STATEMENT BY

TERESA M. TAKAI
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON

INTELLIGENCE, EMERGING THREATS & CAPABILITIES

ON

"Information Technology and Cyber Operations: Modernization and Policy Issues in a Changing National Security Environment"

March 12, 2014

NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS & CAPABILITIES, HOUSE ARMED SERVICES COMMITTEE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 today on information technology (IT) modernization and policy. 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 to 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 ever-increasing cyber threats. 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 a broad overview of the Department's IT landscape; summarize recent directions from the Secretary of Defense to strengthen the DoD CIO; and describe the Joint Information Environment (JIE), DoD's multiyear 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 make us more efficient and better stewards of taxpayer resources. I will also briefly describe some of the activities underway in my office related to my responsibilities for overseeing Positioning, Navigation and Timing (PNT) and spectrum.

Overview of DoD's Information Technology

The Department's FY14 IT budget request was $39.6 billion and included funding for a broad variety of information technology, ranging from command and control systems, commercial satellite communications, and tactical radios to desktop computers, server computing, enterprise services like collaboration and electronic mail, and DoD business systems. These investments support mission critical operations that must be delivered both on the battlefield and in an office environment. They also provide capabilities that enable the Commander-in-Chief to communicate with and direct the military, and that support command and control, intelligence, logistics, medical and other warfighting and business support functions throughout the Department. The overall IT budget includes funding for the Department's cyber activities and efforts. These are designed to ensure that essential Department missions work well in the face of cyber attacks. These cyber efforts continue to receive the highest-level attention and support of the Department.

Secretary of Defense Organizational Review

Recently Secretary of Defense Hagel issued direction to strengthen the role of the DoD CIO. Specifically he affirmed the importance of my office as an OSD Principal Staff Assistant with the responsibilities listed above. As well, he directed actions to add functions, expand authorities, and restore stature to the DoD CIO, with a priority focus on advancing the JIE as a special interest item for the Secretary. The Secretary also directed my office to improve visibility, oversight, and governance of IT resources. And, he reaffirmed the critical importance of addressing the challenges posed by cybersecurity.

My office has completed the development of a plan of action and milestones to implement the Secretary's direction. We are taking actions necessary to increase visibility into IT budgets and spending patterns, and are strengthening our analysis of IT investments and evolving our processes for IT governance and oversight.

Consistent with the Secretary's direction, my office is working closely with others in the Department to identify ways to adapt our existing processes to ensure adaptability to technological advances and ability to defend the network against emerging cybersecurity threats. In particular, we are examining how best to leverage the Department's three core processes - requirements, budgeting, and acquisition - to address the systemic conditions resulting in DoD's stove-piped IT infrastructure. This is critical if we are to achieve the agility and responsiveness from IT systems that warfighters both demand and deserve, and improve our ability to defend against cyber attacks. My office is working closely with the offices of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), Deputy Chief Management Officer (DCMO) and others to make the existing acquisition process more flexible and agile for IT and IT services, while ensuring compliance with enterprise standards.

Joint Information Environment

Mission success depends upon the ability of our military commanders and civilian leaders to act decisively based on the most timely and accurate data and information. 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 information access to the user, improve our ability to not only defend the networks and the data, but make it responsive to constantly changing technological and operational factors. The challenge is amplified because capable adversaries are extremely active in seeking to penetrate DoD systems, compromise command and control, to steal or destroy sensitive and strategic information, to gain an upper hand on U.S. forces and warfighting capability. Consequently, DoD is pursuing the alignment of existing vast IT networks into a Joint Information Environment (JIE) construct. 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, and 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.

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 across software, servers, the network, mobile and fixed user computing, and identity and access control systems. Users and systems will be able to trust their connection from end to end with the assurance that the information and systems involved in a mission are correct and working even during a cyber attack. The JIE architecture will enable cyber operators at every level to see the status of the networks for operations and security and will provide standard resilience and cyber maneuver options for all cyber forces. This will minimize complexity for a synchronized cyber response, maximize operational efficiencies, and reduce risk. Most importantly, unlike the one size fits all networks the department has now, the JIE will provide mission commanders more freedom to take operational risk with the networks since the risks can be contained to the decision support and systems specifically needed for that mission.

- 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 that defines enterprise standards and supports effective fielding of Department capabilities in support of information sharing, as well as sustainment and integration of legacy systems.

The Department plans on utilizing 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. The Department’s efforts are consistent with and support the Federal Data Center Consolidation Initiative (FDCCI) being led by the Federal CIO, and have resulted in the closure of 277 data centers as of first quarter FY14. The Department’s progress in this area has been aided by Section 2867 of the FY12 National Defense Authorization Act.

The Department has established 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; and

- 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.

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 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 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.

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.

Enterprise Services. As previously noted, 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 this 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

the Defense Information Systems Agency (DISA) on a fee-for-service basis. The result is a common DoD enterprise email and contact address list and consolidated email service.

The basis for enterprise email and other services is an authoritative identity service. Defense Enterprise Email is currently used by DISA, the US Army, the Joint Staff, the Office of the Secretary of Defense, Defense Manpower Data Center, Office of Naval Research, Navy Recruiting Command, HQ Air Force, Air Force District Washington, EUCOM, SOUTHCOM, TRANSCOM, AFRICOM and USFJ. As of February 2014, there are 1.6 million enterprise email users on the Department's unclassified network and 150,000 users on the DoD Secret network. Continued adoption and consolidation to this capability is progressing.

Cybersecurity

Cybersecurity is one of the highest priorities of the Administration and the Department. The primary cybersecurity goal of my office is ensuring that essential DoD missions are dependable and resilient in the face of cyber exploits and attacks 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. This approach enables us to move from an approach of bolting on cyber security solutions to one where resilient, mission assurance and cyber security characteristics will be built into the total information environment.

JIE gives certain operational commanders more freedom to take operational cyber security risks. We accomplish 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 at U.S. Cyber Command, and others in the Office of the Secretary of Defense, the Military Departments and Defense Agencies to ensure cybersecurity issues are being addressed.

Single Security Architecture (SSA). 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. 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.

The Defense Industrial Base (DIB) Cybersecurity (CS) /Information Assurance (IA) Program. The DoD's DIBCS/IA Program, overseen by my office, is a successful public/private cyber information sharing program that is a model for other government/industry cybersecurity efforts. 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, so 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' Enhanced Cybersecurity Services program, a broader effort to protect U.S. critical infrastructure

Insider Threat. The threat that insiders will use their authorized access to do harm to the security of the United States has long been recognized by the DoD. This threat can include damage to the United States through espionage, terrorism, or unauthorized disclosure of information, or through the loss or degradation of departmental resources or capabilities, including acts of violence against our greatest asset, our personnel. Information is one of the greatest sources of power, and it must be appropriately protected, with access to our most sensitive information restricted to those with a real "need to know", while still enabling sharing as warranted.

In consideration of damage from disclosures of classified information stolen by insiders, including the WikiLeaks and the more recent unauthorized disclosures, the Department has conducted extensive reviews of its posture, and the Secretary has directed corrective measures be undertaken.

Last year the Under Secretary of Defense for Intelligence (USD(I)) and I released a joint memorandum directing an initial program of required actions and procedures to strengthen our insider threat safeguards. These measures included:

- the revalidation of the need for Privileged Access and the suitability of each person in a Privileged Role (e.g. system administrators) to minimize their numbers to those absolutely required for the mission;
- stronger safeguards on the use of Removable Media, including two person controls for their use in Sensitive Compartmentalized Information Facilities (SCIFs); and
- direction to complete implementation of our Public Key Infrastructure (PKI) efforts. The Department has made excellent progress on these efforts, but we must continue to strengthen our cybersecurity measures.

We have worked with the White House's Senior Information Sharing and Safeguarding Steering Committee to develop further safeguarding measures to mitigate the risks to our most sensitive information. We are about to issue direction to implement these measures, which include tasks to enhance the security culture, improve business practices, reduce the risks associated with "privileged" users, and improve personnel security through Continuous Evaluation.

In all these efforts, we have been working to ensure a comprehensive Department-response. We work closely with USD(I), the Department's lead for Insider Threat, on the Department's plan for an Insider Threat program; with U.S. Cyber Command as we

develop further insider threat mitigation strategies for our networks, and with DISA as we evaluate and develop technical solutions.

DoD Strategy for Defending Networks, Systems, and Data. The DoD CIO published a new Strategy for Defending Networks, Systems, and Data in October 2013. The strategy identifies strategic imperatives to ensure the protection, integrity, and assurance of DoD cyber assets. It is focused in four key areas: establishing a Resilient Cyber Defense Posture; Transform Cyber Defense Operations; Enhance Cyber Situational Awareness; and Assure Survivability against Highly Sophisticated Cyber Attacks. In the near term, we will be finalizing the Implementation Plan for the strategy. To ensure success going forward, we will collaborate closely with others in the Department.

Cyberspace Workforce and IT Acquisition Workforce Development.
A critical component of readiness is a workforce that is properly sized, well trained and equipped. In concert with the Department's JIE transformation, the DoD is implementing a comprehensive strategy to transform legacy and evolving workforces such as IT, information assurance (IA), and cyber mission teams into a cohesive cyberspace workforce. The DoD cyberspace workforce strategy focuses on recruiting, training, and retaining the necessary workforce to build and operate its networks as well as defend U.S. national interests in cyberspace. This community will ensure that the DoD can acquire, structure, operate and defend its information, networks, systems, services and capabilities to achieve operational and strategic advantage in cyberspace. To be successful, it will need to expand learning opportunities from traditional classroom training to include a variety of training environments, including virtual and mobile training; hands-on laboratories; leveraging cyber ranges and focusing on both individual and team cyber skills development in a realistic environment.

The Department is leveraging established training and education venues both internally and externally to maximize professional development opportunities for the cyberspace workforce, and identifying where gaps exist in training and education programs. One new initiative is our collaboration with the Joint Staff and the National Defense University on a cyber-centric Joint Professional Military Education program to educate military and civilian leaders on key cyberspace tenets.

With regard to the IT acquisition workforce specifically, we are collaborating with the USD(AT&L) to strengthen the IT acquisition workforce, with emphasis on improving cybersecurity capabilities. Two years ago, the Under Secretary and I co-signed a strategic plan for the IT Acquisition Workforce which has served as the springboard for a series of ongoing initiatives. These efforts include conducting a comprehensive review and update of the Defense Acquisition University's (DAU) IT acquisition curriculum, and removing roadblocks to training and certification, enabling the Department to achieve a 20 percentage point increase in the certification rate of qualified personnel.

In all of our development efforts, we are collaborating with other acquisition career fields (particularly program management, engineering, contracting, and test and evaluation) and are also working with Acquisition leadership to infuse cybersecurity training across all DAU academic disciplines in recognition of the critical roles many acquisition personnel

perform within the cyberspace workforce. Initiatives include collaborating with AT&L on a Cybersecurity Handbook for Program Managers, in draft, to provide program managers clear and concise guidance on what cybersecurity activities should be conducted at each point in the acquisition process. We are also leading a cross-functional working group in the development of a cybersecurity distance learning course to provide foundational insight on critical cybersecurity issues across the acquisition lifecycle. The goal is to ensure the Department follows an integrated, holistic approach to cybersecurity in the design, development, deployment and sustainment of all our programs, irrespective of one's particular career field. These initiatives, as well as Service-specific efforts will ensure that, together, DoD is creating a robust training and education environment to sustain a world class, mission ready cyberspace workforce. However, today's budget constrained environment limits the speed at which the Department can implement the changes needed to evolve and meet the demands of the cyberspace domain.

Space-based positioning, navigation and timing (PNT) and Spectrum
In addition to my responsibilities for IT and cybersecurity, I am also the Secretary's principal staff assistant for several other critical information capabilities, including PNT and spectrum.

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 which provides our nation and allies the ability to precisely navigate anywhere in the world. Our PNT architecture provides our nation and allies precise target location, the ability to strike with a minimum of collateral damage, navigation capabilities that support logistics, command and control, and friendly force tracking, and precise timing. This latter feature is critical to 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 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 has developed a plan that will make 25MHz of spectrum available to commercial industry on a shared basis, thus achieving 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.

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.