STATEMENT BY

TERRY HALVORSEN

ACTING DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON

EMERGING THREATS & CAPABILITIES

ON

"Information Technology Investments and Programs: Supporting Current Operations and Planning for the Future Threat Environment"

FEBRUARY 25, 2015

Introduction

Good afternoon Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee today on the Department's information technology (IT) budget request. I am Terry Halvorsen, the Acting Department of Defense (DoD) Chief Information Officer (CIO). Since May 2014, I have served as the principal advisor to the Secretary of Defense for information management, IT, cybersecurity, satellite communications, positioning, navigation and timing, spectrum, and nuclear command, control and communications matters. My office provides strategy, leadership, and guidance to create a unified information management and technology vision for the Department and to ensure the delivery of information technology based capabilities required to support the broad set of Department missions.

As the DoD CIO, I have one imperative – to ensure that warfighters have the right IT/Cyber, secure communications equipment and capabilities they need to execute the missions given to the greatest fighting force in the world. In my capacity as the senior civilian advisor to the Secretary of Defense for IT, with responsibility for all matters relating to the DoD information enterprise, my office is driving cultural, business and technical innovation at DoD by better integrating our IT infrastructure, improving alignment, business process improvement, and supporting agile and innovative IT acquisition. This will help change how people at DoD are able to use IT, enabling support to their missions in new, improved ways, whatever the mission requires, from the desk to the desert. Although our prime business is warfighting, DoD is an expansive organization with responsibilities that go beyond warfighting, and include the areas of logistics/supply, personnel, finance, and medicine, among others. If DoD were a Fortune 100 company, it would be at the top of the list. We must adopt the cost culture and practices of the top performing companies to insure every dollar is accounted for and that to the greatest extent possible, we spend those dollars on the business of warfighting.

Today I would like to provide you with an overview of the Department's IT budget, the importance of IT and cybersecurity to our warfighting and business missions, and what we are doing to better manage DoD's IT spend to get more out of each and every dollar. I will highlight the Department's progress in implementing the Joint Information Environment (JIE) – specifically the Joint Regional Security Stacks (JRSS), efforts to strengthen the IT investment review and requirements management process, how we are improving relations with industry, as well as strengthening the IT workforce.

Overview of DoD's Information Technology

The Department's Fiscal Year (FY) 16 IT budget request is $36.9 billion. This request includes funding for a broad variety of IT, ranging from DoD warfighting, command, control, and communications systems, computing services, cybersecurity, enterprise services like collaboration and electronic mail, and, intelligence and 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 a request for $5.5 billion for the Department's cyberspace operations and activities. These are designed to ensure that essential Department missions work well in the face of growing cyberattacks. These cyber efforts continue to receive the highest-level attention and support of the Department.

DoD CIO Priorities

Joint Regional Security Stacks (JRSS)

One of my immediate priorities is to implement the Joint Regional Security Stacks, which are the first or foundational phase of the JIE. JRSS are a regionally based, centrally managed rack of servers, switches, and other equipment that will replace the current set of separate, individualized, localized Service and Agency security systems. This will help to ensure that the Department's facilities are using the same security architecture in order to move toward JIE. This approach takes into account that Military Department, Agency, and Combatant Command cyber and IT environments differ, which results in differing mission-based priorities. They will enable the operations commander and service partners to see a common network picture.

As of today, JRSS version 1.0 has been installed at 10 sites with traffic migration underway at the Defense Information Systems Agency (DISA)'s Defense Enterprise Computing Center (DECC) Joint Base San Antonio (Ft Sam Houston for Army and Lackland/Kelly Air Force Base for Air Force) and failover location DECC Montgomery. The JRSS version 1.0 capabilities enable the Army to sunset their local security enclave protections. Additionally, Joint Management System version 1.0 has been installed at DECC Joint Base San Antonio. This critical phase of the JIE began with the purchase of 15 JRSS for DoD's non-secure Internet Protocol Router Network (NIPRNET) and network upgrade components, which included bandwidth upgrades and Multi-Protocol Label Switching (MPLS) routers, by the Army through DISA in late FY13. The JRSS effort expanded in FY14 and this current fiscal year (FY15) to include Army, Air Force and DISA, the Navy, Marine Corps and Defense Health Agency (DHA) will begin migration work behind the JRSS in FY17.

The FY16 budget request for the Services, DISA, and DHA includes funding to purchase and implement JRSS version 1.5, network upgrade components, and JMS version 1.5 improvements. These investments will provide a global implementation of JRSS 1.5 for NIPRNET; the associated Department of Defense Information Network (DODIN) enhancements will result in for greater bandwidth and enhanced traffic routing and security, and enable the Air Force to sunset their Air Force Network Gateways in FY16.

In FY17, the JRSS version 2.0 will provide capabilities for the Navy, Marine Corps and DHA that will allow these components to sunset their individual gateways and fully leverage the JRSS and network upgrades. DoD is also in the process of planning the installation of 25 JRSS across the globe for the Secret Internet Protocol Router Network (SIPRNET).

When completed the JRSS will provide a more secure environment with improved command and control that operates at lower cost.

Mission Partner Environment/Network (MPE/N)

We are working to develop a more commercially based and robust mission partner environment/network. This approach will provide a more cost-effective, rapidly reconfigurable and multi-level data protection network. It will provide full data media capability to support operations in all environments, with the ability to rapidly add and subtract mission partners. This is a top requirement for all Combatant Commands.

Business Process Systems Review (BPSR) – Improving Alignment of Business Processes and IT Systems

The BPSR is a partnership between my office and that of the Deputy Chief Management Office (DCMO), currently led in an acting capacity by Mr. David Tillotson. Together we are co-leading the Defense Business Council, a review of business processes and the supporting IT systems within the Fourth Estate. We are working with the Defense Business Board (DBB) and industry experts to examine how we do business in the Pentagon and how we can do better. We are exploring the potential to increase government/industry partnerships in diverse areas such as data distribution, with the goal of creating a less costly platform while maintaining our stringent security standards. We are asking the question what businesses do we DOD need to be in and to what level. For the CIO office specifically this means asking what IT businesses should DISA be in and to what level. Based on this question and looking at the available data, I have directed DISA to make the next offering of DISA Unclassafied E-mail a purely commercial solution. I believe this will result in a 20-25% reduction in email costs. The BPSR review will provide the Secretary's senior civilian advisors with information to help them clarify whether their organizations are aimed at Department-wide outcomes and to identify any resources allocated to these outcomes. This effort also identifies potential obstacles to achieving the outcomes such as resource shortfalls and process obstacles, as well as activities that might be improved or eliminated. The overall goal is to increase mission effectiveness, through increased alignment of processes and systems; better understanding of the interrelationships between processes and systems; and to lower the overall costs of doing business through the implementation of cost-driven metrics. Within the office of the CIO, by reviewing contract benchmarks we were able to reduce spend by $10M this year. We were also able to reprogram $20M from DISA contracts without reducing contract work to support JRSS installs. DISA also lowered its rates by 10% and is on track to do the same next year. ,. These are just first examples and by the summer we will have more examples totaling substantially more dollars. The Defense Business Board is providing leaders from key industry sectors like IT and working with us to find area where we can quickly adopt new ideas and practices. One of which is how we are changing the approach to cloud computing.

Cloud Computing

Cloud computing plays a critical role in the Department's IT modernization efforts. Our key objective is to deliver a cost efficient, secure enough enterprise environment (the security driven by the data) that can readily adapt to the Department's mission needs. The cloud will support the Department's JIE with a robust IT capability built on an integrated set of cloud services provided by both commercial providers and DoD Components. We will use a hybrid approach to cloud that takes advantage of all types of cloud solutions to get the best combination of mission effectiveness and efficiency. This means in some cases we will use a purely commercial solution, which we have done with Amazon on public facing data, in others we will use a modified private cloud hosted in commercial solutions, an example could be a shared federal or federal state government cloud, and for our most protected data a DOD private cloud that uses best industry practices.

In the past year, the Department has made significant progress in adoption of cloud. My office completed a major revision to security requirements for commercial and DoD cloud service providers. The resulting Cloud Security Requirements Guide (CSRG) was published on January 12, 2015. In January, we also hosted a DoD cloud day open to commercial cloud service providers, media, and Federal government partners to underscore our message for DoD's new approach to cloud and promote an open dialog between the Department and industry. We are publishing our guides in collaboration with industry and producing truly interactive agility from the commercial and government sector. We have received very positive feedback from industry on this approach.

My office has issued revised guidance on the acquisition and use of commercial cloud computing services, that describes how DoD Components may acquire commercial cloud services and how they are responsible for determining what data and missions are hosted by external cloud service. We have opened the acquisition aperture and services may acquire cloud service directly, using the published guidelines.

In addition, DISA achieved initial operating capability (IOC) for its Cloud Access Point (CAP) in November 2014. The CAP provides an open and standardized means to integrate the computer network defenses between the DODIN and Cloud Service Providers (CSP) thus protecting all DoD missions from incidents that may adversely impact a CSP. DISA also achieved IOC for milCloud, the intended private cloud infrastructure for the DoD, in January 2014. The DISA MILCLOUD is much closer to commercial rates and provides additional security protection. As we continue to move forward in this area, we are improving mission effectiveness, increasing security and realizing efficiencies.

Mobility

DoD continues to evolve areas critical to mobility: the networking infrastructure, devices, and applications. The goal is to reduce the cost of accessing information while integrating a security strategy that protects the data and incorporates the most recent commercial technologies. Specific examples of DoD mobility initiatives include: an effort to simplify the ability to encrypt and authenticate email, layering multiple commercial standards permitting smart phones/devices manufactured by vendors such as BlackBerry, Samsung and Boeing, to handle secret data and the use of commercial cloud providers to globally distribute and synchronize flight information for the Air Force's Electronic Flight Bag program. We are also expanding the use of wireless capabilities.

Key partners in these efforts are DISA and the National Security Agency (NSA), who working together with industry, have developed security protection profiles for several of the major smart phone technologies. The Services are also actively involved in these efforts and are develop mobility applications for a broad range of DOD missions including recruitment, training, logistics (Inventory Management), maintenance, navigation and command and control.

IT/Cyber Workforce
DoD is implementing a comprehensive strategy to transform multiple segmented, legacy personnel management constructs into a cohesive, mission-focused DoD Cyberspace Workforce Framework (DCWF). This effort will enhance the Department's ability to recruit, train, develop, and deploy a workforce capable of interoperating across organizational structures to provide IT, cybersecurity, intelligence and operational capabilities. The DCWF will be the cornerstone of the DoD effort to standardize cyberspace workforce identification, tracking, qualification, and readiness.

To date, DoD has completed coding of over 30,000 DoD IT Management positions (OPM series 2210) with new cyberspace workforce nomenclature. This effort is in the pilot phase to align DoD personnel under the DCWF, while also meeting OPM workforce coding mandates and intent of the National Initiative for Cybersecurity Education (NICE) Workforce Framework. We are also developing new cybersecurity curriculum for the Defense Acquisition University to enhance secure acquisition of information systems and IT, and mitigate supply chain risk. Finally, we are pursuing Joint Professional Military Education accreditation for cybersecurity leadership master's degree at the National Defense University iCollege.

IT Personnel Exchanges with Industry
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. 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. ITEP 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. ITEP allows both DoD and private sector IT employees who work in the IT field (including areas such as system administration, IT project management, network services, software application, cybersecurity, enterprise architecture, internet/web services, data management and system analysis) to participate in a temporary detail to the other sector in order to gain a better understanding of each other's' technology practices and challenges. ITEP is not a 1-for-1 exchange of personnel. Instead, it is an opportunity for the exchange of knowledge, experience, and skills between the DoD and private sectors. Private sector includes nonpublic or commercial individuals and businesses, nonprofit organizations, academia, scholastic institutions, and nongovernmental organizations.

Since 2007, there have been three industry participants that have gone through the program for six – twelve month assignments. These exchanges were positive experiences and highly beneficial to all parties. A Cisco employee is currently detailed under this program to my office, and is assisting with planning, transition, and consolidation of DoD IT systems and services. My office has established relationships with industry and non-profit organizations to increase the overall utilization of this program.
We are also for the first time going to send civilian employees to industry to gain experience in technology and business practices.

Management of Defense Information Technology Systems

The Department is aware of recent Congressional actions and intentions to expand oversight and architecture requirements for DoD IT systems. However, under the recently restructured Defense Business Council, which I co-lead with the Acting DCMO, the Department is actively changing its internal processes to improve that oversight. We believe that the authority already contained within the Clinger-Cohen Act, as well as 10 U.S.C. 2222, is sufficient to allow the Department to more carefully and thoroughly oversee its IT systems and processes. The Clinger-Cohen Act gives the authority and responsibility for information technology enterprise architecture development and management to the CIO. DoD CIO manages its architectural processes using the mission area construct with active involvement of the mission area leads and Principal Staff Assistants. I would also urge the retention of the existing anti-deficiency act language in section 2222 related to obligation of funds. This language is essential for the investment review board's enforcement of the review process and associated decisions. While improving and realigning oversight of information technology systems, the Department looks forward to working closely with the Congress to ensure we are meeting Congressional intent.

Supporting Agile and Innovative IT Acquisitions

The Department's Better Buying Power (BBP) Initiative, as launched by Undersecretary Kendall, is based on the principle that continuous improvement is the best approach to improving the performance of the defense acquisition enterprise. This effort follows the evolution of the two prior BBP efforts with a shift in emphasis toward achieving dominant capabilities through innovation and technical excellence. For the DoD CIO, BBP 3.0 follows onto some things that we are already doing, such as expanding the number of enterprise buys, continuing efforts on enterprise licensing, and working to expand into enterprise hardware. We do understand that we don't drive the business IT market place, Industry does. We can if we are smarter buyers and engage better with industry to understand how the cost dynamics influence the market space and achieve improvements in effectiveness and efficiency. This new focus is important to driving cultural innovation at DoD. In simple business terms, generally buying more of a commodity will lead to a better pricing (much of business IT has been commoditized) and purchasing off an existing contract is quicker than starting a new contract.

Conclusion

In closing, at the DoD CIO we are driving cultural, business and technical improvements and innovation into DoD's IT to better support our mission and business operations. To implement the activities described above and achieve the innovations and transformations necessary in the future requires the efforts of my office, the Department's leadership, and Congress. Lt. Gen Ronnie Hawkins, the Director of DISA, is a key partner in each of these efforts. My office also enjoys a strong partnership with the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, under the strong leadership of Mr. Frank Kendall. Similarly, I have a close relation with Admiral Mike Rogers, in his capacity as both Director of NSA and Commander of U.S. Cyber Command. I continue to work closely with the recently established Principal Cyber Advisor, Mr. Eric Rosenbach.

Finally, as I mentioned above, I partner with Mr. David Tillotson, the Acting Deputy Chief Management Officer, on all DoD business management issues.

My goal is to change how we in DoD are able to use IT, enabling support to their missions in new, improved ways, whatever the mission requires, from the desk to the desert. We are working to do this more effectively and efficiently and to not ever forget that our prime business is supporting the warfighter. I want to thank you for your interest and continued support in Department's IT initiatives and look forward to your questions.