STATEMENT BY

TERESA M. TAKAI
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON

INTELLIGENCE, EMERGING THREATS AND CAPABILITIES

ON

DOD INFORMATION TECHNOLOGY AND CYBER OPERATIONS PROGRAMS

March 13, 2013

NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS AND CAPABILITIES, HOUSE ARMED SERVICES COMMITTEE

Introduction

Good afternoon Mr. Chairman and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee on the importance of information technology (IT) to the transformation of the Department of Defense (DoD), especially during these challenging budget times. I am Teri Takai, the Department's Chief Information Officer (CIO). My office is responsible for ensuring the Department has access to the information, the communication networks, and the decision support tools needed successfully execute our warfighting and business support missions. Our mission is to ensure that these capabilities can be depended upon in the face of threats by a capable adversary in all conditions from peace to war, and particularly in the face of cyber warfare by such an adversary. My focus in accomplishing these responsibilities is to ensure the effectiveness, reliability, security, and efficiency of DoD's IT capabilities for the warfighter, and ensure we are able to take advantage of future technology innovations to support the Department's missions.

I would like to give you an overview of some of the key IT and cybersecurity initiatives and efforts currently underway in the Department and what we are doing to ensure our warfighters have the capabilities they need when going into harm's way. I will start with a broad overview of the Department's IT landscape, and then describe the Joint Information Environment (JIE), which is our effort to restructure much of the underlying network, computing, and cyber security of the department so as to make us more agile in deploying new decision support capabilities, make us better able to mount cyber defense of our core Department missions, and to make us more efficient. I will also discuss the Department's cybersecurity efforts and describe some important initiatives specifically intended to better support our warfighters. Finally, I will discuss the cyber and IT workforce and our efforts to change the way information technology planning and budgeting is done in light of all of the above.

Overview of DoD's Information Environment

The Department's FY14 IT budget request is still being finalized, but will include funding for a broad range of information technology, including: desktop computers, tactical radios, identity management technology, commercial satellite communications, business systems, cybersecurity and much more. These investments support mission critical operations that must be delivered in

both an office environment and at the tactical edge on the battlefield. These investments provide capabilities that enable the Commander-in-Chief to communicate with and direct the military, and to support intelligence activities as well as logistics, medical and other business support functions of the Department. The Department's IT environment is even more complex when one considers that these investments operate in over 6,000 locations worldwide, support the unique needs and missions of the three Military Departments and over 40 Defense Agencies and Field Activities within the Department. Included in the overall IT budget are the Department's cybersecurity activities and efforts that are designed to ensure our information, information systems and networks are protected against known cyber vulnerabilities and are resilient to ever-increasing cyber threats the Department and the nation face. These efforts continue to receive the highest-level attention and support of the Department.

The scale of the Department's networks illustrates the complexity of the Department's information infrastructure and IT budget. The networks reach almost every corner of the globe and connect active duty, reserve and national guard as well as civilians and our contractor support base. This totals roughly 3.7 million people with active cyber identity credentials issued by the DoD public key infrastructure, or PKI. These credentials are contained on the DoD's common access card, or CAC, and they allow each of these people to access the Department's unclassified network and its rich information sharing capabilities. The Department has approximately 25,000 servers that are visible to the Internet, and countless people from DoD's partners access DoD information resources every day and exchange information with DoD personnel.

Joint Information Environment and Joint Force 2020

Increasingly, mission success depends upon the ability of our military commanders and civilian leaders to act quickly and effectively based on the most accurate and timely data and information available. Recognizing that information is a strategic asset, DoD is undertaking an ambitious effort to re-align and restructure how our many IT networks are constructed, operated and defended in order to provide better access to information to the user, improve our ability to not only defend the networks and the data, but make it responsive to the constantly changing technological and operational factors. The challenge is amplified because our adversaries are

trying to use every opportunity to penetrate our critical infrastructure to capture, disrupt, or destroy our information and to do harm to our forces. Consequently, DoD is pursuing the alignment of existing vast IT networks into a Joint Information Environment (JIE). JIE will have federated networks that are built to common standards and configurations, and expanded use of shared IT infrastructure and enterprise services, which include Thin clients, everything over IP, email, and cloud services. The Services will continue to operate and maintain their portion of the JIE, as well as provide mission-unique capabilities while incorporating shared IT transport services and common applications.

The Joint Force faces a shrinking technological lead and growing vulnerability in a variety of systems, most notably in IT. We see increasing emphasis and resource expenditures by our adversaries focused on disrupting our command and control systems. Based on increasing threats in Cyber, decreasing budgets, and the explosion of new IT capabilities and solutions, the Department has engaged in a series of efforts to strengthen and deliver a more agile, secure information capability to enhance combat power and decision-making.

The Chairman of the Joint Chiefs of Staff recently issued "Joint Force 2020" as a vision for how the Joint Force of the future can effectively address security challenges through globally integrated operations. This will help increase the overall adaptability of the force to cope with uncertainty, complexity, and rapid change.

A primary enabler of this vision and strategy is the JIE. First and foremost, JIE will improve mission effectiveness. It is intended to enable and empower our military's decisive edge—our people—by providing warfighters and our mission partners a shared IT infrastructure consisting of federated networks with common configurations and management, with a common set of enterprise services, within a single security architecture.

The JIE will change the way we assemble, configure, and use new and legacy information technologies. It will consist of enterprise level network operations centers that will reduce the complexity and ambiguity of seeing and controlling the numerous networks within DOD; a set of core data centers – significantly reducing the current number of DoD data centers while ensuring the information is secured and available where needed; and standard, single security architecture that will reduce the number of organizationally owned firewalls, unique routing algorithms, and

inefficient routing of information that currently exists today. Together with the single, authoritative identity management and access control, emerging cloud capability, mobile computing devices and data-focused applications, and , common IT enterprise services, JIE will provide the information environment to flexibly create, store, disseminate, and access data, applications, and other computing services when and where needed. It will better protect the integrity of information from unauthorized access while increasing the ability to respond to security breaches across the system as a whole.

On both classified to unclassified domains, our employees, including warfighters, will have the ability to connect to information resources needed from any device, at any time, from anywhere in the world. Furthermore, as individuals move around the world, whether for operational deployment or in support of business operations, their movement within the information environment will be virtually seamless and allow them to immediately operate from any device.

In today's environment, the Combatant Commands (COCOMs) are provided with Military Service-centric IT networks and IT services operating on Service–unique domains. This Service-centric approach extends beyond networks to identity and access management processes, data centers, mission and business applications, commercial off-the-shelf (COTS) hardware and software, and IT procurement practices. The result is an IT infrastructure that does not effectively support the joint warfighting environment.

The ultimate beneficiary of JIE is the commander in the field, allowing for more innovative integration of information technologies, operations, and cyber security at a tempo more appropriate to today's fast-paced operational conditions. Specific benefits include:

- A standardized information and security architecture will improve how DoD operates and secures its networks on a global level. Users and systems will be able to trust their connection from end to end with the assurance that their activity will not be compromised.

- The JIE's standard security architecture will enable cyber operators at every level to see the status of their networks for operations and security and enable commonality in how cyber threats are countered. The Department will know who is operating on its networks and what they are doing, and be able to attribute their actions with a high degree of

confidence. This will minimize complexity for a synchronized cyber response, maximize operational efficiencies, and reduce risk.

- Consolidation of data centers, operations centers and help desks will enable users and systems to have timely and secure access to the data and services needed to accomplish their assigned missions, regardless of their location.

- A consistent DoD-wide IT architecture supports effective fielding of Department capabilities in support of information sharing, as well as sustainment and integration of legacy systems.

There will be investment required to effect the transition from the Department's as-is environment to the desired to-be state. The Department will utilize the Services existing programs, initiatives, and technical refresh to deploy or migrate to JIE standards utilizing specific implementation guidance.

Data Center Consolidation

An important aspect within JIE is the active consolidation of the Department's numerous data centers. These efforts are consistent with and support the Federal Data Center Consolidation Initiative (FDCCI) being led by the Federal CIO

The Department recently compiled a global inventory of its data centers, and is establishing four classes of data centers to assist in the development and execution of our data center consolidation strategy. These four types of data centers are:

- Core Data Center (CDC) – delivers enterprise services and provides primary migration point for systems and applications; these are our most important data centers, strategically located to provide speed of access to global information requirements;
- Installation Processing Node (IPN) – provides local services to DoD installations and hosting systems not suited for CDCs, these will be located at the installation level, and will consolidate the duplicative data centers at the installations;

- Special Purpose Processing Node (SPPN) – provides compute and storage for fixed infrastructure or facilities, such as test ranges, labs, medical diagnostic equipment, and machine shops.
- Tactical/Mobile Processing Node (TPN) – provides support to the deployed warfighter at the tactical edge; these unique "data centers" directly support the warfighter in a disadvantaged or tactical environment, but connect back into the Generating Force information sources and core data centers.

The DoD Core Data Center Reference Architecture was published in October 2012 and provides the foundation for the DoD's data center consolidation efforts as well as supports the emerging Department's Cloud Computing capability, which will be "tied" to data centers.

Significant progress is being made in data center consolidation, and plans are in place close nearly 50% of all DoD data centers within the Future Years Defense Plan with the remaining data centers transforming and conforming to standards to achieve the JIE.

DoD Mobile Device Strategy

Last year, when I testified before this Subcommittee, I described several mobile device pilot efforts the Department had underway. Since that time, my office has approved broader deployment of smart phones and tablet computing for unclassified use within the Department. the DoD Mobile Device Strategy was published on June 8, 2012, which identified IT goals and objectives to capitalize on the full potential of mobile devices in the Department. The strategy focused on improving three areas critical to mobility: the networking infrastructure to support wireless devices, mobile devices, and mobile applications, and a framework will ensure the Department's use of commercial mobile devices is reliable, secure, and flexible enough to keep up with fast-changing technology.

As follow-on to the Strategy, my office recently (on February 15, 2013) issued the DoD Commercial Mobile Device Implementation Plan. The implementation plan establishes a framework to equip the Department's 600,000 mobile-device users with secure classified and protected unclassified mobile solutions that leverage commercial off-the-shelf products, encourage the development and use of mobile applications to improve functionality, decrease

costs, and enable increased personal productivity. The plan orchestrates a series of operational pilots from across the DoD components that will incorporate lessons learned, ensure interoperability, refine technical requirements, influence commercial standards, and create operational efficiencies for DoD mobile users. The DoD Mobile Device Strategy and Implementation Plan aim to align the various mobile devices, pilots and initiatives across DoD under a common security and cost framework that aligns with efforts in the JIE. This is not simply about embracing the newest technology – it is about keeping the Department's workforce relevant in an era when information accessibility and cybersecurity play a critical role in mission success.

Key partners in these efforts are the Defense Information Systems Agency (DISA) and the National Security Agency (NSA), who working together with industry, have developed security configuration baselines for several of the major smart phone technologies and are working on more. The Services are also actively involved in these efforts and will be responsible for helping develop mobility applications.

Enterprise Services

As noted above, enterprise services are those global applications that can be used by many, if not all users within DoD. They are a key element of achieving more effective operations and improved security across the Department. An example of what the Department is doing in this area is Defense Enterprise Email, which is an enterprise messaging tool, built by consolidating existing disparate email servers into a global capable server and operated by DISA on a fee-for-service basis, which provides DoD with a common enterprise directory service and a consolidated email service.

The enterprise directory service is being incorporated by many organizations, and the Defense Enterprise Email is currently used by DISA, EUCOM, AFRICOM, USFK, Defense Manpower Data Center, Office of Naval Research, Navy Recruiting Command, the Joint Staff, and the US Army. As of March 2013, there are 976,000 enterprise email users on the Department's unclassified network and 21,000 users on the DoD Secret network, and continued adoption and consolidation to this capability is expected in the future.

In June 2012, my office completed a report to Congress stating that decisions to consolidate organizational email capabilities beyond the current user community, such as Navy, Marine Corps and Air Force, are being considered and will be validated using a business case analysis.

Cloud Computing

Cloud Computing is becoming a critical component of the JIE and the Department's IT modernization efforts and will enable users the access to data anywhere, anytime on any approved device. One key objective is to drive the delivery and adoption of a secure, dependable, resilient multi-provider enterprise cloud computing environment that will enhance mission effectiveness and improve IT efficiencies. Cloud services will enhance warfighter mobility by providing secure access to mission data and enterprise services regardless of where the user is located and what device he or she uses.

My office recently issued the DoD Cloud Computing Strategy to provide an approach to move the Department to an end state that is an agile, secure, and cost effective service environment that can rapidly respond to changing mission needs. There are two key components of the Department's cloud strategy. The first component is the establishment of a private enterprise cloud infrastructure that supports the full range of DoD activities in unclassified and classified environments. The second is the Department's adoption of commercial cloud services that can meet the Departments cybersecurity needs while providing capabilities that are at least as effective and efficient as those provided internally.

The DoD's Enterprise cloud infrastructure will provide shared technology capabilities for the consolidation of stovepiped services at installations and in core datacenters. It also will define connectivity standards for end-user devices, unmanned clients and other networks. This will enable the Department to develop and deliver new and more integrated enterprise information services that support our warfighters and business support operations, which will improve the effectiveness, security and reliability of those operations.

The DoD CIO continues to investigate new ways to leverage commercial cloud computing innovations and efficiencies to improve the Department. The nature of the Department's mission, and the risk to national security if DoD information were to be compromised, requires the careful evaluation of commercial cloud services, especially in areas of information assurance

(IA) and cybersecurity, continuity of operations, and resilience. To improve our cybersecurity posture with regards to commercial cloud computing, we are participating in the Federal Risk Authorization and Management Program (FedRAMP) and updating our own cybersecurity policies.

I have designated DISA as the DoD Enterprise Cloud Service Broker to facilitate and optimize access and use of commercial cloud services that can meet DoD's security and interoperability requirements, and ensure that new services are not duplicative of others within the Department while consolidating cloud service demand at an enterprise level. In addition, DISA, as the DoD broker, will leverage the FedRAMP standardized security authorization process, including the accepted minimum security baseline for low and moderate services, and ongoing continuous monitoring to ensure that appropriate security controls remain in place and are functioning properly.

Cybersecurity

Cybersecurity is one of the highest priorities of the Department and the Administration. The primary cybersecurity goal of my office is ensuring that essential DoD missions are dependable and resilient in the face of cyber warfare by a capable adversary. This is also a primary concern driving the other improvement efforts, particularly JIE. This focus on mission assurance, rather than on computer or system security, is one of the primary changes in the department's cybersecurity approach. In addition, another change is the focus in JIE of giving certain operational commanders more freedom to take operational cyber security risks. We do this by using "risk zones" in the design of the JIE computing and networks; these zones help keep the risks assumed by a particular mission from spilling over into other missions. This is also a significant change from today's DoD networks which impose more operational constraints on commanders. Other primary cybersecurity goals include improved safe sharing with whatever partners a mission requires, and a continued need to keep a secret. Through refinement of the JIE concept, including the JIE single security architecture, we have concluded that all of these cyber security goals can be achieved, and the Department will have better joint warfighting decision support, better operational and acquisition agility, and better efficiency.

Like other IT efforts, cybersecurity is a team sport within the department, and these efforts span many organizations. In particular, I work closely with General Alexander of Cyber Command in the definition and execution of the Department's cybersecurity program. I also work closely with each of the Services and Agencies and others in the Office of the Secretary of Defense to ensure cybersecurity issues are being addressed.

Given the complexity of the cybersecurity problem, and of DoD's IT environment, there are a wide range of technical and operational efforts aimed at achieving the above cybersecurity goals. Initiatives in support of the dependability and secrecy goals include efforts to remove vulnerability, to shield latent vulnerabilities by layering defenses, and to ensure an understanding of where vulnerabilities still exist. In spite of best efforts to harden DoD systems, an adversary may still succeed, so there are also a variety of efforts to contain, dampen, detect, diagnose, and react to successful or partially successful cyber intrusions and attacks.

A key priority in the last year has been the development of a unifying, joint cybersecurity approach for the design of the JIE. This is the JIE Single Security Architecture (SSA). Although many of the DoD's cyber security initiatives are common across all DoD organizations, each military service has had the ability to make important decisions about how to design computing and networks and about how to structure cyber defenses. This has led to several challenges, such as diversity in the cybersecurity protections of the DoD that does not provide a common level of protection for joint missions (because the IT for these missions is designed and operated by many organizations), and sometimes interferes with the collaborative attack detection, diagnosis, and reaction so necessary in a complex organization like DoD . Finally, the challenge caused by this diversity can interfere with a joint commander's ability to share information with external mission partners.

To solve these problems, the SSA provides for a common approach to the structure and defense of computing and the networks across all DoD organizations. For example, the SSA describes how core DoD data centers and the server computing they contain must be structured, what cyber defenses are required on these computers; what cyber "firebreaks" are necessary as part the internal networks of the data center; how remote management and automation of the data center is to be structured and secured; and what cyber-attack detection, diagnosis, and reaction

capabilities the data center and the remote management system must have. As another example, the SSA defines the structure of the computing and networks on a typical military base. A part of this is that all computer servers that must be located close to end-users (for example print servers) will be located in an installation processing node data center. The computers in this node must be configured and managed to DoD-wide cybersecurity standards and use DoD standard defense and situational awareness tools, and the installation processing node must be outfitted with perimeter defenses that can be configured to meet DoD wide policies. All information about this computing node and its defenses must be shared throughout the joint DoD cyber defense operational structures. A final example is that the SSA requires that the cyber identity credentials from the DoD Public Key Infrastructure (PKI) be used in every access to information in the JIE so as to drive anonymity out of the DoD networks, and it defines how directories that are used in access control decisions must be structured so as to strongly inhibit a cyber adversary's ability to move laterally inside the Department's networks.

This engineering of the cyber security approach "end-to-end" will significantly improve DoD's ability to resist cyber-attacks; to dampen the spread of successful attacks; and to detect, diagnose, and react to attacks in ways that are optimized for joint missions. Owing to the standardization and cyber data sharing of JIE, cyber defenders will have broad visibility into the computing and networks, and via secure remote management and automation, they will be able to much more quickly construct and execute defensive actions. In addition, the risk containment zones the SSA defines in the server computing and the network will enable joint commanders to better contain cyber risk to mission while sharing as broadly with external partners as a mission requires. It will also make development of new decision support capabilities simpler and easier since many program offices will not need to worry about most cybersecurity protections, but will instead be able to build software applications on top of the standard protections and situational awareness capabilities provided by JIE.

Public Key Infrastructure (PKI)

My introduction mentioned the DoD PKI cyber identity credential that is stored on our DoD Common Access Card (CAC) and is used by every DoD user on the unclassified networks. We are also deploying similar cyber identity credentials throughout the Department's Secret networks. This is a central part of efforts to drive anonymity out of the networks, and to drive up

the accountability required for a successful insider threat management program. To date, more than 300,000 smart cards with these PKI credentials have been issued and implementation efforts have begun for cryptographic logon for accounts using these credentials.

The government's secret networks are interconnected to improve interagency sharing of mission essential information. Standardization of the defenses of all of these networks is essential to the security of every agency, including DoD. To help other agencies more quickly drive out anonymity on the secret networks, and to drive up accountability in a cross-organization way via the use of a standard cyber identity credential, in calendar year 2012 DoD initiated work with other federal departments and agencies to provide them the ability to issue PKI cyber identity credentials for the secret networks. DoD's PKI Common Service Provider (CSP) is funded by non-DoD departments and agencies via an OMB-coordinated, shared fee for service cost model and is scheduled to allow other agencies to start issuing PKI credentials in June 2013. This will not only help improve accountability for information access, but as DoD works with the rest of the Government will make interagency sharing safer and easier.

Supply Chain Risk Management

Progress continues in other areas of cyber security. First, rapid uptake of advanced commercial technology remains a key DoD advantage. While globally sourced technology provides innumerable benefits to the Department, it also provides foreign sources with increased opportunity to compromise the supply chain by inserting malware into technology in order to access or alter data, and intercept or deny communications. In response to these risks, DoD is institutionalizing the Trusted Defense Systems / Supply Chain Risk Management (SCRM) strategies described in the Report on Trusted Defense Systems delivered to the Congress in January 2010. Mr. Frank Kendall, the Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L)), and I jointly issued DoD policy in November 2012, which makes permanent the Department's policies to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or components. My office and the office of the USD(AT&L) oversee implementation of this policy and work closely with the Military Services and nine Defense Agencies, including DISA, NSA, the Defense Intelligence Agency, and the Defense Logistics Agency, to achieve full operating capability for the Department.

My office has undertaken efforts to take its lessons learned to the interagency as well. Representatives from this office and DHS worked with the Committee on National Security Systems (CNSS) to develop CNSS Directive 505 - Supply Chain Risk Management, which serves as the supply chain policy that applies to all national security systems within the federal government. DoD also is partnering with other Departments and agencies to explore approaches to managing supply chain risk within critical infrastructures, which are critical to executing DoD missions.

The Defense Industrial Base Cybersecurity/Information Assurance Program

The DoD operates a successful public/private cyber information sharing program that is a model for other government/industry cybersecurity efforts. It is the DoD's Defense Industrial Base (DIB) Cybersecurity and Information Assurance (CS/IA) Program that DoD CIO oversees. This program offers a model standard for government-industry voluntary partnerships on cybersecurity. The program provides two-way cyber information sharing to include classified threat information sharing by the government, with voluntary sharing of incident data by industry, as well as sharing of mitigation and remediation strategies, digital forensic analysis, and cyber intrusion damage assessments. As an example, the DoD provides fast analysis of malicious software reported by industry and quickly shares with the DIB CS/IA participants, and with the rest of the Federal Government, machine readable indicators of the attack that can very quickly be deployed to protect others against new and emerging threats detected by any of the participating companies. While threats cannot be eliminated, the DIB CS/IA program enhances each DIB participant's capabilities to mitigate the risk, thereby further safeguarding DoD information that resides on, or that transits, DIB unclassified networks. Building on this successful model, the DoD partnered with the Department of Homeland Security to put in place a means of using even more highly classified information to protect the networks of participating companies. Under the DIB Enhanced Cybersecurity Services (DECS) program, the government provides highly classified cyber threat information either directly to a DIB company or to the DIB company’s Commercial Service Provider (CSP). This sensitive, government-furnished information enables these DIB companies, or the CSPs on behalf of their DIB customers, to counter additional types of malicious cyber activity. The CSPs provide the protections as a commercial fee-for-service offering; the government is not involved in the financial aspects of

the transaction between a CSP and the participating DIB company. DoD is the government point of contact for the participating DIB companies, through the DoD's DIB CS/IA Program. DHS is the government point of contact for participating CSPs, under the umbrella of DHS' Joint Cybersecurity Services Program (JCSP), a broader effort to protect U.S. critical infrastructure

Future of Cybersecurity.

Transforming cyber defenses and regaining the advantage against cyber adversaries will require new strategic imperatives, such as shifting from reactive to more pro-active cyber defense operations, and focusing a greater portion of cyber defense activities on adversary activities and intent. Currently, the approach to cyber defense is based primarily on policy compliance, hardening configurations, and patching vulnerabilities, which are necessary but not sufficient. As the DoD focuses on cyber defenses driven by intelligence about the potential adversary, this shift will enable improvements to detect, protect, and respond to the threat's quickly changing cyber tactics. The term "active cyber defense" describes this new approach, which is DoD's synchronized real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It operates at network speed by sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems. Adversaries will discover they cannot single out and attack local units without bringing to bear broader DoD support from intelligence and cyber forces. Active cyber defense is a transformational capability in an early operational stage. DoD will refine and evolve its capabilities by leveraging advances in all aspects of cyber operations and integrating national, regional, and organizational cyber defenses into a coherent active cyber defense framework.

Support to the Warfighter

In my capacity as the Department's CIO, I am responsible for overseeing Presidential and Senior Leader Communications; Nuclear Command, Control, and Communications; and Continuity Communications. The Deputy Secretary of Defense recently established a Joint Systems Engineering and Integration Office (JSEIO) under my direction, through the Director of DISA, to manage issues across all three of these critical mission areas. This will ensure a focused end-to-end integration of requirements, configuration management, assessments, and architecture in this nationally critical mission area.

Related and complementary to this function, I co-chair, along with a representative from the Department of Homeland Security, the National Security/Emergency Preparedness (NS/EP) Communications Executive Committee as a forum with members from the Departments of State, Defense, Justice, Commerce and Homeland Security; the Office of the Director of National Intelligence; the General Services Administration; and the Federal Communications Commission. The forum is responsible for ensuring the Federal Government has the ability to communicate at all times and under all circumstances to carry out its most critical and time sensitive missions, and for recommending policy and advising the President on NS/EP communications issues.

Positioning, Navigation and Timing (PNT)

Space-based positioning, navigation and timing (PNT) provides crucial capability to military, civil, and commercial users worldwide. We are working to better integrate the services of the Global Positioning System (GPS) as the primary means of delivering PNT. Precise timing is a key enabler of cyberspace operations and a part of our nation's critical infrastructure. Our PNT architecture provides our nation and allies the ability to precisely navigate anywhere in the world while the precise timing part also enables network encryption, synchronization and integration of data networks within the communications and cyber enterprises. With this understanding, we are working, as a high priority, several infrastructure upgrades to protect this critical piece of cyber terrain.

Spectrum

Spectrum has become increasingly important not only to the Department's missions, but to consumers and the economy of the nation as a whole. The use of the electromagnetic spectrum continues to be a critical enabler of our warfighting capabilities and the Department's cyber operations. Defense leadership is cognizant and sensitive to the unprecedented spectrum demands resulting from the Department's increasing reliance on spectrum-dependent technologies and the rapid modernization of commercial mobile devices. Fully recognizing the linkages between national security and economic prosperity, the DoD is fully committed to the President's 500 MHz initiative to make spectrum available for commercial broadband use, the implementation of more effective and efficient use of this finite radio-frequency spectrum and

the development of solutions to meet these goals while ensuring national security and other federal capabilities are preserved.

To that end, the Department is investing in technologies and capabilities aimed at more efficient uses and management of spectrum, and for increased interoperability with our Coalition partners and with Federal, State, and Commercial entities. DoD already is proactively working with NTIA, other Administration partners, and industry to methodically evaluate spectrum bands, through established deliberate processes. One example is DoD's extensive efforts, actively working with industry, to assess the feasibility of sharing the 1755-1850 MHz band through the NTIA established working groups under the Commerce Spectrum Management Advisory Committee (CSMAC). The CSMAC working groups' effort is an example of an unprecedented collaboration between the DoD and the commercial industry to assess highly complex technical issues with a goal of ensuring practical and balanced spectrum repurposing decisions that are technically sound and operationally viable from a mission perspective. I look forward to working with Congress on future spectrum legislative proposals that achieve a balance between expanding wireless and broadband capabilities for the nation and the need for access to support warfighting capabilities in support of our national security.

Satellite Communications

Over the past year, DoD CIO has established a framework for end-to-end management of the Department's Satellite Communications (SATCOM) enterprise. The work of my office with DISA and the Services has already allowed the Department to realize some benefit as we conclude our analysis of a Commercial SATCOM cost recovery model, implement a converged SATCOM Gateway architecture, establish a plan of action for the Presidential Nuclear Voice Conferencing system integration, and conduct an analysis of alternatives for future protected and narrowband SATCOM requirements. This is especially critical in the Asia Pacific rebalance as the vast oceanic expanse requires additional focus on communications infrastructure that is provided with these efforts.

Asia Pacific Rebalancing

To support the President's and SECDEF's Strategic Guidance to rebalance emphasis towards the Asia-Pacific region, the DOD CIO developed, and is executing, a detailed program of action and

milestones to improve command, control, communications and computer (C4) systems in this area of operation (ref: DOD CIO C4 Strategy Memorandum, 30 Jul 2012). This combined COCOM, Service, and Agency effort involves actions to improve coalition partner information sharing, strengthen existing C4 capabilities in the region, and to add new capabilities based on lessons learned from recent operations in the Middle East. Specific actions include increasing capacity and redundancy for Pacific satellite communications gateways, improving resiliency/throughput of existing communications nodes, adding emergency failover capabilities to support critical communications, enhancing cyber defense/situational awareness, building and improving coalition network capabilities, and implementing a common Joint Information Environment (JIE) to improve network effectiveness, efficiency and security in the Pacific theater.

Workforce Development

A very important element of the Department's cyber defense strategy is ensuring that the right workforce is in place. An initial response to the needs of the Department is the accelerated delivery of cyber personnel in 2013 and 2014. The Department is building a balanced and highly capable military cyber force designed to meet our joint warfighting requirements. As General Alexander has noted, the Department is establishing cyber mission teams to support the Combatant Commands. The Department is focused on recruiting, training and retraining the necessary workforce to defend U.S. national interests in cyberspace. The workforce must be properly sized and properly trained, and there must be career paths that encourage growth and development of cyber defense and related skills, such as system management, cyber mission management, and cyber operations. The Department's IT modernization effort includes a strong cyber defense workforce component that is an integral part of the Department's larger information technology and cyber workforce.

Complementing the Department's cyber defense workforce component, is an enterprise wide cybersecurity awareness program designed to empower every person in DoD with the knowledge, skills and training to make continuously improving cybersecurity decisions. This effort is shared with 22 civil federal agencies.

Information Technology Exchange Program (ITEP)

Section 1110 of the FY10 National Defense Authorization Act (Public Law 111-84) authorized DoD to establish a Pilot Program for the Temporary Exchange of IT Personnel, referred to as the ITEP pilot, which expires September 30, 2013. While there has been limited participation to date, the assignments thus far have been mutually beneficial to DoD and private industry, and DoD has found the authority provides a valuable tool for exchanging innovative ideas with industry.

The ITEP program allows DoD and industry to each experience the challenges each other faces in managing their IT acquisitions, infrastructure and security requirements, and to exchange best practices on these issues.

While the program has been slow to grow and has had limited participation, the internal policies and processes to implement it have been established, and a long term program would help foster DoD relationships with the private sector and sustain the program. To date, an IT Project Management assignment was completed by Vanguard Advisors, LLC, within the Office of the DoD Comptroller and we currently have an ongoing ITEP assignment from Cisco Systems Inc. within my office.

IT Investment Planning

Additional changes to Department processes are necessary to ensure adaptability to technological advances and an ability to defend the network against emerging cybersecurity threats.

In particular, changes to the Department's three core processes – requirements, budgeting, and acquisition – are required to address the systemic conditions resulting in DoD's stove-piped IT infrastructure. My office is working closely with the office of the Deputy Chief Management Officer on efforts to develop a flexible, agile acquisition process that also addresses the DoD's requirements and budgeting processes to institutionalize the agility and flexibility necessary in this rapidly evolving domain. We are leading a group comprised of Comptroller and CAPE to look at innovative options for funding enterprise services. An interactive transition plan template that defines "owner-operator," transition costs and funding strategies was designed and implemented for collecting data associated with the first increment of JIE in Europe. This template will serve as the basis for an integrated cost model that will be used for future IT

investment planning efforts. These are the primary efforts that will assure that the Department is using every dollar most effectively.

Conclusion

Maintaining information dominance for the warfighter is critical to our national security. The efforts outlined above will ensure that the Department's information capabilities provide better mission effectiveness and security, and are delivered in a manner that makes the most efficient use of financial resources. I ask that you strongly support, authorize, and fund the Department's key cybersecurity and Information Technology modernization programs. I want to thank you for your interest in our efforts and I am happy to answer any questions you may have.