

Department of Defense

CYBER OPERATIONS PERSONNEL REPORT



April 2011

**Report to the Congressional Defense Committees
As Required by Public Law 111-84**

Contents

1. Composition of the DoD Cyber Operations Workforce	2
1.1 Dynamic Structural Change within the Department.....	2
1.2 Changing Work Roles and Occupations within the IT/Cybersecurity Community.....	3
1.3 FY09 Cyber Operations Workforce.....	3
1.4 Sufficiency and Balance in the Cyber Operations Workforce	5
1.5 The State of Cyber Operations Personnel Outside of DoD	7
2. Career Progression and Professional Development	10
2.1 Occupational Fields.....	10
2.2 Career Paths	14
2.3 Training and Development	18
3. Recruitment and Retention	25
3.1 Civilian Recruitment Authorities and Incentives	26
3.2 Civilian Retention Incentives	31
3.3 Military Recruitment Incentives	34
3.4 Military Retention Incentives	36
3.5 Recruiting and Retention Standards and Measures	37
3.6 Recruiting and Retention Challenges	37
4. Academic and Cyber Outreach	41
4.1 DoD IT/Cybersecurity Academic Outreach Programs	41
4.2 Maximizing Collaboration to Develop a Skilled IT/Cybersecurity Workforce	45
4.3 New Initiatives Underway to Develop and Attract Future Cyber Warriors.....	50

5. Creating New Public/Private Initiatives	52
5.1 Enhancing DoD’s Certification Programs	52
5.2 Forging New Relationships to Strengthen Cybersecurity Capabilities.....	53
5.3 Exploring Rotational Assignments with Public/Private Organizations	54
6. The Way Ahead	56
6.1 Recruiting and Retention Authorities.....	56
6.2 Compensation	59
6.3 Training Improvements.....	59
Appendix A – Cyber Operations-related Military Occupations	61
Appendix B – Commercial Certifications Supporting the DoD Information Assurance Workforce Improvement Program	65
Appendix C – Military Services Training and Development.....	66
Appendix D: Geographic Location of National Centers of Academic Excellence in Information Assurance.....	79

Introduction

Section 934 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2010 (Public Law 111-84), provided for the Secretary of Defense to submit a report to the congressional defense committees that includes a study on the recruitment, retention, and career progression of military and civilian cyber operations personnel. The NDAA directed that the analysis address the sufficiency of the numbers and types of personnel available for cyber operations, including an assessment of the balance between military and civilian positions and the availability of personnel with expertise in matters related to cyber operations from outside of the Department of Defense (DoD); the definition and coherence of career fields for both members of the Armed Forces and civilian employees, including the sufficiency of training and experience levels required, and measures to improve them if necessary; the types of recruitment and retention incentives available to members of the Armed Forces and civilian employees; identification of legal, policy, or administrative impediments to attracting and retaining cyber operations personnel; DoD standards for measuring effectiveness at recruiting, retaining, and ensuring an adequate career progression for cyber operations personnel; the effectiveness of educational and outreach activities used to attract, retain, and reward cyber operations personnel, including how to expand outreach to academic institutions and improve coordination with other civilian agencies and industrial partners; the management of educational and outreach activities used to attract, retain, and reward cyber operations personnel, such as the National Centers of Academic Excellence in Information Assurance Education; efforts to establish public-private partnerships with respect to cyber-related training; and recommendations for legislative changes necessary to increase the availability of cyber operations personnel. The NDAA defined “cyber operations personnel” as members of the Armed Forces and civilian employees of the DoD involved with the operations and maintenance of a computer network connected to the global information grid (GIG), as well as offensive, defensive, and exploitation functions of such a network.

A Department-wide data call to address the requirements of the congressional reporting requirement was launched on July 28, 2010 by the Office of the Under Secretary of Defense for Personnel and Readiness (OUSD(P&R)), as the lead organization responsible for compiling the report, in conjunction with the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO), the Under Secretary of Defense for Intelligence (USD(I)), and the Office of the Under Secretary of Defense for Policy. The DoD Components have responded and this report reflects the summary analysis of their responses.

The cyber operations workforce is essential to the Department’s mission and we appreciate the opportunity to report on the Department’s needs and progress in this area. This report discusses the Department’s operations and maintenance (O&M), defensive operations and information assurance (IA) workforce.

1. Composition of the DoD Cyber Operations Workforce

“Although it is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air and space. There is no exaggerating our dependence on DoD’s information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field. 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.”

Department of Defense Quadrennial Defense Review Report, February 2010

This report is focused on FY09 Department of Defense Cyber Operations personnel, with duties and responsibilities as defined in Section 934 of the Fiscal Year (FY) 2010 National Defense Authorization Act (NDAA). It should be understood that during the writing of this report, the Department has, and continues to institute, dynamic force structure changes within the Information Technology (IT)/Cybersecurity (IT/Cybersecurity) environment which impact the description, identification and development of the military and DoD civilian personnel supporting DoD’s cyber operations. The Office of the Secretary of Defense, the Joint Staff, Combatant Commanders and the Military Services all acknowledge that as the cyber domain matures to address current and emerging threats, the workforce roles will also evolve to position the Department with address the continuing evolving threats and missions of the Department.

1.1 Dynamic Structural Change within the Department

In the past decade, cyber threats to U.S. National Security have grown exponentially. They are unremitting and when successful, have the capability to do significant damage to both the defense and public digital infrastructure. In response to this rapidly escalating threat, on June 23, 2009, the Secretary of Defense directed the Commander of U.S. Strategic Command to establish the U.S. Cyber Command (USCYBERCOM) as a subordinate sub-unified command charged with integrated cyber defense operations across the military. The USCYBERCOM is responsible for cyberspace operations in support of full spectrum operations to ensure U.S. and allied freedom of action in cyberspace, and to deny the same to adversaries. Each of the Military Services has established corresponding Service Elements which include the Army Forces Cyber Command (ARFORCYBER); the 24th U.S. Air Force; the Navy’s Fleet Cyber Command (FLTCYBERCOM); and Marine Forces Cyber Command (MARFORCYBER). While these organizations are the structural arm for the cyber warfare domain, the cyber operations workforce is deployed throughout the Department, represented within all three Military Departments and throughout the Defense Agencies and Field Activities. Active Duty, Reserve and National Guard military personnel, DoD civilians, and an extensive contractor workforce all perform critical IT/Cybersecurity roles.

1.2 Changing Work Roles and Occupations within the IT/Cybersecurity Community

As the Department focuses its energies on refining and implementing its cyber mission, it has the opportunity to define and shape the occupational fields and competencies that support this important segment within both the public and private sector IT environment. Currently, the application of definitive terms and roles (e.g., cyber or cyberspace workforce, cyber operations, cyber defense, and cybersecurity) are often interpreted and integrated differently.

The process of defining the world of work for a particular occupation or area of specialization requires adherence to proven standards and protocols in keeping with both defense and federal prescriptive job analysis procedures. The DoD, as the largest single employer of IT/Cybersecurity talent within the Federal Government, often assumes a leading role in the identification and development of initiatives impacting the human capital management of, and professional development for, the IT/Cybersecurity community. These initiatives may be DoD-wide, such as the multi-year effort to identify, train and certify the military, DoD civilian and contractor workforce performing IA functions for the Department; or may impact a single occupation, such as acting as the proponent for the federal initiative to identify and describe the competencies for a new Enterprise Architecture occupational specialty title within the IT Management civilian job series.

The Department is currently engaged in efforts within DoD to refine IT/Cybersecurity workforce definitions, and at the federal level via the Federal Chief Information Officers (CIO) Council with a goal to identify the relevant occupations, skill sets and challenges associated with a multi-discipline IT/Cybersecurity workforce. Additionally, in its role as IT Functional Community Manager, responsible for IT and IA personnel, and with shared responsibility for cyber personnel (due to overlapping functional areas), the DoD CIO has undertaken a high priority project to identify enterprise-wide competencies for specific mission critical occupations. The first initiative is identifying competencies for select specialties within the IT Management, or 2210 series, which will support piloting a new DoD-wide Enterprise Competency Management System. Further, there is an effort underway, associated with the National Initiative on Cybersecurity Education (NICE), that the Office of Personnel Management (OPM) is leading to develop a competency model and classification standards for cybersecurity personnel. To support this ongoing OPM project, the DoD CIO and the Department of Homeland Security (DHS) led a federal-wide Cybersecurity Workforce Transformation Working Group in 2010 to identify cybersecurity competencies and tasks. These efforts, as well as other ongoing activities, will ensure consistency of purpose and end products in shaping the IT/Cybersecurity workforce communities.

1.3 FY09 Cyber Operations Workforce

In preparing this report, each reporting Component was required to align its FY09 baseline workforce against a framework of workforce functions to comply with the main structural

elements described in the FY10 NDAA: operations and maintenance of a computer network connected to the Global Information Grid, defensive operations, and offensive/exploitation operations. Recognizing that there are numerous cross cutting cyber disciplines, Components were asked both to describe cyber and cyber-related occupations and to align their military and civilian personnel to the prescribed definitions for reporting purposes. Additionally, as information assurance (IA) is also a critical cyber operation skill, Components were asked to provide the number of personnel performing IA functions full-time, i.e., as their occupation for inclusion in this report.

For this section of the report, the DoD Components reported a total of 163,144 military and civilian personnel within the cyber operations workforce for FY09. The majority of these individuals, 145,437 (almost 89%), were engaged in operations and maintenance (O&M) functions. Defensive operations personnel accounted for the smallest segment of the workforce, with only 3,777 individuals (2%) identified as performing those functions, and another 13,910 individuals were identified with a primary occupation of information assurance. The IA numbers reported are significantly lower than the 46,203 DoD IA personnel included in the FY09 Federal Information Security Management Act (FISMA) report.

The differing numbers are explained by the more inclusive IA workforce definition established by the Departmental issuance, DoD 8570.01-M, "Information Assurance Workforce Improvement Program." By DoD policy, all personnel performing IA functions are included within the IA workforce and must achieve specific training and certification qualifications; many of these IA personnel perform additional work functions such as Systems Administration, Customer Support and Network Services (which are included in the Operations and Maintenance workforce numbers included in this report). As the Congressional Cyber Operations Report data call required organizations to identify their employees as a member of only one group (to avoid double counting people), those performing work across multiple disciplines were often grouped as O&M personnel. Figure 1.1 summarizes the Departmental view of the FY09 Cyber Operations workforce.

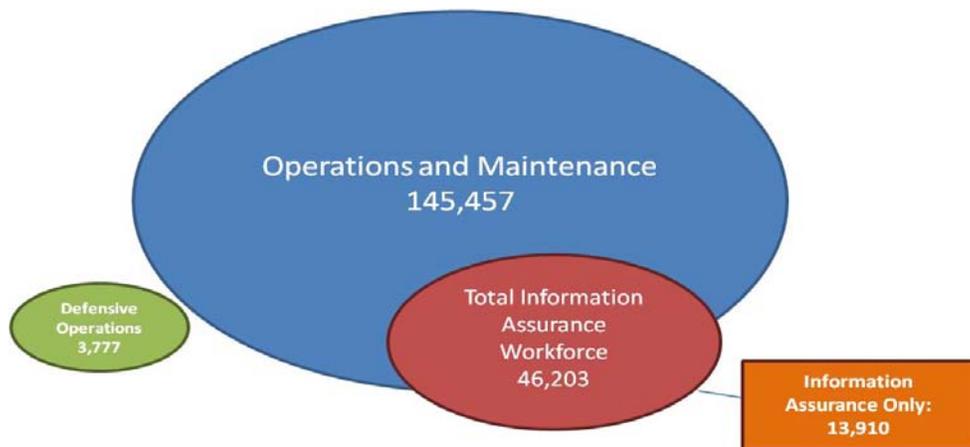


Figure 1.1 FY09 Cyber Operations Workforce

Military Active, Reserve and Guard personnel comprised 83% of the cyber operations workforce numbers reported by the Components, with enlisted personnel making up the largest segment of the workforce, as shown in Figure 1.2 below. Military officers made up the smallest segment of each functional area, while DoD civilian personnel made up the largest segment (61%) of individuals performing defensive operations functions.

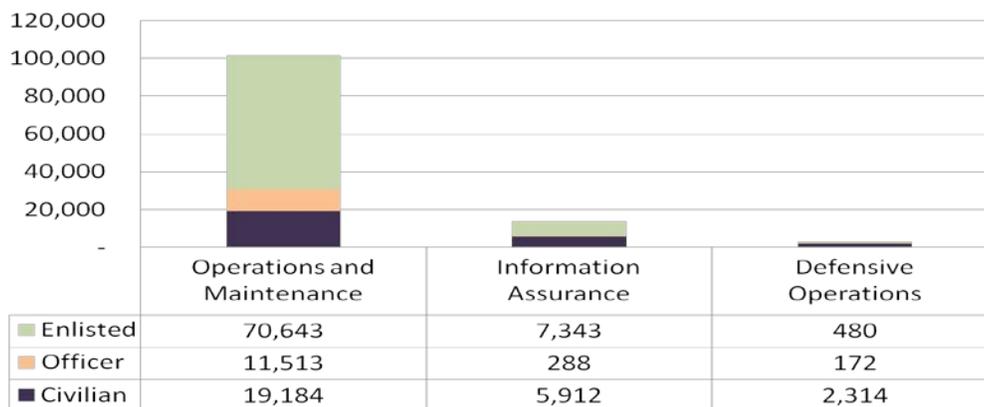


Figure 1.2 FY09 Cyber Operations Personnel by Workforce Category¹

Preparing a response for this Congressional report, as well as participating in other ongoing workforce reviews within the Department, has resulted in increased dialogue regarding the IT/Cybersecurity workforce. The intra-Department dialogue is ongoing and will continue as the cyber domain matures. The Components are continuing to work the long-term effort of identifying and refining the occupations and the number of individuals performing select IT/Cybersecurity functions since cyber operations is a cross-cutting mission area supported by many disciplines. The majority of cyber operations personnel currently falls within traditional IT career fields and perform traditional IT functions.

1.4 Sufficiency and Balance in the Cyber Operations Workforce

In support of this report, all Components were queried as to the sufficiency of their personnel numbers. They indicated specific areas of undermanning and an overarching sense that as the USCYBERCOM and supporting Service Element organizations are matured, additional force structure changes will be required. The Army reported insufficient personnel within the Army Intelligence and Security Command (INSCOM) and is working on a plan to grow capacity in FY12 and beyond. Additionally, they cited concerns that personnel strength was insufficient when INFOCON is raised². The Marine Corps noted gaps in cyber planners, source analysts focusing on the cyberspace domain and mid-level, certified IA technical managers. The Joint Staff and five of

¹ In the FY09 FISMA Report, there were a total of 14,838 DoD civilian, 31,365 military and 19,318 contractor personnel included in DoD's IA population as defined by DoD 8570.01-M.

² INFOCON is the Information Operations condition; it is a system used to reflect changes in malicious internet activity and the possibility of disrupted connectivity.

the Combatant Commands identified insufficient numbers of personnel, with the U.S. Special Operations Command (SOCOM) citing a significant increase in requirements, and the U.S. European Command (EUCOM) stating that shortfalls impacted their ability to train, share and engage the North Atlantic Treaty Organization (NATO) and foreign partners in cyber defense. Finally, six of the Defense Agencies and Field Activities noted insufficient people to meet mission requirements.

In order to address gaps in manning, many of the Components pulled personnel from other assignments to provide short term relief and perform inherently governmental functions. Additionally, all Components are currently supported by contractors who assist in performing critical cyber functions. Data received in support of this report indicated steady requirements through FY15, although many Components included a caveat that their static numbers reflected uncertainty regarding future force requirements. Further, although overall force size may remain constant over time, the Components did indicate shifts by functional area in their forecasts, with increased emphasis on both IA and defensive operations.

The increasing emphasis on IA was particularly demonstrated when the hiring patterns for the DoD civilian IT Management series (the largest civilian IT occupation and the major, single source of civilian IA personnel) were examined for FY09 and FY10. Figure 1.3 demonstrates the large growth in the Operations and Maintenance specialty areas (e.g., Systems Administration, Network Services) as well as IA individuals (denoted, but not limited to, personnel with the specialty title of “Information Security”).³ Information Security hires more than doubled, increasing from 584 to 1,250 new hires from FY09 to FY10. The overall series’ personnel strength grew by 10% and this significant growth was spread across the Components. The Military Services also increased the number of individuals in their traditional IT occupations. Their growth was smaller and largely confined to the enlisted forces; the rate of increase varied by Service.⁴

³ While individuals in the “Information Security” specialty area of the civilian IT Management series represent the largest segment of IA-certified individuals within the series, there are IA-certified individuals in all twelve specialty areas.

⁴ In FY10, the U.S. Air Force also migrated several officer and enlisted occupational codes to newly created cyber occupational codes.

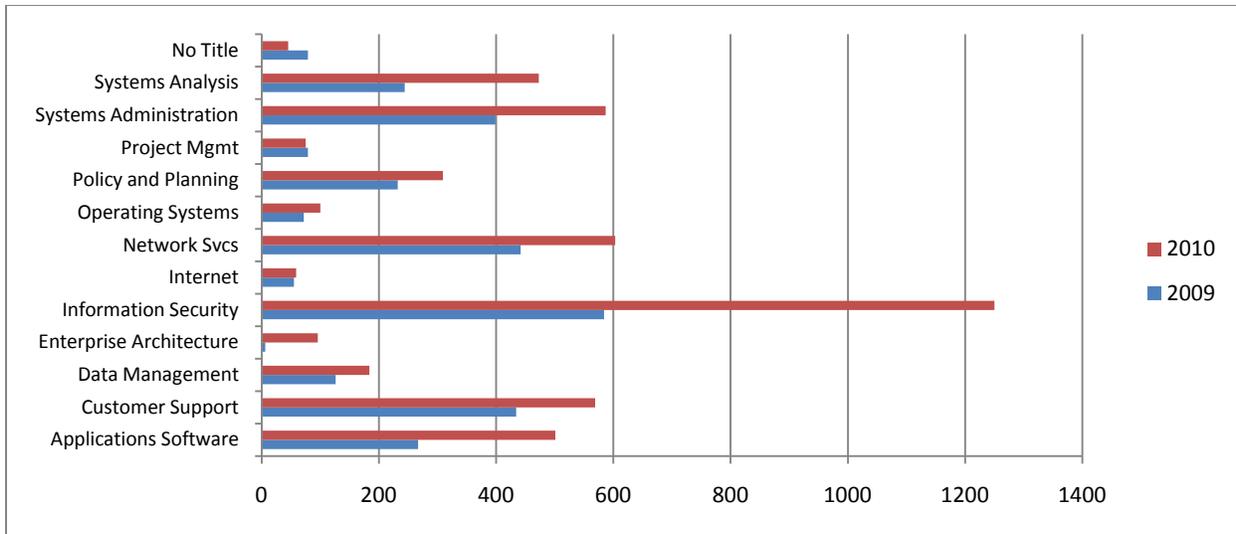


Figure 1.3 FY09/FY10 Hiring Trends in the Civilian IT Management Series

The view of what constitutes an optimal force balance differs by mission and Component. Some Components preferred a higher concentration of military personnel, while others found that the civilians and contractors provided more stability. There are some drawbacks to a high concentration of civilian personnel. They do not have a formal DoD education/training process to develop/maintain their cyber skills and to keep up with technology/threats. The DoD Components have been trying to integrate civilian personnel when possible into military training programs, but opportunities are minimal. The DoD has also developed some remote training opportunities such as the Defense Information Systems Agency’s Virtual Training Environment, but without some surge capacity, organizations do not have enough people to create opportunities for cyber personnel to participate in training or exercises. DoD civilians and contractors currently constitute over 50% of the IA/cybersecurity workforce reported in the FISMA.

Current manpower (manning/organization structure) guidelines and budgeting process do not support creating the capability to respond to “surge” requirements. Surge capacity essentially requires adding additional billets to an organization’s manning/table of organization to respond to emergency system disruptions from attack, malware, system malfunction, etc. Surge capacity also allows cyber personnel to participate in continuous training/education/exercises to keep current with technology and sharpen their skills.

1.5 The State of Cyber Operations Personnel Outside of DoD

The Department of Labor analyzed IT occupations across industry, developing detailed statistics on the 2008 U.S. labor force and projecting IT occupational trends through 2018. Most fields (many associated with cyber operations) are projecting significant growth as shown in Figure 1.4. This anticipated growth, coupled with shortfalls of U.S. students in technical disciplines, continues to concern DoD, the Federal CIO Council, and private industry as we look to sustain the IT/Cybersecurity workforce pipeline. President Obama also cited concern over high school

graduation rates and math and science performance in the 2011 State of the Union Address as factors impacting the country's ability to remain innovative and competitive with other nations.

IT Occupations	2008	2018	Change by 2018
Computer Applications Software Engineers	514,800	689,900	175,100
Network Systems/Data Communications Analysts	292,000	447,800	155,800
Computer Systems Software Engineers	394,800	515,000	120,200
Computer Systems Analysts	532,200	640,300	108,100
Network/Computer System Admins (includes Security Specialists)	339,500	418,400	78,900
Computer Support Specialists: Tech Support/ Helpdesk Techs	565,700	643,700	78,000
Computer/ Information Systems Managers	293,000	342,500	49,500
Computer Specialists, all other	209,300	236,800	27,500
Database Administrators	120,400	144,700	24,400
Computer/ Information Scientists, Research	28,900	35,900	7,000
Computer Programmers	426,700	414,400	-12,300
Computer Operators	110,000	89,500	-20,500
NET INCREASE IN IT JOBS	3,827,300	4,618,900	791,700

Figure 1.4 Bureau of Labor Statistics Projected Change in U.S. IT Workforce

In addition to the Department of Labor forecast on quantities of IT personnel required, other organizations are examining changing roles and skill sets. The Corporate Executive Board conducted a study based on IT and business leader interviews and in-depth reviews of emerging business, social, and technology trends, and supplemented with a survey of over 200 organizations' business and IT leaders in late 2009. Their results were described in two December 2010 publications, *The Future of Corporate IT - How to Prepare for Five Radical Shifts in IT Value, Ownership, and Role* and *The IT Talent Implications of the Future of Corporate IT - A Guide to Filling Emerging IT Skills Gaps*. The study forecasts by 2015 that the overall size of centralized IT will be 75% smaller as IT roles are subsumed and redistributed in functional areas. Skill sets will be changing, rapidly in some cases, and new roles will emerge to support the demand for social media; information management; knowledge workers requirements; externalization of applications development, infrastructure operations and back-office processes through cloud computing; and the shift to true global end-to-end integration as the standalone IT role is diminished. Cybersecurity roles will change less though there will be more focus on end user behavior and a shift of focus from securing devices to information security. Figure 1.5 provides the five emerging shifts that are predicted to fundamentally change how the IT function is organized and managed.

Five Shifts in IT Value, Ownership, and Role	
Information Over Process	Competitive advantage from information technology shifts toward customer experience, data analytics, and knowledge worker enablement; consequently, information management skills will rise in importance relative to business process design.
IT Embedded in Business Services	Centrally provided applications and infrastructure will be embedded in business services and delivered by a business shared services organization.
Externalized Service Delivery	Delivery will be predominantly externalized as vendors expand service provision and internal resources become brokers not providers.
Greater Business Partner Responsibility	Business unit leaders and end users will play a greater role in obtaining and managing technology for themselves where differentiation has more value than standardization.
Diminished Standalone IT Role	IT roles will embed in business services, evolve into business roles, or be externalized. Remaining IT roles will be housed in a business shared service group. The CIO position will expand to lead this group or shrink to manage IT procurement and integration.

Figure 1.5 Emerging Shifts in IT Value, Ownership and Roles
(Source: Corporate Executive Board)

These types of trends are already starting to be seen within DoD, but their full impact is not yet known. DoD’s unique mission requirements will ultimately dictate the appropriate size of the workforce.

2. Career Progression and Professional Development

"AFIT [the Air Force Institute of Technology] graduated its first class over 90 years ago. In those days of wood, wire and fabric, our forefathers realized how important education was to this developing technology. Now, as we stand here again transitioning to cyberspace, we once again realize the importance of education and the need for the collective intellect that has served us over the years.... If we do not pay attention to what is happening in cyberspace, our adversaries will take advantage of us by taking our advantage away. That is how important it is for us to train and educate in this cyber domain."

General C. Robert Kehler, Commander of Air Force Space Command, keynote speaker for the Air Force's first graduating class of cyberspace warriors, October 28, 2010

2.1 Occupational Fields

Civilian Personnel

The DoD's Information Technology (IT) Management series constitutes the largest civilian series serving the IT/Cybersecurity mission. Individuals in this series develop, deliver, manage and support IT systems and services, and can be found in every major DoD organization, ensuring the operability, sustainability and security of the Defense Information Enterprise. Members of the 2210 series perform a wide array of functions which are organized into 12 specialty areas:

- **Applications Software** – translate technical specifications into programming specifications; develop, customize, or acquire applications software programs; and test, debug, and maintain software programs.
- **Customer Support** – provide technical support to customers who need advice, assistance, and training in applying hardware and software systems.
- **Data Management** – develop and administer databases used to store and retrieve data and develop standards for the handling of data.
- **Enterprise Architecture** – analyze, plan, design, document, assess, and manage the IT enterprise structural framework to align IT systems with the mission, goals and business processes of the organization.
- **IT Project Management** – manages IT projects to provide a unique service, product or system.
- **Internet** – provide services that permit the publication and transmission of information about agency programs to internal and external audiences using the Internet.
- **Network Services** – test, install, configure, and maintain networks including hardware (servers, hubs, bridges, switches, and routers) and software that permit the sharing and transmission of information.

- **Operating Systems** – install, configure and maintain the operating systems environment, including systems servers and operating systems software on which applications programs run.
- **Policy and Planning** – develop, implement and ensure compliance with plans, policies, standards, infrastructures and architectures that establish the framework for the management of all IT programs.
- **Security** – plan, develop, implement and maintain programs, policies, and procedures to protect the integrity and confidentiality of systems, networks and data.
- **Systems Administration** – install, configure, troubleshoot and maintain hardware and software to ensure the availability and functionality of systems.
- **Systems Analysis** – consult with customers to refine functional requirements and translate functional requirements into technical specifications.

The other four civilian series most aligned with cyber operations are the Computer Scientist (1550 series), Electronics Engineer (0855 series), Computer Engineer (0854 series) and the Telecommunications Specialist (0391 series). With the exception of the 0391 series, all of these series are considered IT mission critical occupations. Information Assurance (IA), a critical segment of cyber operations predominantly resident within the 2210 series, spans over 180 civilian series in small numbers primarily due to personnel performing IA as a part-time duty. Within the 2210 series, all specialty areas have individuals performing IA functions. Figure 2.1 demonstrates the breakdown of over 12,000 certified IA personnel within the 2210 community by specialty area.

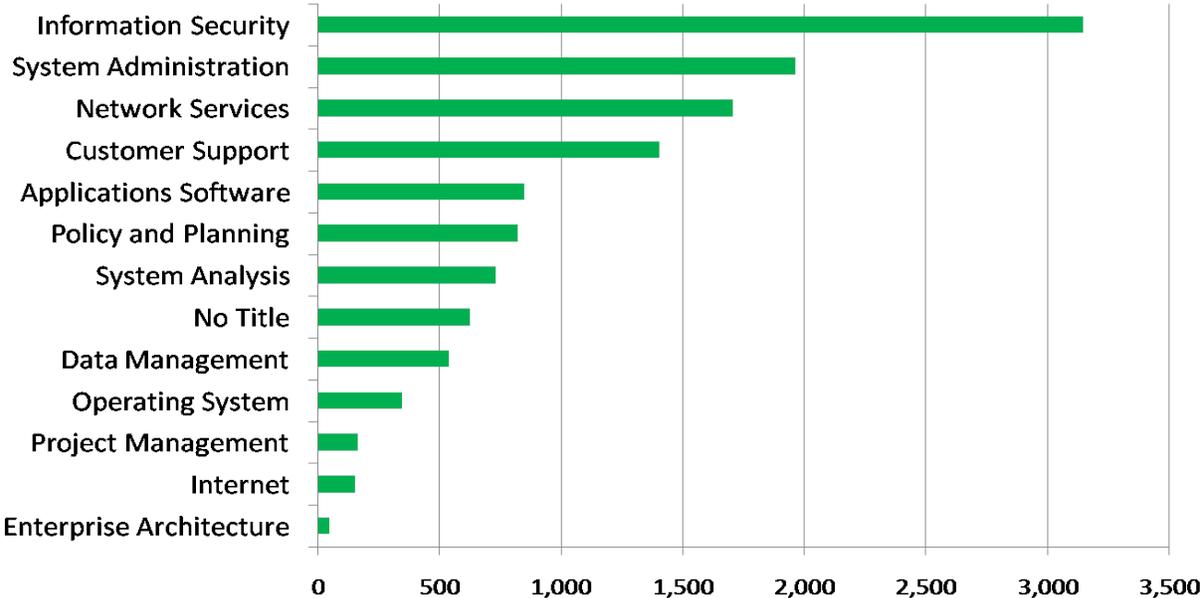


Figure 2.1 Civilian IT Management (2210 Series) Personnel Certified as IA Professionals

Military Personnel

Each of the four Services has cyber-related career fields with primary occupational specialties and additional subspecialties. A listing of these fields is at Appendix A.

Air Force

The recently established U.S. Air Force (USAF) Cyberspace Operations' officer career field, 17D, has two specific specialty codes. Officers with specialty code 17DXA, Cyberspace Defense Officer, plan, organize and perform network defense, exploitation and attack in support of joint, national and Air Force objectives; while those serving as 17DXB, Cyberspace Control Officers, plan, organize and perform network operations to include operations, information assurance and defense in support joint, national and Air Force objectives. There are also subspecialty codes for Electronic Warfare Support Duty (E), Information Operations (U) and Cyberspace Engineering (Z).

The USAF enlisted career field for Cyberspace Operations (another recent occupational category) consists of four specialties at various rated levels of seniority: Air Force Specialty Codes 3D052 and 3D072 in Cyber Systems Operations; 3D073 in Cyber Surety; 3D090, Cyber Operations Superintendent; and 1B4X1, Network Warfare Operator. They also share subspecialty codes Electronic Warfare Support Duty (E), and Information Operations (U). The skill progression within these enlisted specialties includes positions at the Helper, Apprentice, Journeyman and Craftsman levels, with ultimate promotion/assignment as a Superintendent.

Army

The U.S. Army has two officer branch-specific specialties for Cyber Operations; the first, 35G, Signal Intelligence/Electronic Warfare (SIGINT/EW) Officer, is a Military Intelligence (MI) asset whose duties include planning and coordinating for the collection, production and dissemination of SIGINT, and coordinating EW at the tactical, operational and strategic levels. The second officer branch specific specialty is 25A, Signal Officer, a Signal Corps asset. This officer orchestrates core competencies such as enterprise systems, network management, computer network defense/information assurance, and electro-magnetic spectrum operations. These skills and others support the focus areas of mission command, knowledge management and cyberspace operations at all levels of Joint and Army operations.

There are also two additional specialties from the Signal Corps that are referred to as functional area (FA) specialties. These specialties are performed by a subset of personnel who require significant education, training and experience. The Information Systems Manager, FA53A, is a highly skilled computer and information systems management professional. Officers working as Telecommunications Systems Engineers, FA24A, are network engineering and defense professionals who plan, engineer, test and validate the installation, operation, maintenance and protection of Army telecommunication systems using military and commercial technologies. The Army also has warrant officers performing cyber operations functions. These officers possess a high degree of specialization in a particular field in contrast to the more general

assignment pattern of other commissioned officers, operating, maintaining, administering and managing the Army's equipment, support activities, and technical systems. The Army has four Signal Corps and two MI military occupational specialties (MOS); the Signal MOS are 255A, Information Services Technicians, 255N, Network Management Technicians, 255S, Information Protection Technicians, and 255Z, Senior Network Operations Technicians. The MI MOS are 352N, Traffic Analysis Technicians, and 352S, Non-Morse Intercept Technicians.

Army enlisted personnel have a more extensive range of MOS related to cyber operations; 17 MOS are in the Signal Corps, 5 are in MI and 1 MOS, 94E, Radio and Communications Security (COMSEC) Repairer, is in the Electronics Maintenance career field. There is also an additional skill identifier (ASI) associated with the MI MOS, D6, Basic Digital Network Analysis.

Navy

The U.S. Navy has two cyber operations designator codes for officers: 1600, Information Professional, and 1610, Information Warfare. Officers serving in the Information Professional community provide expertise in information, command and control, and space systems through the planning, acquisition, operation, maintenance and security of systems. Career progression for Information Professionals can be tracked using additional qualification designator (AQD) coding: GA1 indicates a Basic Qualification; GA2, Intermediate Qualification; and GA3, representing an Advanced Qualification. The Information Warfare Officer's duties include the application of Information Operations (IO) and SIGINT expertise. Other responsibilities typically include leading IO personnel and advising commanding officers; coordinating information warfare measures in exercises and operations; responsibility for processing real-time signal intelligence; and developing cutting-edge exploitation and defense.

In addition to these officer communities, the Navy has Communications and Systems Officers in both the Limited Duty Officer (LDO) (6420 designator) and Chief Warrant Officer (7420 designator) communities. The differences in the roles of these warrant officers and LDOs are subtle, focusing on the degree of authority and responsibility as well as the breadth of expertise required.

Finally, the Navy has officers in the three primary warfare designators, Surface Warfare (1110), Submarine Warfare (1120) and Aviation (13XX), who by virtue of experience, training or advanced education, may support cyber operations missions.

Within the enlisted ranks, the Navy uses Navy Enlisted Classification (NEC) Codes to identify specialized skill requirements for its occupational ratings structure. There are eight NECs associated with the Information Systems Technician rating. Three are NCO-only positions: NEC IT-2779, Information Systems Security Manager, NEC IT-2780, Network Security Vulnerability Technician and NEC IT-2781, Advanced Network. Similarly, three NECs are entry level to mid-level NCO positions: NEC IT-2709, Joint Force Air Component Commander (JFACC) System Administrator (E3 – E6); NEC IT-2720, Global and Command Control System-Maritime (GCCS-M) System Administrator (E3 – E6); and NEC IT-2782, Defense Message System (DMS) System

Administrator. Lastly, there are two NECs that allow for complete career progression, NEC IT-2730, Naval Tactical Command Support System (NTCSS) System Administrator and NEC IT-2735, Information Systems Administrator.

Similar to the Navy officer community, individuals in other enlisted ratings may be trained to support cyber operations and awarded an appropriate occupational code to identify their specialized skills.

Marine Corps

There are nine officer MOS in five career fields: Intelligence (02); Marine Air Ground Task Force (MAGTF) Plans (05); Communications (06); Signals Intelligence/Ground Electronic Warfare (26); and Miscellaneous Requirements MOS (88). Many of the MOS allow line, limited duty and warrant officers to serve within the same MOS, i.e., all three types of officers can serve as an 8834, Technical Information Operations Officer.

Similarly, there are 11 enlisted MOS in four career fields: one MOS in Intelligence (02); one MOS in MAGTF Plans (05); six MOS in Communications (06) and three MOS in Signals Intelligence/Ground Electronic Warfare.

2.2 Career Paths

Civilian Careers

DoD civilians may enter federal service at any grade, depending on the job for which they apply and their educational/experiential background. Unless they are terminated for cause or the job is eliminated, civilians may continue within the same organization and/or in federal service, with advancement dictated by agency job requirements and their own professional initiative. Civilian personnel careers are not centrally managed, nor do individuals typically change geographical location unless they desire to do so. Although some civilian personnel have Individual Development Plans (IDPs), which are typically developed through consultation with supervisors/mentors, currently DoD does not have robust career management plans by occupational community.

Figure 2.2 displays the grade distribution for the major civilian series in the IT/Cybersecurity community, the IT Management, or 2210 series, for Fiscal Year (FY) 09.⁵ Although this series does not have a specialized education requirement (i.e., a degree is not mandatory for hiring purposes), the work does require the type of skills (analytical, research, writing and judgment) typically gained through college level education or through progressively responsible experience. The 2210 is a two-interval series that has a pattern of GS-5, 7, 9, 11; it then follows a one-grade pattern from GS-11 through 15. The GS-5 level implies a bachelor's degree or similar level of

⁵ Note that a portion of the 2210 population is in alternate pay plans that may be banded by pay range. This chart reflects only the 17,954 individuals in the 2210 series who are under the General Schedule and Related Grades.

experience; while a GS-9 implies a master’s degree or similar level experience. The rapid ascension to GS-9 is likely a combination of the individual’s experienced gained and expertise demonstrated, positional requirements, as well as the need to move these skilled individuals into higher salary levels for retention purposes (compensation issues are discussed in Chapter 3). High school level applicants would not qualify for this series as they would typically qualify at a GS-1 to GS-4 level. This series has been a viable path for enlisted veterans seeking government employment as it does not require a specialized degree.

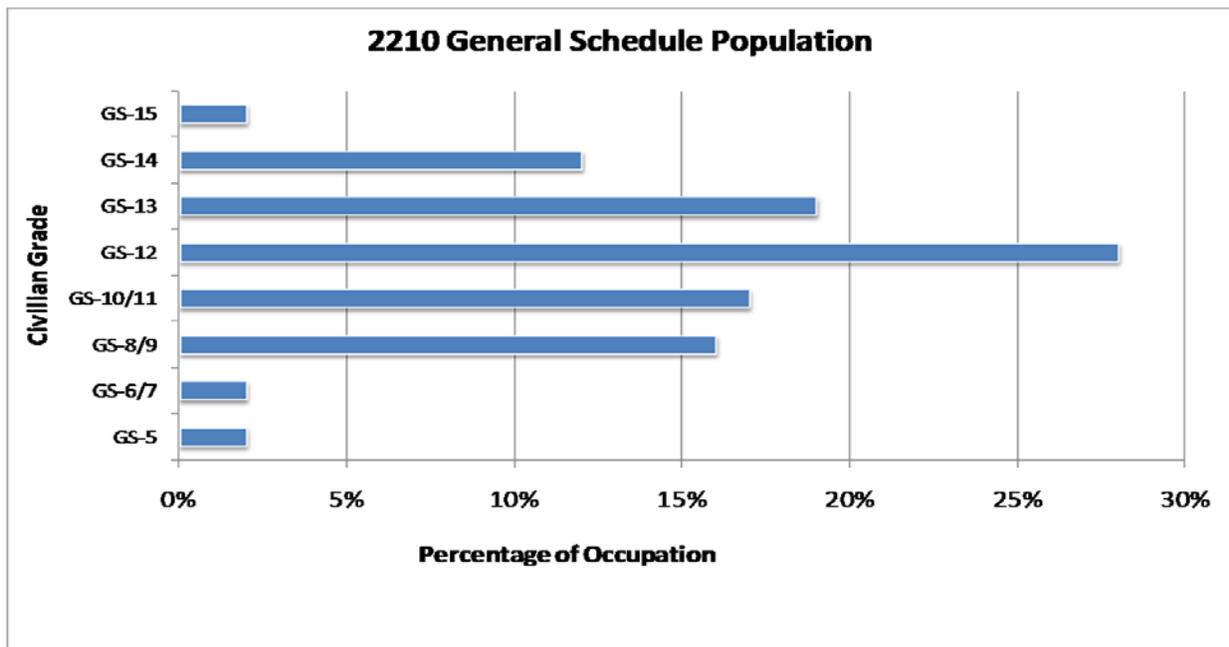


Figure 2.2 FY09 Pay Grade Distribution of the Major Civilian IT/Cybersecurity Occupation

The other three mission critical occupations previously discussed, Computer Scientist and Computer and Electronics Engineers, all have positive degree requirements (i.e., a specified technical degree is required for employment). The minimum starting grade for these series is also a GS-5 in the General Schedule. Many of these individuals are in alternate pay plans and grade bands that enable more flexible management of their career and salary progression.

Military Careers

Military officer and enlisted personnel, with few exceptions, start their careers at the very lowest pay grades and gradually over time, advance in their profession. At the earliest pay grades, advancement or promotion is longevity-based, with most eligible personnel advancing, as long as their professional and personal conduct is satisfactory. As individuals increase in seniority, promotion becomes more competitive and personnel who fail to advance, and/or are in overmanned occupations, may reach Service-mandatory separation milestones. Service members’ job assignments are typically centrally managed by their Personnel Headquarters and

they rotate to new assignments based on Service requirements, their own professional development requirements, their job expertise and their personal desires.

Enlisted Personnel

Enlisted members are “specialists,” trained from Basic Training to perform specific occupational specialties in the military; as they progress through the ranks (there are nine enlisted pay grades), they assume more technical and leadership responsibility. Initially, recruits without higher education or college degrees enter the military with a pay grade of E-1, and are elevated to E-2 usually soon after the completion of Basic Training. There are authorized pay grade advancement requirements in each junior enlisted rank category (E-1 to E-3) that differ by Service. Promotion through the junior enlisted ranks occurs upon attaining a specified number of years of service, a specified level of technical proficiency and/or maintenance of good conduct. Promotion to E-4 and above is generally competitive, although some occupations with long training pipelines may enable individuals to advance to E-4 upon successful completion of their technical training.

Non-commissioned officer (NCO) ranks (or petty officers in the Navy) begin at E-4 or E-5, depending upon the individual Service, and are generally attained between three to six years of service. Junior NCOs may function as first-line supervisors and squad leaders, training the junior enlisted in their duties and guiding their career advancement. While considered part of the non-commissioned officer corps by law, senior non-commissioned officers (SNCOs) (referred to as Chief Petty Officers in the Navy or staff non-commissioned officers in the Marine Corps) may perform duties more focused on leadership rather than technical expertise. Promotion to the SNCO ranks, E-7 through E-9 (E-6 through E-9 in the Marine Corps) is highly competitive. Further, personnel totals at the highest enlisted pay grades of E-8 and E-9 are limited by federal law to 2.5 percent and 1 percent of a Service’s enlisted force, respectively. Depending on individual Service requirements, high year tenure gates may be established for certain pay grades within the enlisted rank structure so that individuals not selected for advancement are denied further reenlistment opportunity after a specified number of years of service.

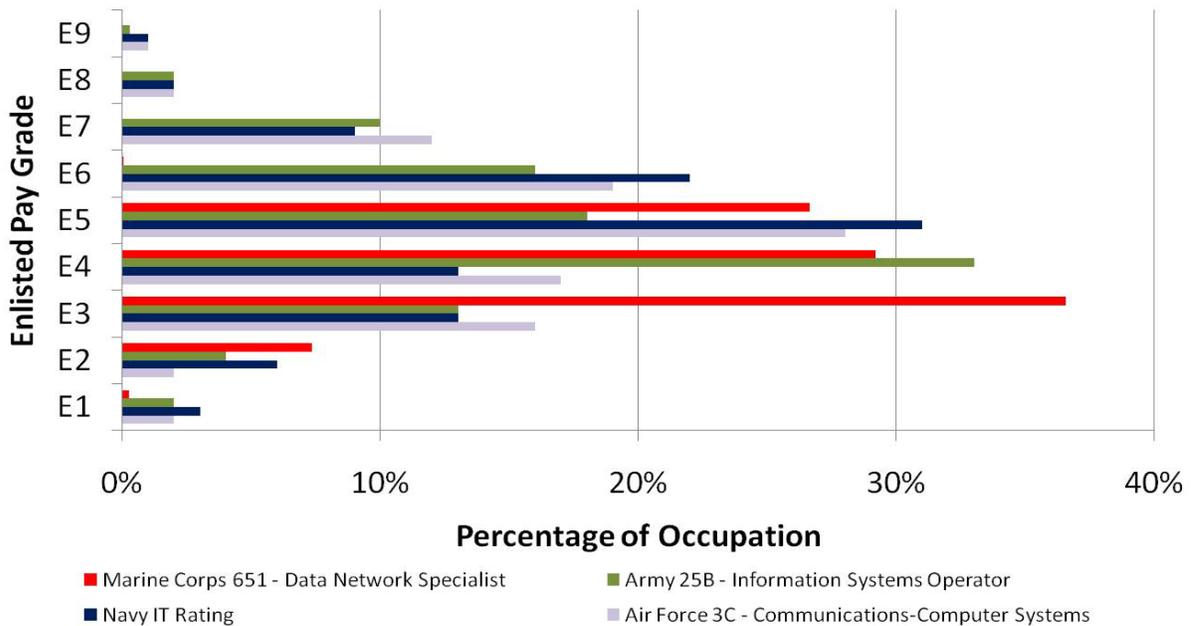


Figure 2.3 FY09 Comparisons of Four Enlisted Cyber Occupations by Pay Grade

Figure 2.3 displays the pay grade distribution for four of the major enlisted cyber operations occupations that existed in FY09: the Air Force 3C Communications field; the Navy Information Systems Technician (IT) rating; the Army 25B Information Systems Operator occupational specialty; and the Marine Corps’ Data Network Specialist occupation. Each occupation is managed differently, with the Army and Marine Corps having a more junior force.

Officer Personnel

Similar to the enlisted ranks, officers typically join their respective Military Service at the most junior pay grade of O-1. Most officers are promoted to grades O-2 and O-3 based on performance and longevity, and with little competition required. Grades O-4 through O-6 are also performance and longevity-based; however, each rank is successively more competitive, with fewer officers promoted upward at each promotion point. The number of total officers in pay grades O-4 through O-6 is controlled by law and promotion flow points are aggressively managed to ensure sufficiently experienced personnel are promoted to meet mission requirements. As Figure 2.4 displays, each Service has separate experiential requirements, based on the distribution of individuals within key IT/Cybersecurity disciplines.

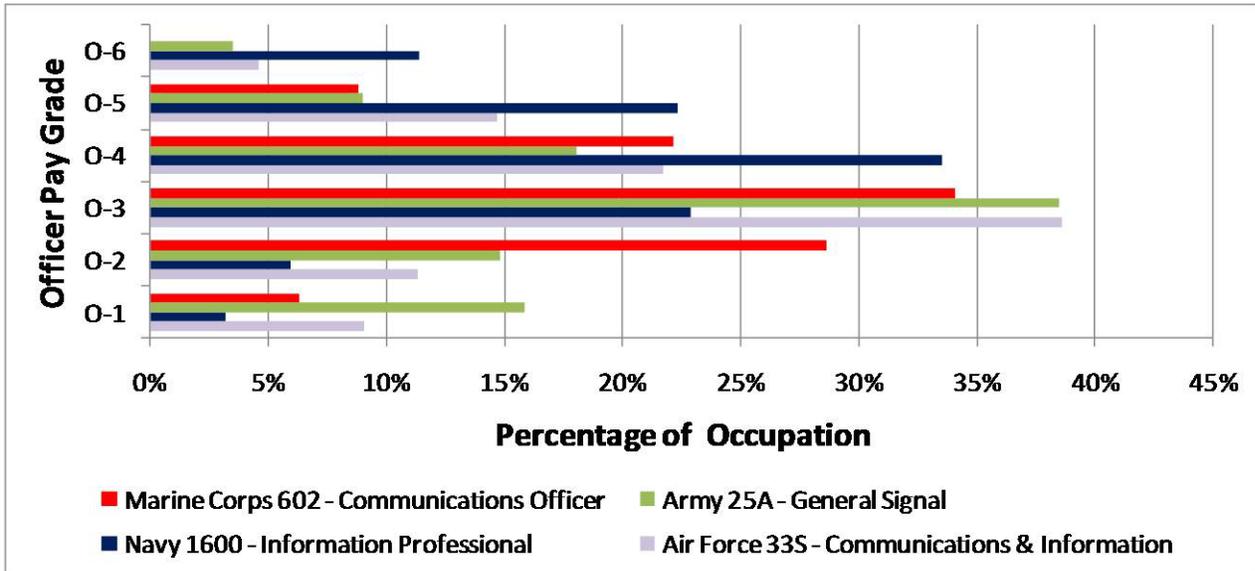


Figure 2.4 FY09 Comparisons of Four Officer Cyber Occupations by Pay Grade

2.3 Training and Development

The DoD, through the Military Departments, Defense Agencies and Defense Activities, is striving to enhance national cyber operations capabilities with a comprehensive training program for DoD military and civilian personnel which includes professional education and certification opportunities.

Figure 2.5 displays a hierarchy of core training and educational programs available for DoD personnel. Although the pay grade ranges display a notional hierarchy of eligibility, unless there are eligibility limitations imposed by Components, academic institutions or DoD regulations, participation in programs is flexible and based on individual position as well as Component mission requirements.

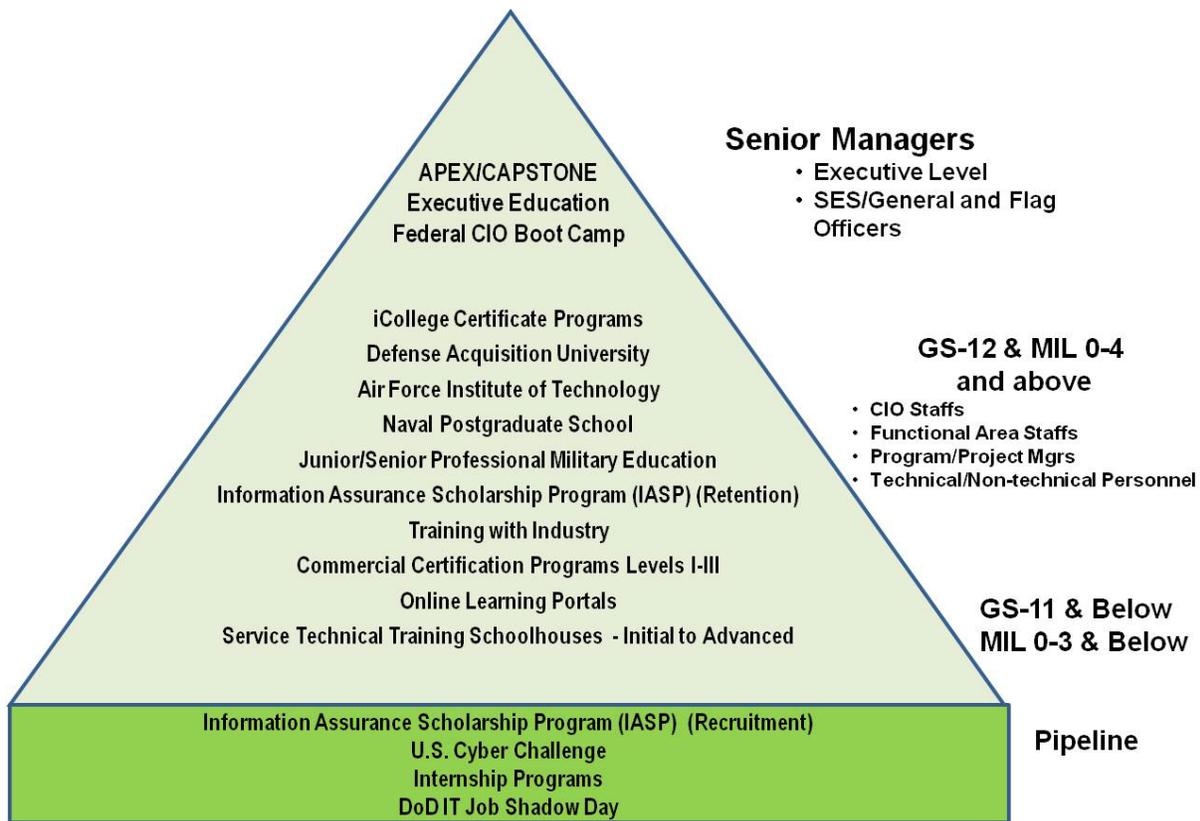


Figure 2.5 DoD Education and Training Opportunities

One of the key IA/cyber training programs, established by the IA Workforce Improvement Program, is described in the departmental issuance DoD 8570.01-M. This manual, which was first promulgated in 2004, provides guidance and procedures for the training, certification and management of the DoD workforce conducting IA functions in assigned duty positions and supports compliancy requirements specified by directive DoDD 8570.01. The program encompasses a formal IA workforce skill development and sustainment process, comprised of resident courses, distributive and blended training, supervised on-the-job training, exercises and certification/recertification.

The DoDD 8570.01 and DoD 8570.01-M requirements apply to all military, civilians and contractors performing IA functions within the Department, regardless of their occupational community. Figure 2.6 provides an overview of IA workforce requirements that apply whether the duties are performed full-time, part-time, or as an additional or embedded duty. Descriptions of applicable duties include:

- IA Technical (IAT): Anyone with privileged system access performing IA functions at computing, networking or enclave levels (e.g., System Administrators, Network Administrators).

- IA Management (IAM): Personnel responsible for managing the security of a DoD information system (e.g., Information Assurance Officers).
- Designated Accrediting Authority (DAA): Personnel responsible for verifying that information systems (IS), policies and procedures are compliant with IA requirements, and granting the authority to operate an IS or network at an accepted level of risk.
- IA Systems Architect and Engineer (IASAE): Personnel responsible for the design, development, implementation and/or integration of DoD IA architecture or system components for use within their Computing Environment (CE), Network Environment (NE) or Enclave.
- Computer Network Defense Service Provider (CND-SP): Personnel assigned to a selected, accredited CND-SP role responsible for performing specialty functions that include Computer Network Defense Analysts (CND-A), Auditors (CND-AU), Infrastructure Support (CND-IS), Incident Responders (CND-IR) and Managers (CND-SPM).

IA Workforce Qualification Requirements	IAT I-III	IAM I-III	IASAE I-III	CND-A, CND-IS, CND-IR, CND-AU and CND-SPM
Initial Training*	Yes	Yes	Yes	Yes
IA Baseline Certification	Yes (within 6 months)	Yes (within 6 months)	Yes (within 6 months)	Yes – IAT and CND (within 6 months)
OJT Evaluation	Yes (for initial position)	No	No	Yes (except CND-SPM)
CE Certification	Yes	No	No	Yes (except CND-SPM)
Maintain Certification Status	Yes (as required by certification)			
Continuous Education	Yes (as required by Component and certification)			
Background Investigation	As required by IA level and DoDI 8500.02	As required by IA level and DoDI 8500.02	As required by IA level and DoDI 8500.02	As required by CND-SP level and DoDI 8500.2
Sign Privileged Access Statement	Yes	n/a	n/a	Yes (except CND-SPM)
*Classroom, distributive, blended, government or commercial provider				

Figure 2.6 Summaries of IA Personnel Qualification Requirements

Specific certifications have been identified as baseline requirements for each IA workforce category and level. Certification providers are CompTIA, Information Systems Audit and Control Association (ISACA), International Information Systems Security Certification Consortium (ISC2),

and the SysAdmin, Audit, Network, Security (SANS) Institute. Personnel in IA Technical categories also must be certified on their local operating system and tools. Components may require their IA workforce to receive additional training or certifications in addition to the baseline requirements. Figure 2.7 provides a matrix of approved DoD baseline certifications by category. These certifications are further described in Appendix B.

IAT Level I		IAT Level II		IAT Level III	
A+ Network+ SSCP		GSEC Security+ SCNP SSCP		CISA GCIH GSE SCNA CISSP (or Associate)	
IAM Level I		IAM Level II		IAM Level III	
CAP GISF GSLC Security+		CAP GSLC CISM CISSP (or Associate)		GSLC CISM CISSP (or Associate)	
IASAE I		IASAE II		IASAE III	
CISSP (or Associate)		CISSP (or Associate)		CISSP - ISSEP CISSP - ISSAP	
CNDSP Infrastructure Support					
CNDSP Analyst		CNDSP Incident Reporter		CNDSP Auditor	
GCIA CEH		SSCP CEH		GCIH CSIH CEH	
				CISA GSNA CEH	
				CNDSP Manager	
				CISSP-ISSMP CISM	

Figure 2.7 Certification Requirements for DoD IA Personnel by Functional Level

The Department is currently updating the DoD 8570.01-M manual to provide additional guidance on training and certification requirements. As the DoD continues to refine the program, it will promote best practices in commercial certifications to enhance DoD IA readiness, and pursue initiatives to reduce duplication and save costs. Further, the Department will establish more guidance on continual training requirements, and use recurring training programs, and periodic certifications in the newest technologies, as well as realistic exercises, to ensure military and civilian cyber personnel have the practical knowledge to operate in a dynamic and changing cyberspace environment.

Civilian Personnel

The DoD 8570.01-M provides a good baseline for training the Department’s IT/Cybersecurity civilian community, but additional training is needed to ensure that Components have adequate

qualified personnel to address current and future mission requirements. Professional development opportunities are provided for the civilian workforce through a variety of means:

- The National Defense University's Information Resources Management College (NDU iCollege) prepares leaders to direct the information component of national power by leveraging information and information technology for strategic advantage. Primary areas of expertise include leadership, IT project management, IA, IT policy, business transformation, and management of acquisition processes and reform.
- Partnerships with local academic institutions and commercial vendors to offer IA training courses.
- Developmental assignments and rotational programs.
- Centralized training that allows migration or use of a DoD required tool-set, such as the Host Based Security System or Retina.
- Tuition assistance for courses or degree-awarding academic program of direct relevance to an employee's cyber position.
- Funded sabbatical to a recognized and accredited university for employees demonstrating outstanding potential.
- Boot camps that prepare information security and assurance personnel for certification.
- Preparatory training and internal rotation opportunities within the Information Assurance Division within an organization for employees expressing an interest in IA.
- Actively providing continuing education events for employees through attendance at trade shows, conferences and classroom-based training to maintain their certifications.
- Individual Development Plan negotiated between employee/supervisor specifying the critical training objectives to be achieved during the year. The plan specifies the type, cost and source of training to be provided by calendar quarter. Training that is web-based or centrally funded by another DoD element is emphasized to minimize costs.

These programs are not as structured as similar IT/Cybersecurity career development programs offered to military personnel; partly because the Department's IT/Cybersecurity civilian workforce does not have defined career paths that link training requirements to required competencies, and also because military service members often receive their training and education as part of a rotational assignment transfer (thus having the training centrally funded and resulting in no gap in command productivity while in training). Further, the civilian workforce is not afforded the same type of routine access as their military counterparts to attend defense schoolhouse technical training courses that may be needed for professional development. The Department is pursuing enterprise-wide competencies and developing career paths for the IT/Cybersecurity civilian community that includes training required to reach the desired level of skills needed. Additionally, the Department is exploring ways to leverage existing military IT/Cybersecurity training for the civilian workforce.

Military Personnel

The Military Departments have well-established IT/Cybersecurity training programs for initial, mid and senior-level military personnel as well as additional training for continuous development. Training is provided for enlisted, warrant officer and officer personnel based on their chosen functional area or the area for which they have been selected. Training programs at all levels are continually being modified to incorporate and meet existing and emerging cyber operations requirements. Appendix C provides specific training examples for each of the Services for initial, mid-level, senior-level and additional advanced training.

Entry-Level Awareness Training

The Air Force added general cyber awareness training to its Basic Military Training (BMT) curriculum for enlisted personnel and conducted its first cyber awareness training course devoted to defending the Air Force networks and operations in cyberspace in October 2010. The course teaches basic operating fundamentals on the Air Force network and the significance of protecting the network to meet the Air Force mission. The curriculum was developed by the Air Force Institute of Technology (AFIT) under the guidance of Air Force Space Command and includes a 3-hour practical application segment. The U.S. Air Force Academy (USAFA), the U.S. Military Academy (West Point) and the U.S. Naval Academy (USNA) have developed similar cyber curricula for officers to provide the necessary basic technical cyber training needed within the DoD. All three service academies have been designated as National Centers of Academic Excellence in IA Education (CAE/IAE). The CAE/IAE program is discussed further in Chapter 4.

Following the general training enlisted recruits receive in BMT for Air Force and Navy, Basic Combat Training (BCT) for Army, Recruit Training for the Marine Corps, and the pre-commissioning training for officers, service members receive initial technical skills training to prepare them to meet the minimum qualifications related to their job.

Initial Skills Training

Initial IT/Cybersecurity skills training is completed post-accession and results in:

- Military Occupation Specialty (MOS) qualification for Army enlisted and warrant officer and Marine Corps enlisted and officer personnel.
- Air Force Specialty Code (AFSC) qualification for enlisted and officer personnel.
- Rating and designator qualification for Navy enlisted and officer personnel respectively.
- Specialty or functional area for Army officers.

This specific training prepares service members for their designated functional area. The duration of this training varies based on the complexity of the job. Samples of initial training are provided in Appendix C. This listing is not intended to be all-inclusive, but to provide an overview of key training needed to be effective in designated positions. The remaining training needed is obtained through organizational and on-the-job training. Following initial training, service

members are assigned to rotational positions throughout their careers where they receive individual and collective training, continual professional military education, on-the-job training and developmental assignments that allow them to expand and hone their skills.

Mid-level Training

As service members begin to focus on both the operational and strategic aspects of cyber operations, they need to expand their knowledge and increase their skills. This is accomplished through mid-level training, with selected examples of this training described in Appendix C. Using the knowledge and skills gained in mid-level training individuals begin to transition to a more strategic environment while maintaining their operational skills. As service members continue to advance, selected individuals will be afforded the opportunity to attend senior-level training. The Services have varied options for service members.

Senior-level Training

Senior military IT/Cybersecurity professionals need to understand the broader spectrum of cyber operations to be strategic leaders and to provide vision and direction for their organizations. As part of their competency development, they require more focus on cybersecurity strategies related to joint, interagency, intergovernmental and multinational environments. Examples of senior-level training to meet those needs are described in Appendix C.

Additional Military Training Available for Continuous Learning

Finally, in addition to the stratified training programs discussed in this chapter, more advanced training programs are available through multiple supplemental courses intended to focus on professional development throughout an individual's career. These courses impart cyber-related knowledge, skills and abilities appropriate to an individual's pay grade and experience, as well as providing new exposure to aspects of the cyber warfare mission area not yet experienced. Individuals may also attend training that will be specific to their duty location and mission. Examples of additional training are described in Appendix C.

3. Recruitment and Retention

"The biggest challenge we currently face is generating the people we need to do this mission. I am optimistic we will get the force we need. We are pushing on the Services to go faster to bring those forces in. My greatest concern is moving fast enough to provide a capability to defend our networks in time were a crisis to occur. We see that as our No. 1 mission -- be ready."

Gen. Keith B. Alexander, Commander, U.S. Cyber Command and Director of the National Security Agency, Testimony before the House Armed Services Committee, September 23, 2010

In the world of information technology, information assurance and cyber (IT/Cybersecurity), the DoD must compete with the rest of the Federal Government and the private sector for highly skilled talent with the necessary technology competencies. Many of the skills that have been determined to be critical to the public sector IT/Cybersecurity community mirror those in demand by the private sector. Additionally, defense job requirements that include knowledge of government procedures and possession of a valid security clearance are lucrative commodities in private industry. Both military and DoD civilian personnel are eligible for recruitment and retention incentives that can be targeted to support occupational skill demands. Military incentive programs are centrally funded and managed by the Military Services' personnel headquarters, while civilian incentives are typically managed by the individual organizational element (e.g., at an agency or command level).

In July 2009, the Partnership for Public Service and Booz Allen & Hamilton conducted a study, *Cyber IN-security, Strengthening the Federal Cybersecurity Workforce*, on the current state of the federal cybersecurity workforce. The study found that the current workforce continues to face serious shortages of highly skilled cybersecurity specialists. According to the study, the inadequacy of the pipeline for potential new talent is the top challenge that threatens the quality and quantity of the federal cyber workforce. The Department's Chief Information Officer, in researching IT workforce demographics for the federal report, *Net Generation: Preparing for Change in the Information Technology Workforce*, also cited similar pipeline issues and concerns in light of the Department of Labor's Bureau of Labor projections on increasing IT jobs and occupational requirements. One recent factor mitigating this issue has been the slowdown of the U.S. economy in 2009 to present. This has attracted individuals to government service (both as military members and DoD civilians) and has also slowed losses from these communities. As a result, use of incentives to recruit and retain individuals has remained fairly static.

The number of civilian new hires has been increasing each year within the IT/Cybersecurity major occupations, as has the overall personnel strength by occupational series. Figure 3.1 displays the growth in new hires from fiscal years (FY) 2007 to 2009.

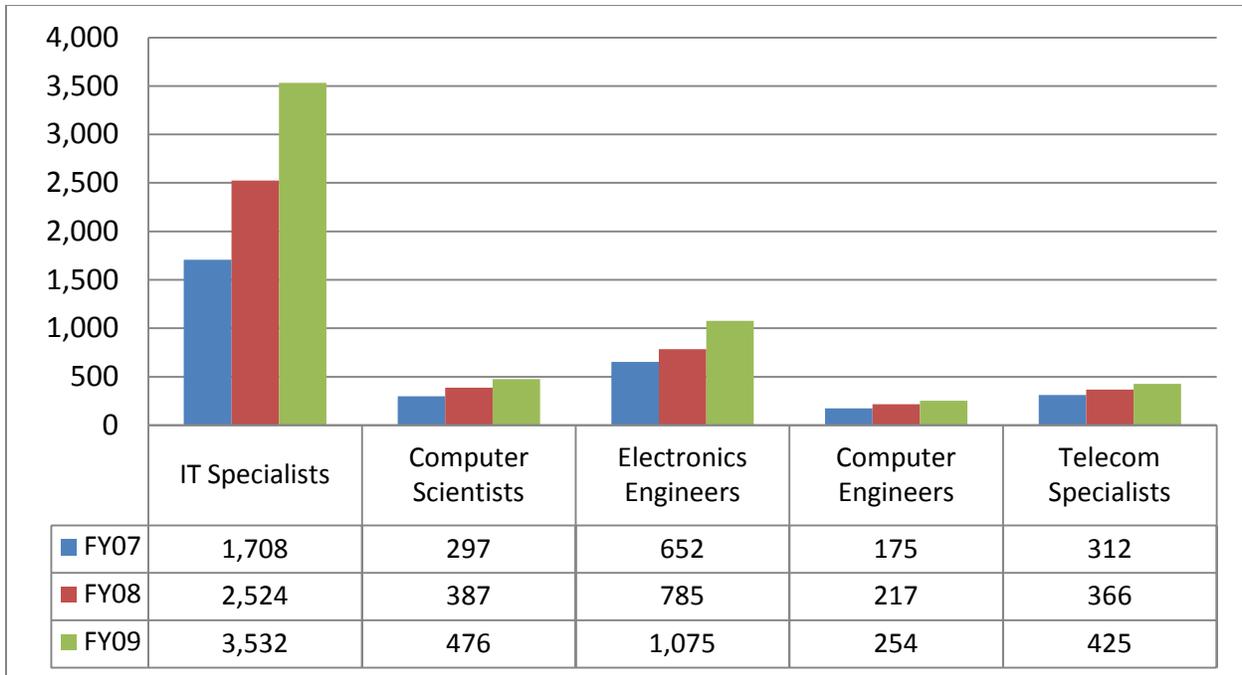


Figure 3.1 Annual DoD Civilian New Hires by IT/Cyber Occupation

3.1 Civilian Recruitment Authorities and Incentives

The following recruitment and retention authorities and incentives are most commonly used within the Department to recruit, retain and develop cyber professionals. The majority of these flexibilities can be applied across occupational specialties and are not limited to IT/Cybersecurity professions.

Hiring Authorities

Direct-Hire Authority for IT Management (Information Security) 2210 Series

Direct-hire authority is designed to provide agencies flexibility to recruit individuals for career-conditional appointments to positions in shortage or critical shortage occupations. In 2003, the Office of Personnel Management (OPM) authorized Government-wide direct hire for the 2210 series IT Specialists, in General Schedule (GS) grades 9 and above, in the Information Security specialty, which is 1 of 12 specialties within the series. Individuals recruited to this specialty area may be appointed to positions without regard to the requirements in title 5, United States Code (U.S.C.) 3309 through 3318.

Schedule A Hiring Authority for the Cybersecurity Workforce

In November 2009, OPM authorized Schedule A hiring authority for select cybersecurity positions within DoD. The occupations under this authority includes both IT and non-IT civilian job series

related to cybersecurity: security administration (0080), intelligence (0132), criminal investigation (1811), operations research (1515), computer engineering (0854), electronics engineering (0855), computer science (1550), telecommunications (0391), and IT management (2210). The authority is limited to positions that require unique qualifications not currently established by OPM to perform such functions as cyber risk and strategic analysis, incident handling and malware/vulnerability analysis, program management, distributed control systems security, cyber incident response, cyber exercise facilitation and management, cyber vulnerability detection and assessment, network and systems engineering, enterprise architecture, intelligence analysis, investigation, investigative analysis and cyber-related infrastructure interdependency analysis. This authority applies only to positions at grade levels 9 through 15 and expires December 31, 2012 (or as otherwise dictated by OPM). No more than 3,000 total positions may be filled during the 3-year authorization period.

Internships

Federal Career Intern Program (FCIP)

The Federal Career Intern Program (FCIP) helped DoD agencies recruit exceptional individuals into a variety of occupations at the GS-5, 7, and 9 grade levels. Agencies could strategically target entry-level positions and create a pipeline of talent that ultimately leads to a journey-level position in the agency. Individuals are appointed to a 2-year internship that provides formal training and developmental assignments as established by the agency. Upon successful completion of the program, interns may be eligible for non-competitive permanent placement within the agency. Individuals with diverse professional experiences, academic backgrounds, and/or relevant skills are eligible for the FCIP. The program is not restricted to students, and career intern appointments could be made at any time during the year.

The FCIP authority is used widely both in DoD and across the Federal Government and is instrumental in bringing in the younger generation to federal service. Agencies favor the program as a way to do targeted recruiting while also reducing the hiring processing time by up to 60%. However, a recent ruling by the Merit Systems Protection Board in November 2010 found that the FCIP violates veterans preference rules and the authority has been eliminated as of March 2011. Executive Order 13562, entitled "Recruiting and Hiring Students and Recent Graduates," was signed in December 2010 and directs OPM to establish a comprehensive structure to help the Federal Government be more competitive in recruiting and hiring talented individuals who are in school or who have recently received a degree. Under this order, OPM will consolidate student and recent graduate programs into a Pathways Programs framework.

Student Career Experience Program (SCEP)

The Student Career Experience Program (SCEP) allows DoD Components to appoint students to positions that are related to their academic field of study. Employment as a student is in the excepted service and public notice is not required. Participants who meet all the requirements of the program may be noncompetitively converted to term, career, or career-conditional

appointments. Components within the DoD have regularly used SCEP to grow their IT workforce by hiring students into developmental positions to address the growing need for cyber professionals. To participate in SCEP, a student must be enrolled or accepted for enrollment as a degree-seeking student in an accredited high school; technical or vocational school; 2-year or 4-year college or university; or graduate or professional school. All students must be at least 16 years old. The Defense Information Systems Agency (DISA) heavily uses the SCEP to recruit new workers with IT/Cybersecurity skills.

Student Temporary Experience Program (STEP)

The Student Temporary Employment Program (STEP) provides DoD employment opportunities to students who are enrolled, or accepted for enrollment, as degree-seeking students taking at least a half-time academic, technical, or vocational course load from an accredited high school, technical, vocational, 2 or 4-year college or university, graduate or professional school. The STEP provides maximum flexibility to both students and managers because the nature of the work does not have to be related to the student's academic or career goals, which benefits both agencies and students. DoD Components can use the STEP authority to recruit and develop talented employees to support changing agency missions, like cybersecurity; ensure that the Government can meet its professional, technical, and administrative needs; and achieve a quality and diverse workforce.

Recruitment Bonuses

The DoD may pay recruitment bonuses to newly appointed defense civilian employees in hard to-fill positions, such as IT/Cybersecurity-related disciplines, in exchange for a signed service agreement. The amount of the bonus may range up to 25% of the new employee's annual rate of pay (or more, with OPM approval), multiplied by the number of years in the agreed service period (which can range between 6 months to 4 years). Payment of the bonus can be in a lump sum, phased installment or other installment plan, as designated by the agency. Organizations must have a pre-established recruitment incentive plan in order to offer a bonus. In FY 2009, 7,704 DoD employees received recruitment bonuses. Figure 3.2 displays the number of individuals in the critical IT/Cybersecurity occupations who received bonuses in calendar year (CY) 2009 and the average bonus by occupation; these are the civilian occupational series most identified with cyber operations.

Civilian Series	IT Specialist	Computer Scientist	Electronics Engineer	Computer Engineer	Telecomm Specialist
	2210	1550	0855	0854	0391
Total Population	30,063	4,773	16,928	3,196	3,293
New Hires	3,532	476	1,075	254	425
Number of Recruitment Bonus Recipients	149	114	439	66	3
% of New Hires Receiving a Bonus	4%	24%	41%	26%	1%
Average Payment	\$9,011	\$7,667	\$8,972	\$5,730	\$12,733

Figure 3.2 CY09 Civilian Recruitment Bonuses Received by IT/Cyber Occupation

Educational Incentives

DoD Information Assurance Scholarship Program (IASP)

The DoD Information Assurance Scholarship Program, managed by the DoD CIO, is a recruitment, retention and academic capacity building program, designed to: 1) increase the number of new college graduate entrants to DoD who possess key IT/Cybersecurity skill sets; 2) serve as a mechanism to build the nation's IA infrastructure through grants to colleges and universities jointly designated by the National Security Agency (NSA) and Department of Homeland Security (DHS) as Centers of Academic Excellence in Information Assurance Education; and 3) serve as a tool to develop and retain well-educated military and civilian personnel who support the Department's critical IT management and infrastructure protection functions.

Relevant academic disciplines for the scholarship program include, but are not limited to, Mathematics, Biometrics, Electrical Engineering, Electronic Engineering, Computer Science, Computer Engineering, Software Engineering, Computer Programming, Computer Support, Data Base Administration, Computer Systems Analysis, Operations Research, Information Security (IA/Cyber), and Business Management or Administration. All academic disciplines must include a concentration in Information Assurance. Recruitment students (non-DoD employees) may be awarded scholarships to complete their junior/senior years of college or a master's or PhD program. Since its inception in 2001, the program has been continually enhanced to meet DoD's requirements for flexible, multi-faceted recruiting and retention tools. To date, 292 IASP recruitment scholars have received assistance in completing their academic degrees; with 228 individuals graduating from the program. Graduates from the recruitment program serve a payback period in critical DoD IT/Cybersecurity billets.

In the Fiscal Year (FY10) National Defense Authorization Act (NDAA), Congress supported the DoD CIO's request to establish an IASP Hiring Authority to be used in conjunction with the scholarship program. This authority enables the DoD Components to hire IASP graduates as members of the excepted service, and to convert their positions to career or career conditional after two years of satisfactory service. With this new authority, DoD Components are able to

create a long-term career path for IASP graduates past their service commitment. This ultimately facilitates the high quality talent that the Department has invested in to remain within DoD to support critical cyber missions. The procedures for using this new authority were issued in a memorandum signed by the Under Secretary of Defense for Personnel and Readiness on April 5, 2010.

The Military Departments, NSA and DISA have all been key participants in this scholarship program. To measure efficacy, one of the key metrics used by the DoD IASP Program Office is feedback from DoD Component supervisors on the quality of DoD IASP students. Their feedback indicates that DoD IASP students have superior skills compared to other IT staff, are well prepared to perform assigned duties and meet the critical IT/Cybersecurity needs of their supporting organizations. The success of the program has resulted in an increased demand from DoD Components for more IASP scholars. Additionally, IASP scholars are noted leaders in the federal cyber arena. Many have published articles in the field of IA in peer-reviewed journals and association magazines. They have also won IA achievement awards and play key roles in the implementation of the federal and DoD cyber strategy.

Federal Cyber Service: Scholarship for Service (SFS)

In addition to the IASP, DoD Components can choose to participate in the Federal Cyber Service: Scholarship for Service (SFS). The SFS is a federal program designed to increase and strengthen the cadre of federal IA professionals who protect the government's critical information infrastructure. This program provides scholarships that fully fund the typical costs that students pay for books, tuition, and room and board while attending an approved institution of higher learning. The scholarships are funded through grants awarded by the National Science Foundation (NSF) in exchange for federal service payback.

DoD Components, like NSA and DISA, with high recruitment demands that cannot be met solely via the IASP due to funding limitations, also participate in the SFS program to meet their cyber personnel needs. Similar to the DoD IASP, the SFS aims to increase and strengthen the cadre of federal information assurance professionals that protect the government's critical information infrastructure. In June 2008, the Air Force established the Cyberspace Technical Center of Excellence at Wright-Patterson Air Force Base, Ohio. Through the Center, scholarship opportunities are provided to non-DoD students who are seeking a Masters Degree in Cyberspace Operations. The Center of Excellence is funded through an SFS grant from the National Science Foundation. Under the SFS program at the Air Force Institute of Technology, students pursue advanced graduate education in exchange for service commitment upon graduation. Recently, the Center for Cyberspace Research was awarded a \$2.1 million capacity-building grant from NSF to continue its successful SFS program.

Federal Student Loan Repayment Program

Section 5379 of title 5, United States Code, authorizes federal agencies to establish a program under which they may repay certain types of federally insured student loans as a recruitment or

retention incentive for highly qualified candidates or current employees. Under this program, agencies may make payments to the loan holder of up to \$10,000 for an employee in a calendar year; the total benefit per employee may not exceed \$60,000. Any employee receiving this benefit must sign a service agreement to remain in the service of the paying agency for a period of at least 3 years. The DoD provided \$14.1 million in student loan repayment benefits to 2,126 employees in calendar year 2009, with 129 individuals in the major IT/cyber occupations receiving benefits. Application of this benefit has remained fairly limited within the IT/cyber community, as shown by the number of recipients in Figure 3.3.

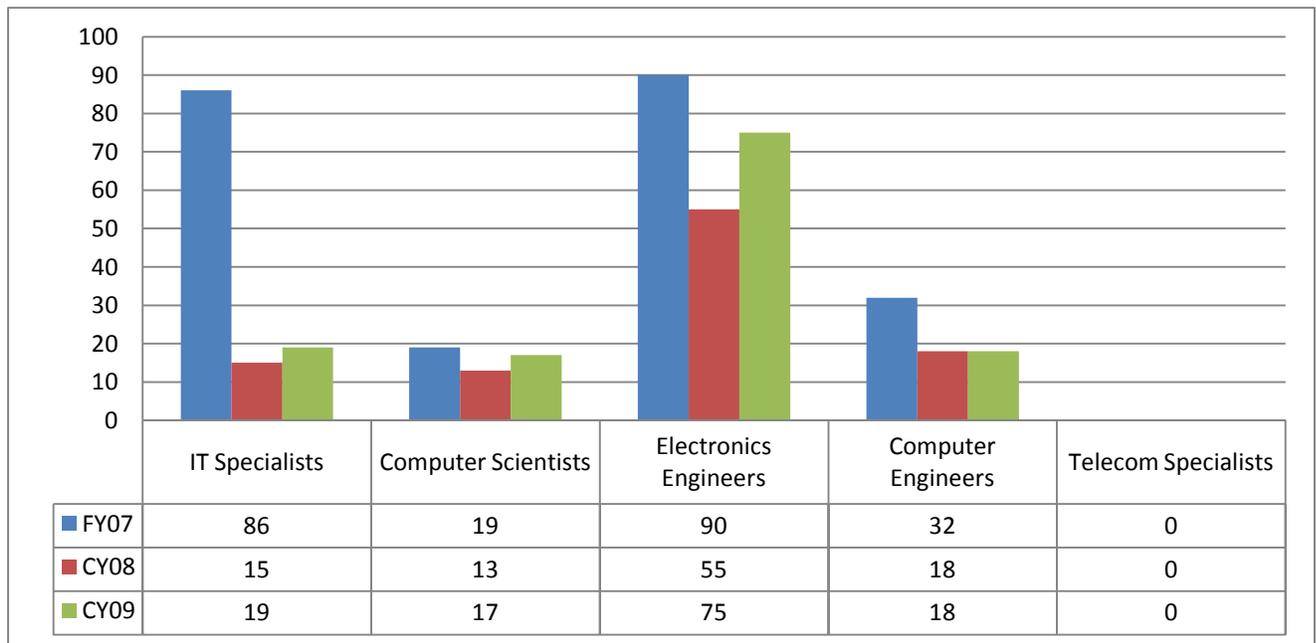


Figure 3.3 Civilian Loan Repayment Program Recipients by IT/Cyber Occupation

3.2 Civilian Retention Incentives

The following retention incentives are most commonly used within the Department to retain and cyber professionals. The majority of these flexibilities can be applied across occupational specialties and are not limited to IT/Cybersecurity professionals.

Retention Bonuses

Agencies may pay individual or group retention incentives based on unique qualifications and critical need. Individual retention incentives may not exceed 25% of an employee’s rate of basic pay and group or category retention incentives may not exceed 10% of the employee’s rate of basic pay, although higher awards may be allowed with OPM approval. Awards may be paid in installments or a single lump sum after completion of the required period of service. In calendar year 2009, DoD paid retention incentives to 11,166 individuals in the Department; less

than 6% (632) of those recipients were in IT/cyber occupations. Figure 3.4 displays a 3-year trend for these occupations.

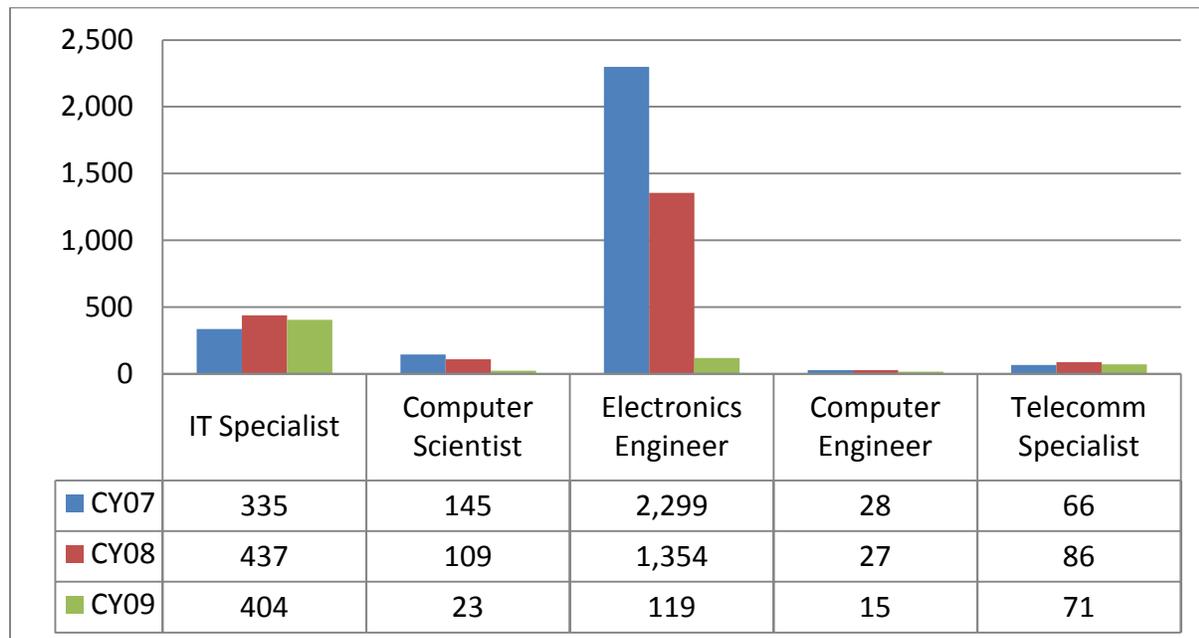


Figure 3.4 Civilian Retention Bonus Recipients by IT/Cyber Occupation

Educational Incentives

DoD Information Assurance Scholarship Program (IASP)

The retention component of the DoD IASP (previously discussed in Section 3.1) enables current DoD civilian and military personnel to attend school either full or part-time to earn degrees in cyber-related disciplines. Master’s and doctoral programs are available through the Air Force Institute of Technology (AFIT); the Naval Postgraduate School (NPS); and the Information Resources Management College (iCollege) of the National Defense University, in conjunction with 27 IASP partner universities across the country. Employees who are selected to participate in the program are paid their regular salary and receive full tuition, paid books and fees in exchange for continued service with the Department. This program has been instrumental in assisting the Department’s current civilian and military IT/IA professionals to obtain the critical skills needed to support the IT/Cybersecurity mission. Since the program's inception, 160 military/civilian employees have received scholarships and 125 have graduated from the program.

Academic Incentive Programs

Some DoD Components have developed programs that offer a retention incentive for individuals who complete certain educational endeavors. One example is DISA, who pays an incentive of \$1,000 to \$3,000 for approved professional credentialing aligned to DISA’s mission and the employee’s individual development plan (IDP), and \$1,000 to \$5,000 for attainment of academic

degrees that meet similar mission and IDP criteria. Both programs require a minimum 2-year service agreement.

Relocation Bonuses

A relocation bonus may be authorized for a current employee who relocates to accept a difficult-to-fill job in a different geographic area. The incentive may not exceed 25 percent of the employee’s annual rate of basic pay in effect at the beginning of the service period, multiplied by the number of years in the service period (not to exceed 4 years). In order to receive a relocation incentive, the employee must sign an agreement to fulfill a period of service with the organization. Payment of the incentive may be as an initial lump-sum payment, in installments throughout the service period, as a final lump-sum payment upon completion of the service period, or in a combination of these methods. DoD is typically the largest user of relocation bonuses within the Federal Government. In 2009, relocation incentives were paid to 3,420 DoD employees; a total of 182 IT/cyber individuals received an average of \$14,155 in benefits.

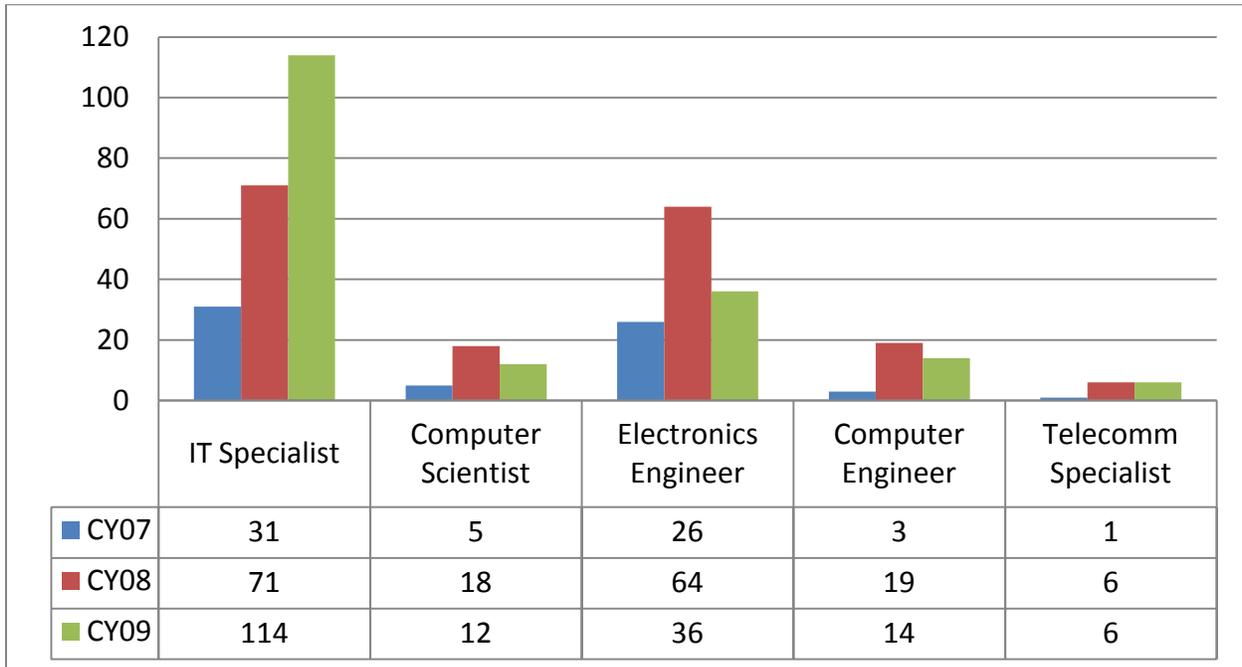


Figure 3.5 Civilian Relocation Bonus Recipients by IT/Cyber Occupation

3.3 Military Recruitment Incentives

Enlisted Personnel

Only 25% of today's youth, aged 17 to 24, qualify for enlistment in the U.S. military.⁶ Medical, physical fitness, and behavioral issues, as well as lack of education, poor quality of education, and substandard performance on aptitude tests, all play a role in eliminating individuals from the eligible population for recruitment. The Military Services use a variety of incentives to attract individuals to enlist, and to fill specific occupational needs. The following incentives are the major recruitment incentives for enlisted military members. They be offered in combination, depending on the needs of the Services.

Enlistment Bonuses

In FY09, enlisted active duty recruits potentially were eligible for an accession enlistment bonus (EB) incentive package of up to \$40,000, depending on the criticality of their skill area and the ease of recruiting individuals to a particular occupation, the length of their total service obligation, and the time of year that the recruits shipped to basic training; National Guard and Reserves were eligible for a bonus up to \$20,000. Additionally, some of the Services stratified their EB incentive program to offer bonuses for individuals scoring higher on the Armed Forces Qualification Test (AFQT) (a test used to identify qualified individuals for military service and to classify them into specific occupational career fields); those with language proficiency or unique physical requirements; or those who entered the service with some college education. The higher bonuses paid in FY09 typically went to individuals in the nuclear field, advanced electronics, linguists, special warfare, and special operations fields such Explosive Ordnance Disposal.

Within the IT/cyber community, the Navy offered up to \$15,000 in EB for recruits in the Information Systems Technician rating who entered military service in select months in FY09; this rating feeds a significant number of more senior, specialized skill areas within the Cyber Operations community. The Marine Corps offered a \$6,000 EB for Special Intelligence System Administrators/Communicators, 1 of 2 entry-level, military occupational specialties (MOS) within the cyber community. The Army offered an EB of \$3,000 to \$20,000 for individuals in the Signals Collector/Analyst, MI Maintenance Integrator and Signals Intelligence Analyst occupations, three military occupational specialties related to the information operations cadre. Although the Air Force authorized EB for a small number of recruited occupations in FY09, with amounts ranging between \$2,000 to \$13,000 (depending on the job and term of enlistment), no cyber occupations were included in the offerings.

Educational Benefits

⁶Dr. Curtis Gilroy, Director for Accessions Policy, Office of the Undersecretary of Defense for Personnel and Readiness, quoted in www.defense.gov news article, *Officials Urge Congress to Protect Recruiting, Retention Incentives*, March 3, 2009.

In addition to enlistment bonuses, the Services may use educational enlistment incentives designed to aid in the recruitment of highly qualified individuals for critical or shortage occupational fields. The usage varies by Service and their use is determined by recruiting goals and occupational requirements.

The Post-9/11 GI-Bill

The Post-9/11 GI Bill provides financial support for education and housing to individuals with at least 90 days of aggregate service on or after September 11, 2001, and became effective in August 2009. Approved courses of study include graduate and undergraduate degrees, and vocational/technical training at an institution of higher learning approved for GI Bill benefits. Tuition and fees are paid directly to the school and cannot exceed the highest in-state tuition charged by a public educational institution in the state where the selected academic institution is located. Additionally, an individual may receive a monthly living stipend and an annual books and fee stipend of \$1,000. This benefit provides up to 36 months of education benefits, and generally, benefits are payable for 15 years following release from active duty.

Other Educational Benefits

The Army, Navy and Marine Corps all have college fund programs referred to as a “kicker,” which increase the value of benefits received under the G.I. Bill and may be offered to designated applicants, depending on individual military service requirements. Additionally, all of the Services may authorize the use of a loan repayment program that provides relief for qualified educational loans up to a maximum of \$65,000. The list of eligible career fields, and the amount of these incentives, varies continuously, based on individual military service requirements and the length of service obligation. Both the Army and Air Force offered their college fund “kicker” to the GI Bill to individuals in all recruited occupations in FY09.

Officer Personnel

Accession Bonus for New Officers in Critical Skills

The accession bonus for new officers authorized under title 37, Chapter 5, provides a monetary incentive to individuals who accept a commission or an appointment as an officer and serve on active duty in a Military Service in a designated critical officer skill for a designated obligation period. Each Service establishes criteria for award and administration of the bonus; its usage is limited and must be approved by the Secretary of Defense before the targeted bonus program is offered and the amount may not exceed \$60,000. For FY09, this bonus was largely used to target health professionals and individuals for intelligence and special operations occupations.

Educational Benefits

Commissioning Programs

The primary academic programs to acquire new officers to military service are the Service Academies and the Reserve Officers Training Corps (ROTC). Both of these programs provide highly competitive, merit-based scholarships for undergraduate education in exchange for an obligated period of active military service. The ROTC program is designed to be very flexible and options differ by Military Service. Individuals may be awarded 2, 3 or 4-year scholarships depending on whether they are accepted into the program as high school graduates or as enrolled college students.

Post 9/11 Montgomery GI Bill

Personnel accessing into the military to become commissioned officers have access to the same GI Bill Benefits as enlisted personnel.

3.4 Military Retention Incentives

Retention Bonuses

Selective Reenlistment Bonus (SRB)

The Selective Reenlistment Bonus (SRB) is the primary monetary force shaping tool to achieve required enlisted retention requirements by occupation or skill set. There are three key bonus zone areas targeted by the Military Services which are tied to years of service: Zone A (17 months to 6 years); Zone B (6+ to 10 years); and Zone C (10+ to 14 years). Factors included in determining the need for SRB include severe undermanning in the designated experiential years of service zone; high training or replacement costs; arduous conditions or unattractive occupation compared to other occupations; and mission criticality of the skill set. The Army and Marine Corps chose to give flat rate bonuses that varied by occupation, while the Navy and Air Force chose to apply an SRB bonus rate per occupation. This bonus rate varies by individual since it is made up of three variables: the individual's monthly basic pay, the SRB multiplier (a factor ranging from 0.5 to 12 (the higher the factor, the greater the criticality of the skill)), and the number of years (or fractions of year) for which the individual is reenlisting. These three factors are multiplied together to derive a service member's SRB award.

In FY09, the Army offered SRB to 12 cyber-related occupational specialties. Award amounts varied between \$1,500 to \$22,000, depending on the occupation, pay grade and zone, and obligated period of service; obligation periods ranged between 1 to 5 years of service. The Navy targeted key specialty areas within its IT Systems rating, including Systems Administrators and Network Operators and Analysts; all three zone areas were targeted, with SRB multipliers ranging from 1 to 3; Air Force also targeted all three zones for Computer Operators and Network Integrators, with similar SRB multipliers. The Marine Corps, the smallest of the Services, provided \$41,000 to \$65,000 in SRB to encourage Zone A individuals to reenlist and laterally

move to key occupations such as Data Network Specialist and IA Technician. Select Marines in these occupations, as well as other key specialties such as Data, Radio and Wire Chiefs, Intelligence Systems Administrator were also eligible for Zone B and C bonuses ranging from \$20,000 to \$52,000. Due to high retention, all Services greatly curtailed SRB service-wide (impacting many, if not all of their career fields) in the last few months of FY09; only Air Force continued to offer SRB to its IT personnel.

Critical Skills Retention Bonus (CSRB)

The Critical Skills Retention Bonus (CSRB) is a financial incentive paid to enlisted members and officers who reenlist or agree to continue serving on active duty for at least one additional year in a military skill designated as critical by the Secretary of Defense. The intent of the bonus is to provide a financial incentive to influence retention decisions of service members in designated critical skills taking into consideration current or projected manning shortages, skill imbalances, and high training or replacement costs. The IT/Cybersecurity communities were not specifically targeted with CSRB in FY09 by any of the Military Services.

3.5 Recruiting and Retention Standards and Measures

Service recruiting goals are typically established by the individual military personnel headquarters to ensure sufficient quantities of both officer and enlisted personnel are recruited by occupation. Officer retention is typically measured by continuation rates to assure enough individuals “continue” from one length of service year to the next. These rates are required to ensure sufficient experienced personnel have been retained before officers are eligible for promotion to the next rank. Enlisted personnel retention is divided into terms of enlistment (First, Second, Third) or zones to ensure enough personnel are retained at various stages of seniority. All targets are set individually by each Military Service commensurate with the health of the occupation and mission requirements. All of the Services stated that they met their military recruiting and retention goals for FY09.

While the DoD CIO serves as the IT Functional Community Manager for civilian IT occupations within the Department, monitoring the health and strategic direction of the community, management of DoD civilians is largely decentralized and is managed by individual organizations. Although there are no overarching recruiting and retention goals, the Department has a Human Capital Planning objective to achieve at least 85% of annual civilian personnel forecasted requirements. In FY09, DoD achieved 99% of forecasted requirements for its four mission critical occupations: IT Management, Computer Science, Computer Engineer and Electronics Engineer.

3.6 Recruiting and Retention Challenges

The Military Departments and Defense Agencies and Activities were asked to describe their recruiting and retention challenges. Figure 3.6 displays the top challenges in order of magnitude. Two organizations, the Defense Information Systems Agency (DISA) and the Defense Contract Management Agency (DCMA) cited Base Realignment and Closure (BRAC) as a retention

issue, as these are the organizations most significantly impacted in the next year as DCMA Headquarters move to Fort Lee, Virginia, and DISA moves to Fort Meade, Maryland. DISA is engaged in a multi-year planning process to facilitate effective continuity of operations during their relocation. Their full measure of success will not be fully known until closer to completion of the relocation.

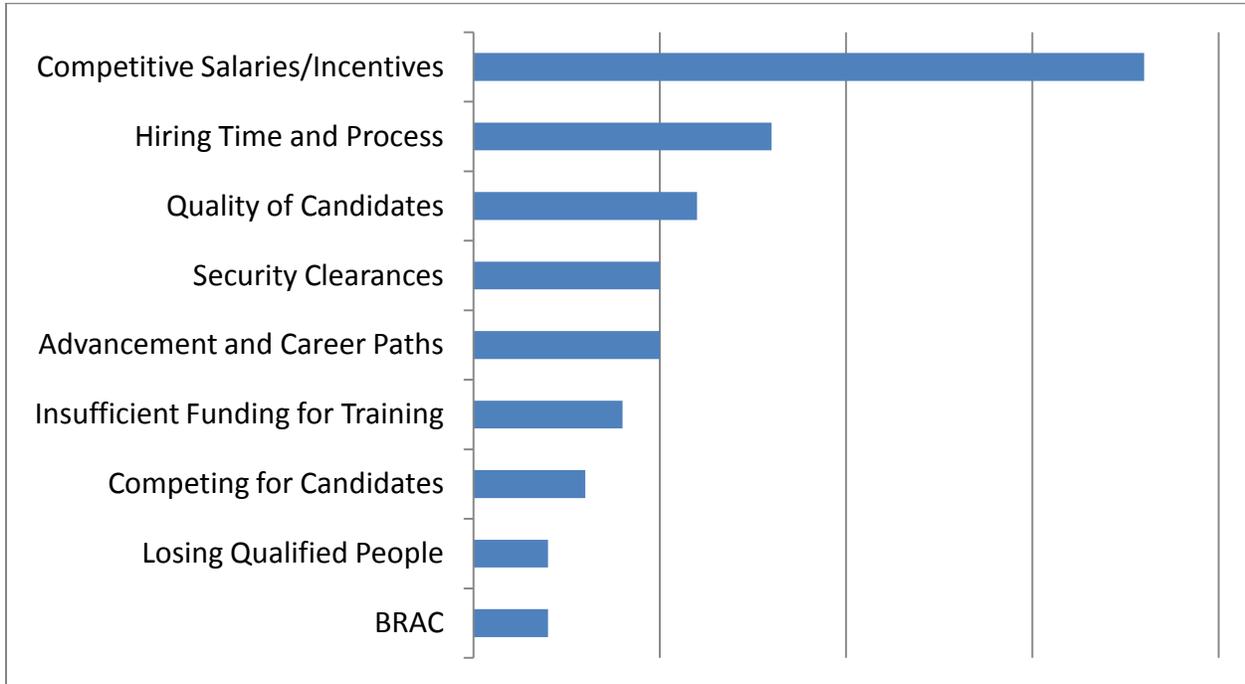


Figure 3.6 Recruiting and Retention Challenges

Administrative issues impacting hiring capabilities included the civilian hiring process and security clearance requirements. A Presidential directive on federal hiring reform and accompanying Office of Personnel Management implementation memorandum were published in May 2010. Time-to-hire is expected to continue to improve as federal and DoD hiring reform practices are instituted, however, improvements will take time to implement and the impact will not be fully realized for some time. Currently, the average time-to-hire in DoD is 80 days (internal hires take less time). In addition to the lengthy hiring process, many DoD IT/Cybersecurity jobs require a security clearance. The DoD and OPM have worked aggressively to improve processing times. In 2010, DoD was able to reduce its average processing time to 60 days, down from an average 325 days. The actual length of time varies per individual case, based on the completeness of the application, the complexity of the application data and level of clearance requested.

In order to assist in the recruiting of IT/Cybersecurity civilian personnel, OPM has provided two types of hiring authority, discussed previously in section 3.1. While these tools have provided some relief in bringing civilian IT/Cybersecurity individuals on board more quickly, DoD would prefer a more flexible and holistic approach to recruiting these skill sets. Rather than fragmented authorities that create large gaps in IT and cybersecurity skill coverage, there should be recognition of the pervasiveness of IT/cyber skills across series.

The quality of candidates also continues to be of concern. Although few Components directly stated “quality” was an issue, the significant response regarding the lack of competitive salaries is considered a proxy for quality in that Components could not attract the more highly qualified individuals with current salary offerings. Additionally, two Components reported that the discontinuation of the National Security Personnel System, and its more flexible pay schedules, had a negative impact on recruiting. The DoD has cited compensation as a concern in previous reports and has specifically identified the erosion in federal-wide special salary rates available to IT personnel in the IT Management, Computer Science, and Computer Engineering occupational fields as a contributing factor.

When IT special salary rates (SSR) were instituted in FY01 for the General Schedule (GS) 2210 series, the special rates were targeted by pay grade, with GS-5s receiving the largest differential (40%) and GS-12s the lowest increase (15%) against GS basic rates. In order to ensure that all eligible employees received an actual pay raise, the special salary rates factored in geographical location. Thus, the special salary rate exceeded locality pay, no matter where the employee’s place of duty. Figure 3.7 demonstrates the financial impact of special salary rates in 2002 for GS-9 personnel in the Washington D.C. area. The value of the rates meant that an individual in an IT occupation could earn \$6,000 to \$8,000 more than a non-IT employee. Unfortunately, the rates have been allowed to erode over time as annual increases to the locality pay tables have outstripped the increases to the SSR; in 2011, a GS-9 in IT earned only \$2,000 to \$3,000 more than a non-IT federal counterpart.

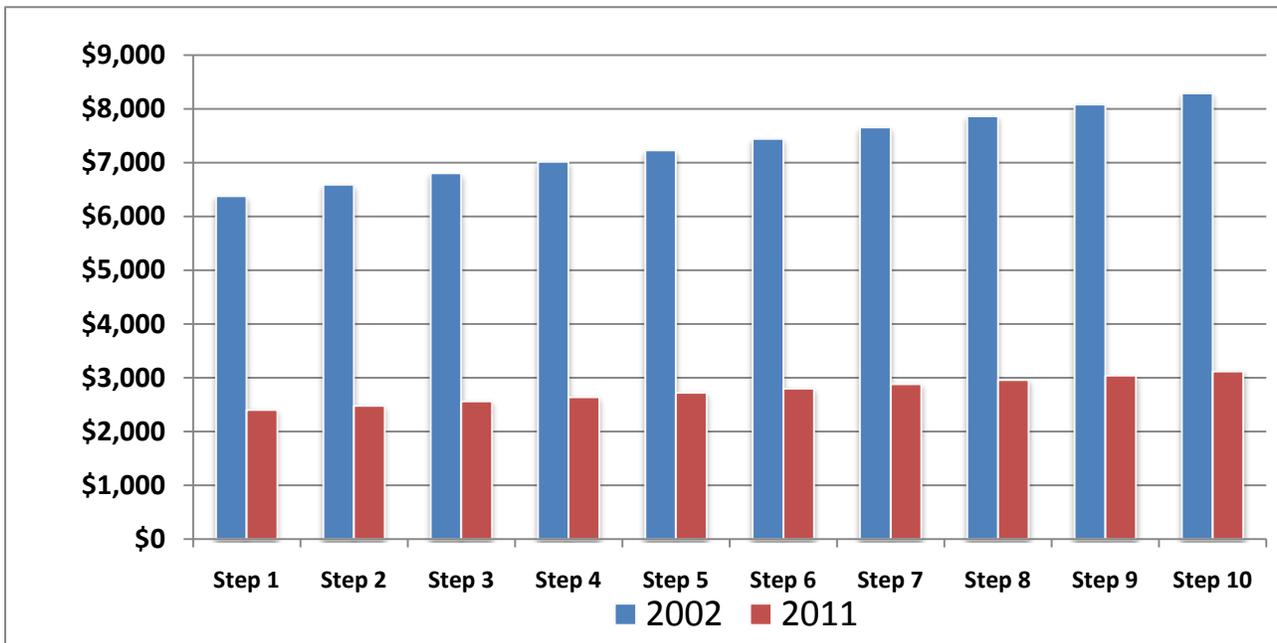


Figure 3.7 The Value of GS-9 IT Special Salary Rates in 2002 versus 2011

Figure 3.8 compares the results of a 2010 *Computerworld* salary survey with the average salary rates for DoD GS-9 to GS-15 personnel in the 2210 series (the largest IT occupational series in the

Federal Government). The differences in salaries for skilled IT personnel are telling, particularly at the lower pay grades. These lower starting salaries, coupled with a 2-year ban on federal pay raises, could have a striking impact on IT recruitment and retention as the economy improves. While IT salaries and industry growth have been somewhat stagnant during the past two years, in January 2011, Google announced its largest hiring plan in the company's history, with hiring numbers expected to grow 33% over 2010's 4,500 new hires. Further, they implemented at least a 10% salary increase for all employees, effective as of January 2011. While this dramatic action may not be the proverbial canary in the coal mine, i.e., a definitive sign of IT industry re-growth, it does indicate how responsive private industry can be, particularly in view of strong competition from a key competitor, Facebook, for skilled personnel. Approximately 10% of current Facebook employees are Google alumni.

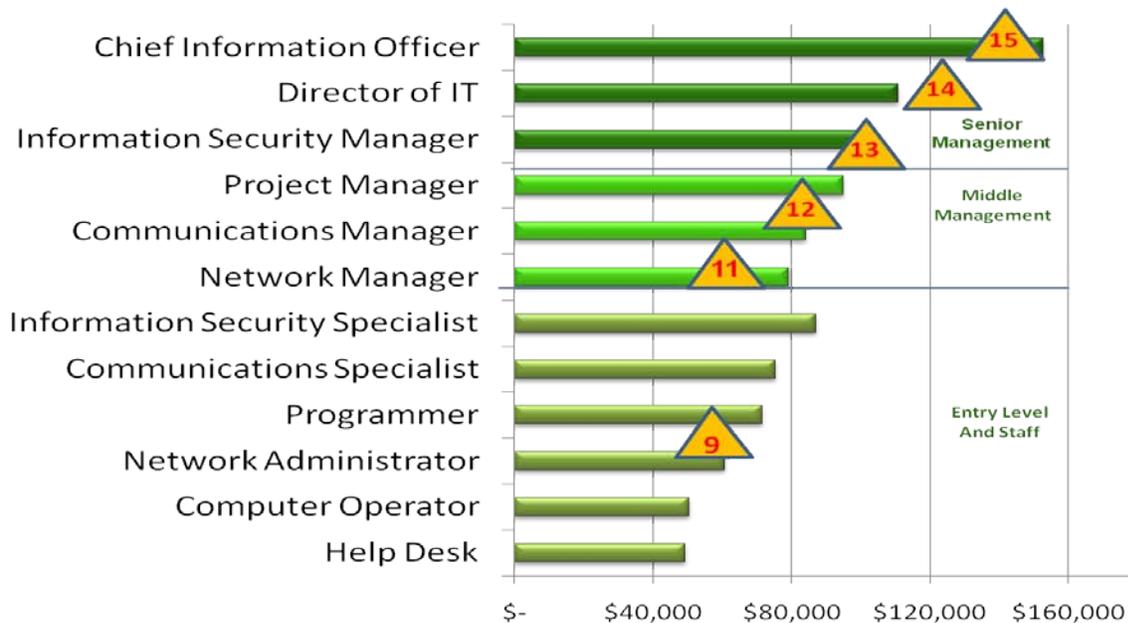


Figure 3.8 Comparing DoD General Schedule IT Salary Average with Select Jobs in Private Industry

In summary, DoD has continuing concerns about the ability to recruit qualified individuals in a timely fashion. The gaps in manning created by the time-to-hire, security clearance processing requirements (both for DoD and contractor personnel) and potentially, the additional training required to compensate for lesser qualified individuals, all have an impact on mission-readiness in this newest warfighting domain.

4. Academic and Cyber Outreach

*“While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, **it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success...**Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, **we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees.** It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950’s, to meet this challenge.”*

--quote from Comprehensive National Cybersecurity Initiative (CNCI) Initiative # 8

The ability of any organization to create a highly skilled, cyber-savvy workforce is challenging. Cultivating such a talent pool of professionals is even more difficult for federal agencies like the DoD, given the additional constraints of security clearance requirements, worldwide resource demands, the stand up of the new Cyber Command infrastructure and increased competition from the private sector. Additionally, DoD faces the long-term challenge of replacing an aging workforce with the critical talent needed to operate, defend and secure our nation’s infrastructure now and in the future. In order to meet these challenges, the Department is investing in the development of new, innovative and progressive programs to cultivate a highly motivated and highly-qualified pipeline of future cyber talent inspired to support the Department in achieving its mission. These programs combine a mix of high touch and high tech activities to engage students and leverages many “best practices” that private sector organizations have traditionally used to pique students’ interest and increase awareness in technical disciplines. The Department’s primary goal is to provide effective educational and outreach activities (through relationships with other government agencies, academia and the private sector) that will motivate and incentivize world-class cyber professionals to pursue careers at DoD.

4.1 DoD IT/Cybersecurity Academic Outreach Programs

Cyber Defense Competitions

In DoD, the Military Departments, Defense Agencies, and DoD schools have established strong programs to educate and engage military students to become future cyber operations personnel. Each year, the National Security Agency conducts a Cyber Defense Exercise (CDX) with teams of students from the nation’s military academies advancing their cyber skills by deliberately hacking into test (non-production) networks while protecting their own test networks against intrusions by other teams. In 2001, the competition started out on a small scale between a few schools. In 2010, the program celebrated its 10th anniversary and now has a total of eight U.S. and foreign academies competing: the U.S. Military Academy (West Point); the U.S. Naval Academy; the U.S. Air Force Academy; the U.S. Coast Guard Academy; the U.S. Merchant Marine Academy; the

Naval Postgraduate School(NPS); the Air Force Institute of Technology; and the Royal Military College of Canada.

The program's success is attributed to the competitive spirit and bragging rights the students gain from participating in the competitions, and also the invaluable cyber defense skills they pick up along the way. Many of the students serve in critical positions where they can apply the cyber skills they have acquired in the competitions.

Additionally, at the Air Force Academy many of the cadets participating in the Cyber Defense Exercises (CDX) are also pursuing the cyber warfare track within the Academy's computer science degree, which requires that they take cryptography, information warfare, and network security courses. To enable some of the training that is also required for a competition like the Cyber Defense Exercise, the Academy has a Cadet Cyber Warfare Club that provides a sandboxed network where cadets can learn the craft of network defense.

The National Defense University's Information Resources Management College (iCollege) also conducts numerous outreach programs during the year to prompt cybersecurity education and awareness. Most recently the iCollege hosted a series of "Cyber Security Challenge" competitions in 2009 and 2010. The exercises involved pitting government agency teams against each other to test their ability to defend their information infrastructure against an onslaught of cyber attacks. Among others, teams participated from the Defense Information Systems Agency (DISA), the U.S. Naval Academy, the U.S. Military Academy, and the Army's Intelligence and Security Command. The exercise was conducted using a "live," but isolated computer and communications network. This enabled participants to exploit vulnerabilities both against each other and against a centralized server repository. Network penetration tools such as Backtrack 4.0 were available to the teams. The exercises capitalized upon knowledge gained from similar competitions such as the CDX and competitions held at conferences such as "Black Hat" and "DEFCON", making them exceptionally attractive to cybersecurity professionals. The NDU iCollege plans to hold future cyber challenges on an annual or semi-annual basis.

Outside of the Military, a successful outreach program for civilians is the Defense Cyber Crime Center (DC3). The DC3 sponsors the Digital Forensics Challenge, with the goal of encouraging young people to develop aptitude and skills in cyber investigations and forensics. As part of the competition, U.S. high school teams are assigned specific tasks that might face a cyber crime analyst--decrypting password-less files, tracing digital intrusion, and reconstructing incomplete data sources. Significant prizes are awarded to individuals who find solutions to digital forensics problems that currently cannot be solved.

Similarly, CyberPatriot, which was initially sponsored by the Air Force Association in 2009, is the world's largest high school cyber defense competition and is used by the Department to educate and motivate the next generation of cyber defenders for the nation. Open to all high schools nationwide, the program reached 25,000 students in 2009 and was expanded in 2010 to reach many thousands more. The DoD continues to be a key sponsor providing expertise and funding. DoD also supports similar cyber defense competitions at the collegiate level, such as the National

College Cyber Defense Competition (NCCDC). The NCCDC, sponsored by the Department of Homeland Security (DHS) and various private sector organizations, brings winners of regional cyber defense competitions together for a 3-day competition each year. Northeastern University won the competition in 2010.

Cyber Boot Camps and Summer Internship Opportunities

The Air Force Research Laboratory (AFRL) Cyber Operations Branch offers a 10-week summer program each year for university students, aimed at developing future cyber officers. The Advanced Course in Engineering (ACE) Cyber Security Boot Camp has been held at Rome, New York, for the past 7 years, and involves between 40 to 60 student applicants from Air Force and Army pre-commissioning programs, some National Science Foundation (NSF) Cyber Corps Fellows and select civilian college students. Boot camp participants attend lectures on cyber warfare presented by faculty from academia, industry and government. At the 2010 event, topics included computer network defense, digital forensics and wireless security. Students are assigned real-world problems to solve and write reports detailing their solutions. For three days each week, students complete internships under scientists and engineers working on military and industry research within the AFRL's Information Directorate.

In addition to academics and research, ACE participants engage in leadership development activities. These activities include weekly 8-mile runs, study in the art of warfare, and staff rides to the Gettysburg and Fort Ticonderoga battlefields. The faculty for ACE is drawn from Syracuse University, West Point, and Norwich University, all which are Centers of Academic Excellence in Information Assurance Education (CAE/IAE). The enrichment programs at these institutions have led to other efforts with DoD and other federal agencies to further promote the development of future cyber talent. For example, Syracuse University partners with the NDU iCollege to offer master's and doctoral degree programs in a variety of IT/Cybersecurity disciplines. Furthermore, the DHS and the NSF have recognized the ACE program as an official internship program for the Federal Cyber Corps, Scholarship for Service (SFS) program. Recent ACE graduates are now working at the Air Force Office of Special Investigations, the AFRL and the National Security Agency (NSA), and there are ACE graduates serving in every squadron under the new Air Force cyber command, the 24th Air Force.

As a result of program success with the ACE summer program, Syracuse University developed a special cyber security course in September 2006 that is offered in 12 high schools in New York State. Today, Syracuse University offers 29 introductory cyber security courses in 148 high schools throughout New York, New Jersey, Maine, Massachusetts, and Michigan. High school students who successfully complete the cyber security courses can receive Syracuse college credits in computer science and engineering.

Career Fairs, Workshops and Conferences

Many DoD Agencies, like DISA, send representatives to University and College career days, and conduct major job fairs where potential employees can interact with DoD representatives. These

activities tend to be very effective in bringing in quality candidates for the recruitment process and are in keeping with the Partnership for Public Service's recommendation that successfully recruiting the youngest generation into the workforce includes both high tech and high touch (individual outreach) activities.

Other organizations regularly host important conferences in the area of computer security and information assurance. For example, NPS in Monterey, California, offers the Workshop in Education for Computer Security (WECS) to educators in community colleges and 4-year universities/colleges who are trying to integrate IA disciplines in their computer science departments. The program's goal is to provide these educators with resources, tools and knowledge on how to teach their students about computer security/IA. Attendees take classes, work on computer lab exercises and engage in discussion groups to help them formulate their information assurance curricula. Participants are required to report back on how they have incorporated workshop materials, practical exercises and teaching styles into their classroom and curricula, thus insuring that information learned at the workshop will be applied in the public sector. The conferences are organized by the NPS' Center for Information Systems Security Studies and Research (CISR).

Aligning DoD Cyber Needs With DoD Science, Technology, Engineering and Mathematics (STEM) Workforce Outreach

In a world where advanced knowledge is widespread and low-cost labor is readily available, U.S. advantages in the marketplace and in science and technology have begun to erode. In a 2008 publication by the Congressional Research Service, it was noted that among an international assessment of 15-year old students, the U.S. ranked 28th in math literacy and 24th in science literacy. Moreover, the U.S. ranked 20th among all nations in the proportion of 24-year-olds who earn degrees in natural science or engineering. To combat these alarming statistics, the Department has ramped up its efforts to develop the next generation of scientists and engineers with the requisite skills to meet the nation's mission needs.

As a result of this new focus, there are several, well-established and effective education and outreach programs that promote academic outreach and education at the kindergarten to high school (K-12) and university level with the goal of developing future Science, Technology, Engineering and Mathematics (STEM) talent for the Department. Additionally, DoD recently published a 5-year strategic plan to reinforce its commitment to increasing the nation's talent pool of STEM professionals. While effective, a key finding from this effort has been that most of the STEM educational and outreach programs across the Department tend to focus on building the nation's pipeline for scientists and engineers, not IT/IA/cyber professionals. Additional effort will be taken to focus on incorporating IT/Cybersecurity disciplines within the broader STEM arena.

4.2 Maximizing Collaboration to Develop a Skilled IT/Cybersecurity Workforce

Through collaborations with government, academia, and industry, the DoD advocates for advancements in IT/Cybersecurity education, outreach, training and awareness. The following reflects several relationships that DoD has cultivated to benefit the Department and its IT workforce.

Partnerships with Government

National Cybersecurity Education Initiative – CNCI/NICE

Having the right people with the right skills and abilities to protect the nation in cyberspace has been identified as one of the most serious economic and national security challenges we face as a nation. Initiative #8 of the broader Comprehensive National Cybersecurity Initiative (CNCI) (an initiative created to protect the nation in cyberspace) was established to help face this challenge head-on with a strategy to build a cyber-savvy nation through training, awareness, kindergarten through post-graduate educational programs, and professional development for federal security professionals.

Originally known as CNCI Initiative #8, this effort was renamed the National Initiative for Cybersecurity Education (NICE) in May 2009. The new initiative, NICE, represents the continual evolution of CNCI Initiative #8, with an expanded scope that reaches beyond solely a federal focus to a larger, national focus. The National Institute of Standards and Technology (NIST) has assumed the overall coordination role for NICE and is currently identifying resources to be applied to this initiative by reviewing all related previous activities, and developing a strategic framework and a tactical plan of operation to support that framework. Co-leading selected activities under the NICE umbrella are DHS, DoD, the Department of Education (DOE), the White House's Office of Science and Technology Policy (OSTP), the Office of Personnel Management (OPM), and the Office of the Director of National Intelligence (ODNI).

While each of the co-leads has specific accountabilities under NICE, implementation of the initiative will be very much a collaborative effort between federal, state and local government, industry, academia, non-government organizations and the general public. Success for this effort will enhance of the overall security posture of the United States. To meet NICE objectives, efforts have been structured into the following four tracks:

- **Track 1: National Cybersecurity Awareness (Lead: DHS).** Public service campaigns to promote cybersecurity and responsible use of the Internet; make cybersecurity popular for children; and promote cybersecurity educational and career pursuit for older students.
- **Track 2: Formal Cybersecurity Education (Co-Leads: Department of Education and OSTP).** Education programs encompassing K-12, higher education and vocational programs related to cybersecurity, with a focus on the science, technology, engineering

and math disciplines to provide a pipeline of skilled workers for private sector and government.

- **Track 3: Federal Cybersecurity Workforce Structure (Lead: OPM).** Personnel management functions, to include defining cybersecurity jobs in the Federal Government and skills and competencies required. New strategies to ensure federal agencies attract, recruit, and retain skilled employees to accomplish cybersecurity missions.
- **Track 4: Cybersecurity Workforce Training and Professional Development (Tri-Leads: DoD, ODNI, DHS).** Cybersecurity training and professional development required for Federal Government civilians, the military and contractor personnel.

The DoD is heavily involved in implementation activities underway in all four tracks of NICE. As a part of Track 3, DoD and DHS, with participation from the Office of Personnel Management and the Office of the Director of National Intelligence have worked to bring together stakeholders across the three agencies to better define a competency taxonomy for IT Infrastructure, Operations, Maintenance and IT/Cybersecurity functions. DoD, as a co-lead of Track 4 is forging new relationships with private sector corporations to develop universal standards for cybersecurity training and education. Additionally, all current DoD educational and outreach programs in the area of IT/Cybersecurity align to the federal mission of NICE.

Cybersecurity Education and Collaboration

The iCollege at the National Defense University has a robust program to improve communication and information sharing in the area of cybersecurity among DoD and its government partners. The iCollege IA certificate and education programs attract federal, state and local government leaders to an array of cybersecurity classes at the college, adding their important voices to the learning environment and enriching the classroom experience. Below are several federal agencies who participate in the iCollege IA certificate programs:

- U.S. State Department
- Federal Bureau of Investigation
- Department of the Interior
- Department of Homeland Security
- Department of Commerce
- Department of the Treasury
- Environmental Protection Agency
- Federal Aviation Administration
- General Services Administration

Moreover, the iCollege cybersecurity education program promotes a strong international presence with international military and civilian leaders from over 25 countries participating in college courses, programs, international conferences and collaboration on capacity-building projects.

IT Job Shadow Day

The DoD IT Job Shadow Day is an annual event designed to assist in recruiting the next generation of rising stars to government service and is held in conjunction with the Federal Chief Information Officers Council federal-wide IT shadow day activities each February. The program provides high school students an opportunity to learn about the Department and interact with top IT/Cybersecurity professionals in DoD. Students also participate in hands-on demonstrations and games to teach them basic attack and penetration techniques and how to crack complex computer codes.

The relationships formed between students and Components at these events have led to internships at DISA and the Defense Criminal Investigation Services Agency, as well as educational outreach activities between DoD Components and the schools throughout the school year. As the numbers of students pursuing IT-related college degrees continue to decline, outreach programs like the IT Job Shadow Day are becoming increasingly important to DoD to motivate and educate future IT professionals and attract them to the Department.

Education Agreements with Centers of Academic Excellence in Information Assurance Education (CAE/IAE)

The CAE/IAE Program serves as the cornerstone of the nation's efforts to promote information assurance (IA) education, and to produce the growing number of IT/Cybersecurity professionals needed to protect, operate and defend our national information infrastructure. Sponsors of the program, NSA and DHS, work in close consultation with the Office of the DoD CIO to accomplish the goal of the CAE program. Since its creation in 1999, the civilian academic community of CAEs has grown from seven 4-year colleges and research institutions to 117. These schools play a vital role in equipping future IT/Cybersecurity professionals with the requisite skills, knowledge and abilities they need to support DoD critical missions. Additionally, several DoD schools have been designated as CAEs: the Air Force Institute of Technology, the iCollege of the National Defense University, the Naval Postgraduate School, the U.S. Air Force Academy, the U.S. Naval Academy, and the U.S. Military Academy (West Point). Like all CAEs, these schools serve as regional centers of IA expertise and provide educational programs aimed at enriching individuals' skill sets and retaining DoD IT personnel.

To be designated as a CAE/IAE, an institution must be a nationally or regionally accredited 4-year college or graduate-level university. Applications are assessed against stringent criteria defined by the Committee on National Security Systems (CNSS), which are intended to measure the depth and maturity of programs of instruction in IA at the graduate and undergraduate levels and applicants must clearly demonstrate how they meet each of the criteria. Designation as a CAE/IAE is valid for five academic years, after which the school must successfully reapply in order to retain its CAE designation.

Given the success of the CAE/IAE program, a Center of Academic Excellence in 2-Year Education (CAE-2Y) program was established in 2009 as an additional means to develop cyber talent. The

CAE-2Y program is available to community colleges that have established a robust IA program, and have successfully mapped their curricula to the CNSS standards. In 2010, six community colleges became the nation's first group of CAE-2Ys. A full list of CAE/IAEs and CAE-2Ys is located at Appendix D.

As mentioned in Chapter 3 of this report, through recruiting and retention scholarships and institutional grants funded by the DoD Information Assurance Scholarship Program (IASP) and the federal Scholarship for Service (SFS) Program, the CAE/IAE program continues to develop for federal employment, a cadre of highly motivated, educated professionals who are knowledgeable in the principles of IT and IA/cybersecurity. As the program continues to evolve and expand, it will remain a vital component of the nation's mission to recruit the best and brightest IT/Cybersecurity talent needed to support future national security needs. The following success stories highlight the meaningful work DoD is achieving through education agreements with CAEs:

National Defense University's iCollege

The Office of the DoD CIO works closely with the iCollege and oversees its IT/Cybersecurity curricula and executive programs. The iCollege, which is a designated CAE, currently has education agreements with over 40 academic institutions across the United States. Graduates of the iCollege's Advanced Management Program, CIO Certificate Program, IA Certificate Programs, Enterprise Architecture Certificate Program, Organizational Transformation Certificate Program or the Information Technology Project Management Certificate Program can apply 9 to 15 graduate credit hours toward participating master's and doctoral degree programs at selected regionally accredited partner universities/colleges. In areas of mutual interest and expertise, faculty members at the iCollege connect with advance knowledge and practice centers at Duke University, The John F. Kennedy School, Harvard University and The George Washington University. The iCollege has also entered into memoranda of understanding with many industry partners to share cybersecurity best practices and tips for improving the security of their network infrastructures. Each year, the iCollege holds an Open House with its partner institutions in order for interested students to discuss and learn more about degree programs available in the area of cybersecurity.

University of Nebraska at Omaha

Since 2008, the Office of the DoD CIO has worked with the University of Nebraska at Omaha to conduct the annual International Cyber Defense Workshop, an exercise providing training to counter escalating network probes and attacks around the world. Unclassified, virtual networks are set up to provide an isolated training ground for the militaries of over 15 allied countries. Students from the University of Nebraska train and participate in exercises on how to recognize, prevent and remediate common network security vulnerabilities. The cyber workshop serves as a key building block to strengthen linkages among cyber centers and assists international partners in building technical proficiencies.

University of Advancing Technology

The Office of the DoD CIO sponsors a class with the University of Advancing Technology (UAT), located in Tempe, Arizona, to develop interactive cybersecurity training and awareness products in support of the DoD's annual security awareness campaign. The class is offered to UAT's network security and gaming students each trimester. To date, students have developed two viable games including "Social Miner," a social networking awareness game, and the "Cyber Hero," a game designed to engage middle school students in cyber. The intent is to make these and future games available in public forums including the Society for Science and the Public's website and via the NSF Advanced Technological Education Program Regional Centers.

The George Washington University

The George Washington University and the US Army have worked together to offer the Science and Engineering Apprentice Program (SEAP), whereby high school through college students are placed in DoD laboratories for eight continuous weeks during the summer. Students with interest in sciences and mathematics work closely with scientists and engineers who act as mentors. The program offers a unique experience for hands-on learning in real world projects, thus encouraging students to pursue careers in science and engineering.

Agreements with Industry

Army School of Information Technology

The Army's School of Information Technology (SIT), at Fort Gordon, Georgia, works with several corporations to the benefit of the students pursuing cyber-related degrees. The SIT has strong vendor partnerships with most of the well known names in IT/Cybersecurity, such as: the Computing Technology Industry Association (CompTia), Adobe, NetApp, the Internet Systems Consortium (ISC), and the SysAdmin, Audit, Network, and Security (SANS) Institute. The SIT is also the largest Microsoft Academy in the United States. The Fort Gordon staff continues to explore additional corporate partners and wants to expand its outreach efforts with Silicon Valley.

International Multilateral Partnership Against Cyber-Threats

The International Multilateral Partnership Against Cyber-Threats (IMPACT) is the first global public-private initiative against cyber-terrorism. The IMPACT program is dedicated to bringing together governments, industry leaders and cybersecurity experts to enhance the global community's capacity to prevent, defend, and respond to cyber threats. In 2009, IMPACT was one of the key sponsors of the DoD Digital Forensics Challenge.

Threat Situational Awareness - Defense Industrial Base

In line with the broader CNCI federal initiative, over 35 major companies from across the defense industrial base are participating in a pilot program with the DoD for shared cybersecurity threat situational awareness and information sharing. The Pilot Program's Policy Operations Working Group is comprised of industry chief information security officers and their defense counterparts and meet quarterly to address both classified and unclassified threat information. The Working Group currently is working to elect representatives to participate in Track 4 of NICE, a federal cybersecurity workforce effort led by DoD and DHS that focuses on training and professional development. As part of this effort, industry representatives will participate with federal agencies in developing a national training standard for individuals performing IT infrastructure, operations, management and IA functions. Following the pilot, the opportunity to participate in this forum will be extended to over 2,650 companies who currently have the ability to store secure information.

4.3 New Initiatives Underway to Develop and Attract Future Cyber Warriors

As stated previously, DoD is committed to developing a cyber-savvy workforce with the necessary mix of cyber knowledge, skills and abilities needed to protect the Department and the nation in cyberspace. To meet its requirements, DoD will continue to enhance and expand current educational and outreach programs, as well as develop new ones in close collaboration with other federal agencies, academia and the private sector. Below are a few initiatives that have recently been launched to develop and attract future cyber warriors.

Navy Cyber Option Scholarship Reservation Program

Current DoD existing cyber education and outreach programs have demonstrated success and provide strong models from which to continually build new programs for attracting and retaining cyber talent. For example, the Department of the Navy has recently launched the Cyber Option Scholarship Reservation (COSR) program, which allows students who demonstrate superior cyber operations potential to be awarded a Naval Reserve Officers Training Corps NROTC scholarship and be commissioned as IT professionals in the Navy's Information Dominance Corps. The Information Dominance Corps leverages the DoD 8570.01-M "Information Assurance Workforce Improvement Program" as a starting point for program structure and development. Navy recruiters are now being provided with overview information related to the Information Dominance Corps, which allows them to enhance their outreach activities and determine which applicants have scholarship potential.

FedRecruit Program

FedRecruit is a Partnership for Public Service initiative aimed at building federal agency capacity and practical know-how in the recruiting, hiring and on-boarding of top entry-level talent in mission-critical occupations. This goal is accomplished by the Partnership offering its agency partners guidance on strategic planning and decision making, a forum to network and exchange

ideas with other federal agencies, and full access to their recruiting materials and experts. Phase I of the initiative focused on the federal acquisition workforce and the agency partners included the Environmental Protection Agency, the National Aeronautics & Space Administration, and the National Nuclear Security Administration. Phase II focuses on building agency capacity in mission critical occupational areas, such as cybersecurity within the IT workforce. The Department of the Air Force is participating in Phase II of the pilot, alongside the Department of Agriculture, the National Oceanic and Atmospheric Administration, Immigration and Customs Enforcement, and the Social Security Administration. At the completion of Phase II, the Air Force will share recruiting materials, lessons learned and resources with other DoD Components.

National Science Foundation – Regional Cybersecurity Centers

Through NICE Track 4, the Office of the DoD CIO is seeking to develop new outreach efforts with the NSF's Advanced Technological Education Program Regional Centers, whose focus is on 2-year colleges, with programs for K-12 prospective teachers. These centers, whose missions align to the NICE and broader DoD IT workforce initiatives, provide K-12 teachers with support for cyber defense exercises and awareness training. Examples of these initiatives include: The Center for Systems Security and Information Assurance, which provides curriculum and instructor training resources to mid-western schools; the Cybersecurity Education Consortium, aimed at providing education and training opportunities for 2-year universities/colleges throughout Oklahoma and surrounding areas, IA and forensic curriculum resources, and professional development opportunities for 2-year university instructors nationwide; and CyberWatch, a DC-metropolitan based effort, whose mission is to increase the quantity and quality of the IT/Cybersecurity workforce. The CyberWatch goals are focused on IA education at all levels, from elementary through graduate school, but especially the community college level, and include curriculum development, faculty professional development, student development, career pathways and public awareness. Additionally, CyberWatch provides best practices, course materials, faculty training and support to schools nationwide looking to develop an information security curriculum.

5. Creating New Public/Private Initiatives

Many DoD Components have well-established programs and partnerships in place to strengthen and train IT professionals, and as the cyber force and domain evolves and matures, existing initiatives within the Department are being expanded and new efforts are being created. To complement these efforts, the DoD is forging new partnerships at the public and private levels.

5.1 Enhancing DoD's Certification Programs

Information Assurance Workforce Improvement Program (IA WIP) Certification Committee

The IA WIP Certification Committee is made up of representatives from every DoD Component who convene, as necessary, to discuss the IA certification needs of the DoD IA Workforce and influence commercial certification vendors to meet those needs. The Certification Committee is actively engaged with the six commercial vendors (CompTIA, the EC Council, the International Information Systems Security Certification Consortium, Incorporated, the Information Systems Audit and Control Association, SANS and the Security Certified Program) currently identified in DoD 8570.01-M as authorized sources to comply with defense IA certification requirements. These commercial vendors rely on the Committee to supply DoD subject matter expertise and best practices to enhance the rigor and relevance of their examinations, while the Committee relies on vendors to provide private sector best practices and global testing platforms on which DoD can certify its IA workforce. The Committee will continue to leverage existing partnerships with DoD 8570.01-M approved certification vendors, but is also pursuing new partnerships, such as with the National Board of Information Security Examiners (NBISE), to continually strength the DoD IT/Cybersecurity workforce.

Virtual Training - Carnegie Mellon University

The Defense Information Systems Agency (DISA) sponsors access to the Carnegie Mellon University Software Engineering Institute Virtual Training Environment (VTE) for more than one-third of the Department's IA workforce. This is a web-based online training platform, virtual technical lab and knowledge library for specialty areas including forensics, incident response and certification preparatory courses. The DoD is partnering with Department of Homeland Security (DHS) to move the Virtual Training Environment to a ".gov" domain environment, whereby all federal users, including DoD personnel, will have access to this training platform.

5.2 Forging New Relationships to Strengthen Cybersecurity Capabilities

Forensics Training - Mississippi State and Auburn University

The Wounded Warrior Training Program is designed for America's wounded, disabled and transitioning veterans. It is modeled after the successful training program completed by over 2,500 law enforcement personnel across the country. Mississippi State University's Forensics Training Center, in collaboration with Auburn University and Tuskegee University, are providing tactical level occupational training to America's veterans through no-cost vocational training in a critical shortage technical skill, digital forensics. The program is funded as a pilot program by the National Science Foundation (NSF). In 2009, the Office of the DoD CIO facilitated the training offered at Walter Reed Army Medical Center, and in 2010, the Office of the Under Secretary for Policy (OUSDP) facilitated the expansion of the program to the Brooke Medical Center in San Antonio, Texas. The pilot administrators' goal is to offer digital forensics training for recovering military personnel at other major Warrior Transition Units across the country. The OUSDP also facilitated private industry partnerships between members of the San Antonio Chamber of Commerce, the Air Force, and other members of the San Antonio community to provide trained Wounded Warriors with internship opportunities. Mississippi State University and Auburn University are proposing to lead a consortium consisting of additional Centers of Academic Excellence in Information Assurance Education (CAEs) to meet this great need for training. They are also considering the inclusion of a program for law enforcement wounded in the line of duty.

National Defense University iCollege

The iCollege is recognized as a global hub for educating, informing and connecting information leaders with value-added knowledge. Last year, the iCollege began hosting international conferences, bringing together senior-level government and private sector representatives from over 20 nations to form relationships and collaborate on cybersecurity matters. Conference speakers were comprised of high-level speakers from organizations such as: CISCO, Microsoft, Google, McAfee, Raytheon, VMware, TIBCO, Amazon, AFCEA, and U.S., Singapore, and Far East governments. The conference was co-hosted with the Institute of Systems Science (ISS) of the National University of Singapore, which is known for its broad-based advanced professional continuing education in information technology.

Other Defense Initiatives

The DoD Components continue to establish local and regional partnerships with colleges and universities that offer specific, accredited programs of study focused on developing future civilian IA professionals with the critical skills needed to fulfill their mission requirements. The Army Intelligence and Security Command (INSCOM) group has recently begun to partner with colleges to increase the capability and awareness of mission critical areas such as high-end computer network and cyberspace operations among future cyber professionals. The INSCOM group is also planning partnerships with ANRC technology experts and the University of Maryland Baltimore

College to obtain quality computer security education for existing cyberspace operations professionals.

5.3 Exploring Rotational Assignments with Public/Private Organizations

The DoD CIO is leading a pilot program to enhance its position and expertise in the field of IT, including emerging areas such as cybersecurity. Section 1110 of the National Defense Authorization Act, fiscal year 2010 (FY10), (Public Law 111-84), authorized the DoD to establish a Pilot Program for the Temporary Exchange of Information Technology Personnel (referred to as the Information Technology Exchange Program (ITEP) pilot. The ITEP pilot authorizes the temporary detail of DoD and private sector employees who work in the field of information technology to participate in an exchange between sectors. In addition to working in the IT field, an employee must be considered an exceptional employee, expected to assume increased information technology management responsibilities in the future, and compensated at the GS-11 or above (or equivalent). The assignment details (planned to commence in the third quarter of 2011) can range from 3-12 months and can be extended up to 1 year. The ITEP pilot has a numerical limitation of no more than 10 employees participating at any given time.

The ITEP pilot can be tailored individually to each employee's professional development or operational interests and provides a unique opportunity for DoD and the private sector to share best practices and the common problems faced by both sectors, such as data strategy, information sharing, and IT security.

The use of rotational assignments has been growing in the last few years at DoD as a viable way to build and improve the skills of its cyber workforce. For example, the Army's School of Information Technology (SIT) at Fort Gordon is cultivating corporate collaborations with industry through the DoD Training With Industry program (TWI). Through TWI, the Army has sent four soldiers to corporations for a year each to work alongside IT/IA professionals. The program also sent two warrant officers to Microsoft, one to Cisco, and one to General Dynamics. To date, these assignments with industry have enabled shared best practices and have forged strong corporate relationships. Within the Department of the Navy, the Naval Sea Systems Command (NAVSEA) has a formalized developmental rotation program for all new employees at the ND-2/3 level. These employees must complete two, 4-6 months rotations at organizations outside their home branch. Cyber personnel at NAVSEA get to choose an appropriate assignment to strengthen their skills. Additionally, the Intelligence and Security Command (INSCOM) group in the Department of the Army is planning to leverage the Intergovernmental Personnel Act (IPA) Mobility program to offer rotational assignments with other federal agencies and industrial partners. The IPA Mobility program will assist INSCOM in the transfer and use of new cyber technologies and problem solving improvements by facilitating professional details of DoD employees between the public and private sector.

Given the changing workforce dynamics in the IT field, DoD will continue to take advantage of rotational programs to proactively position itself to keep pace with the changes in technology. Information technology is the great enabler to an organization's mission success. Industry and

DoD can share best practices and can learn from each other to enhance employee competencies and IT technical skills.

6. The Way Ahead

The Department, which has traditionally viewed cyber as an information technology (IT) discipline, is broadening its definition to include emerging cyber specialties, such as all-source intelligence, law, policy and strategy. As a result, DoD is actively pursuing opportunities to ensure that it has the right number of individuals with the right mix of skills to meet current and future cyber-related missions, regardless of their occupational series. As this work continues, there are several initiatives which can assist the Department to holistically manage IT/Cybersecurity personnel. These include new recruiting and retention authorities, compensation modifications and training improvements which are discussed below.

6.1 Recruiting and Retention Authorities

Establish Comprehensive, Flexible Expedited IT/Cybersecurity Hiring Authority for DoD

Figure 6.1 compares the current IT hiring authorities provided by the Office of Personnel Management (OPM) against the DoD Acquisition hiring authority. The Acquisition community has greater latitude and ability to adjust the authority internally within the Department, based on current mission requirements. This Acquisition authority was provided by Congress. A similar legislative authority, targeted to DoD's IT/Cybersecurity community would enable DoD to strategically manage a multi-discipline community in a holistic manner, using expedited hiring as necessary to achieve timely recruitment and placement of IT/Cybersecurity personnel across occupational series. Within DoD, it has been found that while the majority of cyber professionals are concentrated in five occupational series (IT Management, Computer Scientist, Computer Engineer, Electronics Engineer and Telecommunications Specialist), this functional area of expertise crosses many series. And, placing numerical limitations of the number of hires yearly, fails to recognize the scope of DoD's annual requirements. For example, DoD hired over 4,800 new hires in the civilian IT Management (2210) series in FY10.

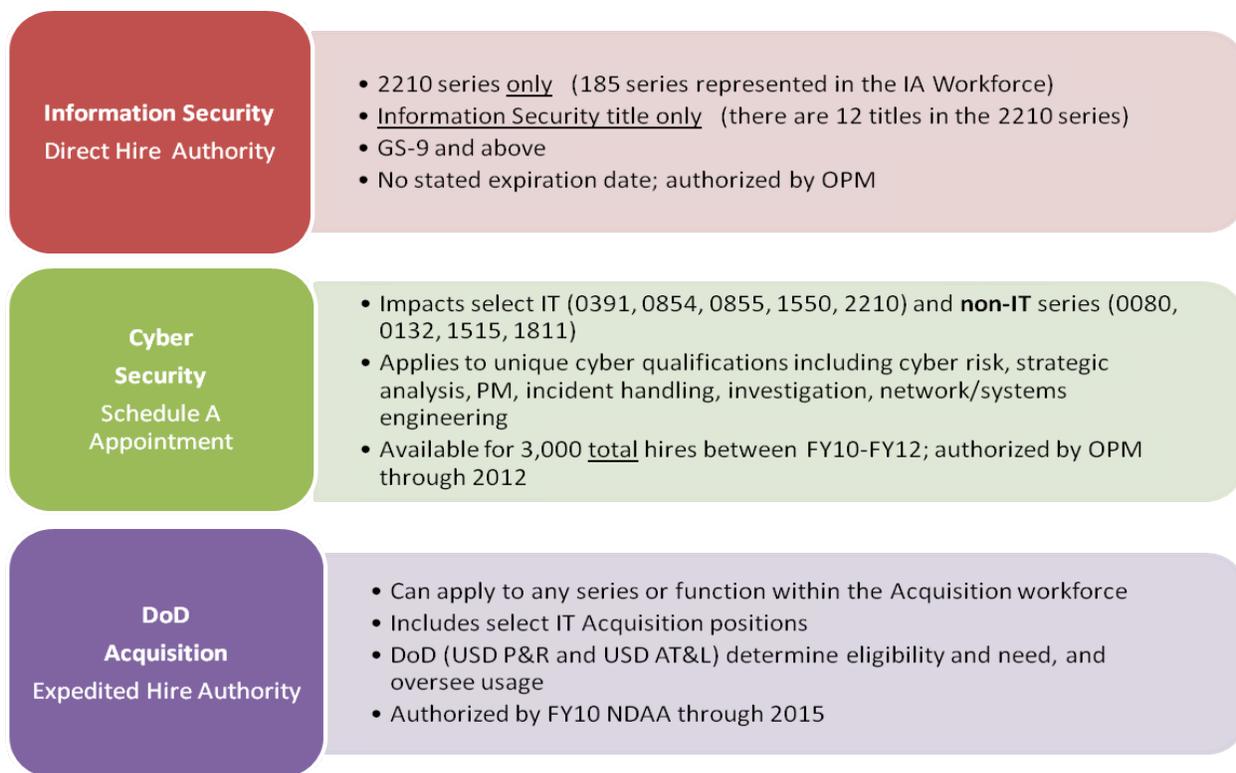


Figure 6.1 Comparison of Hiring Authorities

Increase Capacity for the Information Assurance Scholarship Program

As discussed in Chapter 3, the Information Assurance Scholarship Program (IASP) is designed to recruit and retain the nation’s top IT/Cybersecurity talent, which is critical as we progress in the cyber arena. The IASP has been a proven tool, particularly in recruiting new DoD civilian personnel, however, with a static funding level of \$5M, the capabilities of the program have eroded. Component increasing demands for scholars have gone unmet as shown in Figure 6.2 below. This higher demand, coupled with lower buying power, is impacting the value of the program. Per the College Board, the average cost of college tuition has increased 4.9% annually over the past 10 years, increasing college costs by 50% over the last decade.

In addition to scholarship funding, the IASP is also authorized to grant capacity build funding to CAEs, which helps the schools build their institution’s capacity for IA/cybersecurity research and education. To date, capacity building has been a win-win for both DoD and the schools. For DoD, it has been an effective mechanism for building a strong educational base for the scholarship program and the nation’s cybersecurity academic infrastructure. For the CAEs, it serves as an incentive to increase their IA capabilities, course offerings, and faculty IA re-tooling. Capacity building funds are based on the priorities of the program and can vary year-to-year, given student throughput in the program. This circumstance creates an additional challenge to increase recruitment scholarships to meet Component demand, but also provide capacity building funds to the CAEs.

YEAR	Total Available Funding	Agency Requirements (Requested)	Agency Requirements (Fulfilled)
2001	1.2M	12	12
2002	6.1M	30	30
2003	6.7M	29	29
2004	5.0M	33	33
2005	7.5M	34	34
2006	5.0M	30	23
2007	5.0M	30	21
2008	5.0M	60	46
2009	5.0M	50	32
2010	5.0M	50	26

Figure 6.2 IASP: New Recruits Requested vs. New Recruits Awarded

To remain a vital tool, the DoD IASP requires an increase in funding to accommodate current capacity requirements and unfilled and emerging cyber personnel demands as the Department’s cyber domain evolves. The IASP is a proven recruitment and retention tool that is critical to the Department for addressing current and future cyber warfare requirements and operations.

Establish a Centrally Managed Cyber Workforce Loan Repayment Program

Both military and DoD civilian personnel have existing student loan repayment programs. The problem, particularly for the civilian program, is that it is not centrally managed or funded. Therefore, its utility is marginal at best as most Components have not opted to use it in a strategic manner. Today, the average undergraduate college student is graduating with \$24,000 in educational debt and is also carrying commercial consumer debt on multiple credit cards (which is also being used to partially fund college costs). Those with masters and other postgraduate degrees are carrying more debt. By creating a centrally funded program, this flexibility would be more available for both recruitment and retention of critical IT/Cybersecurity personnel. Any employee receiving this benefit would sign a service agreement to remain in the service of the paying agency for a period of at least 3 years, commensurate with other federal loan repayment program authorities.

6.2 Compensation

Acquire Office of Personnel Management Support to Restore the Value of IT Special Salary Rates

The importance of federal IT special salary rates and their erosion was explained in Chapter 3. These rates have declined in value over the past several years as adjustments in locality pay outstripped the special salary rate. For many locations, the IT special salary rates have been eliminated at several pay grades and dramatically devalued at the remaining eligible pay grades, losing up to 60% of their value. Restoring the value of these rates would improve starting salaries, particularly at the lower civilian pay grades, where the greatest salary differentials exist.

Create Federal-wide IT/Cybersecurity Certification Bonus

A significant challenge that DoD is experiencing is certifying and maintaining its cadre of IT/Cybersecurity professionals with cybersecurity responsibilities. All IA workforce members within DoD have baseline commercial certification requirements and many also require specific operating system certifications, other advanced training, and participation in team training exercises designated by their Component. Many are also in high growth occupations, such as information security and systems administration. The certifications, critical skill sets, experience and security clearances that these personnel gain through working in DoD make them highly sought after by both industry and other agencies. Additionally, the increased burden for the IA workforce to attain and maintain the required skills, commercial certifications, as well as meeting annual continuous learning credits are substantial investments of time and resources. IT/Cybersecurity professionals maintaining these critical skills should be recognized.

6.3 Training Improvements

Adequate periodic training at all levels, accession, entry, mid and senior-level is imperative to ensure that individuals can lead and operate at all levels of cyber operations within the DoD. While the DoD has extensive training, the dynamic nature of IT/Cybersecurity operations and the increased importance of cyber as a warfighting domain initial, mid and senior-level training for service members and civilians there are areas that can be improved. It is recognized that most of these initiatives require additional funding. Examples of these improvements include:

- Expand existing Service Schoolhouse capacity to train civilian Cybersecurity (IA) personnel. Service and agency civilians, as well as expeditionary surge manpower, would be trained to the same proficiency as military personnel, providing an effective posture and surge capabilities in response to incidents.
- Incorporate robust, realistic training exercises into Service schools, educational institutions and collective joint training environments. Continued support and program management of a cyber range environment will ensure its availability as part of a DoD cyber test and evaluation

facilities and resources to support research and development, operational test and evaluation, operational planning and effects testing, and training by replicating or emulating networks and infrastructure maintained and operated by the DoD as well as military and political organizations of potential United States adversaries, and by domestic and foreign telecommunications service providers. This is being addressed as part of the Department's strategy for acquisition and oversight of the DoD's cyber warfare capabilities required by the FY11 NDAA.

- Expand capabilities at the National Defense University's iCollege to bring an advanced curriculum to both the DoD and the federal cybersecurity leadership.

Appendix A – Cyber Operations-related Military Occupations

Specialty Code	Specialty Title
Air Force	
<i>Enlisted</i>	
3DXXX	Cyberspace Support Career Field (Cyber Systems)
1B4X1	On-Net Operations
3DX72	Cyber Transport Systems Craftsman (Cyber Systems Operations)
3DX52	Cyber Transport Systems Journeyman (Cyber Systems Operations)
3DX73	RF Transmission Systems Craftsman (Cyber Surety)
3DX90	Cyber Operations Superintendent OR Cyber Systems Superintendent (Cyber Systems Operations)
<i>Officer</i>	
17DXA	Cyber Warfare Operator (Control)
17DXB	Cyberspace Operations (Defense)
Army	
<i>Enlisted</i>	
25B	Information Technology Specialist
25C	Radio Operator
25E	Electromagnetic Spectrum Manager (Grade E6 – E9)
25F	Network Switching Systems Operator - Maintainer
25L	Cable Systems Installer
25M	Multimedia Illustrator
25N	Nodal Network Systems Operator – Maintainer
25P	Microwave Systems Operator – Maintainer
25Q	Multichannel Transmission Systems Operator – Maintainer
25R	Visual Information Equipment Operator - Maintainer
25U	Signal Support Systems Specialist
25S	Satellite Communications Systems Operator – Maintainer
25T	Satellite/Microwave Systems Chief (Grade E8)

Specialty Code	Specialty Title
25V	Combat Documentation/Production Specialist
25W	Telecommunications Operations Chief (Grades E7 and E8)
25X	Senior Signal Sergeant (Grade E9)
25Z	Visual Information Operations Chief (Grades E7 – E9)
35H	Common Ground Station (CGS) Analyst
35N	Signals Intelligence Analyst
35P	Cryptologic Linguist
35S	Signals Collector / Analyst
35T	Military Intelligence (MI) Systems Maintainer/Integrator
35Z	Signal Intelligence Senior Sergeant
94E	Radio & Communications Security (COMSEC) Repairer
<i>Officer</i>	
25A	Signal Officer
24A	Telecommunications Systems Engineer
53A	Information Systems Manager
35G	Signal Intelligence/Electronic Warfare (SIGINT/EW) Officer
<i>Warrant Officer</i>	
255A	Information Services Technical (Previous 251A and 254A)
255N	Network Management Technician (Previous 250N)
255S	Information Protection Technician
255Z	Senior Network Operations Technician
Navy	
<i>Enlisted</i>	
IT-2709	Joint Force Air Component Commander (JFACC) System Administrator
IT-2720	Global and Command Control System-Maritime (GCCS-M) System Administrator
IT-2730	Naval Tactical Command Support System (NTCSS) System Administrator
IT-2735	Information Systems Administrator
IT-2779	Information Systems Security Manager
IT- 2780	Network Security Vulnerability Technician

Specialty Code	Specialty Title
IT-2781	Advanced Network Analyst
IT-2782	Defense Message System (DMS) System Administrator
<i>Officer</i>	
1600	Information Professional
1610	Information Warfare (Information Warfare specialty)
<i>Limited Duty Officers</i>	
6420	Communications and Information Systems
<i>Chief Warrant Officers</i>	
7420	Communications and Information Systems
7430	Chief Warrant Officers (Cyber Warfare)
Marine Corps	
<i>Enlisted</i>	
0212	Technical Surveillance Countermeasures (TSCM) Specialist
0551	Information Operations Specialist
0619	Wire Chief
0629	Radio Chief
0651	Data Network Specialist
0659	Data Chief
0689	Information Assurance Technician
0699	Communications Chief
2611	Cryptologic Digital Network Technician/Analyst
2629	Signals Intelligence Analyst
2651	Special Intelligence System Administrator/Communicator
<i>Officer</i>	
0206	Signals Intelligence/Ground Electronic Warfare Officer
0215	Technical Surveillance Countermeasures Trained Counterintelligence/Human Source Intelligence Officer
0515	Information Operations Staff Officer
0550	Advanced Information Operations (IO) Planner

Specialty Code	Specialty Title
0602	Communications Officer
0640	Strategic Spectrum Planner
0650	Network Operations and Systems Officer
2602	Intelligence/Electronic Warfare Officer
8834	Technical Information Operations Officer

Appendix B – Commercial Certifications Supporting the DoD Information Assurance Workforce Improvement Program

Certification Provider	Certification Name
Carnegie Mellon Software Engineering Institute CERT®	Computer Security Incident Handler (CSIH)
Computing Technology Industry Association (CompTIA)	A+
CompTIA	Security +
CompTIA	Network+
Electronic Commerce Council	Certified Ethical Hacker (CEH)
International Information Systems Security Certifications Consortium (ISC)2	Certified Information Systems Security Professional (CISSP) or Associate (individual has qualified for the certification except for the number of years experience)
(ISC)2	Certification and Accreditation Professional (CAP)
(ISC)2	Information Systems Security Architecture Professional (ISSAP)
(ISC)2	Information Systems Security Engineering Professional (ISSEP)
(ISC)2	Information Systems Security Management Professional (ISSMP)
(ISC)2	System Security Certified Practitioner (SSCP)
Information Systems Audit and Control Association (ISACA)	Certified Information Security Manager (CISM)
ISACA	Certified Information Security Auditor (CISA)
SecurityCertified Program	Security Certified Network Professional (SCNP)
SecurityCertified Program	Security Certified Network Architect (SCNA)
Global Information Assurance Certification (GIAC)	GIAC Certified Intrusion Analyst (GCIA)
GIAC	GIAC Certified Incident Handler (GCIH)
GIAC	GIAC Security Expert (GSE)
GIAC	GIAC Security Essentials Certification (GSEC)
GIAC	GIAC Security Leadership Certificate (GSLC)
GIAC	GIAC Systems and Network Auditor (GSNA)
GIAC	GIAC Information Security Fundamentals (GISF)

Appendix C – Military Services Training and Development

Initial Skills Training

This listing provides an overview of key training needed to be effective in designated positions and is not intended to be all-inclusive. Following initial training, service members are assigned to organizations where they receive individual and collective training, continual professional military education, on-the-job training and developmental assignments which allow them to expand and hone their skills.

Air Force

- *Air Force Cyberspace Support (3DXXX)* enlisted personnel attend Initial Skills Training (IST) and are developed through professional continuing education and on the job training. As part of the efforts to professionalize the workforce, Cyber Systems, Cyber Surety and Cyber Transport personnel are required to pass Security+ certification prior to completing IST. In addition, Client Systems Airmen are A+ certified prior to completing IST.
- *Air Force Undergraduate Cyberspace Training (17D and 1B4)* - provides training to Cyberspace Operations Officers civilians and international officers (trained under the provisions of the Air Force Security Assistance Program) in the knowledge and skills necessary to perform duties across the spectrum of the cyberspace domain. This training presents an introduction to Cyberspace domain fundamentals and operations, doctrine and guidance, organizations, roles and responsibilities, network fundamentals/management, and deployed communications systems. Cyberspace Operations Officers are Security+ certified as part of their Initial Qualification Training.

Army

Army Signal Corps specialties:

- *Enlisted:*
 - *Information Technology Specialist (25B)* - trains enlisted soldiers to install, operate, and perform unit maintenance on multi-functional/multi-user information processing systems, peripheral equipment and auxiliary devices. Perform input/output data control and bulk data storage operations. Transfer data between information processing equipment and systems. Troubleshoot automation equipment and systems to the degree required for isolation of malfunctions to specific hardware or software. Restore equipment to operation by replacement of line replaceable unit (LRU). Perform system administration functions for the tactical Defense Message System (DMS).
 - *Radio Operator /Maintainer (25C)* - training focuses on operating and maintaining single channel High Frequency (HF), Very High Frequency (VHF), Tactical Satellite (TACSAT) radios, Joint Tactical Information Distribution System (JTIDS) Network Control Station (NCS) and special communication systems such as the Special Operations Communications Assemblage (SOCA).

- *Visual Information (VI) Equipment Operator (25R)* - training focuses on operating and performing unit and higher levels of maintenance on television receivers/monitors and cameras; studio accessories consisting of computer controlled video switchers and audio mixers/consoles, synchronous generators, distribution equipment, and amplifying equipment; motion/still photo imaging equipment; closed circuit systems; visual imagery satellite, microwave, Radio frequency (RF) transmission and cable distribution systems associated with VI operations; operates and maintains VI equipment used for Battlefield Video Teleconferencing and in a Video Teleconferencing facility
- *Warrant Officers:*
 - *The Information Services Technician (255A)* - trains and certifies Signal Warrant Officers for appointment and initial assignment as an Information Services Technician. The three phases of this course provide instruction and practical exercises in the installation, application, and management of computer operating systems, e.g., MS Windows Server; Cisco Certified Network Associates Technologies; Voice over Internet Protocol (IP); Fundamentals of Wireless Networking; Network Scanning, Network Management; MS Windows Technologies; Mail Server; SQL Server; MS Active Directory; SharePoint Server; Adobe Connect Collaboration Service; Network Applications; Security +; DIACAP Process; Digital Radio Transmission Systems; Joint Network Node; Video Teleconferencing and Audio Visual Technologies, and Digital Tactical Operations. The course also provides instruction in the Military Decision Making Process.
- *Officers:*
 - *The Signal Basic Officer Leaders Course (25A)* - consists of a common track as follows: Training and Doctrine Command (TRADOC) Common Core, Signal Theory, Information Technology and Signal Core. The Brigade Combat Team/Division (BCT/DIV) track consists of Joint Network Node (JNN), Network Operations, Brigade-level (S-6) and the BCT/DIV Planning Exercise. The Network Enterprise Technology Command (NETCOM) Track consists of Integrated Theater Signal Battalion, Network Operations and the NETCOM Planning Exercise. The Battalion S-6 Track consists of Combat Net Radio (CNR), Command Post Node, Digital Tactical Operation Center, and Battalion S-6 Planning Exercise. All tracks attend the Capstone Exercise. Detailed instruction includes Army Operations doctrine; information systems, communications planning, execution and management; information systems/communications interface; communications requirements unique to a Maneuver Battalion or Brigade; offense; defense; leadership; electronics; combat net radio; tropospheric scattering; property accounting; telecommunications; Communications Security (COMSEC); training management; military justice; information systems; Signal tactics and doctrine; S-6 functions; Force XXI Battle Command Brigade and Below (FBCB2); and Joint Node Network (JNN) and modularity topics (equipment overview, equipment orientation).

Army Military Intelligence (MI) specialties:

- Enlisted:
 - *Signals Collector/Analyst Course (35S)* - training focuses on the operation of signals intelligence/electronic warfare equipment and preparation of technical reports, searching the radio frequency spectrum to collect and identify target communications, selecting categories of electro-optic or foreign instrumentation signals and performing basic signals analysis to determine parameters for identification and processing.
 - *MI Systems Maintenance/Integrator Course (35T)* - training focuses on performing entry level maintenance tasks associated with intelligence and electronic warfare (IEW) equipment and systems; introduces electricity and advanced electronic theory, advanced concept and troubleshooting theory which includes basic and advanced computer concepts and advanced troubleshooting skills using the Army's most advanced IEW systems. Further, the training includes basic analog and digital electronics; communications theory (receivers, recorders, and multiplexing/de-multiplexing; transmission line repair techniques; computer architecture/operating systems fundamentals; automated messaging; and network operations/troubleshooting.
- Warrant Officers:
 - *Signal Intelligence Analysis Technician (352N)* – trains to supervise and perform analysis and reporting of intercepted foreign communications and non-communications at all echelons. They will also train to perform intermediate analysis of intercepted communications and non-communications information. Additionally, prepare and maintain SIGINT technical data and Electronic Order of Battle (EOB) information.
- Officers:
 - *Signals Intelligence (SIGINT)/Electronic Basic Officer Leader Course (35G)* – training to manage Signals Intelligence collection, exploitation, processing, production and dissemination functions, systems and organizations. Training includes organizational structure, procedures, functions and products of military and national-level components; familiarization on skills and knowledge needed by signals analysts, collection managers, and officers in SIGINT positions. Signal Intelligence / Electronic Warfare Officer duties include planning, directing, managing, coordinating and participating in the collection, production and dissemination of signals intelligence (SIGINT) and the conduct of electronic warfare (EW) at tactical, operational and strategic levels.

Navy

- Enlisted:
 - *Navy IT 'A' School* - provides enlisted personnel an introduction to computers, networks and information security. Graduates receive CompTIA A+ and Microsoft Desktop certifications.
 - *Global and Command Control System-Maritime System Administrator (IT-2720)* - training provides enlisted personnel to perform the basic operation of the Global Command and Control System - Maritime (GCCS-M) system with regard to the system administration functions. Responsible for backing-up and restoring data, assigning or changing user accounts and passwords, profiling administration procedures, monitoring Command, Control, Communications, Computers, and Intelligence (C4I) system interfaces and log-in requirements, analyzing emergency shutdown occurrences, and controlling printer utilities and data base purging requirements.
 - *Information Systems Administrator (IT-2735)* - training provides enlisted personnel basic and in-depth levels of instruction in Local Area Networks (LAN) and Metropolitan Area Networks (MAN), with focus on system administration. Prepares these technical personnel to administer commercial network operating systems within the functional areas of configuration, system, and performance management. Manage/maintain internal site networks to include but not limited to MS Exchange, NetWare, Novell, UNIX, and Windows NT. Conduct first level network software and hardware corrective actions.
- Warrant Officers:
 - *Communications and Information Systems (742X)* - enhances warrant officers' expertise in information, command and control, and space systems through the planning, acquisition, operation, maintenance and security of systems. The officer technical specialists in the field of automated data processing using electronic digital and analog computer systems. They direct and supervise personnel concerned with the preparation of data for processing and operation of all automated data processing equipment; technical advisors concerning the capabilities, limitations, and reliability of data processing equipment, procedures, and techniques.
- Officers:
 - *Basic Intelligence Officer Course (9600)* - trains to assist in collection, evaluation, and dissemination of naval intelligence in support of surface, air, and antisubmarine warfare units and operational staffs; to participate in reconnaissance missions and in interrogation of prisoners; to maintain order of battle information and intelligence plots; to prepare and develop intelligence reports and to develop intelligence estimates.

- *Communications, Plans and Operations Officer (9615)* - trains to formulate communication plans and prepare communication annexes to operation plans and orders; to review communication plans prepared by higher authority. Prepares necessary supporting plans and provides information and advice on their implementation; to maintain liaison with communication planning staffs of other services and agencies and to supervise collection, evaluation, and display of communication information.

Marine Corps

- Enlisted:
 - *Signal Intelligence (SIGINT) Analysis (2629)* - enlisted Marines are trained to perform duties that encompass all facets of signals intelligence analysis and supervision of selected collection and EW/COMSEC operations. As analysts, they develop and maintain records on technical aspects of target emitters; develop and maintain communications order of battle files, situation maps, and other related SIGINT files. Analysts prepare and issue reports to include intelligence reports, technical reports, and summaries.
 - *Data Network Specialist (0651)* - provides in-depth studies of small computer systems. Topics covered include: The installations and configuration of Marine Corps hardware and software; Installation and configuration of workstation and server operating systems; Installation and configuration of messaging systems; Installation, operation and maintenance of Local Area Networks (LAN) and Wide Area Networks (WAN); Troubleshooting Techniques; and information Assurance.
- Warrant Officers:
 - *Strategic Spectrum Planner (0640)* - trains warrant officers to develop the skills to supervise and manage the planning and use of the electromagnetic spectrum for all communications and radio location requirements, to provide technical and administrative guidance for the certification of equipment utilizing the electromagnetic spectrum, and to develop and supervise the Joint Communications Electronic Operating Instructions (JCEOI) and associated communication publications and documents.
- Officers:
 - *Signals Intelligence (SIGINT) Officer Course (0206)* - teaches operational and administrative tasks required of a Marine SIGINT officer. Emphasis is placed on SIGINT requirements in Marine Air Ground Task Force (MAGTF) operations. Other areas of instruction include: tactical communications, introduction to intelligence, electronic warfare, SIGINT organizations, SIGINT collection, SIGINT assets, analysis, intelligence preparation of the battlespace, SIGINT planning and dissemination.

- *Basic Communications Officer's Course (0602)* - provides Marine officers the professional training at the career level for selected Communications Officers in communications and command and staff duties in order to qualify them for assignment to appropriate command and control billets in the Fleet Marine Force. Selected basic school graduates receive familiarization training in command and staff duties, responsibilities of the small unit communications officer, and the communications systems of units of the Marine Division, Marine Aircraft Wing, and Marine Logistics Group. Signals intelligence officers receive familiarization training in communications systems within the Marine Division, Marine Aircraft Wing, and Marine Logistics Group and prepare and present instruction in other schools of the Marine Air-Ground Training and Education Center, as required. Marine Corps Reserve communications officers review communication requirements, resources, planning considerations, and employment techniques within the Fleet Marine Force.

Mid-level Training

As service members begin to focus on both the operational and strategic aspects of cyber operations they need to expand their knowledge and increase their skills. This is accomplished through mid-level training. Using the knowledge and skills gained in mid-level training individuals will be able begin to transition to a more strategic environment while maintaining their operational skills. As individuals continue to advance, selected individuals will be afforded the opportunity to attend senior-level training. The Services have varied options for service members. Selected examples of mid-level training are described below:

Air Force

- *Advanced Cyberspace Officer Training* - attended by Air Force officers and civilian equivalents, this professional development course provides knowledge and skills necessary to perform duties of a Cyberspace Officer at the field grade level. It presents current and emerging communications and information programs, initiatives and technologies impacting the Department of Defense total force concept for the cyberspace warrior in a fixed and deployed environment.
- *Air Command and Staff College* - the Air Force's intermediate professional military education school which prepares field grade officers of all services (primarily majors and major selects), international officers, and US civilians to assume positions of higher responsibility within the military and other government arenas. It is geared toward teaching the skills necessary for air and space operations in support of a joint campaign, as well as leadership and command and focuses on shaping and molding tomorrow's leaders and commanders. Students in cyberspace electives have the opportunity to perform in-depth research and build contacts with experts in the cyberspace community. An example of this is *Blue Horizons Program*, which affords students the opportunity to do in-depth research in future technology programs, and often the topics are cyber-related. The college's academic environment stimulates and encourages free expression

of ideas as well as independent, analytical, and creative thinking. Students who successfully complete the 10-month resident program of study receive a master's degree in Military Operational Art and Science.

Army

- *Signal Officers' Career Course* - provides Signal officers the academic instruction supporting the leader, tactical, and technical skills needed to lead company-size network units and to serve as network operations (cyber) planners at battalion and brigade staff levels. The Telecommunications Systems Engineer course provides advanced cyber training associated with engineering telecommunications systems into integrated networks, developing a network security architecture, assessing network design plans, conducting operations and defense of the network, planning future NETOPS, preparing technical specifications documents, and evaluating cyber technologies.
- *Information Systems Manager Course* - provides advanced cyber training associated with planning/managing the integration and security of computer hardware, software and data communications; supervising the installation operation, administration, maintenance and defense of information systems and local area networks at all organizational levels to include multinational, joint and service agencies.; writing and maintaining accreditation plans for information systems and networks; planning/managing information assurance /computer network defense procedures; planning/coordinating procedures for contingency operations during system emergencies, outages, degraded operations or downtime for maintenance; and performing life-cycle management processes, including configuration management, for automated systems, hardware and software.
- *U.S. Army Command & General Staff School* - educates and trains intermediate level Army Officers, International Officers, Sister Service Officers and Interagency leaders prepared to operate in full spectrum Army, joint, interagency, and multinational environments as field grade commanders and staff officers. Students who successfully complete the 10-month resident program of study receive a Master of Military Art and Science Degree.

Navy

- *Joint Cyber Analysis Course* – a 24-week intensive course that provides joint cyber warriors with advanced technical background in computer network operations (CNO). During the course of their training, students learn to think logically and analytically; master a significant body of knowledge to tackle very complex problems; and fulfill tactical CNO mission requirements. Upon graduation they are well-equipped to serve in a wide range of roles and functional areas within the CNO community.
- *Network Security Vulnerability Technician Course* - trains Sailors to recognize microcomputer operating systems (i.e., MS-DOS, Windows NT, UNIX, and Novell Netware) vulnerabilities and perform corrective actions to ensure maximum system availability and assist the Information Systems Security Manager with the System Security Plan (SSP) and

systems accreditation. Students learn to use commercial off-the shelf software and operating system specific tools to perform virus protection and detection, system backups, data recovery, and auditing functions. They also learn to create, configure, and maintain user and group accounts across multiple operating systems and assess protocol and proxy service vulnerabilities and their relation to firewalls. Sailors develop and implement solutions, with regard to protocol and proxy service vulnerabilities, guarding against hostile attempts of compromise or inadvertent disclosure of sensitive material and verify and write Access Control Lists and programs screening routers. Graduates receive CompTIA Security + Certification.

- *Global Command and Control System-Maritime (GCCS-M) System Administrator Course* - trains Sailors to perform basic operation of the GCCS-M system with regard to system administration functions. They learn to back-up and restore data, assign or change user accounts and passwords, profile administration procedures, monitor C4I system interfaces and log-in requirements, analyze emergency shutdown occurrences, and control printer utilities and data base purging requirements.
- *Naval Tactical Command Support System (NTCSS) System Administrator Course* - trains Sailors to coordinate, implement, operate and maintain the software of the NTCSS system and establish and monitor security procedures. Their responsibilities include controlling and establishing directories, security management files, individual access files and controlling and monitoring network resources and utilities.
- *Joint Network Attack Course* - trains military cyber warfare personnel to support Joint Force Commanders conducting Information Operations. It trains cyberwarfare decision makers in basic internet protocol (IP) and non-IP network technologies and trains students how to conduct IO planning and develop supporting documentation.
- *College of Naval Command and Staff* – enables students to pursue studies in each of the Naval War College's three core subject areas: Strategy and Policy, Joint Maritime Operations, and National Security Decision Making. While this basic curriculum is essentially the same as that of the more senior students enrolled in the College of Naval Warfare, individual courses are tailored to the experience level and career needs of the College of Naval Command and Staffs mid-grade officers. Students who successfully complete the 10-month resident program of study receive an accredited Masters of Arts in National Security and Strategic Studies.

Marine Corps

- *Marine Analysis and Reporting Course* - provides instruction on Signals Intelligence Analysis, Traffic and Cryptanalysis, Battlespace Preparation and Signals Intelligence Reporting.
- *Technical Surveillance Countermeasures Fundamentals Course* - teaches the techniques and measures to detect, neutralize, and/or exploit a wide variety of hostile and foreign penetration technologies that are used to obtain unauthorized access to classified and sensitive information. It includes instruction in the areas of basic electronics technology;

mathematics; theory and analysis of electrical and electronic circuits; semiconductor and integrated circuits; amplifiers; power supplies; feedback principles; oscillators; modulation techniques; single and multiple conversion receivers; spectrum and time domain signal analysis; digital logic principles; applications, operation and use of state-of-the-art test, measurement, and diagnostic equipment.

- *Basic Computer Network Operations Planner Course (BCNOPC)* - prepares students to develop and refine operational concepts (CONOPS) and plan the integrated, synchronized, and coordinated employment of Computer Network Exploitation (CNE), Computer Network Attack (CNA), and Computer Network Defense (CND) activities. Students are taught the unique requirements for intelligence support to Computer Network Operations (CNO) planning; the various CNO authorities, capabilities, organizations, and legal considerations and the basic policies and processes necessary to gain approvals for CNE, CNA, and CND to support the Land Component Commander. The BCNOPC describes how CNO elements (CNE, CNA, and CND) relate to each other; to other Information Operations Capabilities (EW, MILDEC, OPSEC, PSYOP, etc.); and in general, to both friendly and adversary operations in cyberspace.
- *Joint Information Operations Planner Course* - establishes a common level of understanding for information operations (IO) planners and IO capability specialists who will serve in joint operational-level IO billets. The course focuses on Joint Operations Planning and Execution System, Joint Intelligence Preparation of the Environment, IO Planning, Interagency Planning & Coordination, Military Deception, and Operations Security.
- *Expeditionary Warfare Course* - provides Marine Captains and selected officers from other Services and countries career-level, professional military education and training in Command and Control, Marine Air Ground Task Force Operations, Naval Expeditionary Operations, combined arms, ethics based leadership, operational culture and tactical decision-making in order to prepare them to serve as commanders and staff officers at appropriate levels in the Operating Forces up to and including the Marine Expeditionary Brigade.
- *Marine Command and Staff College* - educates and trains its joint, multinational, and interagency professionals in order to produce skilled war fighting leaders able to overcome diverse 21st Century security challenges. The Command and Staff College offers students the option of completing the requirements for a Master of Military Studies degree.

Non-Commissioned Officers – All Services

- As enlisted personnel progress through the ranks to become Non-Commissioned Officers (NCOs), they attend military specialty courses directly related to their service, primary specialty and grade level. As part of their professional military education (PME) junior NCOs (E4 – E6) attend a basic job specialty/leadership course and later, as senior

NCOs, they attend advanced job specialty/leadership courses (E6 – E8). As they reach the pinnacle of their career, senior enlisted leaders (E8 – E9), demonstrating potential for service at the highest levels, are selected for attendance at one of the most senior Non-Commissioned Officer Academies: the U.S. Air Force Senior Non-Commissioned Officer Academy (AFSNCOA), the U.S Army Sergeants Major Academy (USASMA), the U.S. Navy Senior Enlisted Academy (SEA) and the U.S. Marine Corps Sergeant Major/Master Gunnery Sergeant Symposium.

Senior-level Training

Senior military IT/Cybersecurity professionals need to understand the broader spectrum of cyber operations to be strategic leaders and to provide vision and direction for their organizations and institutions. As part of their competency development, they require more focus on cyber security strategies related to joint, interagency, intergovernmental and multinational environments. Examples of senior-level training to meet those needs are described below.

- *Air War College* - prepares students to lead in a joint environment at the strategic level across the range of military operations; to develop cross-domain mastery of joint air, space and cyberspace power and its strategic contributions to national security; and to advance innovative thought on National Security, Department of Defense and Air Force issues. Students in cyberspace electives have the opportunity to perform in-depth research and build contacts with experts in the cyberspace community. An example of this is the *Blue Horizons Program*, which affords students the opportunity to do in-depth research in future technology and cyber-related programs.
- *Army War College* - educates current and future leaders on the development and employment of land power, supports the operational and institutional force, conducts research, and publishes, to inform thought on national security and military strategy and supports the Army's strategic communication efforts. In November 2010, the Army War College updated its *Information Operations Primer* which is used by students, faculty and staff in the ongoing study of this topic. Additionally, the College's Strategic Studies Institute has conducted a series of seminars in cybersecurity topics of interest.
- *Naval War College* - focuses on three main areas: Joint Military Operations which focuses on joint war fighting at the theater-strategic and operational levels of war; National Security Decision Making which educates students in the effective selection and leadership of military forces within the constraints of available national resources; and Strategy and Policy which is designed to teach students to think strategically and to prepare for strategic leadership positions. Individual areas of study (AOS) include Information Operations; students in this AOS explore issues across operational, technical, policy and legal areas of the information environment in order to foster a comprehensive understanding of the challenges of operating in the information environment and the integration of information planning across the spectrum of conflict. Additionally, the

College has a series of research groups where select students examine key areas of interest to the Chief of Naval Operations.

- *Marine Corps War College* - educates selected senior officers and civilians on decision-making across the range of military operations in a joint, interagency, and multinational environment. Graduates are prepared to assume senior leadership positions of increasing complexity through the study of national military strategy, theater strategy and plans, and military support to those strategies within the context of national security policies, decision-making, objectives, and resources.
- *National War College (NWC)* - educates future leaders of the Armed Forces, State Department, and other civilian agencies for high-level policy, command, and staff responsibilities. The NWC conducts a senior-level course of study in national security policy and strategy for selected U.S. and foreign military officers and federal officials. The curriculum emphasizes the joint and interagency perspective. Reflecting this emphasis, 59 percent of the student body is composed of equal representation from the land, air, and sea (including Marine and Coast Guard) Services. The remaining 41 percent are drawn from the Department of State and other federal departments and agencies, and international fellows from a number of foreign countries.
- *Industrial College of the Armed Forces* - provides graduate-level education to senior members of the U.S. Armed Forces, government civilians, foreign nationals and private industry. These future executives will be better prepared for leadership and success in developing national security strategy and policy, with a focus on evaluating, marshalling, and managing national resources.
- *School of Advanced Warfighting* - provides a follow-on, graduate-level professional military education for selected field grade officers who have completed the Marine Corps or sister service command and staff college course. The course develops complex problem solving and decision making skills that can be used to improve the war fighting capabilities of an organization at the operational level of war.
- *Keystone Course* - educates Command Senior Enlisted Leaders (CSELs) currently serving in or slated to serve in a general or flag officer level joint headquarters or Service headquarters that could be assigned as a joint task force. Keystone parallels the Capstone course for newly selected General and Flag Officers in that the learning will be focused on “those that do”. The course will visit the Combatant Commands, Joint Task Forces and senior leadership (both officer and enlisted) in the Washington arena to explore the relationships and challenges of operating in a joint environment.

Additional Military Training Available for Continuous Learning

Along with current training offered, more advanced training programs are available through multiple supplemental courses intended to focus on professional development throughout an

individual's career. These courses impart cyber-related knowledge, skills, and abilities appropriate to an individual's pay grade and experience, as well as provide new exposure to aspects of the cyber warfare mission area not yet experienced. Individuals may also attend training that will be specific to their duty location and mission. Examples of additional training are described below.

- Air Force's *Cyberspace 200 Course* is presented at the secret level, is for cyberspace professionals at the 6-11 year point of their careers. Students' career experience and training are leveraged with course curriculum to enhance their understanding of cyberspace system acquisition, capabilities, limitations and vulnerabilities so they can better plan, direct, and execute defensive and offensive cyberspace operations at the operational level of war while integrating with air and space operations.
- The Air Force's *Cyberspace 300 Course*, presented at the Top Secret/Sensitive Compartmentalized Information level is for cyberspace professionals in the second half of their careers. Students' career experience, training, and education are leveraged to develop a strategic focus for the integration and application of cyberspace capabilities in joint military operations.
- The Air Force also uses developmental opportunities including degree-awarding programs through the Air Force Institute of Technology, Education with Industry, and Expeditionary Warfare School. In addition, a cyberspace cross flow program is in development to bridge experiences between core cyberspace operations personnel and cyberspace specialists (analysts, acquisitions, forensics, et al).
- Within Army, cyber-related training certifications are available for military and civilian personnel including Security +, Network Manager Course, CIISP, Computer Network Defense, Unix System Administrators Security Course and IA courses. It is extremely difficult for Army Reserve Troop Program Unit soldiers to attend and afford these training sessions, with average weekly tuition rates of \$1500/week or more. Formal, recognized cyber operations personnel certifications are available through some academic partnership universities, including University of Maryland University College (UMUC), Carnegie Mellon, Massachusetts Institute of Technology (MIT), University of Oklahoma for cyber security, information technology security, information security engineering however limited tuition assistance is available. These range from bachelor's degrees to doctorate degrees, but involve commitments to 5 to 7 years of academic study.
- The Department of Navy CIO has developed a *Flag-Level Information Assurance Indoctrination Course* that is provided in a symposium environment for senior leaders in all the Fleet concentration areas and at the new *Flag Officers Course*.
- The Navy's Credentials Program Office (CPO) is significant to implementation of the IA Workforce Improvement Program by administering the enterprise Certification Voucher Program. Exam vouchers are centrally funded and dispersed. The CPO's Credentialing Opportunities On-Line (COOL) website provides Sailors information on IA commercial certifications.

- The Naval Postgraduate School (NPS) has developed several distributed and resident programs to provide more accessibility and flexibility. These programs consist of an accredited graduate level four-course curriculum to provide subject matter expertise and as an iterative step towards a Master of Science degree. Additionally, the NPS offers both a resident and distance learning Certified Information Systems Security Professional (CISSP) prep course available as an elective in all of the Computer Science and Information Systems degree programs.
- The Marine Corps sends its Marines and civilians to academic and industry programs to obtain education and certification on subjects such as CISCO, Microsoft and LINUX network fundamentals and administration and cyberspace ethics as well as courses on exploitation and analysis of network operations. The Marine Corps is building cyber-specific courses with the Expeditionary Warfare School, Command and Staff College, School of Advance Warfighting and the Marine Corps Warfighting University.

Appendix D: Geographic Location of National Centers of Academic Excellence in Information Assurance

(see attached map)

Appendix D: National Centers of Academic Excellence in Information Assurance Education (CAE) And Research (CAE-R)

Military

Academic Institutions

Naval Postgraduate School
 U.S. Military Academy at West Point
 U.S. Naval Academy
 U.S. Air Force Academy
 Air Force Institute of Technology
 College of the National Defense Univ

Anne Arundel CC
 Arizona State Univ
 Auburn Univ
 Boston Univ
 Cal State Poly Institute, Pomona
 Cal State Univ, Sacramento
 Cal State Univ, San Bernardino
 Capella Univ
 Capitol College
 Carnegie Mellon Univ
 Champlain College
 Clark Atlanta Univ
 Colorado Technical Univ
 Dartmouth College
 Dakota State Univ
 DePaul Univ
 Drexel Univ
 East Carolina Univ
 Eastern Michigan Univ

Idaho State Univ
 Illinois Institute of Technology
 Illinois State Univ
 Indiana Univ
 Indiana State Univ
 Indiana Univ of Pennsylvania
 Iowa State Univ
 Jacksonville State Univ
 New Mexico Tech

James Madison Univ
 Johns Hopkins Univ
 Kansas State University
 Kennesaw State Univ
 Metropolitan State Univ
 Mississippi State Univ
 Missouri Univ of Science & Technology
 Moraine Valley CC
 New Jersey City Univ
 New Jersey Institute of Technology
 Pace Univ
 Polytechnic Univ
 Princeton Univ
 Prince George CC
 Purdue Univ
 Regis Univ
 Rochester Institute of Technology

Rose State College
 Rutgers, The State University of NJ
 Saint Cloud State Univ
 Southern Methodist Univ
 Southern Polytechnic State Univ
 State University Of New York, Buffalo
 Stevens Institute of Technology
 Syracuse Univ
 Texas A&M Univ
 The Pennsylvania State Univ
 The Univ of Texas at Dallas
 Towson Univ
 Univ of Advancing Technology

Univ of Alabama, Huntsville
 Univ of Alaska Fairbanks
 Univ of Arkansas at Little Rock
 Univ of Arizona, Tucson
 Univ of California at Davis
 Univ of California, Irvine
 Univ of Connecticut
 Univ of Dallas
 Univ of Denver
 Univ of Detroit, Mercy
 Univ of Houston
 Univ of Idaho
 Univ of Illinois at Chicago
 Univ of Illinois at Springfield
 Univ of Illinois at Urbana-Champaign
 Univ of Kansas
 Univ of Maryland, Baltimore County

Univ of Maryland, College Park
 Univ of Maryland University College
 Univ of Massachusetts, Amherst
 Univ of Memphis
 Univ of Minnesota
 Univ of Missouri-Columbia
 Univ of Nebraska, Omaha
 Univ of Nevada, Las Vegas
 Univ of New Mexico
 Univ of New Orleans
 Univ of North Carolina, Charlotte
 Univ of North Texas
 Univ of Pittsburgh
 Univ of South Carolina
 Univ of Tennessee at Chattanooga
 Univ of Texas at El Paso
 Univ of Texas, San Antonio
 Univ of Tulsa
 Univ of Washington
 Virginia Polytechnic Institute & State University
 Walsh College
 West Chester Univ of Pennsylvania
 West Virginia Univ

Polytechnic University of Puerto Rico

East Stroudsburg Univ of PA
 Florida State Univ
 Fort Hays State Univ
 Fountainhead College of Technology
 George Mason
 Georgetown
 George Washington Univ
 Georgia Tech
 Hagerstown CC

Norfolk State Univ
 North Carolina A&T State Univ
 North Carolina State Univ
 Northeastern Univ
 Norwich Univ
 Nova Southeastern Univ
 Ohio State Univ
 Oklahoma City CC
 Oklahoma State Univ
 Our Lady of the Lake Univ

