STATEMENT BY

TERESA M. TAKAI

ACTING ASSISTANT SECRETARY OF DEFENSE

FOR NETWORKS AND INFORMATION INTEGRATION

AND

DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON

EMERGING THREATS AND CAPABILITIES

ON

IMPROVING MANAGEMENT AND ACQUISITION OF INFORMATION
TECHNOLOGY SYSTEMS IN THE DEPARTMENT OF DEFENSE

APRIL 6, 2011

Good afternoon Mr. Chairman and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee on Terrorism, Unconventional Threats and Capabilities on the importance of information technology (IT) to the transformation of the Department of Defense (DoD). I am Teri Takai, and I am the Acting Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) and the Department's Chief Information Officer (CIO). My testimony today will focus on how the DoD is leveraging information technology to securely deliver mission critical information capabilities to the men and women of the Department of Defense and our mission partners.

Department of Defense Information Technology (IT) Overview

The Department's FY12 IT budget request of $38.4 billion includes funding for desktop computers, tactical radios, identity management technology, commercial satellite communications, and more. These investments support mission critical operations that must be delivered in an environment of ever-changing requirements and ever-increasing demand for additional information capability. Where in the past the Department sought to balance the "need to know" with the "need to share," today, the warfighter expects to have and needs to have the latest information in order to complete the mission. The increasing use of social media, smart phones and tablet computers has made information sharing an expectation. This expectation requires new capabilities, particularly in the "edge" or tactical environments that have limited availability to persistent, high speed

connections. Our challenge today is ensuring our networks can securely support the

information demands of our users – users who require access to information anywhere

and anytime across the DoD Information Enterprise (IE), allowing them to make

informed decisions in the execution of their missions. To meet this challenge, DoD

networks must be designed and optimized to more effectively and efficiently support

mission operations, for both garrisoned users and those at the "edge".

Information Assurance or Cybersecurity. DoD networks are under constant attack from

cyber security threats launched from the Internet or from malicious software embedded in

email attachments, removable media, or embedded in the hardware the Department

procures. Every device connected to the network is susceptible to cyber vulnerabilities.

While working to efficiently respond to the information demands of our users, we must

be ever vigilant in protecting our information environment from cyber threats.

Just over $2.8 billion of the Department's $38.4 billion IT budget request is devoted to

information assurance or cybersecurity activities that defend the Departments

information, information systems and communications networks. The Department's

FY 2012 information assurance budget request includes increased funding to address

insider threat and cyber vulnerabilities such as those identified in the WikiLeaks incident,

among other things. Specifically, we have requested funding to support deployment of a

Public Key Infrastructure (PKI)-based identity credential on a hardened smart card for

use on the Department's secret classified network, a successful technology very similar to

the Common Access Card (CAC) we use on our unclassified network. We have also

identified funds needed to: deploy Host Based Security System (HBSS) to secure our

classified systems; provide an automated capability to continually monitor the

configuration and security state of DoD networks; and improve identity management

capabilities across the Department.

Operational Efficiencies. The DoD is planning for the investment and implementation of

these IT and information assurance capabilities within today's current resource

constrained environment. Recognizing this budget environment, in August 2010, the

Secretary directed a number of initiatives to achieve savings in acquisition, sustainment,

and manpower costs, while not degrading the Department's ability to execute its

missions. Among these is the consolidation of the Department's IT infrastructure while

simultaneously defending that infrastructure against growing cyber threats.

DoD IT Enterprise Infrastructure Optimization Strategy and Plan

My office is responsible for leading the development of a strategy and plan for

consolidating the Department's IT infrastructure in five (5) broad areas: network

services; computing services, application and data services, end-user services, and IT

business processes. I plan to issue the DoD IT Enterprise Infrastructure Optimization

Strategy and Plan this quarter. This plan represents the Department's strategy and initial

roadmap to achieve the goals of improving mission effectiveness and heightening the

Department's security posture. By delivering a streamlined, rationalized, and simpler

network through consolidation of information technology infrastructure across the Department, this strategy will deliver efficiencies that can be redirected to mission capabilities. This plan commits us to changing policies, cultural norms, and organizational processes to provide lasting results. The initial focus is on obtaining tangible results in Fiscal Years (FY) 2011-2012, while planning for aggressive consolidation through FY 2015. This consolidation will make us better positioned to embrace emerging technology and provide cutting-edge capabilities to our warfighters. It is intended to provide the Department with the flexibility required to respond to and incorporate emerging technologies, while taking corrective action on those efforts not producing required results.

The result of these consolidation initiatives will be a DoD Information Environment that provides the warfighter with the required information and services needed to accomplish their mission. This standardized information and network infrastructure will eliminate the organizational barriers to information sharing and eliminate seams which attackers can exploit to gain access to vital information or systems. It will also increase the flexibility of defense networks to incorporate or respond to changes in emerging technology by minimizing the disparity within the Department's information architecture.

IT Investment Planning

The transformation of DoD's IT capabilities described above is a very ambitious undertaking – one that will reap tremendous benefits to the Department and our Nation

when completed. It will require agility, as well as new processes, to both keep abreast of technological advances and 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.

IT Workforce

The Department recognizes that the development, education and continuous training of our workforce is critical to ensuring the success of our IT and IA investments, and essential to our ability to utilize new capabilities and defend against emerging threats. I work closely with the office of the Under Secretary of Defense for Personnel and Readiness on that objective and I am working closely with other elements of the Department to ensure that we understand the evolving IT and IA workforce needs of the Department.

The Information Technology Exchange Program (ITEP) pilot, reauthorized by the FY 2010 National Defense Authorization Act for DoD, is one mechanism that the Department is pursuing to that end. Under this collaborative learning venture, DoD and

private industry organizations share best practices through the exchange of high performing personnel in IT functional areas such as IT Acquisition and Information Assurance (IA). ITEP provides an opportunity for both industry and the Department to learn from each other – to enhance employees' IT competencies and technical skills and infuse both DoD and industry with new ideas in this fast-evolving discipline. The program allows private company IT and IA employees to be detailed as employees to the DoD, with the private company continuing to pay the employee's salary. Similarly, DoD IT and IA professionals could be detailed to the private sector to gain experience; these employees would remain federal workers and their salaries would be paid by the DoD.

Through this exchange program, industry and government can gain a better understanding each other's IT management policies and procedures. The program will strengthen IT competencies and skills of employees from both federal and private sectors, and has the opportunity to change the dynamics of the way the public and private sectors share best practices and knowledge in the future.

My Office is responsible for implementing ITEP and we have created a guide to assist participating DoD Components with the implementation. The Department's goal is to have ITEP pilot participants on board by June 2011. In October 2011, we will formally report to the Congressional defense committees on the implementation and benefits of the program in the first of a series of annual reports.

Summary

Maintaining an information advantage for our users is critical to our national interest. The efforts outlined in this brief 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. My job is to provide the vision and leadership within the Department to ensure that these efforts satisfy the users' requirements effectively, efficiently and securely.

I want to thank you for your interest in our efforts and I am happy to answer any questions you may have.