DEPARTMENT OF THE NAVY

INFORMATION MANAGEMENT / INFORMATION TECHNOLOGY / CYBERSPACE

STRATEGIC PLAN

FY 2010 - FY 2014

There is no doubt that the integrity and security of our computer and information systems will be challenged on an increasing basis in the future. Keeping our cyber infrastructure safe is one of our most important national security challenges.

The Honorable Robert Gates
Defense Secretary
June 2009

Foreword

Today, Information Management, Information Technology (IM/IT), and Information Resources Management have been subsumed by the newer term called "cyberspace." Cyberspace, cybersecurity, and cyber attack have become common terms in our lexicon. In just a few short years, much has changed on the IM/IT landscape. This includes our reliance on an increasingly networked infrastructure, a growing threat to network security, and myriad information solutions to conduct our mission. The term "information technology" is defined as any equipment or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. In May 2008, the Department of Defense (DoD) defined cyberspace as, "a global domain within the information environment consisting of the interdependent network of IT infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." These evolutionary terms will continue to help define the battle space in which we operate, currently and in the future. Cyberspace has been added to the title of this plan to underscore its importance within the Department of the Navy (DON) and the changes that have occurred in the information environment.

How cyberspace affects our daily lives and all levels of the DoD and the DON cannot be overemphasized. From daily decisions in shipboard maintenance shops to quickly disseminating key intelligence data for operational decisions by the commander on the battlefield, information and its protection are highly critical to making the right decision when needed.

Key to ensuring the DON has timely access to needed information in the future is to lay out plans today that provide decision-makers at all levels of the organization with the requisite tools. The Department of the Navy Chief Information Officer (DON CIO) has established such a strategy and it is reflected in this document. When successfully implemented, this strategy will provide the Department with:

- An agile and integrated Enterprise Architecture for the Naval Networking Environment (NNE).
- Consolidated and interoperable networks.
- Streamlined, cost effective services across the DON enterprise.
- Proactive network security countering threats before intrusion occurs.
- Protected infrastructure critical to the free flow of information.
- Ubiquitous access to requisite data and services – anytime, anywhere.
- A trained Cyber/IT workforce with the necessary tools to quickly perform their job.
- An IT investment strategy for the entire Department.

This is the vision going forward. It is based on meeting specific "markers" over the next several years leading up to the NNE. This strategic plan addresses those markers or objectives for the period 2010-2014. To make this vision a reality requires a focus on achieving those markers as well as the flexibility to adjust to a dynamic environment. Under the leadership of the DON CIO, success will ultimately rest with both internal and external organizations; in particular the Navy and Marine Corps. Together, we will ensure that we never put our Sailors and Marines in harm's way without the requisite information or required tools to manage that information.

SECRETARY OF THE NAVY
The Honorable
Raymond Edwin "Ray" Mabus

CHIEF OF NAVAL OPERATIONS
Admiral Gary Roughead

COMMANDANT OF THE MARINE CORPS
General James F. Amos

CIO Leadership Team

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER

Mr. Terry Halverson

DEPARTMENT OF THE NAVY
PRINCIPAL DEPUTY CIO

Ms. Barbara H. Hoffman

DEPARTMENT OF THE NAVY
DEPUTY CIO (MARINE CORPS)

MajGen George J. Allen

DEPARTMENT OF THE NAVY
DEPUTY CIO (NAVY)

VADM David J. "Jack" Dorsett

In the 14 years since Chief Information Officers for Federal agencies were established, Information Management and Information Technology have become increasingly important and have become integrated within, and critical to, Navy and Marine Corps capabilities and functions. This strategic plan describes the Department of the Navy CIO's vision, mission, governing principles, goals, objectives, and key performance indicators for IM/IT to support the warfighter and the entire Department. It is driven by, and aligned to, the overarching departmental goals articulated by the Secretary of the Navy, the goals and objectives outlined in the Department of Defense Information Enterprise Strategic Plan, and the goals of the DOD IT Efficiencies Roadmap.

Warfighting is dependent on networks to move information to support warfighting decisions. To underscore the importance of cyberspace-related activities within the DoD, the U.S. Cyber Command, the U.S. Fleet Cyber Command/10th Fleet, and Marine Forces Cyber Command were established to develop a framework for cyberspace operations. Cyberspace is changing and evolving continuously; our strategic goals must adapt to keep up and policies must be informed by operational realities. We must lead and govern in an uncertain national security environment, while understanding the military, civil, and physical conditions of the battle space. The cyber threat is real and ongoing; therefore, we must anticipate and prevent successful attacks on data and communication networks. We must enhance our cybersecurity readiness and work with critical IT infrastructure owners to identify and remove or mitigate risks.

To accomplish our mission, we must operate as an "aligned" DON enterprise by ensuring all IT activities are grounded in effective governance, with standard architecture, information assurance, and management practices. The new norm must be to consolidate and centralize where it makes sense, ensuring maximum use of Enterprise solutions and services. We must leverage the DoD IT Efficiencies Roadmap efforts and strive for efficiency in all our endeavors, while preserving the highest levels of mission effectiveness. Together, we must create a Naval Networking Environment (NNE) that ensures our information enterprise infrastructure securely and efficiently leverages the full range of information resources enabling rapid, on-demand, ubiquitous access to authorized users and systems in support of the Joint information environment and all Navy and Marine Corps specific strategic, operational, and tactical missions, as well as the DON's business functions. Our goal is to create a NNE that will ensure delivery of "the right content, anywhere, anytime, to the right entity." The NNE will evolve as warfighting objectives and missions evolve.

Technology continues to advance and new tools become available almost daily. As the tools, often referred to as Web 2.0, become mainstream, the DoD and DON are looking at ways to leverage them to break down silos of information and create an information-centric network. As part of this effort, we must also focus on ensuring that these tools are a secure addition to our network.

As a Department, we must continue to build an IM/IT governance framework that harnesses DON IT efficiencies and leverages our limited resources. As a Department, we must continue to build an IM/IT governance framework that harnesses DON IT efficiencies and leverages our limited resources. To this end, we need to maximize the value and assess the risks of IT investments by requiring a clear strategic or financial return for each IM/IT investment. The IT investment environment is outcome based, as highlighted by the Key Performance Indicators for each goal. IT approaches such as open architecture, "Green IT," virtualization, cloud computing, and telework reduce the unnecessary use of resources, creating a more streamlined approach to IM/IT investment. This includes moving from decentralized to centralized management where appropriate, thereby minimizing duplication and providing for more efficient delivery of capabilities to the warfighter. Our decision making should be architecture driven, balancing people, process, and technology as a basic function of how we do business.

The intent of this plan is to provide a long-range vision that describes desired departmental outcomes over the next four years and identifies how they will be achieved and measured. Some of the goals and efforts listed here are ongoing and have been in progress throughout previous strategic plans. As we plan for the future, it is helpful to reflect on the progress of past efforts. To that end, success stories are provided to illustrate the advancement we have made toward meeting our goals.

Executing this plan throughout the DON enterprise will strengthen alignment to IM/IT goals and help clarify resource priorities by making better informed decisions at strategic national through tactical levels. The Command Information Officer, in concert with the Command and Control, Communications and Computers Officer, and Knowledge Management Officer, serve an important role to advise on issues regarding IM and alignment of IT investments to business priorities and assigned missions. For the IM/IT workforce, this plan provides an understanding of the direction of IM/IT in the DON, and how their contributions support this broader vision. For the warfighter, this plan lays out our efforts to ensure that their jobs are made easier through the rapid, economical, and appropriate deployment of IM/IT.

Vision

A Naval warfighting team enabled with information superiority to lead and win.

Mission

Enable Decision Superiority.

Deliver secure, interoperable, and integrated IM/IT capabilities to the Sailor and Marine to support the full spectrum of warfighting and warfighting support missions.

Linking Strategy to Execution

DON IM/IT Strategic Alignment

Wars and conflicts of the 21st century are increasingly being fought using net-centric warfighting techniques requiring close integration at multiple technology levels – networking, data, applications, and infrastructure. To continue delivering and expanding our net-centric capabilities, the Department of the Navy Information Management/Information Technology and Cyberspace Strategic Plan (Strategic Plan) is aligned to and driven by the warfighting requirements outlined in the Quadrennial Defense Review Report, the Department of Defense Information Enterprise Strategic Plan, and the Secretary of the Navy Objectives, consistent with the overall management guidance in the President's Management Agenda and the 21st Century Seapower Strategy.

The Information Dominance OPNAV N2/N6 (Navy) Strategy and the Marine Corps Information Enterprise Strategy are similarly aligned to the Strategic Plan and are collectively driving the definition and rollout of key programs such as the Next Generation Enterprise Network, the DON's next-generation IM/IT infrastructure. This strategic alignment validates the vision, mission, and goals of the Strategic Plan, ensuring common goals, objectives, and performance measures. The DON's ability to continue this alignment and build upon it is critical to providing the naval warfighter with the tools needed to win. The DON NNE strategy will align to and support applicable DoD and DON guidance. The NNE will be comprised of the information, information resources, assets, and processes required to achieve an information advantage and share information across the DON and with mission partners.

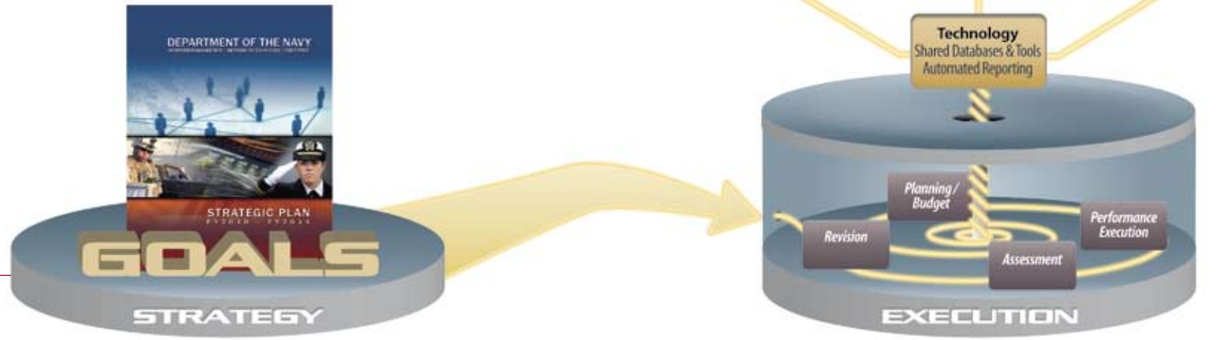
The DON Deputy Chief Information Officers (Navy and Marine Corps) will forge ahead as a team to provide the integration of net-centric warfighting capabilities with the right resourcing to achieve information dominance. Information dominance provides operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Measuring for Success

Performance management is a key part of an integrated strategic planning/performance management cycle. The DON IM/IT Performance Measurement Program is designed to bridge the gap between strategic planning and results, and help ensure the DON IM/IT organization has the tools and information required to successfully meet its goals and objectives and ultimately, deliver on its mission – to provide the warfighter with the best IM/IT capabilities possible. The NNE strategy will include alignment and interoperability of DoD and DON IT solutions, guided by strategies and enterprise architectures developed and maintained to meet specific needs.

This Strategic Plan will be measured by metrics derived from the Key Performance Indicators for each goal. The results of the metrics will be analyzed each quarter using Balanced Scorecard principles. A trend analysis will be developed annually. The results of the trend analysis will provide the tenets that will be mapped into a review of the Program Objectives Memorandum to allow leadership the visibility to continuously assess the right metrics and dynamically adjust our allocation of resources as necessary to successfully execute our mission.

Similarly, DON-wide IT governance has been aligned by establishment of IT governing bodies which inform the DON Information Executive Committee (IEC), thereby providing consistency of policy at all DON levels.



Integrate Strategic Planning and the Performance Management Cycle

Governing Principles

The Department of the Navy IM/IT team will:

- Lead and govern in an uncertain national security environment.
- Align Department-wide IM/IT efforts with Departmental priorities, goals, and objectives.
- Promote and foster a climate of transparency and openness.
- Deploy interoperable, Joint IM/IT solutions to enhance the Department's effectiveness.
- Ensure ubiquitous, secure access to information.
- Lead continuous, capability-enhanced IM/IT transformation.
- Utilize outcome-based performance measures.
- Apply continuous process improvement initiatives to improve Department efficiencies.
- Optimize information resources by maximizing return on investments, increasing efficiency, expanding the use of enterprise solutions, and measuring the contribution of IT investments to Department effectiveness.
- Adopt and share best practices.

Strategic Planning Process

In this strategic planning cycle, we continue to use the vision, mission, and goals that were developed to span the time frame from FY 2009 through FY 2016. They provide the long-term focus and direction for the DON IM/IT Investment guidance, which serves as the basis for approving the funding and procurement of all DON IM/IT initiatives. Working with the Services, the NNE Roadmap will define the specific actions and milestones that will need to be funded and implemented in each fiscal year.

The DON Strategic Plan for FY 2010-2014, specifies the objectives and sub-objectives that will be implemented for each goal during this four-year period. The Department is consistently working to define and refine performance metrics for the objectives in this plan, so that our progress can be clearly measured. The Strategic Plan also provides the methodology to move our IM/IT vision, mission, governing principles, goals, and objectives from concept to reality. From this process we have seen numerous successes during the past two fiscal years, some of which are highlighted in the success stories associated with each goal of this plan.

Goals

- Sustain and expand a secure, interoperable, and robust net-centric naval IM/IT infrastructure.
- Protect and defend our naval information, networks, and critical infrastructures to maximize mission assurance.
- Take advantage of emerging technologies to enhance mission accomplishment.
- Create, align, and share information to provide the knowledge necessary to enable effective and agile decision making and mission support.
- Ensure IM/IT investments deliver required capabilities to the Department.
- Develop a highly competent IT and cyber total force to support cyberspace responsibilities.

GOAL 1

SUSTAIN AND EXPAND A SECURE, INTEROPERABLE, & ROBUST NET-CENTRIC NAVAL IM/IT INFRASTRUCTURE

Winning our Nation's battles and succeeding in complex security environments demands we harness the power of information more effectively than our adversaries. We must ensure that our networks are robust, secure, and seamless and that they support an information environment attuned to 21st century threats and challenges.

Major General George J. Allen
Director, Command, Control, Communications, and Computers (C4) and DON Deputy CIO (Marine Corps)
January 2010

Description

We will operate, sustain, and expand our global information infrastructure to provide secure, robust, interoperable, and end-to-end connectivity to all our Sailors, Marines, and Civilians. This infrastructure's common architecture and technical standards will ensure that the naval component of the Department of Defense Global Information Grid maintains interoperability with Joint forces, allied coalitions, and interagency partners. Interoperability must also include partnerships outside the Federal Government. The Naval Networking Environment (NNE) will provide the Department of the Navy's component of the Global Information Grid. Coincident with the release of DON EA v1.0, the DON CIO also established initial formal review and approval processes for proposed EA content. These processes are intended to ensure that:

The intended use of the proposed EA content has been adequately identified. The proposed content is at an acceptable level of maturity and has been reviewed by the appropriate subject matter experts. Key executive stakeholders have agreed on the value of incorporating the proposed content into the DON EA. In addition, the DON CIO issued DON EA policy and procedures that leveraged existing IM/IT investment review processes as a mechanism for ensuring that the Department's programs, projects, initiatives, and investments comply with the requirements of the DON EA.

The DON EA with its careful tracking of DON EA compliance and waiver request metrics has resulted in an ancillary benefit of providing the DON with new insights into the quality, practicality, and successful implementation of existing policy and guidance. Expansions and refinements to the DON EA are scheduled to be released each February and July and will continue to be focused on ensuring that the Department's EA is both focused and actionable.

Objectives

1.1 Provide secure, robust, and interoperable connectivity across the Department.

1.1.1 Implement a DON IM/IT and Cyber Investment Strategy and Framework which ensures all activities align to the DON's NNE goals.

1.1.2 Develop and leverage national and international strategic partnerships to ensure naval spectrum-dependent systems and equipment have sufficient electromagnetic spectrum available for operations and training.

1.1.3 Continue IT efficiency initiatives, such as the Marine Corps' Legacy Network Consolidation efforts, the Navy's Cyber Asset Reduction and Security program, the Navy and Marine Corps Portal and Data Center Consolidation efforts, as well as enterprise-wide implementation of the Consolidated Afloat Networks and Enterprise Services (CANES) Common Computing Environment and Afloat Core Services.

1.1.4 Publish an NNE Roadmap that will guide the DON toward a future net-centric enterprise environment bound by a common enterprise architecture and standards, a common investment strategy, governance, and operational construct consistent with network operations.

1.2 As part of the DON Enterprise Architecture (EA), define, implement, and enforce a set of standards, which supports a DON-wide strategy for fielding up-to-date systems that enable net-centric operations across the NNE and within Joint and Coalition environments.

1.2.1 Leverage and align to DoD provided Enterprise Services and Joint Information Environment initiatives to the maximum extent practicable, in order to ensure consistency, interoperability, efficiency, and alignment.

1.3 Implement a DON portal strategy that consolidates and federates existing Secretary of the Navy, Navy, and Marine Corps portals and aligns with DoD portal initiatives.

1.4 Develop and promulgate the DON Net-Centric Data Services Strategy, which will outline the path ahead for identification of Authoritative Data Sources and Services, to be leveraged across the Department.

Key Performance Indicators

- Percent completion of an NNE Roadmap to guide and shape the development and prioritization of the activities required to transition to a net-centric enterprise environment.
- Percent completion of the update to the Next Generation Enterprise Network (NGEN) Enterprise Interoperability Policy, which will mandate the critical first steps required to ensure NGEN lays the foundation for the successful implementation of the NNE.
- Formalized DON EA Governance Structure to ensure authoritative architecture information supports the NNE initiative by the end of FY 2010.
- Percent completion of the plan to transition from the Navy Marine Corps Intranet (NMCI) to NGEN, and for enterprise implementation of the CANES Common Computing Environment and Afloat Core Services.
- Reduce the number of networks/points of presence within the DON NNE.

Success Stories

NMCI and ONE-NET: A Step Closer to Full Interoperability

Until recently, NMCI users traveling to overseas naval facilities have been unable to utilize the Outside Continental United States Network (ONE-NET) to remotely access NMCI services.

In 2009, engineers supporting ONE-NET from the Theater Network Operations and Security Center in Bahrain and the Space and Naval Warfare Command Systems Center Pacific, successfully launched ONE-NET – NMCI Traveler Community of Interest in Bahrain. The Community allows an NMCI laptop to plug into the ONE-NET network and reach back to NMCI resources in the Non-secure Internet Router Network (NIPRNET) enclave.

The ONE-NET program office plans to obtain the Authority to Operate and extend Traveler coverage to all 78 ONE-NET locations around the globe. The Traveler solution demonstrates ONE-NET's efforts to meet the first strategic objective of the NNE: the "ability to log on to the network and securely access data from anywhere in the NNE."

DON EA v1.0 - Focused and Actionable

In July 2009 the DON CIO published DON Enterprise Architecture (DON EA) v1.0 and began enforcing compliance with the EA as of October 2009. These events marked an initial milestone toward implementing a focused and actionable EA for the Department. Although this release of the DON EA only contained a small set of initial artifacts based on existing laws, regulations, and policy, it was nonetheless an important first step toward establishing the foundational governance, policy, and procedures necessary to ensure DON programs, projects, initiatives, and investments are aligned with and supportive of Departmental goals and objectives.

Coincident with the release of DON EA v1.0, the DON CIO also established initial formal review and approval processes for proposed EA content. These processes are intended to ensure that:

- The intended use of the proposed EA content has been adequately identified. The proposed content is at an acceptable level of maturity and has been reviewed by the appropriate subject matter experts.
- Key executive stakeholders have agreed on the value of incorporating the proposed content into the DON EA.

In addition, the DON CIO issued DON EA policy and procedures that leveraged existing IM/IT investment review processes as a mechanism for ensuring that the Department's programs, projects, initiatives, and investments comply with the requirements of the DON EA. The DON EA with its careful tracking of DON EA compliance and waiver request metrics has resulted in an ancillary benefit of providing the DON with new insights into the quality, practicality, and successful implementation of existing policy and guidance. Expansions and refinements to the DON EA are scheduled to be released each February and July and will continue to be focused on ensuring that the Department's EA is both focused and actionable.

> Our technology has improved dramatically, our platforms have gotten better and more capable in almost exponential fashion, but the thing that has improved the most, the thing that nobody can touch us on are the Sailors on the deck plate, and the Marines in the field. Nobody can build the type of force that we do.
>
> The Honorable Ray Mabus
> Secretary of the Navy
> October 2009

GOAL 2

PROTECT AND DEFEND OUR NAVAL INFORMATION, NETWORKS, & CRITICAL INFRASTRUCTURES TO MAXIMIZE MISSION ASSURANCE

Potential adversaries are working to offset our strengths and level the playing field. We can no longer afford inefficiencies incurred with stove-piped networks, systems, and processes. Unless we leap ahead to develop a rigorous and comprehensive approach to control the electromagnetic spectrum and cyberspace, we will risk losing our competitive advantage.

Vice Admiral David "Jack" Dorsett
Deputy CNO for Information Dominance (OPNAV N2/N6) and DON Deputy CIO (Navy)
May 2010

Description

We will actively defend our people, information, networks, and critical infrastructures to provide assured information delivery, system and network access, and information protection. The security and protection of our systems, networks, and information depend on the implementation of sound Information Assurance (IA) concepts and principles. To ensure the best return on investment, governance will be strengthened by providing coordinated and consistent IA policy across the Department of the Navy and fostering a culture of accountability. We will ensure safeguards are in place to protect Personally Identifiable Information (PII). Additionally, we will establish world-class network cybersecurity protocols to defeat our enemies in their attempts to access our networks. We will implement Critical Infrastructure Protection (CIP) measures, to protect our mission-critical capabilities and ensure information is available and secure. While maintaining security is vitally important, the warfighter must be able to access information securely and have a high confidence in that information. Anticipating verifiable threats, mitigating identified vulnerabilities, and employing proactive self-defense protection strategies while ensuring availability, will enable effective net-centric operations. The Naval Networking Environment (NNE) will include a set of integrated, phased programs that will transition the DON towards a future net-centric enterprise environment. It is a highly secure and reliable enterprise-wide voice, video, and data network environment that focuses on the warfighter first, providing ubiquitous access to data, services, and applications from anywhere in the world.

Additionally, we will establish world-class network cybersecurity protocols to defeat our enemies in their attempts to access our networks. We will implement Critical Infrastructure Protection (CIP) measures.

Objectives

2.1 Anticipate and prevent attacks on data and networks.

2.1.1 Ensure Secure Internet Protocol Router Network (SIPRNET) remains the Services' primary warfighting network through appropriate network operations and infrastructure upgrades.

2.1.2 Implement Non-secure Internet Protocol Router Network (NIPRNET) hardening consistent with United States Strategic Command/Joint Task Force-Global Network Operations (USSTRATCOM/JTF-GNO) goals. Specifically, implement Data at Rest (DAR) encryption for classified and unclassified networks and deploy and maintain Host Based Security Systems (HBSS).

2.2 Improve the governance of Information Assurance & Computer Network Defense (IA & CND) within the DON by clarifying the roles and responsibilities of the DON Senior Information Assurance Officer (SIAO) and DON Deputy Chief Information Officers (Navy and Marine Corps).

2.2.1 Institutionalize the DON SIAO's role in the Certification and Accreditation (C&A) processes as defined in the DON IA and C&A process.

2.2.2 Develop the security requirements for NNE to guide the investments needed for mission assurance and cybersecurity.

2.3 Safeguard the use, collection, storage, and dissemination of PII.

2.3.1 Implement a comprehensive plan to reduce significantly the number of DON personnel affected by the loss or compromise of PII to include: a reduction in the use, collection, and display of Social Security Numbers; improved privacy awareness training; implementation of data loss prevention tools; increased number of approved Privacy Impact Assessments (PIA) and System of Records Notices; and improved privacy security throughout the life cycle of all IT systems.

2.4 Improve secure, mission-driven access to DON information and services.

2.4.1 Implement a comprehensive plan to Public Key Enable all DON unclassified and classified networks, to include implementing Cryptographic Log On (CLO) for all unclassified networks; aligning with the DoD initiative to implement CLO on all classified networks; and extending Public Key Infrastructure protection capabilities to Personal Electronic Devices.

2.5 Prepare for and operate through cyberspace degradation or attacks.

2.5.1 Ensure systems and circuits are certified and accredited in accordance with the Defense Information Assurance C&A process, and reduce the number of systems and circuits obtaining a waiver for continuation of Interim Authority to Operate (IATO) for 360 consecutive days or more.

2.5.2 Improve performance on the annual C&A requirements compliance evaluation.

2.6 Improve mission assurance by strengthening CIP.

2.6.1 Conduct required vulnerability assessments on DON critical assets.

Key Performance Indicators

- Percentage of DON systems compliant with Federal Information Security Management Act standards (e.g., current ATO, security testing, and contingency plan testing).
- Percentage of systems that have completed PIAs.
- Percentage of annual infrastructure vulnerability assessments being conducted.
- Number of DAR, HBSS, CLO, and NIPRNET hardening goals completed.
- Reduce the percentage of personnel impacted by PII breaches.

Success Stories

Computer Network Defense Roadmap

In this age of network-centric warfare, computer and network technologies are diffused into virtually all military systems and interconnected military units operate cohesively. The threats posed by adversaries to this environment are advanced, persistent, and always changing. CND is essential to achieving assured networked forces, information sharing, situational awareness, speed of command, and mission effectiveness.

The DON CND Roadmap, available at www.doncio.navy.mil, covers the ongoing nature of implementing CND to meet the range of computer network threats. The roadmap shows the high-level linkage of CND strategy to operations, the alignment of CND to the naval mission, and the importance of CND from the most senior levels of leadership within the DON to the deck plate. Finally, the roadmap defines the Department's CND efforts and makes clear the strategic outcomes of these efforts.

Protecting Data at Rest

The increased use of removable storage and a more mobile workforce has contributed to an increase in identity theft activity. To remedy this situation, an enterprise DAR encryption tool is being employed that provides a first line of defense against data loss for hard drives and portable storage media.

With implementation of DAR encryption ongoing across the NMCI network, results have already been positive. When thieves stole DON laptops and external hard drives, they were unable to access much of the PII on the devices because DAR encryption software prevented it. What began as perhaps the DON's largest PII breach in 2009, ultimately affected few personnel. A Navy recruiter's laptop containing PII from civilian applicants was recently stolen from a locked government vehicle and it too, was protected by enterprise DAR encryption software. Similar incidents show that the Department's DAR encryption solution has decreased the number of DON personnel impacted by PII losses.

CIP SAT Going Purple

A Critical Infrastructure Protection (CIP) Self-Assessment Tool (SAT) was developed using the Defense Critical Information Protection benchmarks for commercial dependencies and Defense Threat Reduction Agency benchmarks for antiterrorism and force protection. CIP SAT, an interactive web-based tool, enables base commanders to assess their critical infrastructure using an automated tool and produce a thorough report of an installation's CIP posture. The report would identify vulnerabilities that could jeopardize the execution of Mission Essential Tasks, which could severely impact warfighter's mission or even result in mission failure.

The Defense Critical Infrastructure Protection Office saw the tool's potential and funded its modification for use throughout DoD. The tool was modified to accommodate all of DoD and renamed Defense CIP Self-Assessment Tool (DSAT). DSAT was accredited in March 2010. The tool is available for DoD use on the SIPRNet.

In the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace.

2010 Quadrennial Defense Review

GOAL 3

TAKE ADVANTAGE OF EMERGING TECHNOLOGIES TO ENHANCE MISSION ACCOMPLISHMENT

Emerging technology provides the lynchpin in realizing superior warfighting and business process operations. Key to rapid and agile insertion of emerging technologies to enhance mission accomplishment is rigorous up front systems engineering.

Rear Admiral Jerry K. Burrough
Chief Engineer, Space and Naval Warfare Systems Command
July 2009

Description

Emerging technologies provide a means to improve warfighting and business process operations. Just as information is power, emerging technology maintains warfighting technological superiority over its adversaries. The White House, Office of Management and Budget, Congress, Department of Defense, and Department of the Navy have set direction for improving transparency to citizens, "greening" energy use, reducing costs, and utilizing the power of the Internet and new emerging technologies (Web 2.0/3.0 and cloud computing). The DoD and DON have also set the goal of providing Joint Military Department operations and net-centricity.

The DON's Naval Networking Environment (NNE) will align our people, business processes, information architecture, and information assurance, while optimizing our IM, IT, IRM, and cyber investments in support of Navy and Marine Corps warfighting and warfighting-support missions and functions. The NNE must be capable of quickly and cost-effectively inserting new technologies to increase the IT capacity and capabilities that support the warfighter and business domains. Having such fiscal acquisition processes will enable rapid technology insertion into the NNE, which will provide commanders the flexibility needed to operate their networks as required, in the face of emerging threats and to meet mission requirements. The use of Web 2.0 tools has enabled enhanced communication and collaboration across the DON. The DON Chief Information Officer uses blogs, podcasts, wikis, and chat to communicate quickly and effectively across the Department. Other organizations are experimenting with these tools as well. The Space and Naval Warfare Command (SPAWAR) is using these tools, primarily blogs, to reduce its dependence on email and increase the penetration of information across the organization.

Objectives

3.1 Develop the NNE net-centric and data-centric strategy and architecture for global interoperability and ubiquitous access for the Navy and Marine Corps. The strategy encompasses governance, standards, architecture frameworks, and energy efficient IT optimization.

3.1.1 Develop an NNE Roadmap, which will communicate the vision and guide the development of requirements for acquisition, associated plans, policies, and processes to achieve the future naval networking vision.

3.1.2 Continue to refine DON Enterprise Architecture (EA) and data strategy, policy, and governance in support of a net-centric environment that ensures information dominance.

3.1.3 Promulgate policy to direct that all enterprise network initiatives must be interoperable within the NNE to provide rapid and seamless access to data and services across the DON.

3.1.4 Facilitate Enterprise Software Agreements with information technology providers which will incorporate emerging software licensing models such that software licensing terms and conditions are net-centric and do not restrict information sharing in support of DON, DoD, and Intelligence Community missions.

3.1.5 Encourage innovation in use of technologies to optimize operations and management of DON networks and leverage the DON and DoD Research, Development, Test and Evaluation (RDT&E) community to expedite introduction of new technologies.

3.2 Promote and foster information sharing within and across communities that is transparent, participatory, collaborative, and secure.

3.2.1 Develop an integrated strategy that uses new and emerging Web 2.0 technologies to enable more streamlined information exchange with key internal and external stakeholders in support of warfighting and warfighting-support missions and functions.

3.2.2 Identify risks and mitigation strategies to securely leverage social media technologies including Web 2.0, social networking websites, video-sharing sites, wikis, blogs, and mashups, both internal and external to the DON.

3.3 Implement a DON Electronic Stewardship Plan.

3.3.1 Integrate "Green" IT electronic stewardship to reduce the DON's carbon footprint.

3.3.2 Leverage cloud computing and virtualization to optimize IT infrastructure within the DON.

Key Performance Indicators

- Percent completion of a Stewardship plan that measures carbon footprint reduction as NNE is implemented.
- Percent completion of a DON "Green" IT Energy document that describes Web 2.0 uses, information assurance, security, and privacy risk mitigation guidelines in the NNE environment.
- Percent completion of a portfolio of net-centric Enterprise Software Agreements whose application licenses support the common software environment for the NNE, have significant usage across the DON, and enable information sharing within and across communities.

Success Stories

Consolidated Afloat Networks and Enterprise Services (CANES)

In April 2009, the Navy established an enterprise-wide policy which mandated that all IT applications and systems on Navy ships and submarines integrate within the CANES infrastructure, thereby establishing a single Common Computing Environment (CCE) and associated Afloat Core Services (ACS). In July 2009, the Navy established planning for a single Cyber Asset Reduction and Security (CARS) based process for implementing CANES, CCE, and ACS.

OGC Incorporates Web 2.0

The Office of the General Counsel's (OGC) internal collaboration site, OGConline, incorporates Web 2.0 technologies built around communities of legal practice. OGC consists of approximately 675 civilian attorneys and 25 uniformed Navy and Marine Corps Judge Advocates supported by over 200 staff members. Personnel are located throughout the Department of the Navy in the United States and overseas. OGC online is a Common Access Card restricted site limited to OGC personnel. The Web 2.0 technologies incorporated into the site include blogs, file sharing, forums, wikis, personal Facebook-like pages, avatars, customizable content, and content tagging. Hundreds of blog posts have been added to the site and over 1,000 files have been uploaded by users across the community. OGC will continue to embrace emerging technologies to ensure expert, effective, efficient, and timely legal services to the Department.

Sharing Knowledge with Web 2.0 Tools

The use of Web 2.0 tools has enabled enhanced communication and collaboration across the DON. The DON Chief Information Officer uses blogs, podcasts, wikis, and chat to communicate quickly and effectively across the Department. Other organizations are experimenting with these tools as well. The Space and Naval Warfare Command (SPAWAR) is using these tools, primarily blogs, to reduce its dependence on email and increase the penetration of information across the organization. Originally envisioned as a way for projects and management to share information, the blogs have provided payoffs far greater than anticipated. Some of SPAWAR's blog successes include:

- Sharing presentations across the organization through embedded video. A videotaped Office of the Secretary of Defense DeVenCI program office visit led to funding and technology exchanges to improve unmanned systems.
- Editing draft policy and infrastructure decisions with the help of the workforce. Through comments on blog posts, people impacted by such decisions could ask questions and help guide the policy makers.
- Publicizing project highlights across the organization. In the past, project highlights were sent in Microsoft Word documents to leadership and were unavailable to the rest of the workforce. Now posted on blogs, these highlights provide insights into projects and technologies previously unknown across SPAWAR.
- Sharing technology news from conferences to people too busy to attend. A recent keynote speech by the Chief Executive Officer of Nokia was shared with engineers at SPAWAR.

Over the past two years, the SPAWAR blogosphere has grown to more than 200 blogs which receive more than 4,000 hits a week from hundreds of unique visitors. The blogs and other Web 2.0 tools have helped shrink organizational and geographic distances within SPAWAR.

> The fact is timely access to accurate information (data in sound context) is the keystone to making sound business and warfighting decisions. And, getting connected to "the Network" provides us the ability to access and search for information that we require.
>
> Mr. Robert J. Carey
> Department of the Navy Chief Information Officer
> April 2008

GOAL 4

CREATE, ALIGN, & SHARE INFORMATION TO PROVIDE THE KNOWLEDGE NECESSARY TO ENABLE EFFECTIVE & AGILE DECISION MAKING & MISSION SUPPORT

Our brave Sailors and Marines deployed far from home in harm's way are the heart and soul of our organization. What they know and how they translate that knowledge through sound decisions into action will define how successful we will be. And so, we are committed to providing them the information and tools they need to accomplish their mission and defend the cyberspace domain in an increasingly complex technology-based environment.

Mr. Robert J. Carey
Department of the Navy Chief Information Officer
November 2009

Description

We will integrate technology and processes to effectively provide secure, assured, accurate, and timely, operationally relevant information to the warfighter and to those who support the warfighter. This rapid exchange of all source knowledge will be critical to the effective employment of our intelligence capability, battlefield awareness, insight, and weapons capabilities. Similarly, we will emphasize seamless knowledge transfer between people and applications in designing and deploying future support processes. We will move from a culture that rewards the retention of data and information to one that rewards effective knowledge stewardship. The purpose of the Naval Networking Environment (NNE) strategy will be to provide direction for future DON information technology and information management (IT/IM) capabilities and to ensure that the DON is supporting mission effectiveness and efficiency, while embracing the fact that each Service-level Component has its own unique missions. The benefits and promise of shared information and services will be realized through policies and standards that are developed and enforced in accordance with this strategy. The use of Web 2.0 tools has enabled enhanced communication and collaboration across the DON. The DON Chief Information Officer uses blogs, podcasts, wikis, and chat to communicate quickly and effectively across the Department. Other organizations are experimenting with these tools as well. The Space and Naval Warfare Command (SPAWAR) is using these tools, primarily blogs, to reduce its dependence on email and increase the penetration of information across the organization. Originally envisioned as a way for projects and management to share information. Along with required indoctrination courses, the process assists new personnel (specifically those that have not served on a staff before) with gauging their skill on the training systems and computer programs.

Objectives

4.1 Enable the Information Value Chain of identity management, information assurance, data strategies, content management, and collaboration through implementation of NNE to achieve knowledge management.

4.1.1 Prepare a Department-wide, comprehensive, standards-based content management strategy for implementation with NNE.

4.1.2 Manage records effectively and continue Department-wide implementation of Electronic Records Management (ERM).

4.1.3 Manage bandwidth constraints to support rapid knowledge exchange, particularly for tactical users.

4.2 Define the enterprise architecture and way ahead to enable net-centric information sharing to achieve Maritime Domain Awareness (MDA), in order to facilitate effective decision making for all maritime-related missions.

4.2.1 Create a "To-Be" architecture that defines systems, processes, and services to enable effective MDA.

4.2.2 Develop a migration and implementation plan to align resources and investments to achieve the MDA "To-Be" architecture.

4.3 Leverage the DON Enterprise Architecture to guide the transition to net-centricity leading to Knowledge Dominance.

4.3.1 Develop and govern a geospatial defense-wide infrastructure/framework to connect decision making across multiple domains.

4.3.2 Develop a migration and implementation plan to align resources and investments to achieve the MDA "To-Be" architecture.

4.3.3 Leverage the DON Enterprise Architecture to guide the transition to net-centricity leading to Knowledge

Key Performance Indicators

- The number of commands implementing ERM.
- Percent completion of the DON content management strategy.
- Percent completion of the national "To-Be" MDA Enterprise Architecture.

Success Stories

Paperless Command Indoctrination Process

The Center for Security Forces, Naval Amphibious Base, Little Creek, VA applied tenets of knowledge management to significantly improve the new personnel indoctrination process at headquarters and throughout 13 distributed learning sites. Online courses replaced many of the traditional indoctrination meetings. New personnel complete these courses at their pace and when it is best for their work schedule, and progress is tracked by the Executive Director and Command Master Chief.

These online courses do not replace traditional face to face meetings with key members of command leadership. They augment those meetings with customized indoctrination assistance based on individual talent levels and needs.

Along with required indoctrination courses, the process assists new personnel (specifically those that have not served on a staff before) with gauging their skill on the training systems and computer programs required of their new staff function. Often, new staff members will not openly admit that they do not understand or are not familiar with a facet of their new job. Rather than muddling along or being embarrassed, this new process allows a person to privately tutor themselves and receive support from a mentor to answer specific questions.

KM – From Concept to Practice

DON Knowledge Management (KM) has progressed from a fledgling notion to an actionable concept integral to our operations and business. The DON CIO's early KM strategy was focused on *selling* KM to the rest of the Department. Now, KM is *practiced* across the Department, with numerous commands assisting and leading the way.

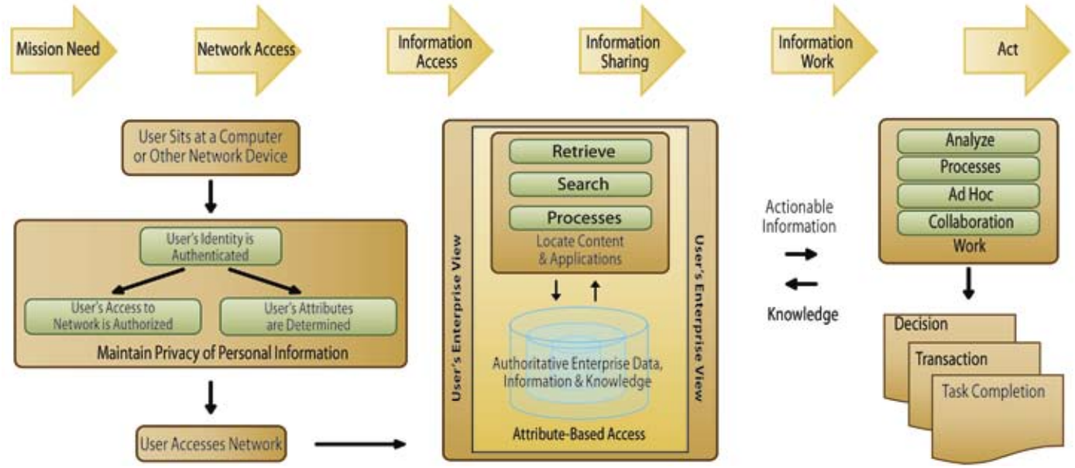
The DON CIO Command KM course is often the first resource commands use when starting a KM initiative. Since 2005, the course has been taught 23 times to over 450 students from 75 Navy, Marine Corps, Army, and Joint commands.

Annually, the DON CIO hosts two DON KM workshops, one on each coast. In 2010, more than 200 participants from over 75 commands attended. When these events began in 2006, the presentations focused on KM fundamentals. Now they are focused on actual KM experience, lessons learned, and best practices that attendees can implement at their own commands.

Tactical Training Group Pacific directly increases the effectiveness of information and knowledge flow throughout Pacific Fleet Strike Groups and provides valuable training to the Navy IT/KM workforce. Annually, the command teaches courses to over 600 students. Courses include the Afloat Knowledge Management Course, Network Centric Warfare Commanders Course, Sea Combat Commander 101, and the Joint Maritime Tactics Course.

Many commands have implemented KM programs. For example, COMPACFLT, COMSECONDFLT, and COMTHIRDFLT all have KM Officers. These commands have applied resources to reap the benefits of KM. While command KM objectives vary, they all have one thing in common; the successful teams did not implement KM for KM's sake. Rather, they applied KM processes directly to command challenges.

Information Management Value Chain



GOAL 5

ENSURE IM/IT INVESTMENTS DELIVER REQUIRED CAPABILITIES TO THE DEPARTMENT

Our IT/IM investments play a critical role in direct support of the war fighter. To ensure we are delivering on this growing set of requirements, we need to better align investment management at the DON enterprise level so we get the most efficient and effective systems possible, and at the best cost to the Department.

The Honorable Robert O. Work
Under Secretary of the Navy
December 2009

Description

We will select efficient and effective IM and IT investments based on validated user requirements. Investments will align with strategic priorities, established in Presidential, Federal, DoD, and DON guidance; align and comply with DoD and the DON Enterprise Architectures; and be interoperable within the Joint and Coalition environments. Cost visibility and uniform evaluation criteria will provide the ability to quantify the return on investment and total cost of ownership in a standard manner across all programs and investments. The Naval Networking Environment (NNE) Roadmap will identify key milestones, activities, timelines, key policies, and frameworks needed to ensure:

- Decision agility: We must be able to make decisions in near real time and adjust our network security within months, not years. IT-based opportunities will require "in-execution year" decisions. We must achieve Unity of Command/Effort and Governance to ensure that decisions are made and enforced rapidly across the enterprise.
- An aligned budget process: Today's process is inconsistent with Moore's Law and the effects of the Information Age. Our present Program Objectives Memorandum (POM) cycle, while excellent for the acquisition of ships, tanks, and planes, does not support nascent IT changes in the 21st century.
- A streamlined acquisition process: Like our budget process, today's acquisition processes best support the acquisition of aircraft and ships, but do not support IT cycle times and the realities of the cyber threats we face. The Federal Acquisition Regulation/Defense Federal Acquisition Regulation and Department of Defense 5000 series, along with the SECNAV 5000 series, allow for tailoring.

Objectives

5.1 Select the most efficient and effective IM/IT/cyber investments based on validation of user and warfighter requirements.

5.1.1 Implement a DON IT portfolio management process that provides the standards for the selection and management of IM/IT investments.

5.1.2 Continue to expand and refine the DON Enterprise Architecture (EA) in support of critical IT investment management decision making. Formalize DON EA governance, review, and a configuration management process.

5.2 Implement an enterprise-wide approach to DON IT/cyberspace investment management to optimize capabilities, operational effectiveness, and cost-efficiency. Map DON IM/IT/cybersecurity spending to mission priorities.

5.2.1 Transform DON spectrum, wireless, and telecommunications management and acquisition to centralize DON efforts, identify efficiencies, and improve performance.

5.2.2 Continue implementation of a Clinger-Cohen Act confirmation process that aligns with the Two-Pass/Six-Gate acquisition oversight process. By proactively engaging with selected DON programs, program quality, and Clinger-Cohen Act processing time will be improved.

5.2.3 Implement a DON-wide IT Asset Management (ITAM) process that builds on the Functional Area Managers governance structure, meets the ITAM requirements of the DoD, and utilizes the DON CIO Enterprise Commercial IT Strategy Team to efficiently identify and aggregate DON IT hardware and software requirements to maximize use of the IM/IT Enterprise Agreements in acquiring products and services.

5.2.4 Reduce the cost of the network as commercial off-the-shelf (COTS) capabilities increase over time. This will provide the opportunity to enhance network performance while reducing costs.

5.3 Ensure budget and acquisition processes effectively align with NNE objectives, POM cycles, and emerging Service IM/IT/cyber requirements.

5.4 Act as an advocate for change to the Financial Management Regulation (FMR), Federal Acquisition Regulation/Defense Federal Acquisition Regulation, Department of Defense 5000 series, and SECNAV 5000 series, when obstacles are encountered that create an unresponsive IT acquisition process.

Key Performance Indicators

- Processing time to align the Clinger-Cohen confirmation process with the Two Pass/Six-Gate acquisition process.
- Formalization of overarching DON EA governance process by the end of FY 2010.
- Implementation of a DON-wide ITAM process by the end of FY 2012.
- Improved alignment of available IM/IT investments with user and warfighter priorities.
- Advancement of the strategic vision for emerging spectrum technology.
- Percent completion of the new Enterprise-wide telecom and wireless policies.

Success Stories

DON Quickly Upgrades Telecommunications for Haiti

In the wake of the 2010 Haiti earthquake, over 20,000 Sailors, Marines, and Soldiers were dispatched to assist the country in dealing with its overwhelming medical and humanitarian needs. To effectively deliver this relief, access to robust telecommunications services was essential. The surviving Haitian telecommunications infrastructure could not deliver the voice and data services needed to support this major DoD effort. In addition, numerous personnel were moved to Naval Base Guantanamo Bay (GTMO) which served as a logistics hub for material, due to its close proximity.

To meet this surge of telecommunication needs, DON telecommunications experts worked to reconfigure and expand the available classified and nonclassified networks. Additional high-speed data links were brought up on GTMO to expand NIPRNET and SIPRNET access, as well as satellite communications terminals. To support voice communications on GTMO, a mobile cellular system and satellite phones were activated.

Through these efforts a dramatic increase in voice and data services was made available in a matter of days. This allowed DoD to operate a more coordinated and effective relief operation than would have been possible with the available infrastructure in Haiti.

Lean Six Sigma Project

The DON CIO executed central management of the DON Continuous Process Improvement (CPI) Software Portfolio. In doing so, the DON CIO was able to:

- Achieve a potential cost avoidance of $24M over the program life and $6M over the Future Year Defense Plan.
- Provide access and support to the CPI applications (Minitab and iGrafx) across all DON networks.
- Provide this access 90 percent faster than previously accomplished (less than 1 day versus 20 days) to the Navy Marine Corps Internet user community.
- Greatly improve clarity of software requirement and asset usage from gross estimates to automated tracking of personnel usage.
- Substantially improve contractual compliance and establish policies that identified and ameliorated many of the burdensome management processes associated with software management in the DON (security, software approval, testing, etc.).
- Establish software configuration control for minimal cost, resulting in the approximately 2,000 CPI user group using the same software version.

Students Graduate from First Spectrum Management Course Taught in Iraq

Fourteen Iraqi frequency managers graduated from a course on spectrum management taught by members of the U.S. Defense Information Systems Agency's Joint Spectrum Center. The Multi-National Security Transition Command-Iraq, Communications Directorate, taught them how to use, operate, manage, and maintain client-server hardware and software associated with a spectrum management software application provided by the Coalition to the Iraqi Government. The students will use their new knowledge and expertise in frequency management to facilitate the implementation of the security agreement between the Coalition and the Government of Iraq. A train-the-trainer component of the course was designed to hand over teaching responsibility for future courses to Iraqis. Approximately 150 Iraqi Ministry of Defense employees will receive this training over the next two years.

Every IT professional in the Navy and Marine Corps has to think of themselves as a warrior. The network is their weapon.

The Honorable Robert Work
Undersecretary of the Navy
April 2010

GOAL 6

DEVELOP A HIGHLY COMPETENT IT & CYBER TOTAL FORCE TO SUPPORT CYBERSPACE RESPONSIBILITIES

There's a lot of difference in the Navy of forty years ago that I was in and the Navy of today, but the most important difference and the biggest difference is our people. Today's Sailors and Marines are the most competent, the most professional group of men and women that the Navy and Marine Corps have ever had.

The Honorable Ray Mabus
Secretary of the Navy
January 13, 2010

Description

We will develop and execute DON IT and Cyber Total Force objectives to enable the development and sustainment of the optimum mix of competencies, proficiency, and experience required to support the full range of operations in cyberspace. Our emphasis will be to ensure that the collective capabilities of the DON Cyber/IT total workforce professionals are fully supported throughout their lifecycle and IT operations. We will strive to develop an environment that is attuned to the needs of our diverse workforce and supports a positive work life balance. As the Federal Government, DoD, and DON move forward in the cyberspace domain, and new tactics, policies, and technologies emerge, we will focus on objectives that will enable the Cyber/IT workforce to effectively execute DON missions. Through the use of smart IT, we can increase teleworking options that will empower the mobile workforce and maximize their ability to get the job done wherever they may be. Personnel recruited as six-year obligation receive "C" School (advanced skills) training as part of their initial training before transfer to their first permanent change of station (PCS). Those recruited as four-year obligations receive "A" school (basic skills) training prior to their first PCS station. IT "A" school will increase from an 11-week course to a 19-week course with labs. These Sailors will graduate with A+ Certification and Microsoft Certified Professional commercial certifications. Sailors who go right into "C" school will receive additional commercial certifications. Personnel recruited as six-year obligation receive "C" School (advanced skills) training as part of their initial training before transfer to their first permanent change of station (PCS). Those recruited as four-year obligations receive "A" school (basic skills) training prior to their first PCS station. IT "A" school will increase from an 11-week course to a 19-week course with labs.

Objectives

6.1 Provide workforce capabilities that fully support cyberspace operations.

6.1.1 Assess and establish workforce roles, responsibilities, manpower, and training requirements for DON IT unified cyberspace operations.

6.1.2 Together with DoD, Navy, and Marine Corps cyberspace leadership, track and measure the effectiveness of DON cyberspace workforce initiatives.

6.1.3 Develop policies and guidance as needed to address workforce issues.

6.2 Develop competency-based planning and management processes.

6.2.1 Provide guidance to support fundamental changes in processes and culture.

6.2.2 Implement competency development, management and usage procedures.

6.3 Support required capabilities by recruiting a qualified and experienced workforce.

6.3.1 Ensure DON IT workforce procedures take full advantage of all available Federal, DoD, and DON processes and resources.

6.3.2 Promulgate guidance regarding work place and work life balance supporting improved IT Workforce employee satisfaction.

6.4 Develop and manage the DON Cybersecurity/Information Assurance Workforce (CS/IA WF).

6.4.1 Improve identification and documentation of the CS/IA WF.

6.4.2 Improve availability and quality of required IA certification training and testing.

6.4.3 Implement CS/IA WF continuous learning requirements.

Key Performance Indicators

- Increased percentage of certified and qualified personnel in the Cybersecurity/IA workforce.
- Increased availability and use of IT workforce training opportunities.
- Increased number of workforce transitioned to competency-based recruitment, development, and promotion.
- Increased number of initiatives that strengthen career transition from uniformed to civilian service.

Success Stories

Marine Corps Communications Training Centers

With a staggering increase in cyber attacks on DoD IT systems and infrastructure, there is a critical need for knowledgeable Command, Control, Communications, and Computer (C4) personnel. MajGen George Allen, Headquarters Marine Corps, Director C4, has identified C4 training as the number one priority to aggressively attend to the cyberspace domain warfighting mission. In rapid response, the Marine Corps Training and Education Command revolutionized the way the Marine Corps trains and now commercially certifies its C4 personnel through Communication Training Centers (CTC). Co-located with all three Marine Expeditionary Forces, the CTCs provide commercial certification training and testing for active duty and reserve Marines and Civilians who are part of the C4 community, but moreover, for any Marine identified as part of the CS/IA WF.

Underway Information Assurance Training on USS Abraham Lincoln (CVN 72)

To meet DoD mandated workforce security standards, USS Lincoln's Combat Systems Information Officer and the IAWF from both the carrier and escort ships set out to determine the most effective way forward. Sailors took Security+ commercial training via three different methods: Navy e-Learning SkillSoft courses, Carnegie Mellon Virtual Training Environment to include labs and mentors, and instructor administered courses while Lincoln was on deployment. Information Systems Technician Chief Petty Officers from the Combat Systems Department administered and proctored all the commercial certification exams using the Pearson VUE electronic testing platform. Over 97 percent of the 115 member workforce were certified while underway on a seven month deployment. As the cybersecurity field rapidly evolves, being able to train and test while deployed will help the Navy achieve not only DoD IAWF requirements but also DON continuous learning requirements. While some Sailors thrive in classrooms, others do well in the e-Learning or Virtual Training Environment. According to LCDR White, "Deck plate leadership from the Chief Petty Officers, which includes training, mentoring, and motivation of the Sailors, was the key to our success."

Navy's IT of the Future

In the core Information Systems Technician rating, Sailors will experience an entirely new training path. This rating, now part of the advanced technical field, allows the Navy to recruit initial accession Sailors to both four-year and six-year obligations. Personnel recruited as six-year obligation receive "C" School (advanced skills) training as part of their initial training before transfer to their first permanent change of station (PCS). Those recruited as four-year obligations receive "A" school (basic skills) training prior to their first PCS station. IT "A" school will increase from an 11-week course to a 19-week course with labs. These Sailors will graduate with A+ Certification and Microsoft Certified Professional commercial certifications. Sailors who go right into "C" school will receive additional commercial certifications. Fleet Sailors will receive "delta" training to make sure all ITs are part of a standard workforce, and upon completion of training, will hold the new Navy Enlisted Classification with the commensurate commercial certifications. Other IT core communities, supporting the cyberspace and cybersecurity missions, will engage in new training pipelines. Examples of training path revisions are found in the Submarine Community which established a full time Local Area Network (SUBLAN) Navy Enlisted Classification to include an upgraded training path with commercial certifications, and the Information Professional Officer community which is moving to an updated curriculum with commercial certifications.

"We need men and women who by their personal integrity, their sense of moral purpose and their acceptance of the requirement for hard work will exemplify the best in the leadership traditions of the Navy and of our country. This is not `just another program.' Nor is it a project to breed unthinking conformity to a rigid set of values. It is designed to make us aware of our duties and responsibilities as leaders and to act accordingly. Through this program the already great strength of the Navy will be increased even more, and through it we will respond more effectively to the challenge which confronts our country."

Admiral Arleigh A. Burke
30 April 1964

CONTACT INFORMATION

DON Chief Information Officer
Mr. Terry Halverson ..... (703) 602-1800

DON Principal Deputy CIO
Ms. Barbara H. Hoffman ..... (703) 601-0116

DON Deputy CIO (Navy)
VADM David J. "Jack" Dorsett ..... (703) 614-0281

DON Deputy CIO (Marine Corps)
MajGen George J. Allen ..... (703) 693-3462

Departments

Clinger-Cohen Act
Confirmation and Certification ..... (703) 602-6845

Critical Infrastructure ..... (703) 602-4412

Cyber / IT Workforce ..... (703) 601 0605

Cybersecurity ..... (703) 602-4412

Emerging Technology ..... (703) 602-6800

Enterprise Architecture ..... (703) 602-6847

Enterprise Commercial IT ..... (703) 607-5658

Enterprise Networks ..... (703) 602-6800

Investment Management ..... (703) 604-7039

Information Sharing ..... (703) 607-5653

Maritime Domain Awareness ..... (703) 602-5608

Performance Measurement ..... (703) 412-4669

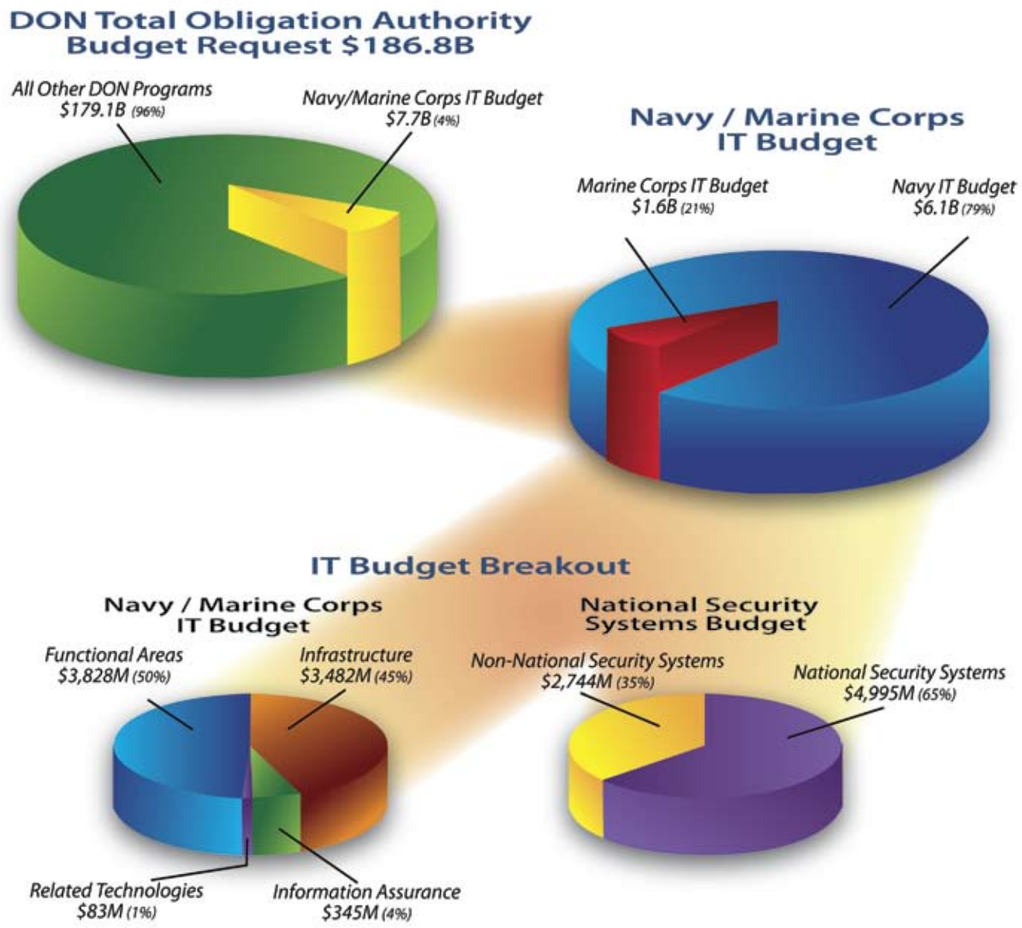
Privacy and Civil Liberties ..... (703) 601-0081

Records Management ..... (703) 607-5653

Navy and Marine Corps Liaison ..... (703) 602-6800

Telecom, Spectrum and Wireless ..... (703) 602-0427

PRESIDENT'S DON IT BUDGET REQUEST FOR FY 2011



ACRONYMS

ATO .....Authority to Operate
C&A .....Certification and Accreditation
C4.....Command, Control, Communications, and Computers
CANES .....Consolidated Afloat Networks & Enterprise Services
CARS .....Cyber Asset Reduction and Security
CCE .....Common Computing Environment
CEO .....Chief Executive Officer
CIO.....Chief Information Officer
CIP .....Critical Infrastructure Protection
CIP SAT .....Critical Infrastructure Protection Self-Assessment Tool
CLO .....Cryptographic Log On
CND .....Computer Network Defense
CPI .....Continuous Process Improvement
CS/IA WF .....Cybersecurity/Information Assurance Workforce
CTC .....Communication Training Centers
DAR .....Data at Rest
DoD.....Department of Defense
DON CIO.....Department of the Navy Chief Information Officer
DON.....Department of the Navy
EA .....Enterprise Architecture
ERM .....Electronic Records Management
HBSS .....Host Based Security System
IA .....Information Assurance
IATO .....Interim Authority to Operate
IM.....Information Management
IT.....Information Technology
ITAM .....IT Asset Management
ITMC .....IT Management Council
ITSG .....Marine Corps Information Technology Steering Group
JTF-GNO.....Joint Task Force-Global Network Operations
MCEN .....Marine Corps Enterprise Network
MDA .....Maritime Domain Awareness
NGEN .....Next Generation Enterprise Network
NIPRNET .....Non-secure Internet Protocol Router Network
NMCI .....Navy Marine Corps Intranet
NNE.....Naval Networking Environment
OCONUS .....Outside the Continental United States
OGC.....Office of the General Counsel
ONE-NET .....OCONUS Network
PCS .....Permanent Change of Station
PIA .....Privacy Impact Assessment
PII .....Personally Identifiable Information
RDT&E.....Research, Development, Test & Evaluation
SECNAV .....Secretary of the Navy
SIAO.....Senior Information Assurance Officer
SIPRNET .....Secure Internet Protocol Router Network
SPAWAR .....Space and Naval Warfare Command
SUBLAN.....Submarine Local Area Network
USSTRATCOM U.S. Strategic Command
WAN.....Wide Area Network

WHENEVER AMERICA NEEDS SOMETHING DONE, WHETHER FIGHTING OUR WARS OVERSEAS, PROVIDING A BALLISTIC MISSILE DEFENSE SHIELD, TAKING DOWN A TERRORIST CELL, DETERRING PIRATES, TRAINING PARTNERS, REASSURING ALLIES, OR PROVIDING SUPPLIES TO VICTIMS OF A NATURAL DISASTER… WHATEVER AMERICA NEEDS DONE – CALL ON THE NAVY AND MARINE CORPS.

THE NAVY AND MARINE CORPS ARE YOUR FLEXIBLE RESPONSE FORCE FOR DOING WHATEVER MISSION IS GIVEN TO THEM AND DOING THAT MISSION INCREDIBLY WELL. IT IS THESE FINE SAILORS AND MARINES STANDING IN FRONT OF YOU AND THEIR SHIPMATES ALL OVER THE WORLD WHO WILL GET THE JOB DONE, WHATEVER THE JOB IS -- FOR AMERICA.

THE HONORABLE RAY MABUS
SECRETARY OF THE NAVY
OCTOBER 26, 2009

Department of the Navy
Chief Information Officer

1000 Navy Pentagon
Washington, DC 20350-1000
www.doncio.navy.mil