



DEPARTMENT OF THE NAVY
CYBER/IT WORKFORCE
STRATEGIC PLAN FY2010 - FY2013

Foreword

This Department of the Navy (DON) Cyber/Information Technology (Cyber/IT) Workforce Strategic Plan FY 2010 – FY 2013 both reaffirms what is best about the DON Command, Control, Communications, and Computers (C4), IT, and Cybersecurity Workforce and gives us new strategic-level goals to accomplish. All of you in the Cyber/IT community have worked hard to transform the way the Navy and Marine Corps design, operate, and defend the Global Information Grid (GIG) as we fight in cyberspace. In return, you deserve strong support from your workforce and community management leadership.

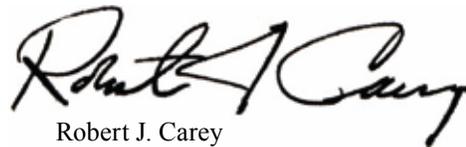
Over the past several years we have developed direction, plans, and guidance to help your command carry out its workforce planning and, more importantly, to help you achieve your career goals. We will increase our efforts to provide the best workforce planning framework to support your career goals.

Through this Cyber/IT Workforce Strategic Plan,

my office, in partnership with the Navy and Marine Corps, has defined DON goals related to the Cyber/IT Workforce for the next three years. We will use this strategic plan as a roadmap and ensure that all goals are met. You are already on the path to achieving some of them. You are making a difference to improve mission assurance, cybersecurity, and business transformation while providing leadership to the joint cyber operational community.

I never forget we are the face of 33,000 employees working in a rapidly changing world to provide the high level of IT capability our operational mission demands. Our challenges are huge but we will meet those challenges.

As we endeavor to develop the best Cyber/IT Workforce in the Department of Defense, I am proud to be working not only with your commanders, but also with you, the Cyber/IT professional, to provide direction that will enable you to define your individual career goals.



Robert J. Carey
Department of the Navy
Chief Information Officer
Cyber/IT Workforce Community Leader

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

~Mr. Robert Work, Under Secretary of the Navy

Introduction

The Department of the Navy Cyber/Information Technology (Cyber/IT) Workforce Strategic Plan is the workforce planning alignment keystone for IT and Command, Control, Communications, and Computers (C4) community managers. This plan aligns with our objective to develop a highly competent Cyber/IT Total Force that is capable of implementing, integrating, securing, and executing sustained operations across the full cyberspace domain.

Workforce planning and strategic alignment are important to the success of the workforce. Proper planning helps ensure that each professional has the tools and capabilities needed to be an effective cyber warfighter, sustain a robust capability in cyberspace, and achieve enterprise business objectives within the Naval Networking Environment. Strategic alignment helps to ensure consistency across the Department and helps with the creation of common goals and objectives.

The DON's emphasis on workforce planning has evolved to meet today's workplace challenges. During the past few years the Department has:

- Operated under the initial DON Information Management/Information Technology (IM/IT) Workforce Strategic Plan, which defined a systematic approach to IM/IT Workforce planning;
- Developed a yearly IT Workforce goal for the DON IT Strategic Plan to ensure workforce alignment across the Department;
- Established a DON IT Integrated Process Team (IPT) focused on supporting the DON Cyber/IT Workforce and ensuring enterprise consistency and solutions;
- Instituted a Cybersecurity/Information Assurance Workforce Management, Oversight, and Compliance Council (IAWF MOCC) to support Command Information Officers, IA Managers and ensure compliance with IA workforce policies and guidance;
- Published the National Security Personnel System

It is the fundamental responsibility of our government to address strategic vulnerabilities in cyberspace and ensure that the United States and the world realize the full potential of the information technology revolution. The status quo is no longer acceptable. The United States must signal to the world that it is serious about addressing this challenge (cybersecurity) with strong leadership and vision.

-Cyberspace Policy Review

(NSPS) position description guidance for the 2210 (IT Specialist) and 1550 (Computer Scientist) occupational series;

- Led civilian IT competency development, now accepted as standard across the Department; and
- Under DoD leadership, joined forces with other Services in a comprehensive cybersecurity initiative to determine relevant workforce competencies.

DON Cyber/IT Workforce goals and objectives enable standards to be developed to sustain the optimum mix of competencies, proficiency, and experience required. We will support an environment that is attuned to the needs of our diverse workforce and 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 continue to focus on objectives that will enable the Cyber/IT Workforce to effectively execute DON missions.

Purpose

This plan provides further direction for, and definition of, the DON Information Management/Information Technology/Cyberspace Strategic Plan FY2010 – FY2014, Goal 6: “Develop a Highly Competent IT and Cyber Total Force to Support Cyberspace Responsibilities.”

This plan establishes the DON's priorities for ensuring workforce excellence. It identifies the goals and objectives that will allow the DON to recruit, manage, develop, sustain, and retain a workforce engaged in network operations, information assurance, information management, information warfare, and computer network defense, as well as a workforce involved in the design, development, and implementation of IT National Security and business systems and programs.

This plan provides a roadmap for the DON for the next three years. Manpower, Personnel, Training, and Readiness staffs note that today's Cyber/IT Workforce will be different from the Cyber/IT Workforce of the future.

Vision & Scope

The DON vision is to develop a Cyber/IT Workforce that can ensure the warfighter's freedom of action in cyberspace, where:

- DON missions and operations continue under any cyber situation or condition.
- The Department has ready access to its information and command and control channels, and its adversaries do not.

DON Cyber/IT challenges are not restricted to just IT business practices, cybersecurity, or mission and personnel readiness. There are many obstacles to realizing and sustaining this vision, among them:

- Significant and talented adversaries that are more networked and decentralized;
- Cybersecurity threats and attacks that have become constant;
- Non-secure legacy systems and networks;
- Constantly changing technology;

- The “flash to bang” speed of technology;
- Evolving IT/cybersecurity mission requirements;
- Non-traditional and emergent training requirements; and
- Cross-functional community collaboration.

IT Workforce Goals

To meet the requirements of the cyberspace domain, a highly educated, skilled, and fungible workforce is an advantage to our leadership. As the face of IT and cyber evolves, shaping a workforce involves defining the required education and competencies to support the mission, goals, and changing environment of the organization.

Metrics are an important aspect of community management. Community managers should collect workforce metrics to ensure demographic distribution, diversity, geographic location, grade levels, competencies, and skills are visible to Cyber/IT leadership and manpower analysts to ensure a healthy and appropriately dispersed workforce is in place.

The goals are designed to focus our efforts and provide the framework for effective IT workforce human capital planning. DON Cyber/IT Workforce Goals are:

- **Goal 1:** Provide workforce capabilities that fully support cyberspace operations.
- **Goal 2:** Develop competency-based planning and management processes.
- **Goal 3:** Support required capabilities by recruiting a qualified and experienced workforce.
- **Goal 4:** Develop and manage the DON Cybersecurity/Information Assurance Workforce.

As we progress toward the future we will strive to implement our goals and objectives as expressed throughout this document.

Cyberspace: Warfighting Domain



The President’s Comprehensive National Cybersecurity Initiative (CNCI), along with the Defense Department’s cyber realignment, impact the structure and required capabilities of our cyber workforce. The country, as a whole, must establish and maintain cybersecurity awareness and digital literacy. Military strategists advise that powerful and often asymmetric advantages can be derived from “information dominance”- that is, the unfettered control and access to information, along with the ability to control and directly manipulate an adversary’s information.

The *National Military Strategy for Cyberspace Operations*, a comprehensive plan to ensure U.S. military superiority in cyberspace, includes fundamental and enabling strategies to achieve our DON Cyber/IT Workforce goals. The future DON Cyber/IT Workforce must be able to meet the strategic imperatives outlined in concepts of: offensive/defensive operations, integration, information sharing, ability to operate through degradation, responsive and flexible command relationships, and unified command and control.

Defining the Cyber/IT Workforce

Cyberspace is a decentralized domain typified by increasing global connectivity, ubiquity, and mobility, where power can be wielded remotely, instantaneously, and inexpensively. The rules of the game are fluid, and the adversaries remain cloaked in anonymity. In this ambiguous war, the actual threat is unpredictable or sometimes indecipherable, and it is difficult to tell whether either side is gaining ground.

Amid the flurry of technological advancement, the Department seeks cyberspace capabilities that maintain our freedom of action and that of our allies and partners, while ensuring superiority over potential adversaries in militarily-relevant portions of the domain. This environment presents enormous challenges and unprecedented opportunities to the DON Cyber/IT Workforce.

The graphic in Figure 1 depicts the entire range of cyber work. It is imperative that we develop aligned and specific workforce roles for the entire Cyber/IT Workforce. This plan primarily addresses the goals and objectives of the Cyber/IT Workforce engaged in the circles represented by Network Operations/Information Assurance and Cyber/IT Management functions. Computer Network Operations and Law Enforcement/Counter Terrorism are outside the scope of this strategy.

Due to the nature of daily tasks, individuals may move in and out of specific mission areas. However, personnel who are either part of the Cyber/IT Workforce, full- or part-time, will be considered in the DON Chief Information Office (CIO) workforce planning methodology. The DON Cyber/IT population is

We will not defeat our cyber adversaries because they are weakening, we will defeat them by becoming collectively stronger, through stronger technology, a stronger cadre of security professionals, and stronger partnerships

~ Howard Schmidt
National Cybersecurity Coordinator

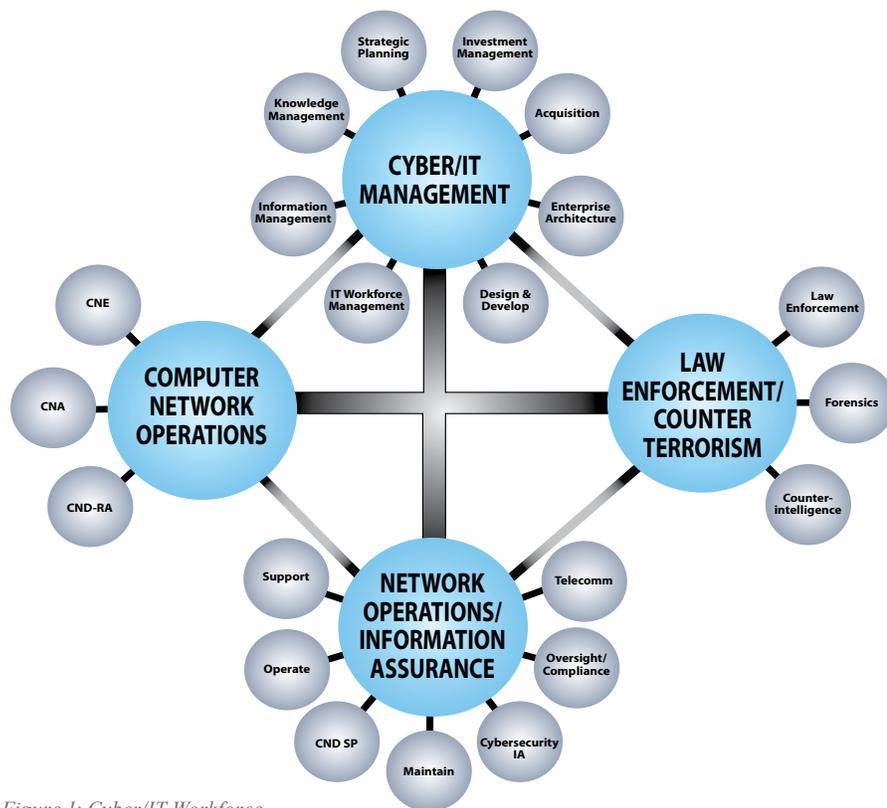


Figure 1: Cyber/IT Workforce

defined as those employees who carry out work on a daily basis that falls into one or more of the following areas:

- **Manage:** Functions that concern overseeing a program or other aspects of a cyber, security, or technical program at a high level and ensuring its currency with changing risk and threat.
- **Design:** Functions that concern scoping a Cyber/IT program or developing procedures and processes that guide work execution at the program and/or system level.
- **Implement:** Functions that concern putting Cyber/IT programs, processes, or policy into action within an organization, either at the program or system level.
- **Evaluate:** Functions that concern assessing the effectiveness of a cyber program, policy, or process in achieving its objectives.

The workforce is further broken down into three categories depending on the amount of time spent carrying out information tasks. The three groupings are defined as:

- **Core Cyber/IT Professionals:** Those personnel who are responsible for providing cyber capabilities needed across the DON. They require specialized and concentrated competencies, reinforced with foundational and continual training and education.
 - **Expert Users:** Those employed in jobs for which they require an increased knowledge of the cyberspace domain and cyber warfighting mission. Their required level of IT expertise is specifically associated with the jobs they need to accomplish.
 - **Information System Users:** Those who require foun-

dational IT skills, including the use of word processing, e-mail, on-line research tools, web, and decision making aids. For these individuals — who include virtually every member of the DON — IT is a tool required to execute their primary jobs. Note: this group is not part of the Cyber/IT Workforce.

Strategic Guidance and Alignment

Statutory and regulatory authorities (see Appendix D) established the position of Agency CIO and assigned specific roles, authorities, and responsibilities to the CIO. Under these authorities, the DON CIO issues workforce policy and guidance as necessary to ensure the Department has well-trained, highly qualified Cyber/IT professionals who create, support, and defend the Department’s information advantage. The DON CIO works in strategic partnership with key stakeholders throughout the IT Community as well as other communities (e.g., Human Capital, Acquisition, the Joint Chiefs of Staff, the Military Departments, and Defense Department) and other

federal agencies, including the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), and the Federal CIO Council, to address current and emerging skill and technological requirements.

The leadership guidance regarding workforce management will continue to evolve as the career path and training solutions change to meet cyberspace operational, IT warfighter, and business missions. OPM, DoD, and DON human capital strategies must complement and reinforce cyber total force management direction and policy. The DON CIO sits on the Federal and DoD CIO Councils and will continue to represent the Navy and Marine Corps operational and business requirements to these higher level organizations. At the same time, the DON CIO is a conduit to transmit the guidance of these organizations to the DON, Navy, and Marine Corps. Rapid and effective understanding of the guidance provided by these organizations is critical to workforce and Departmental missions.

The importance of effective workforce planning, programming, budgeting, and execution is evident in the constant struggle for personnel and funding. The opportunities and constraints outlined in law and policies, including the impacts of the Quadrennial Defense Review (QDR), require workforce

The opening rounds of the next war will be in cyberspace - the Navy must be ready to prevent wars as well as win them; to that, we must understand how we will live, operate, and win in cyberspace.

*- ADM Gary Roughead
Chief of Naval Operations*

plans to be linked to missions, goals, and objectives.

The OPM *Human Capital Assessment and Accountability Framework* and the associated *Standards for Success* provide guidance to agencies for the achievement of human capital objectives. This framework will serve as a roadmap in our efforts to evaluate our current workforce and in conducting future workforce requirements analysis and planning.

Workforce Demographics

The current DON civilian Cyber/IT Community is made up of 13 occupational series. Two of the series are currently designated as DoD Mission Critical Occupations (MCOs); they are IT Management (series 2210) and Computer Scientist (series 1550). MCOs within other communities include series that have an IT component; they are Computer Engineer (series 0854) and Electronics Engineer (series 0855). Information Assurance (IA), which is part of the larger IT community, crosses series boundaries and is a critical functional area. There are approximately 12,407 civilians in the Cyber/IT community (USN: 10,608, USMC: 1,799). The military Cyber/IT Community has approximately 21,695 members (USN: 13,997, USMC: 7,698).

Significant demographic changes are shaping the size and availability of talent. Our workforce is becoming more diverse, and those just entering the workforce have never known a time without the Internet. Both digital natives (those immersed in IT from the beginning) and digital immigrants (those who were not) will play a major role in the future of the DoD. Meeting the expectations of such a wide range of individuals will be challenging. The DON must be able to attract and retain a committed and capable workforce during an era in which the United States workforce is aging and private industry job markets are shifting.

As baby boomers continue to comprise the largest segment

of the workforce, the DON must continue to utilize recruiting and retention incentives for the subsequent generations. An antiquated qualification and hiring process will not suffice for young workers. Additionally, ineffective and cumbersome pay, assessment, development, and promotion processes will not serve the Federal Government workforce any better.

Demographic trends show that issues such as an aging workforce, diversity, and lengthy recruitment processes for entry level personnel continue to be significant factors in supplying the human capital and talent needed to reach our strategic goals. We continue to emphasize the need for workforce planning, particularly succession planning, and knowledge transfer as methods to address potential talent and experience deficits.

The Cyber Initiative — with its resultant workplace shift — will be felt across the workforce and will shape the future. When coupled with the additional impacts of new technologies resulting from Global Information Grid (GIG) efforts, technology evolution, and the increased collaborative environment in which the workforce will operate, it becomes evident that significant policy and process changes will be required. As the DON transforms into a net-centric enterprise environment, we must increase the ability of our forces by qualifying them to meet operational requirements.

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

~ DepSecDef Memorandum
"The Definition of Cyberspace"



The Work People Do

Our Cyber/IT personnel are involved in the engineering, design, development, installation, operation, servicing, and restoration of computer networks, systems and applications. Our personnel continuously work to protect DON information systems and information from unauthorized access, disruption, destruction and denial of service.

This workforce integrates directly with the personnel responsible for those activities that seek to disrupt, deny availability and/or destroy opposition information systems and capabilities. They also interact directly with law enforcement and counterintelligence personnel to ensure the security of information systems and information while fully supporting enforcement of applicable law and statute addressing unauthorized access, or attempted unauthorized access, to information systems.

The Cyber/IT Workforce works on the following networks. The Navy Marine Corps Intranet (NMCI) provides roughly 650,000 Navy and Marine Corps user accounts servicing over 3,000 locations across the continental United States, Hawaii, Cuba, Guam, Japan, and Puerto Rico. This network is designed to provide secure, universal access to integrated voice, video, and data communications and a common computing environment across the DON.

Outside the Continental United States the OCONUS Navy Enterprise Network (ONE-NET) provides roughly 41,000 users at shore installations overseas a single integrated network with a full range of services, and a centralized control authority.

For the afloat forces, the Information Technology for the 21st Century (IT-21), to be replaced by the Consolidated Afloat Networks and Enterprise Services (CANES) effort, is a portfolio of acquisition programs that provides networking capabilities to the fleet.

The Marine Corps Enterprise Network (MCEN) is comprised of the garrison network (both NMCI and Legacy), deployed/tactical networks, garrison communications capabilities, and infrastructure that supports Marine Corps operational and business IT requirements.

Collaboration: The Future

While technology has enabled an increased agility that the DON must continue to improve upon, use of collaboration technology must be tempered by the need for security. Web 2.0 technologies are useful, yet the risks they pose to our networks can be very serious. Web 2.0 security processes and tools will be required to ensure the availability and confidentiality of our systems.

The largest areas of emphasis for the DON workforce will be cyber and collaborative environments. As Cyber/IT professionals operate and collaborate with professionals in the areas of Computer Network Defense Response Action (CND RA), Computer Network Attack (CNA), and Computer Network Exploit (CNE), new operational constructs will evolve. Collaboration technologies will affect both how we operate the networks and how we go about our business and development of new technologies.



Table 1: DON Civilian Cyber/IT Community

Series	USN	USMC
2210 – IT Specialist	6,688	1,354
1550 – Computer Scientist	2,734	45
0332 – Computer Operator	50	55
0335 – Computer Clerk and Assistant	207	20
0390 – Telecommunications Processor	54	17
0391 – Telecommunications	586	126
0392 – General Telecommunications	47	9
0394 – Communications Clerical	15	5
1410 – Librarian	94	32
1411 – Library Technician	214	125
1412 – Technical Information Services	62	11
1420 – Archivist	12	N/A
1421 – Archivist Technician	5	N/A

Note: Marine Corps numbers include non-appropriated fund (NAF) personnel. The series 1420 and 1421 are not considered part of the Marine Corps Cyber/IT community.

Table 2: DON Military Cyber/IT Community

Rank	USN	USMC
Officers	1,842	1,091
Enlisted	12,155	6,607

Education Trends for the Future IT Workforce

In the economy of the 21st century, the skills, training, and workforce preparation of our people are key factors in the Department's ability to maintain its competitive edge. The transition to a knowledge-based economy continues to fuel demand for well-educated workers. Maintaining a highly skilled workforce will be a key component of a competitive advantage in the federal workforce.

The Cyber/IT Workforce must constantly upgrade its skills and have the ability to adapt to changing technology and product demands through the development of a work culture that emphasizes lifelong learning. Education and training must become part of a process that continues well past initial entry into the military or civilian workforce. This need for continuous training poses challenges to organizations and workers. Employers and workers must adopt a more integrated approach to work and training. Technology-assisted/virtual learning — as part of a “blended solution” — offers the potential to support lifelong learning both on the job and through traditional public and private education.

As demand for IT skills and resources increases, many IT occupations will be at the leading edge of job growth, both in terms of demand for specific occupations, as well as sheer volume. The structure of the DON's mission has been shifting to an increased focus on the protection of military information and assets and the importance of technology to support the warfighter. This change in mission is also causing a shift in the occupational structure of the Department's cyber workforce and represents a growing need for more IT personnel with technical and business skills as well as oversight, command, and control skills to support future DoD networked missions. Employment opportunities are increasing faster in IT occupations, particularly at the mid to senior levels. The need for people with more in-depth skills is growing faster than the available talent pool.

Whether training is achieved during on- or off-duty hours, those desiring to design, manage, operate, and defend our cyberspace must gain technical expertise. Future technical degree requirements will predominately include the computer science, computer engineering, computer information systems, cybersecurity, and information science fields of study. Continuous learning will remain a crucial requirement for all IT positions.

While there is an increased demand for employees with bachelor's degrees, an expected 11.2 percent shortfall industry-wide is expected, which means there will be almost 98,000 fewer IT graduates than needed. If engineering degrees are excluded

As one of the Nation's leading employers, the Federal Government is in need of highly skilled individuals to meet agency staffing needs and to support mission objectives. Our veterans, who have benefited from training and development during their military service, possess a wide variety of skills and experiences, as well as the motivation for public service, that will help fulfill Federal agencies' staffing needs.

— Mr. Barack Obama
President of the United States

Our ability to support the warfighter through the defense and management of our networks is a direct result of an agile, talented, and dedicated Cyber/IT Workforce.

— Mr. Robert J. Carey
Department of the Navy CIO

from the estimate of available IT graduates, the gap increases to 20.5 percent, or a shortfall of almost 179,000 individuals industry-wide. Additionally, the DoD requirement for security clearances further reduces the available pool of candidates, necessitating continuous focus on growing the IT professional talent pool. The bright spot on the recruitment scene is that veterans with Cyber/IT skills will continue to form an available talent pool.

Given the rapid pace of technology change, academia is not producing the number of science, technology, engineering, and mathematics graduates with the requisite skills needed for entry-level IT positions within the DON. We expect some new college graduates will possess skills in critical emerging areas, such as Cybersecurity, IT Project Management, and Computer Networking, when they graduate. However, there is a growing need for these new hires to enter the workforce prepared not only with strong IT skills, but also with business skills. Most new hires receive minimal exposure to these skills as part of their current college IT curriculums. To offset the skills shortfall, the DON must provide job specific training and advanced degree opportunities to new hires. This additional education and training helps to close the skill gaps and provides new hires with the necessary IT and business skills needed to effectively support mission-critical situations. Additionally, commands must provide new employee orientation initiatives and on-the-job-training to help new hires assimilate into the DON culture. These educational and training activities can be costly and time-consuming but are necessary investments to develop a highly skilled and agile IT workforce.





Competing for Talent

The DON must compete with the rest of the Federal Government and the private sector for highly skilled technical talent that holds the necessary Cyber/IT competencies it needs to complete its mission.

Generally and not surprisingly, some of the most highly sought-after skills within the DON are those that involve information/data architecture and cybersecurity. Additionally, knowledge of government practices and procedures along with possession of a valid security clearance are characteristics highly sought after across both the public and private sector.

The Department of Labor (DOL) has analyzed occupations across industry and developed detailed statistics for future projection of occupational information until 2016. According to DOL projections, the greatest percentage of new IT job growth will be in network systems/data communications analysts and computer applications/software engineers. New job creation is being influenced by changing technologies and the increasing demand for security of data and systems as well as the growing need for collaborating, working in a networked mobile environment, adopting new technologies, integrating systems, and developing and maintaining secure software and systems, all of which will drive the demand for IT professionals.

Several occupations in high-demand — Database Administrators, Computer Systems Analysts, Computer Support Specialists, and System Administrators — align to the 2210 series. Computer Science and Computer Software Engineering professions will also continue to be in high-demand, given the increasing need to develop and test software for the Internet and mobile devices as well as the need to safeguard software, pre-

empt attacks, and ensure availability, integrity, authentication, confidentiality, and non-repudiation of mission critical systems. To meet the need for occupations in high-demand, the DON needs to identify primary skill gaps, determine which jobs are priority, and develop recruitment and retention strategies. Within these occupations, both technical and business skills are needed for the future.

By strategically managing the workforce, collaborating with local personnel resource managers, and focusing on our people, DON leadership works to improve performance, enhance accountability, and provide the best work environment for our people.

The DON Cyber/IT Workforce Strategic Plan is important to the success of the workforce. It details the strategy to develop a highly competent Cyber/IT Total Force that is capable of implementing, integrating, securing, and executing sustained operations across the full cyberspace domain. The following goals represent the enterprise vision for workforce management.

As DON workforce planners, we are concerned about our technological capacity if recent trends are not reversed. We believe the demand for Cyber graduates and experienced IT employees will continue to increase as the focus on secure systems and mobile, pervasive computing heightens. We'll continue to address the need to develop a skilled workforce talent pool to support the future networked mission.

-Mr. Chris Kelsall, Director of Cyber/IT Workforce

Goal 1

Provide Workforce Capabilities that Fully Support Cyberspace Operations

Description

Identify evolving training, education, and certification requirements and maximize learning opportunities for the workforce.

Objectives

- 1.1 Assess and establish workforce roles, responsibilities, manpower and training requirements for DON IT unified cyberspace operations.
- 1.2 Together with DoD, Navy, and Marine Corps cyberspace leadership, track and measure the effectiveness of DON cyberspace workforce initiatives.
- 1.3 Develop policies and guidance as needed to address workforce issues.

Priority Areas to Expand, Improve, or Capitalize

IT Job Shadow Day: For the past few years, the DON has participated in an agency-wide IT Job Shadow Day program. This day-long event provides high school students an opportunity to learn about the work of federal IT professionals and allows the CIO the opportunity to solicit their interest in a federal IT career.

Internships: Several commands have established internship programs for high school and college students, and other commands are exploring the possibility of establishing internship programs.

Outreach: Efforts are underway to promote more outreach and coordination with academia to address skill gaps and develop competency frameworks for critical IT functions that are linked into the recruitment process.

Governance: CIO governance roles and responsibilities related to the operational mission and workforce areas are un-

der constant study and will evolve to meet the new cyberspace domain.

Innovative Practices and Solutions: A diverse and geographically dispersed workforce is engaged, innovative, and collaborative. Flexible and productive work arrangements are supported in our work environments. The future will require this trend to continue.

Successful Workforce Management Initiatives

Senior Professional Educational Offerings: Naval Postgraduate School (NPS) offers advanced educational programs in the area of software engineering and computer engineering that cater to the unique needs of the DON. The NPS degree programs include master's and doctoral degree programs in computer and software engineering. The software engineering master's program is tailored to provide the skills needed to plan, design, and implement large-scale software-intensive systems using the best available science and technology. A master's degree in computer science is also offered at the university with a software engineering track. The NPS doctorate-level software engineering program is the oldest in North America, and an initiative is underway to use its curricula as a model for industry and academia software engineering programs.

Operational Leadership Cyberspace Training: The DON developed a Flag and Senior Executive Service (SES) course titled "Decision Superiority in Cyberspace." The course educates Flag/SES level personnel on the importance of IT systems to the operation of the naval force, how they affect their commands, the fundamentals of an IT network, threats and risks to our systems and information and how to defend against them, current and future systems and technologies, and current governance structures for the IT in the Department.



Goal 2

Develop Competency-Based Planning and Management Processes

Description

Transition the civilian IT workforce to a formalized Functional Community Management (FCM) framework. Implement and manage the development and use of standardized and validated competencies within the IT community.

Objectives

- 2.1 Provide guidance to support fundamental changes in processes and culture.
- 2.2 Implement competency development, management, and usage procedures.

Priority Areas to Expand, Improve, or Capitalize

Career Paths: Total Force FCM provides comprehensive identification, planning, assessment, and reporting capabilities that support mission readiness. Creating and supporting vibrant career and professional development opportunities attracts new members to the workforce and keeps current personnel mission-ready. Human capital planning will support community management through defined career path guidance.

Business Acumen: As the focus has shifted to align IT priorities to mission capabilities, so has the thinking on the right competency mix for information professionals. The need to integrate technology into business processes has created a greater desire for business acumen and interpersonal skills combined with expected technical skills.

In-sourcing: Public Law No. 110-181, added a new section to Title 10, United States Code, “Guidelines on In-sourcing New and Contracted-Out Functions.” The law requires DoD to issue guidelines and procedures to ensure that special consideration is given to using DoD civilian employees. In “Guidance for Determining Manpower Mix,” commands determine the

appropriate mix of military, civilian, and private sector support, including guidance for risk assessments to be used when identifying and justifying activities that are inherently governmental functions or commercial activities. The shift toward in-sourcing is attributed to a need for government personnel to be sufficiently involved in oversight and control of government operations to mitigate risk.

Expeditionary Requirements: In conjunction with another DoD initiative to make the total force more agile, DoD, DON, and the other services, are examining the role civilian personnel should play in expeditionary support. The Civilian Expeditionary Workforce (CEW) is “a ready, trained, and cleared workforce for rapid response and quick assimilation into new environments” to support a variety of operational, humanitarian, and civilian affairs missions, as well as to backfill deployed DoD civilians. FCMs validate requirements and maintain and report to the commands on both individual employee and functional community readiness. While Component Human Resources offices would be responsible for managing the recruitment and staffing of positions identified as expeditionary, the FCMs coordinate on sourcing requirements. DON CIO, as the IT FCM, is responsible for management and oversight of the IT CEW.

Successful Workforce Management Initiatives

Competency Development: The DON workforce management team engaged with Navy and Marine Corps civilian personnel management to develop IT competency requirements. Strong foundational competencies such as communication and leadership are becoming increasingly important for IT professionals. Looking forward, the DON will continue to seek IT professionals who understand business fundamentals and are able to collaborate and work with individuals at all levels throughout the Department, from end-users, to engineers, to executives. The most sought-after information management and technical professionals understand how technology works and possess the competencies listed in the competency continuum listed in Figure 2 below.



Figure 2 – Competency Continuum

Note: Appendix A describes some of the high-level IT competencies required for our civilian workforce.

Goal 3

Support Required Capabilities by Recruiting a Qualified and Experienced Workforce

Description

Develop and oversee implementation of policy and processes that support disciplined workforce management through effective workforce identification, recruiting, sustainment, development, retention, and planning.

Objectives

- 3.1 Ensure DON IT Workforce procedures take full advantage of all available Federal, DoD, and DON processes and resources.
- 3.2 Promulgate guidance regarding workplace and work-life balance supporting improved IT workforce employee satisfaction.

Priority Areas to Expand, Improve, or Capitalize

Workforce Management Structures: DON organizations are establishing workforce management teams to examine current and future workforce requirements to ensure successful transition to the cyber mission. Improving workforce planning and management by identifying, coding, and tracking the force levels and competency requirements of today's Cyber/IT Workforce and forecasting these same requirements for the "workforce of the future" is labor-intensive, but necessary to create and sustain a total force solution able to meet current and surge defense requirements.

Recruitment Strategies: Recruitment strategies include a number of actions that have been ongoing over the past several years, such as career fairs, executive recruitment searches, scholarship programs, assistance with hiring/interview teams for agency positions, telecommuting, and tuition assistance guidelines.

Employing the IT Net Generation: The *DoD CIO Net*

Generation: Preparing for Change in the Federal Information Technology Workforce identified the need for a significant cultural shift to attract and retain younger workers. Within the workplace, the Net Generation wants flexibility in work hours, pay for performance, the ability to have their voices heard, continual performance feedback, and access to advanced technology and social networking applications.

Wounded Warrior: The Veterans Individual Training Assistant Link (VITAL) is a special program developed by the Commander, Navy Installations Command (CNIC). The program is designed to help wounded, severely ill, and injured Marines, Sailors, and other Service members recovering in the care of military treatment facilities (MTF). It assists in transition from a military career into the Federal Civil Service for employment within the Navy Installations Command's IT Services department (Code N6).

Diversity Initiatives: Value and integrate diversity into workforce planning.

Successful Workforce Management Initiatives

IT Careers Web Site: The DON staff developed a new career web site (www.donhr.navy.mil/ITCareers) that seeks to attract applicants (particularly those in the younger generation) through a branding strategy. The site provides information on opportunities throughout the U.S. and around the world to pursue careers at the cutting edge of technology and business management.

Position Descriptions: The DON staff published Position Descriptions (PD) that were used as templates. Supervisors were encouraged to use these formatted PDs and adapt them as necessary to specific job functions to ensure all Cyber/IT personnel understand the full scope of their responsibilities.



Goal 4

Develop & Manage the DON Cybersecurity/ Information Assurance Workforce (CS/IA WF)

Description

Empower the CS/IA Workforce through full integration of cybersecurity tactics into cyberspace operations.

Objectives

- 4.1 Improve identification and documentation of CS/IA Workforce.
- 4.2 Improve availability and quality of required IA certification training and testing.
- 4.3 Implement CS/IA Workforce continuous learning requirements.

Priority Areas to Expand, Improve, or Capitalize

Sustained CS/IA Workforce Management: CS/IA leadership established workforce tracking systems to collect IA Workforce metrics on any given day. The need to update the electronic systems to ensure data validity will be constant.

Continuous Learning: Commercial certifications are the required baseline knowledge and/or skill for a CS/IA professional. Continuous learning must become a way of life. As time and funding permit, there are several initiatives to enhance cybersecurity education, training, and exercise of knowledge and skills for DON cybersecurity personnel.

Cybersecurity/IA Identification & Training: Because CS/IA work is performed in many different positions and places throughout the DON, it is not easy to identify the work by looking solely at job titles or organization charts. Therefore, DON CIO workforce managers are working with domestic law enforcement and counterintelligence cybersecurity workforce managers to determine where competencies and training may align to reduce overall service training cost and eliminate redundancy.

Exercises: The application of Systems Administration Simulators Toolkit (SAST) to create realistic and secure environments for training and exercises will rapidly build cybersecurity experience and reinforce learning without disrupting live networks.

Scholarships: The DoD CIO established the Information Assurance Scholarship Program (IASP) to assist in recruiting and retaining highly qualified personnel in IT/IA fields like software engineering to meet DoD's IT requirements for war-fighting and security of its infrastructure. The IASP retention program enables current DON civilian and military personnel to attend school either full- or part-time to earn degrees. Master's and doctoral programs are available through the Naval Postgraduate School (NPS), the Air Force Institute of Technology (AFIT), and the Information Resources Management Col-

lege (IRMC), in cooperation with 27 IASP partner universities across the country.

Successful Workforce Management Initiatives

Navy Credentialing Opportunities On-Line: The Navy's Credentials Program Office developed the Navy Credentialing Opportunities On-Line (COOL) to define commercial certifications which best map to Navy ratings, jobs, designators, and collateral duties. Among other things, it outlines the path, work, training, and experience required to progress in the Cybersecurity/IA Workforce.

DON Cybersecurity/Information Assurance Workforce Management Oversight and Compliance Council (CS/IAWF MOCC) : The CS/IAWF MOCC meets on a regular basis to ensure implementation of workforce requirements. Implementation of the enterprise workforce vision is illustrated in Figure 3 below.

1 Professionals Knowledgeable & Skilled...

- Completed background investigation
- Understand IA responsibilities
- Prepared to apply IA to their jobs roles

2 Jobs Identified/Filled...

- IA positions identified
- Positions filled with qualified IA personnel
- New jobs resourced through POM cycle

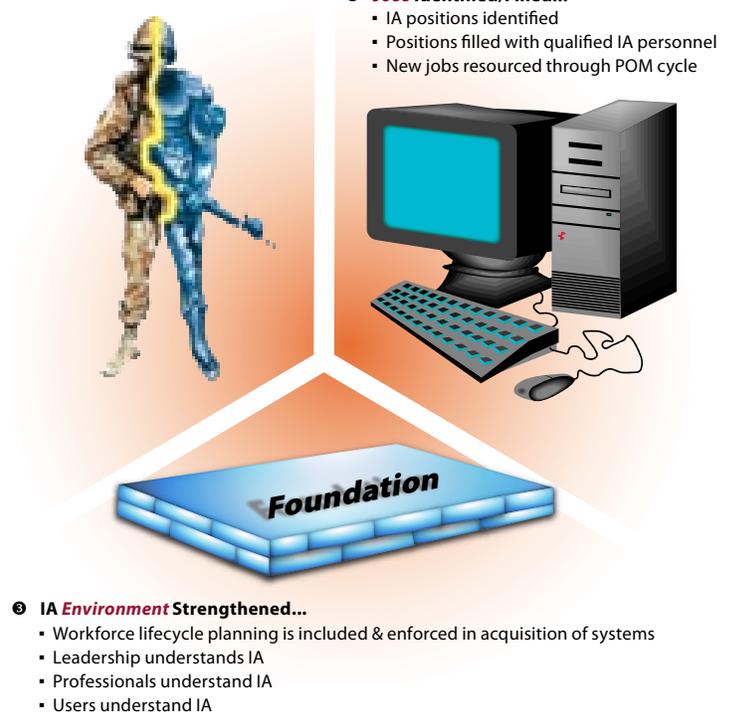


Figure 3 - Cybersecurity Workforce Vision

Appendix A

DON 2210 Competencies

Competency	Definition
Application/ System Reengineering	Transform applications and systems to utilize current technologies and methodologies to meet new business and regulatory requirements.
Capital Planning and Investment Control	Manage the process and information required to make sound investment decisions that support organizational mission.
Data Management	Manage plans, policies, programs, and processes to enhance the value of data and information assets.
Enterprise Architecture	Develop and manage the enterprise structural framework to align IT strategy, plans, and systems with the missions, goals, and processes of the organization.
Information Assurance	Protect and defend information and information systems in order to ensure accessibility, confidentiality, validity, integrity, authentication, availability, and non-repudiation.
Information Resources Management	Develop strategy and plans for management of IT resources in order to enable organizational missions.
IT Policy and Planning	Develop and promulgate IT strategy, policy, guidance, and plans to ensure consistency and compliance.
IT Project Management	Execute an IT project from initiation to sustainment to fulfill established requirements that meet specified business missions.
IT Business Process Reengineering	Redesign business processes or supporting IT to improve warfighter capabilities and support systems.
IT Capacity Management	Ensure that IT capacity meets current and future business requirements and performance metrics.
IT Configuration Management	Maintain inventory and change control supporting process improvement.
IT Customer Support	Provide functional and technical support to customers to ensure delivery of IT capabilities.
IT Forensics Operations	Process and analyze evidence found in Information Technology assets to support investigations.

Competency	Definition
IT Hardware Management	Ensure hardware meets system requirements in order to provide IT capabilities.
IT Knowledge Management	Create organizational efficiencies through collaboration and knowledge sharing derived from intellectual assets and processes. Integrate and display information from disparate sources to aid the decision making process.
IT Life Cycle Management	Manage the life cycle of information systems and services to ensure IT capabilities meet current and future organizational missions.
IT Operational Performance Measurement and Management	Conduct periodic performance assessments to ensure that IT activities, processes, or components are achieving desired results.
IT Software Development	Develop software solutions which provide integrated Information Management and IT capabilities to meet specified warfighter and business requirements.
IT Specifications Analysis	Define the IT specifications needed to execute tasks to support end user functional requirements.
IT System Design	Design software, hardware, and technology architectures that optimize users' performance to accomplish required business outcomes.
IT Systems Analysis	Measure and identify the effectiveness of IT products and services to maximize the performance of related systems.
IT Systems Integration	Link discreet computing subsystems and software applications in order to deliver IT services.
IT Test and Evaluation	Test and evaluate IT technologies during development and acquisition to ensure internal and external requirements are met.
Network Management	Organize and direct the operation, administration, maintenance, and provisioning of networked systems in order to ensure availability and integrity of information.
System Administration	Direct and control IT Systems to ensure effective system operation.
Technical Documentation Development	Develop and revise technical and operational documentation to support software installation operations, security, and maintenance.

Appendix B

Glossary

Civilian Expeditionary Workforce (CEW): A ready, trained, and cleared workforce for rapid response and quick assimilation into new environments to support a variety of operational, humanitarian, and civilian affairs missions.

Competency: An observable, measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics needed to perform work roles or occupational functions successfully.

Community: A subset of the organization's workforce, grouped from the highest organizational perspective by similarity of occupation, competencies, and career experience. The purpose of communities is to cultivate and manage a set of skills in the workforce, across the programs, lines of business, departments, or lower level organizational units.

Community Leader: A senior leader who represents and provides guidance for the community at the Chief of Naval Operations (CNO) or the Commandant of the Marine Corps (CMC) levels. Depending on the community, there may be a Civilian Community Leader at the DON level, in addition to those at each service.

Community of Interest: A collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and therefore must have shared vocabulary for the information exchanges.

Community Program Manager: A senior action officer within the service component, who acts as an advocate for the community and serves as the execution arm of the Community Leader.

Computer Network Defense (CND) Response Actions (RAs): CND RAs are deliberate, authorized defensive measures or activities that protect and defend DoD computer systems and networks under attack or targeted for attack by adversary computer systems/networks. RAs extend DoD's layered defense-in-depth capabilities and increase DoD's ability to withstand adversary attacks. (Chairman of the Joint Chiefs of Staff Instruction 6510.01E August 2008, Page GL-7)

Computer Network Attack (CNA): Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 3-13)

Computer Network Defense (CND): Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks. (JP 6-0)

Computer Network Defense Service Provider (CND-SP): Functional work area that is comprised of CND-SP Analyst (CND-A), CND-SP Infrastructure Support (CND-IS), CND-SP Incident Responder (CND-IR), CND-SP Auditor (CND-AU), and CND-SP Manager (CND-SPM).

Computer Network Exploit (CNE): Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. (JP 6-0)

Computer Network Operations (CNO): The set of offensive and defensive tactics, techniques, and procedures used by the U.S. military to achieve information dominance in the digital realm.

Cyber/IT Workforce: Military and government civilians who plan, budget, manipulate, control and archive information throughout its life cycle; develop, acquire, implement, evaluate, maintain and retire information, information systems and IT; develop the necessary policies and procedures; and apply measures that protect and defend information and information systems.

Cyberspace: A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (DepSecDef Memorandum "The Definition of Cyberspace," 12 May 2008)

Cyberspace Operations: The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. (CJCS Memo 19 Aug 2009)

Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation. (National Security Presidential Directive 54/Homeland Security Presidential Directive 23)

Cybersecurity Workforce (CSWF): A) IT Infrastructure, Operations, Maintenance and IA: Personnel who have significant responsibilities for designing, operating, or maintaining the security of Federal IT infrastructures, systems, applications, and networks. This CSWF area includes individuals who have responsibility for maintaining the confidentiality, integrity, and availability of the information contained in and

transmitted from those systems and networks; B) Domestic Law Enforcement and Counterintelligence: Personnel who analyze cyber events and environments to investigate potential threats or those individuals who participate in law enforcement, counterintelligence, and other types of investigatory activities involving IT systems, networks, and or digital evidence; and C) Specialized CS Operations: Personnel who are engaged in highly specialized CS operations or those personnel charged with CND Response Actions and Network Attack Sensing and Warning. (OPN memo of November 2009, Information Request for Cybersecurity Competency Models)

Department of the Navy Chief Information Officer (DON CIO): Federal Chief Information Officers were mandated by the Clinger-Cohen Act of 1996 to address information management and information technology at the enterprise level. The Secretary of the Navy established the office of the Department of the Navy Chief Information Officer in 1997 to provide top-level advocacy in the development and use of IM/IT and to create a unified IM/IT vision for the Department. The DON CIO develops strategies, policies, plans, architectures, standards, and guidance, and provides process transformation support for the entire Department of the Navy. Additionally, the DON CIO ensures that the development and acquisition of IT systems are interoperable and consistent with the Department's objectives and vision.

Global Information Grid (GIG): The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network. (DoD Directive 8000.01 March 2009)

Information Assurance (IA): Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DoD Directive 8500.1E Certified Current April 23, 2007, E2.1.17)

Information Assurance Workforce (IAWF): The IAWF includes but is not limited to; uniformed military, civilian, or contractor personnel with privileged access, system administrators, system architects, system engineers, computer network defense service providers, certifying agents and their subordinates, red team, blue teams, green teams, and IA managers who perform the responsibilities or functions described in DoD 8570.01-M, "Information Assurance Workforce Improvement Program," 19 Dec 2005 and SECNAV 5239.2-M, "DON Information Assurance (IA) Workforce Management Manual to Support the IA Workforce Improvement Program," 29 May 2009. These indi-

viduals are considered to have significant "security responsibilities" and must receive specialized training and be reported.

Information Assurance Scholarship Program (IASP): The Information Assurance Scholarship Program, authorized by Chapter 112, Title 10, United States Code, is designed to assist in recruiting and retaining highly qualified personnel in the field of Information Assurance (IA) to meet the DoD's IT requirements for national defense and the security of its information infrastructure.

Information Assurance Workforce Management Oversight and Compliance Council (IAWF MOCC): DON enterprise oversight council instituted in support of federal and DoD direction to strengthen the CS/IAWF using methodologies compliant with FISMA, DoDD 8570.01-M and SECNAV M-5239.2. (SECNAV INST 5239.20, "Department of the Navy Cybersecurity/Information Assurance Workforce Management, Oversight, and Compliance", 17 June 2010)

Information Management: The function of managing an organization's information resources by the handling of knowledge acquired by one or many different individuals and organizations in a way that optimizes access by all who have a share in that knowledge or a right to that knowledge (Joint Publication 1-02 DoD Dictionary of Military Terms, pg 260; JP 3-0)

Information Operations: The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. Also called IO. See also computer network operations; electronic warfare; military deception; operations security; psychological operations. (Joint Publication 1-02 DoD Dictionary of Military Terms, pg 260; JP 3-13)

Information Superiority: The 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. (Joint Publication 1-02 DoD Dictionary of Military Terms, pg 261) See also information operations. (JP 3-13)

Information System: The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. (Joint Publication 1-02 DoD Dictionary of Military Terms, pg 261) See also information; information operations. (JP 3-13)

Job Analysis: The process of identifying and defining, at an appropriate level of detail, the basic duties and responsibilities of a job in terms of both job tasks and employee competencies needed to perform those duties and responsibilities. The competencies derived from the job analysis must be relevant or demonstrate a linkage to the tasks or duties of the job.

Mission Critical Occupations: Occupations that are core to the Department's mission imperatives and without which the success of mission execution would be jeopardized.

Net Generation: This group is also known as the Millennial Generation or Generation Y. This generation includes people born between 1978 and 1994. Characteristics of the generation vary by region, depending on social and economic conditions. However, it is generally marked by an increased use and familiarity with communications, media, and digital technologies.

Network Operations: An organizational and procedural framework intended to provide DoD information systems and computer network owners the means to manage their systems and networks. This framework allows IS and computer network owners to effectively execute their mission priorities, support DoD missions, and maintain the IS and computer networks. The framework integrates the mission areas of network management, information dissemination management, and information assurance. (DoD 8570.01-M Chg 1 May 2008, AP1.21)

Non-Appropriated Fund Personnel: Employees that are paid from funds that are not appropriated by Congress. DoD non-appropriated fund (NAF) employees work in military exchanges and morale, welfare, and recreation programs.

Systems Administration Simulators Toolkit (SAST): The SAST is used to develop simulated environmental variables, and synchronous and asynchronous network attacks. It supports the IA Range, which provides a non-production, operationally realistic environment reflective of GIG IA/CND capabilities and network services found at the NetOps Tier 1-3 levels for cyber exercises, Computer Network Defense Service Provider (CNDSP) training, and integration test and evaluation.

Appendix C

Acronyms

AFIT	Air Force Institute of Technology	IA	Information Assurance
C4.....	Command, Control, Communications, and Computers	IASP.....	Information Assurance Scholarship Program
CANES	Consolidated Afloat Networks and Enterprise Services	IAWF MOCC.....	Information Assurance Workforce Management Oversight and Compliance Council
CEW.....	Civilian Expeditionary Workforce	IM/IT	Information Management/Information Technology
CL	Community Leader	IPT	Integrated Process Team
CMC.....	Commandant of the Marine Corps	IRM.....	Information Resources Management
CNA	Computer Network Attack	IRMC	Information Resources Management College
CNCI.....	Comprehensive National Cyber Initiative	IT-21	Information Technology for the 21st Century
CND.....	Computer Network Defense	MCEN.....	Marine Corps Enterprise Network
CND RA	Computer Network Defense Response Action	MCO	Mission Critical Occupations
CNDSP.....	Computer Network Defense Service Provider	NAF	Non-Appropriated Fund
CNE	Computer Network Exploit	NMCI.....	Navy Marine Corps Intranet
CNIC.....	Commander, Navy Installations Command	NPS	Naval Postgraduate School
CNO	Computer Network Operations	OCONUS	Outside the Continental United States
COOL.....	Navy Credentialing Opportunities On-Line	ONE-NET	OCONUS Navy Enterprise Network
CFCM	Component Functional Community Manager	OMB	Office of Management and Budget
Cyber/IT.....	Cyber/Information Technology	OPM.....	Office of Personnel Management
CS/IA	Cybersecurity/Information Assurance	OSD.....	Office of the Secretary of Defense
DISA	Defense Information Systems Agency	PD.....	Position Description
DoD.....	Department of Defense	QDR	Quadrennial Defense Review
DOL	Department of Labor	SAST.....	Systems Administration Simulators Toolkit
DON CIO	Department of the Navy Chief Information Office	SES.....	Senior Executive Service
FCM.....	Functional Community Management	USMC	United States Marine Corps
GIG.....	Global Information Grid	WF	Workforce
HR.....	Human Resources	VITAL	Veterans Individual Training Assistant Link

Appendix D

Legislative Foundation

Laws

- *Federal Information Security Management Act of 2002*, Title III of E-Government Act of 2002 (PL 107-347), 17 Dec 2002
- *Clinger-Cohen Act*, 40 USC 11315
- *Paperwork Reduction Act*, 44 USC 3506
- *E-Government Act*, 44 USC 3501, Section 209, Federal IT Workforce Development
- *Information Assurance Scholarship Program (IASP)*, 10 USC 2200 *et seq.*
- *Code of Federal Regulations*, Title 5, Chapter I, Part 930, Subpart C, Section 930.301

Executive Branch Regulations

- OMB Circular A-130, *Management of Federal Information Resources*
- OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*

DoD Directives & Instructions

- DoDD 8500.1, *Information Assurance (IA)*, 24 Oct 2002
- DoDI 8500.2, *Information Assurance (IA) Implementation*, 6 Feb 2003
- DoDD 8570.1, *Information Assurance Training, Certification, and Workforce Management*, 15 August 2004
- DoDD O-8530.1, *Computer Network Defense (CND)*, 8 January 2001
- *Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy*, August 2009

DON Memorandums

- DON memorandum to CNO and CMC, "Designation of the Department of the Navy Deputy Chief Information Officer (Navy) and the Department of the Navy Deputy Chief Information Officer (Marine Corps)," 22 Aug 2005

PHOTO CREDITS

U.S. Navy photos by: Mr. John F. Williams; Lance Cpl. Joel Abshier; MC3 Brooks B. Patton; MC3 David A. Brandenburg; MC3 James R. McGury; MC2 Ace Rheaume; MC2 Kiho Park; MC1 Michael W. Pendergrass; MC Leonard Adams;
Additional photos provided by: Naval Air Systems Command & ©Fotolia.com