 17, 2005; Dr. Nancy M. Dixon, "CompanyCommand: A Professional Community That Works," *ASK Magazine,* Issue 27, Summer 2007

DoD INFORMATION GO

1 INFORMATION AS A STRATEGIC ASSET

A robust DoD Information Enterprise provides the Department and mission partners access to discoverable, authoritative, relevant, trusted, and actionable information and services to enable effective and agile decisions for mission success.

2 INTEROPERABLE INFRASTRUCTURE

A more robust, reliable, rapidly scalable and interoperable infrastructure provides connectivity and computing capabilities that allow all DoD users and mission partners to access, share, and act on the information needed to accomplish their missions.

3 SYNCHRONIZED & RESPONSIVE OPERATIONS

The DoD Information Enterprise infrastructure, critical assets, and capabilities are operated, secured, and defended in a synchronized manner by all DoD Components to support commanders in achieving mission success.

ENTERPRISE GOALS

4 IDENTITY & INFORMATION ASSURANCE

A unified and resilient DoD Information Enterprise where only authorized users (including mission partners) have ready access to their information; missions continue under any cybersecurity situation; and associated components perform as expected and act effectively in their own defense.

5 OPTIMIZED INVESTMENTS

An integrated DoD Information Enterprise investment and portfolio management capability that maximizes the contribution of information-related investments to national security and defense outcomes.

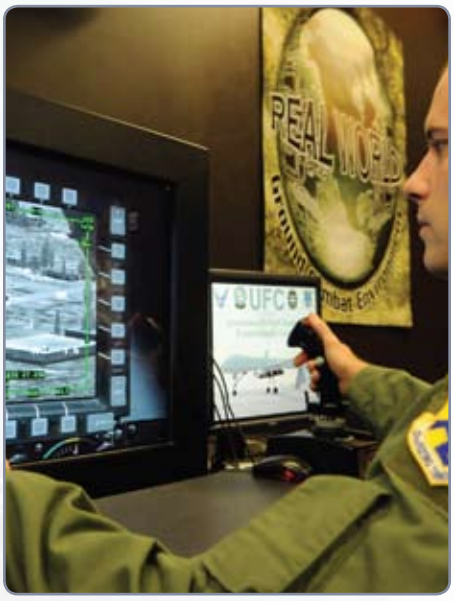
6 AGILE IM/IT/IA WORKFORCE

An agile IM/IT/IA workforce able to dynamically operate, defend, and advance the DoD Information Enterprise.

1 INFORMATION AS A STRATEGIC ASSET

A robust DoD Information Enterprise provides the Department and mission partners access to discoverable, authoritative, relevant, trusted, and actionable information and services to enable effective and agile decisions for mission success.

Information is an asset—a source of power and a force multiplier. DoD and mission partners will obtain an information advantage when timely, secure and trusted information is available to all decision makers. We are moving rapidly to achieve a service-oriented information enterprise where all data assets, services and information sharing solutions must be visible, accessible, understandable and trusted by all authorized users, except where limited by law, policy or security classifications. Independent data efforts across Combatant Commands (COCOMs), MILDEPs, Defense Agencies and Field Activities, and with mission partners will be aligned and leveraged to improve data quality, integration, transparency and sharing. Once achieved, warfighters will get the critical information they need to make timely decisions affecting operations.



DoD's transition from Component-centric, non-interoperable capabilities to joint net-enabled capabilities will be accomplished with community-based solutions and technical solutions such as Service Oriented Architectures (SOAs). Using process-based approaches, communities will identify needed services, define necessary data characteristics, and ensure authoritative sources of information are identified, to support effective information sharing and problem solving. In particular, loosely coupled enterprise services will be available for authorized users to discover and use. For greater efficiency, these services will be brought together in shared services centers or "clouds," which are addressed in depth in the Interoperable Infrastructure goal. Cloud computing centers enable data and service transparency, and provide the foundation to run enterprise services securely and consistently across the DoD. These centers are enhanced by cross domain solutions (services) that enable information flow from one domain to another.

Providing an information advantage for DoD people and mission partners rests largely upon the ability of the Department to improve its processes by finding, fielding, and exploiting new technologies. Through community-based pilots and experimentation, DoD will mitigate risk by evaluating how well new technologies support agile information sharing, permit alternative uses, and provide cost-effective solutions in response to dynamic mission environments.

The 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. By collaborating on the standardization of required data and services, DoD and mission partners will improve their interoperability as necessary to achieve their mission goals. Additionally, DoD will establish methods, policies, and procedures that allow authorized interagency mission partners and non-governmental organizations appropriate access to information needed in support of national security missions.

Through the objectives of this goal, DoD together with its mission partners will foster an improved information sharing culture. These improvements will lead to increased availability of mission-essential information. By promoting innovative approaches to sharing and using the information, DoD will achieve an information advantage with shared awareness, interoperable solutions, and greater collaboration across the spectrum of joint and combined operations with mission partners.

OBJECTIVE 1: Current, accessible, secure and reliable information will be available to all authorized users, both known and unanticipated.

Key Performance Indicator: Assessment of improvement in our ability to provide current, relevant, and reliable information via protected, trusted and net-centric data sharing solutions.

Strategy Elements:

- Develop and implement cloud computing techniques, such as the CIO Storefront's "publish from the desktop" paradigm, to enable transparent data access and visibility.
- Establish and implement the framework (e.g., methods, policies, and procedures) to identify and empower authoritative bodies for sharing the most commonly used DoD data concepts and assets.
- Increase the prevalence of metadata tagging in order to make more information discoverable and understandable.
- Enhance data registry usage and effectiveness, to support the visibility and accessibility of tagged data, by improving policies and procedures.
- Improve information sharing with mission partners by participating in federal information sharing initiatives such as those identified in the DoD Information Sharing Implementation Plan.
- Improve information sharing with the public by participating in federal open government and transparency initiatives.

OBJECTIVE 2: A balanced suite of DoD Enterprise Services will be visible, accessible, understandable and trusted, enabling net-centric information sharing via a service-oriented information enterprise.

Key Performance Indicator: Assessment of status of activities to deliver a synchronized suite of DoD Enterprise Services that are visible, accessible, understandable and trusted.

Strategy Elements:

- Guide the development and integration of DoD Enterprise Services that extend across the Information Enterprise to achieve a balanced set of near-, mid-, and long-term mission outcomes, and enable delivery of tangible warfighter and intelligence operator capabilities by implementing a dedicated enterprise services strategic planning process.
- Establish and implement a DoD Enterprise Services Governance Framework to organize, evaluate, and synchronize enterprise services, solutions, and initiatives, and identify resources to enable early implementation across the DoD Information Enterprise.
- Leverage emerging cloud computing techniques for access to Core Enterprise Services (messaging, content delivery, collaboration, people/service discovery, content discovery, metadata discovery, etc.) and to provide scalable, on-demand—and where feasible, cross domain—solutions for critical mission needs.
- Establish and implement a DoD Enterprise Services Security Framework to enable dynamic access control to shared resources and services.
- Enhance service registry usage and effectiveness through improved guidance and governance that leads to better visibility, accessibility and increased reuse of enterprise services.

OBJECTIVE 3: Community-based solutions will be used to identify, specify, coordinate, and deliver net-centric data and services that improve information sharing and collaboration.

Key Performance Indicator: Evaluate the degree to which community-based solutions are being used to provide information sharing capabilities and services.

Strategy Elements:

- Increase the availability and magnitude of collaborative networking user forums, technical assistance, guidance, training tools and artifacts across user communities to support information sharing.
- Increase the use of Internet-based capabilities (Web 2.0) that support collaborative development, fielding, and use of community-based information sharing solutions.

OBJECTIVE 4: Pilots and experimentation will accelerate insertion of new information technology, mitigate risks, and advance shared enterprise services to improve information sharing within DoD and with mission partners.

Key Performance Indicator: Assessment of the degree to which pilots and experimentation transition to sustained capabilities.

Strategy Elements:

- Advocate and sponsor risk mitigating, community-based experiments and pilots to identify, refine, and field promising data and services that support interoperable, joint, multinational, and interagency operations.
- Partner with industry, Federally Funded Research and Development Centers, and academia to identify and generate innovative net-centric data and services solutions for information sharing challenges.
- Increase the availability of information sharing lessons learned from joint experiments, operational concept development, combat operations and other missions.

OBJECTIVE 5: Interoperability, collaboration, and improved information sharing capabilities will be achieved between DoD and mission partners.

Key Performance Indicator: Assessment of improvements in information sharing capabilities between DoD and mission partners.

Strategy Elements:

- Increase interoperability between DoD and mission partners through agreed-upon technical procedures and data standards, which include naming conventions, schemas, interface specifications, and characteristics.
- Improve collaboratively-developed information sharing capabilities, procedures and services between DoD and mission partners, including federal, other public, private and international enterprises.
- Remove regulatory and cultural barriers that impede information sharing and interoperability by adjusting policy, and establishing operating protocols, Memorandums of Understanding, and Memorandums of Agreement necessary for joint, interagency and industry relationships.
- Improve the information sharing culture by providing incentives to DoD activities to share information, as appropriate, with agencies, mission partners, industry, and citizens.

UCORE - FACILITATING INFORMATION SHARING

Information sharing between the DoD and its mission partners has been hindered by the evolution of systems that were not designed to communicate with each other. These legacy systems form data stovepipes joined by point-to-point connections and constrained by proprietary formats that require manual entry (and re-entry) of data, and laborious deciphering and costly mediation. Eliminating these barriers is essential for effective information sharing.

The Universal Core (UCore) was developed to break down barriers to information sharing by using agreed-upon representations for the most commonly shared and universally understood concepts of "who," "what," "when," and "where." Designed to be simple to understand, explain and implement, UCore is a federal information exchange specification that supports the White House's National Strategy for Information Sharing.

UCore V2.0 was released on March 31, 2009. The Department of Justice (DOJ), the Office of the Director of National Intelligence, the Department of Homeland Security (DHS), and DoD collaboratively developed and endorsed it, drawing on several hundred participants from across the federal government and industry over an 18-month period. This collaboration not only ensured that requirements from many stakeholders were considered, but also significantly increased the likelihood of adoption by socializing the latest changes as they were refined. Organizations are using or evaluating UCore for a variety of important national missions including command and control, ballistic missile defense, counterterrorism, maritime domain awareness, combating improvised explosive devices, and suicide prevention.

The Army recently used UCore in their Executive Support System to create an interoperable solution to monitor and track various units' readiness to deploy. The solution combines data from multiple, disparate sources; uses a community vocabulary and common data schema; and maps information into UCore-based messages that can then be translated and displayed by these disparate sources. In just five weeks, five different iterations of unit readiness data were created. The speed and accuracy of the data displays demonstrates that UCore can be used to achieve high levels of interoperability and promotes the sharing of information between anticipated and unanticipated users.

Navy and the U.S. Northern Command (USNORTHCOM) engineers incorporated UCore into commercial off-the-shelf products to create a mobile force tracking capability. In this project, a UCore-based script was created to enable positional data from Blackberrys and Windows mobile devices to be transmitted and displayed on USNORTHCOM's unclassified common operational picture. This was a low cost, simple deployment that has broad applicability to DoD Homeland Defense-related missions. Through DoD's partnership with DHS and DOJ, this capability is also available to state and local entities in support of emergency response and management missions.

DoD and other federal departments and agencies have acknowledged the value of UCore to improve information sharing between known and unanticipated users and save cost/time through reuse and modular design.

ACQUISITION VISIBILITY (AV) SOA

Until recently, DoD generally limited the collection and dissemination of acquisition information to mandatory reports, which were mostly manually compiled and took months to complete. Consequently, the resulting data was frequently no longer current enough to enable the most accurate acquisition milestone decisions.

On February 29, 2008 DoD began managing its Defense acquisition data in a new way by demonstrating that a SOA approach could be used to make acquisition information more broadly available in real time. This initial demonstration presented authoritative values for 61 data elements (including earned value management and unit cost data) from 12 Major Defense Acquisition Programs (MDAPs). A second pilot project further enhanced data availability to 148 data elements (including budget, milestone, Science & Technology, and program administration data) for 103 MDAPs. The overall AV SOA effort has included implementing role-based security, establishing a production capability, bringing additional data elements under governance and enabling access to information on even more programs. A March 2009 memorandum from the Under Secretary of Defense for Acquisition, Technology & Logistics (USD(AT&L)) acknowledged the success of the AV SOA Pilot and directed governance and use of SOA to make acquisition data immediately available to authorized users.

One of the most desirable features of the new AV SOA model is that each request for data generates a unique request from the authoritative source for the data needed. In this concept, called "data as a service," the data request immediately returns the authoritative data along with the pedigree of that data. These results show that commercial information technology tools, when combined with data governance that includes careful regulation of the data definitions and technical standards, permit secure and transparent use of data from disparate sources.

The successful implementation of AV SOA allows Defense acquisition decision makers to accurately assess the status of the Department's portfolio of MDAPs, valued at approximately $1.6T. The AV SOA effort offers a profoundly better approach in which data is simply and transparently available, as soon as it is developed, to anyone throughout the enterprise who has a legitimate need for it.

2 INTEROPERABLE INFRASTRUCTURE

A more robust, reliable, rapidly scalable and interoperable infrastructure provides connectivity and computing capabilities that allow all DoD users and mission partners to access, share, and act on the information needed to accomplish their missions.

Achieving mission success in today's operational environment, which increasingly involves joint, combined, and non-military partners, requires a dynamic and interoperable infrastructure consisting of communications, transport, and computing capabilities. Gaining and maintaining a persistent and dominant information advantage requires robust world-wide connectivity to enable highly effective information sharing across DoD and with its mission partners. A reliable and rapidly scalable information infrastructure is the foundation for realizing enterprise alignment through greater integration of applications, services and systems, thereby strengthening operational effectiveness and efficiency. This goal focuses on delivering the integrated DoD Information Enterprise infrastructure that the Department needs to harness the power of information.

One major challenge facing the Department today is transforming from its legacy of system-specific infrastructures to a shared infrastructure that can deliver capabilities at varying levels to consumers and providers of the Department's data and services. This goal seeks to transform the DoD GIG infrastructure into a more dynamic and adaptable shared environment that is sufficient to support global net-centric operations. As DoD moves further along the net-centric operations path, the Department must transform its infrastructure concept to support new service-oriented approaches, such as cloud computing and virtualization, for sharing, storing, processing and transporting information. Several beneficial outcomes of this approach will be a smaller physical footprint, and reduced need for skilled touch-labor, logistics and electrical power. These outcomes have mission effectiveness benefits for the warfighter and support achieving national environmental objectives through green IT approaches.

One aspect of this goal focuses on making shared and virtualized computing resources globally available, driven by the shift from individual military service-focused efforts to a more Department-wide net-centric approach. This new direction will allow for a more dynamic and broader allocation of computing resources that will provide needed computing capabilities to the joint force more rapidly and efficiently. In addition, DoD's communication and computing capabilities will be optimized to strengthen network operations and dynamic allocation of these resources. In order for benefits of these approaches to be realized, the Department needs to have DoD Components consider shared computing capabilities as the preferred option for providing services. Furthermore, migration from non-Internet Protocol (IP) and circuit-switched networks to DoD Unified Capabilities (UC), to include IP networks (v4 or v6), is an integral piece of DoD's migration to a converged IP network. To support mission needs, DoD wired and wireless transmission capability must be sufficiently sized, reliable, available, and flexible to accommodate even the bandwidth-constrained users at the tactical edge. In parallel, switching and routing

capabilities will enable DoD to interface common or disparate communications media or networks, in order to move data and information end-to-end across multiple transmission media. However, this strategy is intended to apply to those DoD and mission partner elements that are persistently connected to the DoD's IP information environment.

Ensuring the continued stability and global interoperability of the Internet while increasing security and reliability for all users should be one of the Department's priorities. A robust, resilient Internet is also a key enabler of DoD's ability to carry out a global, modern national defense strategy. Ultimately, it is in DoD's interest that the Internet remains open, stable, and secure.

The robust information environment envisioned by this goal demands an aligned approach to achieve a joint infrastructure. This requires a shift in the way that DoD Components think about meeting their computing and information transport needs. The following objectives and strategy elements will enable the Department to manage and measure progress towards the accomplishment of this goal.

OBJECTIVE 1: Shared and virtualized computing resources will be globally available to increase mission effectiveness and efficiency.

Key Performance Indicator: Assessment of the degree to which DoD computing service providers make shared and virtualized computing resources globally available on an IP-based network.

Strategy Elements:

- Better leverage the Defense Acquisition System (DAS), the Planning, Programming, Budgeting and Execution System (PPBES), and the Joint Capabilities Integration Development System (JCIDS) to ensure that DoD Components in their Analysis of Alternatives consider shared computing capabilities as the preferred option for providing services—as available and as consistent with national security needs, before acquiring or maintaining dedicated, program-specific resources.
- Provide an appropriate mix of government and commercial capabilities to increase effectiveness and efficiency through greater use of shared computing resources in the DoD Information Enterprise to include the tactical edge.
- Identify and remove the obstacles that are impeding greater use of shared computing resources.
- Develop and implement an approach for delivering shared and virtualized computing resources to users at the tactical edge.
- Increase the use of standards to support federation of computing capabilities across the Department.
- Develop and increase the use of authoritative enterprise-level architectures to provide design patterns that constrain and guide infrastructure solutions.
- Develop and implement a DoD data center realignment and consolidation strategy to achieve more efficient use of resources in support of national green IT initiatives, balanced against risks such as potential single points of failure.

OBJECTIVE 2: DoD's computing capabilities will be developed such that they enable NetOps to perform dynamic allocation of these resources.

Key Performance Indicator: Assessment of the Computing Service Providers that are NetOps enabled.

Strategy Elements:

- Implement dynamic manageability and control over computing infrastructure to enable integrated security and situational awareness (SA) of computing capabilities.
- Better leverage DAS, PPBES, and JCIDS to ensure that DoD Components incorporate functionality into shared computing resources that enables NetOps monitoring, control, and dynamic allocation of these resources.
- Ensure that enterprise-level architectures provide the standards for, and are used to guide, the inclusion of NetOps functionality into shared computing resource solutions.

OBJECTIVE 3: DoD wired and wireless transmission capability will be sufficiently sized, reliable, available, and flexible to support DoD's mission needs.

Key Performance Indicator: Assessment of the Net-Centric Capability Portfolio wired and wireless programs that comply with the DoD IEA and net-centric architecture, and are on schedule.

Strategy Elements:

- Develop and field transport capability identified by the Net-Centric Capability Portfolio (e.g., satellite communications (SATCOM), radios, mobile ad hoc networking) through evolution to a single virtual DoD terrestrial and SATCOM network providing capabilities and services from the sustaining base to the tactical edge and allowing dynamic allocation of these resources.
- Increase the application of advanced information transport technologies through research and development and by leveraging commercial capabilities.
- Transition DoD networks to Unified Capabilities, to include IPv6, and migrate from circuit-based technology to a converged (voice, video, and data) IP network and UC services environment.
- Ensure the optimal availability of electromagnetic spectrum to support DoD missions, improving DoD overall spectrum efficiency and influencing spectrum availability in the U.S. and worldwide.
- Increase the number of applications and services that are proposed for development and fielding that have assessed their operational bandwidth implications.

OBJECTIVE 4: Routing and switching capabilities will enable DoD to interface common or disparate communications media or networks, in order to move data and information end-to-end across multiple transmission media.

Key Performance Indicator: Assessment of communication bridges, satellite gateways, and satellite control capability gaps that are being closed across air and ground SATCOM.

Strategy Elements:

- Expand wireless reach where no or limited communications infrastructure exists, through research to determine how best to address the need, then implementing the solutions identified.
- Provide sufficient satellite gateway capabilities for COCOMs to support the warfighter.
- Continue developing tactical and theater satellite gateways to support migration to IP and to extend the reach of DoD's federated IP networks to the tactical edge.
- Enable users to place secured and unsecured calls and interface with the public-switched telephone network by providing a solution that allows mobile user access to the Defense Switched Network.

OBJECTIVE 5: A globally open, stable, and secure Internet will support DoD's ability to collaborate and cooperate within the Department and with mission partners.

Key Performance Indicator: Assessment of the Internet's ability to support DoD collaboration and cooperation within DoD and with mission partners.

Strategy Elements:

- Advocate DoD equities at international technical and governance meetings (Internet Engineering Task Force, Internet Corporation for Assigned Names and Numbers, Internet Governance Forum, Réseaux IP Européens, and American Registry for Internet Numbers/North American Network Operators' Group).
- Develop and test operational exercises, working with the Internet Root Server community and the ASD(NII)/DoD CIO Mission Assurance office, to determine the best approach to keeping the Internet open, secure, and stable under a range of threats.
- Promote the development of international cyberspace legal frameworks, working internally within DoD and externally with international partners, to increase the security and stability of the Internet.

GIG CONTENT DELIVERY SERVICE (GCDS)

The lack of communication and the inability to rapidly access data and share information has been a persistent challenge to users at remote locations. In the past, users suffered from inconsistent and non-secure connections in accessing web-based applications and products. The DISA-provided GCDS—the first DoD enterprise cloud service—is an accredited, distributed computing platform deployed globally on both the Non-classified IP Router Network (NIPRNet) and Secret IP Router Network (SIPRNet). GCDS addresses the above challenge by optimizing the delivery of mission content and applications through standards-based, web technologies.

The primary GCDS users are globally dispersed warfighters who must rapidly access mission data, providers who are adding increased capabilities to data centers, and owners of applications desired by end users. One benefit GCDS offers is global routing of content. The National Geospatial-Intelligence Agency (NGA) and U.S. Central Command (USCENTCOM) currently use this capability to allow forward deployed personnel to pull imagery data from the NGA to the area of responsibility.

GCDS significantly improves availability, scalability and overall performance through the use of multiple remote sites with replicated data—if one site is unreachable, data is automatically provided by the next available one. Scalability is improved when the remote site, instead of the data center, serves increased traffic. All of these changes enhance the user experience through better page load time and immediate, reliable access to web content.

GCDS reached new heights in 2008 by exhibiting tremendous growth and success. Some notable accomplishments include an 83 percent increase in customer web applications, doubling of network capacity and increased customer satisfaction for 24-hour customer support. Testimonials include an end user from the Combined Joint Task Force (CJTF) 76 Continental U.S. (CONUS) who stated, “GCDS has made a very significant improvement in CJTF-82’s ability to collaborate, share information, and disseminate information between CONUS and Afghanistan.” In addition, LtCol Randy Ross, Chief C2 Systems Branch (USCENTCOM CCJ3) stated, “No debating that our ability to effectively access information will continue to increase in importance throughout the battlefield. To this end, GCDS will be leveraged as an effective weapon towards ensuring information flow.”[3]

[3] David Honeywell, “GIG Content Delivery Services GCDS Presentation”, DISA Conference, April 2009

BATTLEFIELD AIRBORNE COMMUNICATIONS NODE (BACN) & RAPID ATTACK INFORMATION DISSEMINATION EXECUTION RELAY (RAIDER) COMMUNICATIONS CAPABILITIES

With several incompatible Tactical Data Links and data and voice communications systems currently employed throughout the Services, the ability to pass time-sensitive information to warfighters in the air and on the ground is not an easy task. As commanders are forced to deal with ever increasing amounts of tactical information, lack of information exchange across the battlefield can be detrimental. Increasing situational awareness, reducing the kill chain timeline and providing reliable Command and Control (C2) communications have long been critical warfighter needs.

C2 is the backbone of military operations. BACN and RAIDER are new systems that together significantly enhance C2 ability. BACN translates a diverse array of incoming signals and re-formats that data into information sent to receivers operating on different systems. The BACN concept was first introduced in 2004, then demonstrated in Joint Expeditionary Force Experiment (JEFX) 2006 and 2008, and has since gone on to prove its value to the warfighter in combat. BACN expands, stabilizes and improves communications, with no changes required to warfighter training, equipment, or procedures.

RAIDER acts as a ground gateway to facilitate airborne and land mobile network communications. RAIDER can provide range extension and translation for data links while supporting up to 500 warfighters on the ground, using various voice and data communications systems. When coupled with the vast array of radio equipment and connection options installed in RAIDER, ground mobile users have an unprecedented ability to access information.

During JEFX 06, RAIDER acted as a wireless IP-network connection point to provide communication users on the ground with beyond line-of-sight reach-back connectivity to the GIG, and allowed access to tactical data and imagery hosted on BACN. More recently, BACN has supported close air support, convoy, time sensitive targeting and air drop missions with great success. Based on over 700 contact situations, there has been an approximately 25% reduction in the time it takes for ground units to establish communications with close air support aircraft. This improved communications speed has also enabled an approximately 45% increase in kinetic results—bombs on target in support of our ground forces.

These results are not just limited to combat operations. BACN provides the United Nations World Food Program convoy commander with the ability to mitigate attack exposure through continuous contact with air support and ground command channels in complex, mountainous terrain. BACN also enables coalition forces (U.S., British, French, and Dutch) to extend and unify the air picture with air track, aircraft orbit and targeting information. These airborne and ground gateways link air-to-air, air-to-ground, and ground mobile networks and share large amounts of information with operational resources. In summary, BACN and RAIDER combine to give pilots and ground personnel an ability to communicate among disparate systems in the most challenging circumstances.[4]

[4] Derived from the following sources:
- David L. Richards, Capt, USAF, "News from the Source—BACN Update", *Air Force Print News Today*, July 28, 2009
- Lt.Gen. Michael W. Peterson, USAF, "Which emerging technology will have the biggest impact on your organization in the future?" *AFCEA Signal Magazine*, June 2006
- 1Lt Larry van der Oord, "Advancing communication capability to the tactical edge", *Intercom*, June 2007
- Wikipedia, "Battlefield Airborne Communications Node (BACN)"

3 SYNCHRONIZED AND RESPONSIVE OPERATIONS

The DoD Information Enterprise infrastructure, critical assets, and capabilities are operated, secured, and defended in a synchronized manner by all DoD Components to support commanders in achieving mission success.

The Synchronized and Responsive Operations goal of this strategic plan is for all DoD Components to operate, secure, and defend the DoD Information Enterprise consistently. Operating in this coordinated manner will contribute significantly to mission success, help achieve and maintain cyberspace superiority within a contested environment, and support authorized users' access to timely and trusted information when and where it is needed.

This goal entails establishing GIG situational awareness from the tactical edge to the core, improving NetOps capabilities, enhancing C2 capabilities for allocating and managing DoD IE resources, and strengthening enforcement of DoD IE policies and standards. Information sharing across organizational boundaries and functional disciplines will be the norm. DoD personnel will increasingly rely upon timely access to trusted, secure information that is shared to facilitate decision-making processes at all levels of the command structure. Improving DoD IE customer satisfaction and confidence will be essential to achieving the Department-wide culture changes necessary to overcome barriers to information sharing.

Effective operations in cyberspace, in particular, must be assured through proactive operations management and unrelenting vigilance by the DoD IE support community. To achieve and maintain the dominant position in the militarily-relevant sectors of cyberspace, DoD must plan and execute its IE operations in a manner that leverages our technological advantage over potential adversaries and continually widens that gap.

DoD IE operations must strive towards establishing and maintaining a balance among many competing priorities (including the need for increasing network security while still ensuring overall mission success) by understanding and proactively managing operational risks to the DoD Information Enterprise. DoD IE operations must enable a persistent, dominant information environment that supports broader national, DoD, and IC objectives that assure U.S. and Allied freedom of action in cyberspace and supported domains.

Four objectives will need to be accomplished to realize this goal. First, DoD IE operations will assure the availability, protection, and integrity of the DoD Information Enterprise, which encompasses DoD and IC networks, systems, enterprise services,

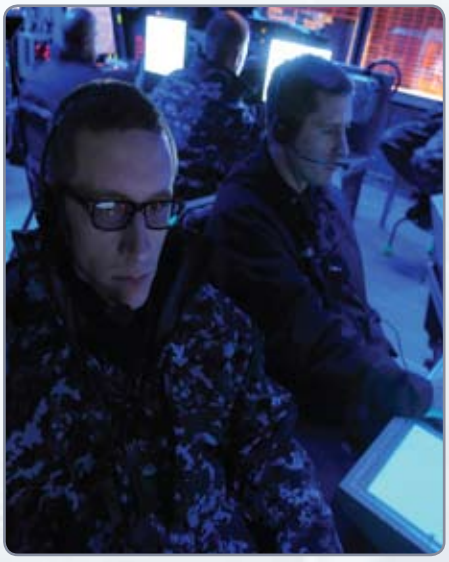
and information. At the same time, DoD IE operations must actively work to ensure that interfaces to other government and non-government mission partner networks and to the Internet remain available and secure enough for DoD to conduct business across the Department and with its mission partners. Second, DoD IE operations will provide accurate and timely information about IE health and mission readiness to decision makers at all levels, along with the control capabilities they need to implement C2 IE decisions for mission success. Third, DoD and IC policy and standards for fielded IT systems, enterprise services, and capabilities will be established and aligned to permit more efficient and responsive operation of the DoD Information Enterprise, and support an appropriate risk-management posture. Finally, common configuration management processes across the IE will be used to consistently identify, control, account for, and verify GIG infrastructure, systems, services, and applications, and will make their status visible to the IE operations community.

OBJECTIVE 1: The availability, protection, and integrity of the DoD and IC networks, systems, enterprise services, and information will be assured through capabilities that enable the Department to balance competing priorities, thereby managing risk to the IE.

Key Performance Indicators: Assessment of customer satisfaction with the availability, protection, and integrity of DoD and IC IE networks, systems, enterprise services, and information. Assessment of the ability of interfaces to other mission partner networks to remain available and secure enough to ensure DoD mission success.

Strategy Elements:

- Integrate and consolidate network management, electromagnetic spectrum management, and management of computing, systems, enterprise services, and applications for all IE resources under DoD jurisdiction to provide comprehensive service assurance on an end-to-end basis, and as appropriate, coordinate these efforts with the IC.
- Organize the DoD IE operational management community to improve unity of effort and speed of action.
- Establish the organizational structure and acquire the requisite tools to collaboratively monitor, control, and manage risk through the operation of IA/GIG network assurance systems, services, devices, and capabilities across DoD Components.
- Establish the means to proactively monitor and manage the end-user experience, by providing one-stop customer service support and by monitoring and controlling service levels and quality of service on an end-to-end basis—integrated across networks, computing platforms, systems, applications, and services.



OBJECTIVE 2: Decision makers at all levels will be provided accurate, timely, and complete information about the health and mission readiness of the DoD Information Enterprise and will be provided the control capabilities they need to quickly, securely, and consistently implement C2 IE decisions that ensure mission success.

Key Performance Indicator: Assessment of C2 IE decision cycle improvements resulting from providing decision makers with accurate, timely and complete information about the health and readiness of the IE and its ability to support all aspects of Computer Network Operations.

Strategy Elements:

- Improve the availability of IE situational awareness information to warfighters in a mission-relevant form and means, and ensure that SA information provides visibility across and into all components of the IE.
- Improve the technical capabilities of the IE environment to enable network risks to be managed and mitigated by dynamically adapting the network to changing threat environments or events.
- Achieve unity of effort by establishing and implementing standardized tactics, techniques, procedures, and concepts of operation that are employed across the enterprise to align DoD IE operations and defense with mission assurance requirements.

OBJECTIVE 3: DoD and IC policy and standards for fielded IT systems, enterprise services, and capabilities will be established and aligned to permit more efficient and responsive operation of the DoD Information Enterprise.

Key Performance Indicator: Assessment of the degree of improvement in establishing and aligning DoD policy and standards and IC policy and standards for fielded IT systems, enterprise services, and capabilities.

Strategy Elements:

- Improve the alignment of organizational responsibilities and reporting channels to provide centralized management oversight of compliance/enforcement of all operational aspects of the DoD IE.
- Establish and implement enterprise-wide NetOps and operational IA governance, policy, processes, procedures, and standards, in coordination with those of the IC.
- Enhance the enterprise-wide Certification and Accreditation process for IE infrastructure, enterprise services and other critical assets to enable the dynamic management of operational risks.
- Establish and implement a risk management process for consistent assessment of operational risk against standard enterprise criteria.

OBJECTIVE 4: Common configuration management processes across the DoD IE will be used to consistently identify, control, account for, and verify GIG infrastructure, systems, services, and applications, and will make their status visible to the IE Operations community.

Key Performance Indicator: Assessment of the extent to which standard configuration management processes are adopted across the DoD IE to enable DoD to have agile responses to specific threats and maintain consistent interoperability with all mission partners.

Strategy Elements:

- Establish consistent configuration management processes for managing GIG infrastructure, information systems, services, and applications to achieve a secure, interoperable net-centric environment.
- Implement an enterprise-wide common configuration management technical framework and process to identify, control, account for, and verify GIG configuration items to ensure interoperability and security.
- Manage configuration item data to enable sharing that data through net-centric approaches that support overarching GIG situational awareness objectives.

INTEGRATION OF THE COMBATANT COMMAND THEATER NETOPS CONTROL CENTERS WITH DISA THEATER NETOPS CENTERS

The U.S. European Command (USEUCOM), the U.S. Africa Command (USAFRICOM), and DISA are using a new approach of co-locating NetOps staff to address NetOps situational awareness information sharing for their respective portions of the GIG. The USEUCOM and USAFRICOM Theater NetOps Control Centers now have their NetOps watch officers located in the DISA-EUR Theater NetOps Center (TNC) facility. The watch officer function includes assessing mission impact, based on DISA System Control Officer information for the status of their portion of the GIG. The U.S. Pacific Command (USPACOM) also follows this model and has now placed four of their controllers at the DISA-PAC TNC.

In addition, Army 5th Signal Command has installed a workstation on the DISA-EUR TNC floor for SA of the Army network in Europe. Similarly, the North Atlantic Treaty Organization (NATO) also recently installed a workstation on the DISA-EUR TNC floor for the SA of the NATO network.

This early stage of "manual integration" has realized tremendous benefits with respect to manning, response time, and general communication. Watch officers are able to communicate directly with each other because they are working face to face and can view one another's workstation screens for relevant SA information. They are able to work jointly to troubleshoot network problems and deal with emergent congestion issues. The underlying NetOps support systems are still separate, stovepiped applications that are planned for more direct integration in the future. Nonetheless, improvements in sharing SA information have already been achieved without building point-to-point interfaces among the existing systems.

4 IDENTITY AND INFORMATION ASSURANCE

A unified and resilient DoD Information Enterprise where only authorized users (including mission partners) have ready access to their information; missions continue under any cybersecurity situation; and associated components perform as expected and act effectively in their own defense.[5]

The Department's emphasis on identity and information assurance has greatly increased in recent years; however, our adversaries remain determined to take advantage of greater access and concealment opportunities in the global information environment. While it is critical to make information available to the widest range of DoD Information Enterprise partners to increase our effectiveness, the Department must ensure that its Information Enterprise is secure. As DoD culture evolves, it is vital that we optimize the balance between the principle of need-to-know with that of our need-to-share. It is imperative that we escalate our capabilities to protect the Department against threats, accelerate transformation to a net-centric enterprise with assured information access, ensure the survivability of GIG-dependent missions, and ensure integrity of our defense platforms. The Identity and Information Assurance goal represents a common vision and corresponding objectives for all DoD Components. It supports business, warfighting, and intelligence missions across all Tier 1 Joint Capability Areas, with specific focus on computer network defense tasks in Force Application, the information assurance tasks in Net-Centric, and related information management tasks in Corporate Management and Support. As the DoD enterprise moves forward to achieve this important goal, it demonstrates that it has the willingness and mechanisms to align its culture and conduct to changing information assurance demands. The power of the Identity and Information Assurance goal comes from being part of a larger, combined force, where all parties of the DoD operational enterprise work collaboratively to achieve all goals in this plan.

The Identity and Information Assurance goal focuses on assurance as a means to prepare the DoD Information Enterprise to identify and effectively respond to adverse events; to ensure the integrity and authenticity of identity information (while maintaining privacy); and to protect and defend information and information systems. To achieve this goal, it is crucial that we recognize our dependence on the Internet, that we grasp the implications of our increased reliance on external

[5] Note: The Identity and Information Assurance goal for the DoD IE Strategic Plan is being developed in coordination with the Cyber, Identity, and Information Assurance (CIIA) Strategy. The DoD IE SP&R is the umbrella strategic plan for the DoD Information Enterprise and, as such, includes the goals, objectives, and strategy elements of the CIIA Strategy. Detailed information on the CIIA Strategy can be found at: http://www.defenselink.mil/cio-nii/docs/DoD_IA_Strategic_Plan.pdf

infrastructures, and that we establish protection and risk management strategies to complete our mission. To this end, the goal identifies four objectives that collectively describe an integrated view for focusing near-term activity and aligning long-term investment to achieve a common vision.

Achievement of this goal and its four objectives is expected to yield key targeted outcomes for the Department.

- To ensure the extended information assurance community is organized for unity of purpose and speed of action, so that each DoD organization and community of practice understands its role and works together to align policies and leverage joint decision processes.
- To enable secure mission-driven access to information and services, rendering DoD information securely accessible to all who need it and unavailable to our adversaries.
- To anticipate and prevent successful attacks on data and networks so attacks can be stopped at the perimeter and attackers quickly identified.
- To prepare for and operate through attack on or degradation of the global information environment, by ensuring readiness levels are sustained and enterprise capabilities recover quickly from any incident.

Key to the Department's strategy is its focus on building and operating the GIG as a joint global enterprise. This enterprise network approach, coupled with skilled users, first responders, and defenders—and in partnership with the intelligence and homeland security communities, and the private sector—will allow us to more readily identify and respond to attacks on or through the global information environment. Further elements of the strategy are: to coordinate identity and information assurance implementation across organizations; to secure posting of information throughout the enterprise based on dissemination controls, information tagging, provenance, and pedigree; to integrate and analyze monitoring information from various sources in order to identify network events that require intervention; to minimize where an attacker can go through techniques, such as cordoning off portions of the network, in order to isolate attacks and protect the healthy; and to ensure the cross domain integration of responses to these events.

OBJECTIVE 1: The extended information assurance community will be organized for unity of purpose and speed of action to enable mission success.

Key Performance Indicator: Assessment of improvements in ability to behave as an identity and information assurance enterprise and improvements in its agility.

Strategy Elements:

- Lead and govern in an uncertain environment by setting enterprise direction, including establishment and communication of priorities and objectives, policies, standards, and performance measures; fostering a culture of accountability; and providing insight and oversight to ensure coordinated and consistent identity and information assurance implementation across organizations.

- Design for the fight by delivering the right capabilities on the right time line; synchronizing and integrating capabilities across the enterprise; leveraging technology; successfully investing by continually aligning programs, initiatives, and activities with enterprise priorities and warfighter requirements; and by managing risk.

- Develop the workforce by providing a continuum of IA learning activities from basic literacy to advanced specialties, by recruiting and retaining highly qualified IA professionals in needed positions, and by keeping workforce capabilities current.

- Partner for strength by leveraging unique capabilities of a wide set of national and international organizations; by working proactively with critical infrastructure owners and operators; by expanding engagement with other organizations on risk reduction; and by engaging with U.S. Government interagency efforts focused on developing Internet standards and governance policy to protect the security and stability of the Internet infrastructure.

OBJECTIVE 2: Secure mission-driven access to information and services will be enabled across the global defense enterprise.

Key Performance Indicator: Assessment of improvements in our ability to access information and services securely to perform our mission.

Strategy Elements:

- Secure data in transit by enabling private information flows through robust, ubiquitous cryptographic services achieved by employing cryptographic products that protect against corruption and by modernizing key management services.

- Manage access among users, services, data, platforms and facilities based on mission needs and supporting functions. Key strategies are: identity management using credentials (including roles) for individuals and non-persons (e.g., devices) for authentication within the enterprise; managing privileges by decoupling access management from applications; automating access management; and managing resources by generating standardized security attributes (metadata) for enterprise information (including privacy information) and services.

- Assure information sharing by enabling secure information management; by providing a full suite of secure sharing solutions for publishing, discovery, and collaboration across security domains, networks, enclaves, Communities of Interest, and mission partners; and by enabling secure posting of information for the DoD Information Enterprise based on dissemination controls, information tagging, provenance, and pedigree.

OBJECTIVE 3: The Department will be prepared to anticipate and prevent successful attacks on data and networks.

Key Performance Indicator: Assessment of improvements in our ability to anticipate, prevent, and identify the sources of attacks on data and networks.

Strategy Elements:

- Understand the battlespace by aligning audit, sensor, forensic and incident management sources across the extended enterprise.[6] Key strategies are to: know the adversary to be able to characterize adversarial behavior and capabilities in order to adjust defenses; know the network and network vulnerabilities; and understand consequences of potential threats to the DoD Information Enterprise and supported missions.
- Prevent and delay attackers from getting in the GIG by applying knowledge of the network, vulnerabilities, and adversaries to harden GIG entry and by embracing tactics, techniques, and procedures that favor defenders. Key strategies are to: defend perimeters by layering and strengthening internal security zones; harden hosts and networks by establishing and enforcing security configurations; and tighten network defenses using Red Teams, Blue Teams, and other means.
- Prevent attackers from staying in or acting by lowering the value of an attack for an attacker and reducing consequences of an attack. Key strategies are to: detect and diagnose malicious activity; constrain privileges; remove static cyber conditions that attackers depend on and employ active defenses where appropriate; prevent masquerading; and constrain freedom of movement to limit the attacker, using means such as data-at-rest (DAR) encryption.

OBJECTIVE 4: The Department will be able to prepare for and operate through attack on or degradation of the global information environment.

Key Performance Indicator: Assessment of improvements in our ability to prepare for and prevail in performing our mission through various levels of attack on the global information environment.

Strategy Elements:

- Develop and maintain trust in data, platforms, and networks by guaranteeing integrity and availability of these assets, to include processors and controllers embedded in defense platforms. Key strategies are to: assure availability of these assets by matching product assurance to mission criticality; engineer for survivability so that critical assets operate despite sophisticated attack; and maintain integrity to improve confidence that information and communications technology components and data are sound.
- Strengthen cybersecurity readiness using key strategies to: enable coordinated event response by linking communications and operations across the extended enterprise; implement realistic exercises for operating in a degraded, untrusted, or non-functioning information environment; and identify critical assets to improve planning for continuity of operations.
- Sustain missions using key strategies to: respond to cybersecurity events and execute courses of action by dynamically defending and fighting through adverse effects; sustain mission-critical functions under degradation; and reconstitute critical assets to a trusted state to support ongoing mission operations.

[6] Extended enterprise includes Federal, State, local, tribal, coalition partners, foreign governments and security forces, international organizations, non-governmental organizations, and the private sector, as defined in the DoD Information Sharing Implementation Plan.

DoD FENDS OFF JULY 2009 CYBER ATTACK

Governments, technology companies, media, infrastructure providers and even our citizens are frequent targets of cyber attacks. Currently over 140 countries are estimated to have active cyber weapons programs, with more being added monthly. U.S. government officials routinely say their computers are probed millions of times a day, and likewise, the Chairman of the Joint Chiefs of Staff has voiced concern that Pentagon networks are under near-constant attack. A May 2009 report from the Government Accountability Office confirmed that in FY 2008, federal agencies experienced three times the number of threats or incidents than in FY 2006.[7]

One particularly widespread and unusually resilient computer attack that began July 4, 2009 included U.S. government targets of the Defense Department, National Security Agency, Treasury Department, Secret Service, State Department, Federal Trade Commission and Federal Aviation Administration. For three days, this siege against U.S. and South Korean computer networks leveled a series of attacks that were among the broadest and longest lasting assaults perpetrated on government and commercial web sites in both countries. While the attacks succeeded in knocking out web sites of several government agencies, they had minimal impact on the Defense Department. Defense officials confirmed Pentagon networks were struck but the intrusions were detected quickly. The defenses that DoD had established enabled its sites to operate throughout the entire attack. DoD continues to apply aggressive cyber defense measures to maintain the success demonstrated during the July 2009 attack.[8]

DoD ATTACK SURFACE REDUCTION

There have recently been two other significant wins in the DoD IA arena. Both reduce DoD's cyber attack surface substantially and both are the result of great team efforts.

The first is completion of DoD Demilitarized Zone (DMZ) Increment Zero—a solution that blocks all inbound Internet connection attempts, except those bound for servers specified on a whitelist. This required all public-facing servers to register on a whitelist, which was used to allow entrance to NIPRNet traffic bound for authorized destinations only. This approach shields the vast majority of DoD computers from Internet attack. It is an important step in the overall restructuring of the NIPRNet for better security and information sharing. The effort was highly collaborative and involved multiple agencies and commands. ASD(NII)/DoD CIO sponsored and led the effort, ensuring all DoD organizations registered their outward-facing servers and participated in the implementation. Joint Task Force-Global Network Operations developed the CONOPs, ran practice drills with potentially affected organizations, and managed the roll out of blocking functionality. DISA engineered, built, and tested the whitelist registration tool. Like many DoD-wide efforts involving substantial change, this was a challenge, but the Department pulled together to ensure success.

[7] Kevin Coleman, "Cyber Attacks on Supply Chain Systems," *Defense Tech*, April 15, 2009
[8] Lolita C. Baldor, "Federal Web Sites Knocked Out by Cyber Attack," Associated Press, July 7, 2009

The second big win was the first DoD Domain Name System (DNS) .mil proxy going live in early September, 2009—an important step in building a far more defensible DoD/Internet perimeter. Before the .mil proxy went live, many DNS servers were visible to the Internet and subject to attacks and reconnaissance. Now the .mil proxy sits at the logical boundary between DoD and the Internet and answers DNS Internet queries about DoD addresses. These proxies provide more central control of DoD network information being given to the outside world. Once all .mil proxies are functional later in 2010, all internal DNS servers will be shielded. This achievement was a great team effort within DISA and required concerted effort across many organizations.[9]

DEPARTMENT OF THE NAVY (DON) PERSONALLY IDENTIFIABLE INFORMATION (PII) AND THE DATA-AT-REST (DAR) SOLUTION

Identity theft is one of the easiest crimes to perpetrate and is one of the worst things that can happen to our sailors and marines, who may not have the means to remedy the damage caused to their accounts due to operational deployment. The loss of privacy data can be expensive to affected personnel, negatively affects morale, degrades our public image, and can be costly to the command/unit responsible for the loss. Recent PII breach reports highlight the need for the DON to protect against the risks of loss and compromise of privacy sensitive data. More than 80 percent of DON breaches are preventable and are the direct result of human error. With growing use of removable storage, a more mobile workforce and an increase in identity theft, endpoint data protection controls must be employed to greatly diminish the human error factor.

An enterprise DAR encryption tool provides a common management platform for implementing a complete array of endpoint data protection controls. In the event a device with PII or other sensitive information is physically lost or stolen, a DAR solution provides a first line of defense against data loss for all hard drives and portable storage media. While the DAR solution is not the complete answer to PII losses, it is estimated that over half of the DON breaches reported today would be mitigated to "low risk" once the encryption tool is fully implemented.

With implementation ongoing across the Navy Marine Corps Intranet (NMCI) network, results have already been very positive. What began as perhaps the DON's largest and most egregious PII breach in 2009 ended with a very small number of personnel impacted due, in part, to the fact that the stolen laptops and external hard drives were encrypted. A Navy recruiter laptop containing PII from civilian applicants was recently stolen from a locked government vehicle and it too, was protected by encryption. Similar examples of the increasing use of data encryption are driving down the number of DON personnel impacted by PII data losses.[10]

[9] Richard Hale and Mark Orndorff with ASD(NII)/DoD CIO contributed to this story.
[10] Steve Muck with the Secretary of Navy DON CIO contributed to this story.

5 OPTIMIZED INVESTMENTS

An integrated DoD Information Enterprise investment and portfolio management capability that maximizes the contribution of information-related investments to national security and defense outcomes.

In response to federal, executive, and Departmental guidance, DoD has made great progress establishing an investment decision-making process based on an assessment of potential return on those investments. The Department has also made great progress building processes to support recommendations to terminate or to continue programs based on their performance relative to expectations. However, optimizing the total investments supporting DoD's IE remains a complex challenge.

The goal to optimize investments in support of the DoD IE is based on realizing the vision to institutionalize IT investment management best practices. Investment review boards that govern DoD IT investments across missions are central to this vision. These review boards will be tasked to review the strategic relevance of all significant investments. Review boards will thereby provide due diligence in the requirements phase of the acquisition lifecycle and ensure comprehensive justification for investments. The vision also relies upon a mature, federated DoD Enterprise Architecture (EA) that will enable mapping of required capabilities to investments, improving decision making and driving mission performance.

Further, the vision includes acquisition approaches that take advantage of opportunities to modernize the DoD while reducing redundancy and enforcing compliance requirements. Improved IT acquisition steps will include: leveraging internal research and development, considering innovative information sharing approaches in its Analysis of Alternatives, as well as exploiting cutting edge technology products being developed by industry partners. All decision processes will support IT Portfolio Management recommendations to speed acquisition, budgeting, or requirements processes where appropriate, and resist support for programs that do not provide capability in a reasonable amount of time. These mechanisms support the decisions to start, stop, accelerate or modify IT investments at any point along the investment lifecycle.

The achievement of this goal is dependent upon establishing a culture that views the acquisition, management, and retirement of IT investments in terms of strategic enterprise value, capability performance, gap severity, risk, financial efficiency and environmental impact. Ultimately, through federated efforts across the enterprise, DoD will become an organization that optimizes the value of IT investments by managing their contributions as part of capability-based portfolios.

Although the Clinger-Cohen Act (CCA) and its associated federal guidance have resulted in significant efforts to improve DoD's IT investment practices, many opportunities for improvement remain. Achieving the goal of optimizing IT investments will be driven by wider adoption of IT investment governance, greater utilization of DoD EA, increased agility in acquisition processes, coordinated management of IT portfolios, improved oversight of compliance with applicable regulations, and the establishment of an environmentally responsible IT culture focused both on cost efficiencies and the reduction of the IT influenced carbon footprint.

OBJECTIVE 1: DoD IE governance will effectively align and optimize IT investments and capabilities with DoD goals and priorities.

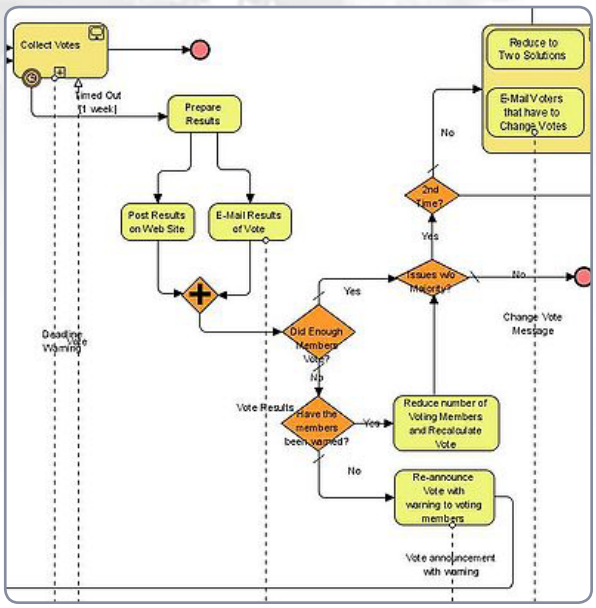
Key Performance Indicator: An assessment of the degree to which DoD IT investments and capabilities align to and support the DoD IE Strategic Plan and Roadmap.

Strategy Elements:

- Improve the synchronization of review board decision-making processes with related JCIDS, DAS, and PPBES processes.
- Improve compliance with IT Capital Plan requirements to increase accountability and transparency throughout DoD.
- Exercise tiered portfolio performance oversight to improve compliance with comprehensive enterprise-wide investment management guidance.
- Integrate and synchronize compliance with Title 40/CCA requirements into JCIDS, DAS, and PPBES processes.
- Increase the degree of alignment of Title 40/CCA process improvements with other DoD transformation initiatives such as the Business Transformation Agency's Business Capability Lifecycle and the new IT systems acquisition process that is required by law.

OBJECTIVE 2: The federated DoD Enterprise Architecture will guide and inform IT investment decisions to achieve improved mission performance.

Key Performance Indicator: An assessment of the degree to which IT investment decisions are guided and informed by the DoD Enterprise Architecture.



Strategy Elements:

- Require portfolio and program managers to produce architectures that are authoritative, discoverable, accessible, registered in the DoD Architecture Registry System and available for reuse throughout the DoD Information Enterprise.
- Ensure that all approved IT investments have architectural descriptions that are aligned to at least one Segment Architecture and comply with architecture policy and approved IT standards.
- Increase the use of DoD EA reviews as part of the IT investment decision process.

OBJECTIVE 3: DoD acquisition processes will better support the rapid deployment of IT capabilities and financial efficiency.

Key Performance Indicator: Assessment of the degree to which the mechanisms for rapid deployment of IT capabilities are utilized throughout the Department.

Strategy Elements:

- Leverage pilots and experiments as a mechanism to field IT capabilities.
- Increase the use of an *Adopt before Buy—Buy before Create* (ABC) approach for selecting IT investments during the Analysis of Alternatives.
- Increase the utilization of flexible acquisition models to support specific and widely varying DoD capability requirements.
- Establish more comprehensive mechanisms for informing the DoD community of all new and emerging IT capabilities.

OBJECTIVE 4: Broadly implemented IT investment portfolio management processes will systematically and continuously enable the Department's ability to efficiently deliver information technology capabilities.

Key Performance Indicator: An assessment of the degree to which complete and accurate data associated with IT investments is maintained and made available in support of an enterprise-wide approach to IT investment portfolio management.

Strategy Elements:

- Increase the alignment of DoD IT investments with Federal Enterprise Architecture segments.
- Institutionalize an IT investment portfolio capability that analyzes investments based on their contribution to achieving portfolio goals (cost savings, performance improvements, sun-setting of legacy applications, etc.).
- Maintain an accurate and complete inventory of DoD systems to support all reporting requirements.

OBJECTIVE 5: Environmentally responsible and resource efficient (i.e., green) approaches will be promoted and adopted across the DoD IT investment lifecycle.

Key Performance Indicator: An assessment of the degree to which DoD acquires and manages IT according to federal mandates for environmentally responsible and resource efficient approaches.

Strategy Elements:

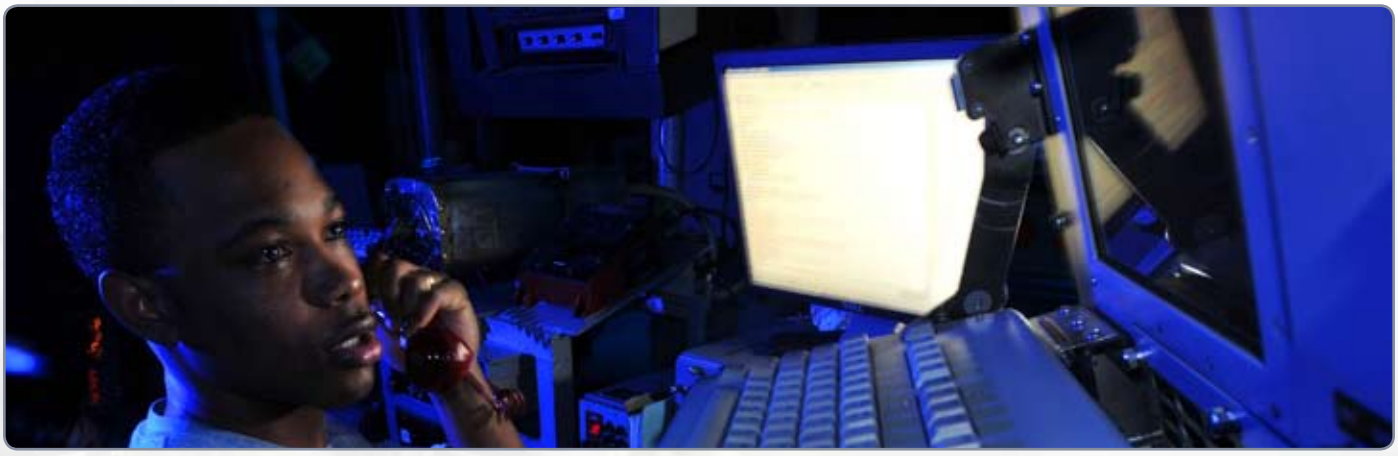
- Incorporate green IT considerations in the DoD acquisition process.
- Incorporate assessment of compliance with federal green IT policy into DoD management oversight processes and practices.
- Promote the incorporation of reducing, reusing, and recycling of IT products and services into IT investment policies.

GREEN IT INITIATIVE DRIVING DON DATA CENTER EFFICIENCIES

The Navy-Marine Corps Intranet (NMCI) is the largest purpose-built network in the world. It runs on 40 server farms and is used by more than 707,000 sailors, marines, and civilians in 620 locations in the United States and Japan. Thus, the task of virtualizing the NMCI's underlying server infrastructure—without disrupting service—has proven to be an enormous technological challenge. Yet the rewards have been significant, reaping the Navy and Marine Corps better network performance and reliability, significant financial savings, and a reduced impact on the environment.

The environmental benefits of the project came as a pleasant surprise to Greg Burke, director of network operations center services for NMCI. "After the first wave of the project, we realized just how significant the environmental impact of virtualization was," he says. "Not only were we reducing our footprint by purchasing fewer pieces of equipment for hardware refresh—resulting in less hardware waste—but we were also using significantly less power and cooling energy for the server farms."

When the project is complete, it is expected to achieve a 9-to-1 consolidation of servers, saving the military an estimated $1.6 million per year in power and cooling costs, a reduction of more than 65 percent. Moreover, the organization will avoid spending $1 million on new machines when it comes time to refresh its gear. Additionally, the Navy expects to save 40 to 70 percent of its server farm floor space. From an environmental standpoint, the virtualization project has reduced the Navy's carbon emissions by 6,800 tons—the equivalent of taking 2,550 cars off the road—and the Navy expects that number will reach 7,466 tons of CO_2 by the time the project is complete.[11]



[11] Excerpted from Ted Samson, "U.S. Navy Enlists Virtualization to Supercharge Intranet," *Infoworld*, April 22, 2009

6 AGILE IM/IT/IA WORKFORCE

An agile IM/IT/IA workforce able to dynamically operate, defend, and advance the DoD Information Enterprise.

Timely, trusted and shared defense information is powered by transformative technology solutions that are envisioned, implemented and secured by a highly skilled workforce providing IM, IT, and IA mission capabilities. Rapid technology advancements, coupled with increasing cyberspace challenges, require agile, forward thinking information resource managers and technologists who can quickly implement cost-effective innovations while also enabling secured information sharing and collaboration. Strategic workforce planning supports the development of a broader balanced "workforce of the future" with the experience, aptitude and creativity to deliver enterprise services that support Combatant Commanders. Supported by this mission-ready force, the Department will achieve and maintain a persistent and dominant information advantage for ourselves and our mission partners.

DoD currently employs over 168,000 IM/IT/IA professionals within its military and DoD civilian workforces, collectively known as the IT workforce. These numbers are expected to grow to meet emerging and expanding mission requirements. The DoD will provide competency-based education and training to develop a mission-ready force. To sustain a total force that meets normal and surge defense requirements, Functional Community Management (FCM) will be applied to support mission needs across the DoD Information Enterprise. The Department will promote innovative practices and diversity to develop an engaged and collaborative workforce.

Additionally, the Department will identify and support valued IT career and professional opportunities to attract new members to the workforce and retain current, mission-ready personnel.

OBJECTIVE 1: Strategic workforce planning will enable a mission-ready "workforce of the future."

Key Performance Indicator: Assessment of accession and separation trends relative to meeting the workforce needs of the future.

Strategy Elements:

- Target the Net Generation to create a broader-based workforce.
- Incorporate the needs of a multigenerational workforce into recruitment and retention efforts.
- Support planning by improving the accuracy and timeliness of information used for defining manpower, personnel, and training needs.

OBJECTIVE 2: Education, training, certifications, and continual development opportunities will support a competency-based Total Force.

Key Performance Indicator: Improvements in levels of education, training and certifications, relative to defined targets.

Strategy Elements:

- Assessment of DoD Component utilization of DoD IT education and training institutions to drive DoD Component utilization and improvements.
- Target professional development to meet career and mission requirements.
- Apply a comprehensive approach to identify and meet critical learning needs.

OBJECTIVE 3: IT Functional Community Management within and across DoD Components will provide comprehensive identification, planning, assessment and reporting capabilities that support mission readiness.

Key Performance Indicator: IT FCM progress in providing comprehensive reporting capabilities.

Strategy Elements:

- Determine the competencies and skills required to acquire, build, populate, operate, and defend the DoD Information Enterprise.
- Define the civilian force skill sets in a DoD-wide competency taxonomy.
- Populate DoD-wide personnel systems and management tools with required occupation and skill identifiers.
- Support community management through defined career paths and guidance.

OBJECTIVE 4: Cybersecurity/IA capabilities, a critical component of the FCM, will be fully integrated into workforce management and sustainment efforts.

Key Performance Indicator: Improvement in IA workforce levels relative to targets by role and certifications.

Strategy Elements:

- Ensure cybersecurity/IA mission is sufficiently manned to secure and defend DoD information assets during normal operations and to surge in response to incidents.
- Train and certify the cybersecurity/IA workforce to meet DoD requirements.
- Identify and track cybersecurity/IA positions and people in Defense manpower and personnel systems.

OBJECTIVE 5: A diverse and geographically dispersed workforce that is engaged, innovative, and collaborative.

Key Performance Indicator: Comprehensiveness of IT workforce recognition programs across the Department of Defense.

Strategy Elements:

- Encourage and recognize innovative practices and solutions.
- Promote flexible and productive work arrangements.
- Value and integrate diversity into workforce planning.

DEVELOPING THE "WORKFORCE OF THE FUTURE" TAKES DIFFERENT APPROACHES

The ever-changing demands of the Department's IT world have led the MILDEPs and Defense Agencies to implement innovative and effective programs to develop a workforce with the IM/IT/IA skills to solve today's and tomorrow's challenges. Four standout programs from the Army, Marine Corps, Navy, and Defense Contract Management Agency (DCMA) illustrate the variety of approaches being used. The Army established the Army Knowledge Leader (AKL) program, an intensive two-year, multi-dimensional professional development experience designed to develop leadership, business and technology competencies to support the Army CIO mission. The AKL program is grooming a cadre of dynamic, young professionals interested in fast-track leadership opportunities within public service. Individuals receive one-on-one, senior-level mentoring and team training in select subject areas. Additionally, they perform a series of targeted developmental assignments in key organizations where they focus on project management skills, transformative technology delivery and IT policy development.

The Marine Corps Training and Education Command revamped its Communications-Electronics School classroom training and revolutionized the way the Marine Corps trains and commercially certifies its command, control, communications, and computer (C4) personnel through Communication Training Centers (CTCs). The CTCs are co-located with the Marine Expeditionary Forces and provide training for active duty and reserve Marines and civilians who are part of the IA workforce. Specific CTC-developed courses support the DoD IA certification mandate and provide training for operating system certification.

In 2009, the Naval Education and Training Command provided IT Management personnel the ability to identify and participate in online training linked to the competencies that support their occupational specialty (IT 2210). Using curricula validated by the DON CIO, coursework available through Navy E-Learning has been mapped to occupational areas such as systems administration, network analysis and data management. This capability provides a valuable professional development tool to the IT Management community, which is the backbone of the DoD and federal government-wide IT workforce. Enrollment in these online courses, while targeted at the IT 2210 Community, is open to all DON government civilian and military personnel.

The CIO IT Leadership Program at the DCMA provides integrated, inclusive professional development opportunities to meet individual career needs for the 200 DCMA Customer Service Organization's IT professionals and the agency's succession pipeline requirements. Participants complete core competency training within their IT career specialty and targeted leadership coursework, as well as other mandated certification requirements. These credentials qualify individuals for the DCMA CIO

Professional Certification at the middle or senior management levels. DCMA has awarded 106 certifications to date, about equally split between middle and senior management. DCMA credits the program with enabling them to identify and develop potential high performers who are well-rounded, have good interpersonal skills, and have the aptitude and the attitude to take on new professional challenges. As a result of the CIO IT Leadership Program, the agency has created a viable succession plan to support a scheduled Base Realignment and Closure move and projected workforce retirements.

These examples illustrate how four quite different approaches to meet the development needs of today's personnel help the Department create, develop and sustain the workforce of tomorrow.

AIR FORCE INSTITUTE OF TECHNOLOGY (AFIT) CYBERSPACE RESEARCH PROGRAM RECOGNIZED

AFIT's Center for Cyberspace Research (CCR) is DoD's leader for advanced graduate-level cyberspace education and research. Masters and doctoral programs push the cutting edge in theories, techniques and applications for advancing the state of the possible in cyberspace, DoD's newest warfighting domain. Students move from classroom theories for defensive and offensive cybersecurity into laboratory applications that test the capabilities of defense cybersecurity operations, while authoring masters theses and doctoral dissertations geared towards advancements in cybersecurity that range from the software application to the network enterprise.

The year 2009 was a banner year for the CCR. The institution was jointly designated as a National Center of Academic Excellence in Information Assurance Education Research for academic years 2009-2014 by the National Security Agency and the Department of Homeland Security in recognition of its comprehensive defense education and research programs. It was awarded a renewal grant in the amount of $2.1M by the National Science Foundation to continue its participation in the Scholarship for Service fellowship program that recruits and educates talented civilians to work for federal, state, or local governments on cybersecurity issues. The CCR also leads the development of Professional Continuing Education curricula for the Air Force's emerging cyberspace workforce and continues to develop and strengthen relationships with cyberspace-related research, education, and training communities within the Air Force, with its DoD service partners, with federal agencies, and with civilian academic and commercial research organizations around the globe.

REFERENCES: Links to references for the DoD Information Enterprise Strategic Plan can be found on the Intellipedia wiki at this URL: **https://www.intelink.gov/wiki/DoD_CIO/DoD_IESPR/Reference_Documents**

ASD(NII)/DoD CIO
6000 Defense Pentagon
Washington, DC 20301-6000
http://cio-nii.defense.gov