STATEMENT BY

TERRY HALVORSEN
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON
EMERGING THREATS & CAPABILITIES

ON

"Fiscal Year 2017 Information Technology and Cyber Programs: Foundations for a Secure Warfighting Network"

MARCH 22, 2016

NOT FOR PUBLICATION UNTIL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

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 Department of Defense (DoD) Chief Information Officer (CIO). I am the principal advisor to the Secretary of Defense for information management, IT, cybersecurity, communications, positioning, navigation, and timing (PNT), spectrum management, and senior leadership and nuclear command, control, and communications matters. These latter responsibilities are clearly unique to the DoD, and my imperative as the CIO in managing this broad and diverse set of functions is to ensure that the Department has the information and communications technology capabilities needed to support the broad set of Department missions. This includes supporting our deployed forces, cyber mission forces, as well as those providing mission and business support functions.

Today, I would like to provide you with a brief overview of the Department's IT and cyberspace budget, and highlight the Department's IT priorities. I will also discuss some of the ways in which my office is moving forward in today's dynamic environment, to try and take advantage of technology advances while also recognizing the potential vulnerabilities these technologies may introduce that our adversaries are eager to exploit.

DoD FY17 IT Budget Overview

IT is critical to the Department's warfighting, command, control, and communications systems, computing services, cybersecurity, intelligence and business missions. The DoD fiscal year (FY) 2017 total IT budget request is $38.2 billion, which includes $6.8 billion for the Department's cyberspace operations. The FY2017 cyberspace request represents a $900 million increase from the FY2016 enacted cyberspace budget, and represents increases for our Cyber Mission Forces and other defensive and offensive cyberspace activities. As the Secretary explained, this investment will further our network defenses, build more training ranges for our cyber warriors, and develop cyber tools and infrastructure needed to provide viable cyber options for managing conflict escalation as part of the full range of tools available to the United States.

DoD IT Priorities

The Department's IT priorities, which include modernizing DoD networks, improving information sharing with mission partners, improving DoD cybersecurity, data center consolidation and leveraging cloud technology, and empowering mobile data access, are structured to improve security, efficiency, and effectiveness for DoD IT in the future.

Modernize DoD Networks

The concept of modernizing and integrating the Department's networks and systems to help ensure efficient, effective, secure information sharing with the DoD's internal and external partners is called the Joint Information Environment (JIE). JIE is anticipated to drive a more secure, effective, and efficient IT environment. Its framework comprises a number of discrete,

but related, elements that when integrated should more securely provide the Department with IT capabilities, such as computing and information storage, transfer, and sharing. An important conceptual IT modernization effort, work toward a complete JIE end state will be ongoing.

DoD's top priority to enable the JIE is the Joint Regional Security Stacks (JRSS). Today, DoD has approximately 1,000 disparate security suites facilitated by separate, individualized, localized Service and Agency systems, with more than 5,000 firewalls. Transitioning to the regionally based, centrally managed suite of security appliances, known as JRSS, is anticipated to simplify and secure this environment and significantly reduce the Department's "attack surface" to fewer than fifty points on the network. JRSS provides the baseline for a more coherent, singular security architecture for DoD's cyber defenders. By normalizing security for data and networks across the Services, and consolidating the Department's security posture across its infrastructure, JRSS will increase visibility of the Department's networks and improve cyber situational awareness of those networks, and is essential to the overall cybersecurity of DoD networks, but it also will help DOD reduce costs, improve configuration management, and advance functionality across the network.

Information Sharing with Mission Partners

Coalition communications is an area of critical concern for the Combatant Commanders. The Department regularly works with expected – and sometimes unexpected – mission partners in a range of scenarios. DoD partnered with China and Cuba to provide disaster relief in Haiti, and works with many diverse international partners to help defeat ISIL and train partner nations. The need to securely, reliably, affordably share information with all mission partners has increased exponentially over time, and it likely will only continue on this same course.

To support this need to securely share information with mission partners, DoD is working to implement a commercially based, robust mission partner environment or capability known as the Mission Partner Environment – Information System (MPE-IS). MPE-IS is designed to provide a more cost-effective, rapidly reconfigurable and secure data protection network that enables information sharing to support operations in all environments, giving our Combatant Commanders the flexibility that they need to rapidly add and subtract mission partners as an operation requires. This capability not only allows Commanders to safely, reliably, affordably share the data needed to complete the mission, but to securely separate the information that needs to stay offline, or make it available to a separate set of partners so those partners who need data, have access to it when and where they need it.

Data Center Consolidation and Leveraging Cloud Technology

DoD continues to work to reduce the cost of its IT across the Department through data center consolidation. While I am not yet satisfied with the savings achieved or the current savings projections to-date, the DoD continues to reduce the number of physical sites and administrators needed to operate facilities to not only save money and reduce our footprint, but to also improve security. The Department's data center consolidation efforts support our cybersecurity posture by automating reporting and patch management, and placing vital system assets behind a sustainable layered defense.

While DoD has projected $1.8 billion in cumulative savings through FY2018, the Department is taking steps to aggressively drive more savings. As an example, following a review of Defense Enterprise Computing Centers (DECCs), the Defense Information Systems Agency (DISA) identified two DECCs for closure: DECC Pacific, and DECC Warner Robins. These actions will deliver near term savings without impacting operations. The DECC closures enable DoD to save the resources programmed for facility upgrades, and the migration of capabilities to other sites improves facility utilization overall.

Additionally, the near term establishment of on-premises commercial cloud hosting capabilities for high impact-levels and the increased availability of off-premises commercial cloud capabilities will provide DoD users with the most efficient compute and storage solutions available. Recently the Department established an on-premises commercial cloud capability at the Navy's Allegany Ballistics Lab, and we are engaged in the acquisition of several other on-premises commercial solutions within the Services and DISA. Our objective is to create a competitive environment to increase efficiencies and drive down costs. DoD has also established several options for off-premises cloud services for public facing systems, and we are continuing our efforts with industry to provide commercial cloud services for higher security levels. We are working closely with the Intelligence Community to develop classified cloud capabilities, with both on-premises and off-premises solutions being explored.

Installation-level consolidation of data center facilities supporting local or specialized capabilities will further reduce inventories and enhance savings. DoD is using inventory data to identify instances of multiple data centers within installation boundaries. This information will be used to directly task affected DoD Components to consolidate facilities into a single instance per installation where possible. We have tasked DoD Components to quantify rates for delivering co-location services and Infrastructure as a Service (IaaS) using a common costing tool. The objective is to drive workload to the most efficient providers of these baseline services. Further, using a consistent method to establish these rates enables more direct comparisons to industry providers of like services, thereby enabling the Department to make sound business decisions.

To ensure DoD Components move aggressively, we are taking steps to leverage the authorities provide by the FY2012 National Defense Authorization Act regarding the approval of data center related obligations to drive the Department toward more efficient data center solutions. We are linking the approval of data center obligations to achievement of the requesting Component's Data Center Consolidation and efficiency objectives as documented in their Data Center Consolidation Implementation Plan. DoD Components failing to realize objectives will be denied the ability to obligate funds until corrective actions are taken.

Reducing the data center workload through application rationalization over time (principally within the Business Mission Area (BMA)) will result in additional savings. My office is working with the office of the Deputy Chief Management Officer to review the Department's BMA portfolio beginning with the OSD Components. This review involves a functional review of the systems coupled with total ownership cost estimates to assist in identifying which systems should be retained, re-engineered, or retired. While some application rationalization actions may

be realized in the near term, it is important to realize these efforts are often longer term due to the impact on business processes, data stores, and the need to maintain operations. DoD is committed to making this an ongoing process to ensure DoD drives to and maintains an optimized BMA systems portfolio. Lessons learned from application rationalization within the BMA will be extended to the other defense mission areas as appropriate.

Improving DoD Cybersecurity

Cyber intrusions and attacks by both state and non-state actors have increased dramatically in recent years, putting DoD missions and information at risk. Adversaries continually adapt and evolve in response to cyber countermeasures, threatening DoD networks and systems. DoD is attacked every day in cyberspace, and technology itself allows our adversaries to adapt faster than in any other area of warfare.

Nearly every one of the successful network exploitations that DoD has experienced can be traced to one or more human errors on the network, which makes raising the level of individual awareness and performance in cybersecurity absolutely paramount. DoD is working to transform its cybersecurity culture by improving human performance and accountability through a prioritized a list of key cyber efforts known as the Cybersecurity Discipline Implementation Plan. The plan, which aligns to the Secretary's Cyber Strategy, provides a roadmap to aggressively eliminate preventable cyber vulnerabilities that can put DoD missions at risks. My office tracks overall progress toward the plan through the "DoD Cybersecurity Scorecard," which focuses on four key lines of effort:

1. **Strong Authentication** – to degrade adversaries' ability to maneuver on DoD networks. The Department is mandating the use of approved, more secure two-factor authentication, utilizing DoD Public Key Infrastructure to reduce the ability of adversaries to use stolen credentials to obtain access to DoD networks and systems and degrade adversaries' ability to maneuver in DoD networks. This effort will eliminate the use of weak authentication for users logging-on to DoD networks. Many users still access DoD networks and systems with insecure methods such as usernames and passwords. These methods are very prone to theft from even unsophisticated adversaries.

2. **Device Hardening** – to reduce internal and external attack vectors into DOD information networks. DoD is requiring that all DoD computers be configured to the Department's security standards and that those configurations are kept up to date by patching aggressively. Establish protections such as the inability to click on hyperlinks to reduce spear phishing, which eliminates a significant method that adversaries utilize to successfully attack DoD networks by diminishing use of e-mail as a conduit for access DoD networks.

3. **Reduce the Attack Surface** – to reduce external attack vectors into DOD information networks. The Department is requiring that every Internet-accessible DoD website be protected by DoD Enterprise Security, in a demilitarized zone (DMZ).

4. **Alignment to cybersecurity/computer network defense service providers (CNDSP)** – to improve detection of and response to adversary activity. The Department is requiring that

every DoD mission, computer and network device be properly defended by ensuring that it is monitored by a CNDSP. This ensures that every computer is being tracked for adversary behavior.

Finally, key to the Department's cybersecurity and overall cyberspace operations is our personnel. To address the Department's increased need for skilled cyber personnel as well as the need to increase the cybersecurity skills of IT personnel (e.g., systems administrators) my office is developing a comprehensive strategy to transform multiple segmented, legacy personnel management constructs into a cohesive, mission-focused DoD Cyberspace Workforce Framework. This effort will enhance the Department's ability to recruit, train, develop, and deploy an IT and cyberspace workforce capable of interoperating across organizational structures. To that end, the Department appreciates the authority granted by Congress last year that provides DoD enhanced hiring authority in Cyber and we will continue to work with Congress to identify other authorities that can help DOD recruit and retain personnel in this critical domain.

Empower Mobile Data Access

The Department continues to expand the number of commercial mobile devices that can be used by DoD users. The Department's mobile portfolio includes unclassified and classified mobile capabilities. The basic foundational infrastructure is in place to support the DoD Mobile Unclassified Capability (DMUC), and includes a mobile device manager and a mobile application store and Gateway for unclassified mobility that will leverage commercial carrier infrastructure and provide entry points for classified services. The Department has adopted a multivendor approach, allowing the DoD Components to use the latest commercial devices that offer more capabilities – like mobile apps and GPS – to meet mission needs. These devices, and their applications, are appropriately managed to meet DoD security requirements, but allow the user to have both a personal and work identity that provides flexibility for personal use capabilities, such as personal email or mobile apps for banking, news, and travel information. Moving forward, DoD will evaluate new mobile devices for approval, ensure the mobile infrastructure complies with DoD security policy, and adopt mobility focused business processes to enhance mission effectiveness, promote ubiquitous data access, improve user experience and reduce cost.

A significant challenge in mobility is securing mobile devices, while keeping up with the rapidly changing pace of mobile technologies. As a result, modernizing the DoD security approval process for mobile is one way in which DoD is empowering mobile data access for its users.

Mobile progress on the tactical edge illuminates the untapped potential of mobile capabilities. Tailored applications demonstrate the advantage of adapting mobility to military needs. For example, Air Force flight crews have replaced their heavy paper-based navigational charts and flight manuals with an Electronic Flight Bag (a tablet), which more easily and efficiently allows them to conduct their flight-management tasks. Tactical users have been provided the Android Tactical Assault Kit, a mobile device connected to a tactical network/radio, providing users with up-to-the-second information about the surrounding environment and capabilities such as voice, text chat, video, images, and an interactive, shared, moving map.

New Initiatives

In addition to the above IT priorities, there are several other recently announced initiatives that my office is leading for the Department.

The Deputy Secretary of Defense recently signed a memo directing the Department to complete a rapid deployment and transition to Microsoft Windows 10 Secure Host Baseline. U.S. Cyber Command is the lead for this effort, in consultation with the Chairman of the Joint Chiefs and my office. This mandate – a first in the history of the Department's IT – was based on the need to strengthen our cyber security posture while concurrently streamlining the IT operating environment. DoD desktops, laptops, and tablets using Microsoft Windows will be migrated to a single version of the operating system, improving the Department's cyber posture by establishing a common baseline for our cyber defenders. This migration, which is not without challenges, to a single operating system should also improve the effectiveness and efficiency of how information is shared, while posturing the Department to take full advantage of other technologies and practices that could potentially have a tremendous impact on DoD far beyond the IT/cyberspace environment.

My office is also overseeing the design and implementation of IT to support the recently established National Background Investigations Bureau (NBIB). DISA is responsible for the design and development effort, and $95 million is included in DISA's FY2017 budget request to initiate this effort. The objective is to replace the current background investigations information systems with a new and more reliable, flexible, and secure system in support of the NBIB. DoD will support OPM as they continue to operate the current system. The Department is also conducting a full cybersecurity assessment of the current OPM background investigation infrastructure that will be used to determine the near-term steps that the Department can take to assist OPM with the operation of the current system, as well as near-term steps that OPM itself can take to enhance the security of the current system. It will also inform DoD's design and instantiation of the new investigation system IT infrastructure.

As noted in my introduction, as DoD CIO I am also responsible for PNT, frequency spectrum matters, nuclear command, control and communications, senior leader communications and satellite communications. We are making important progress to enhance DoD's existing positioning, navigation, and timing technologies, including the nationally critical Global Positioning System (GPS). My office is also responsible for overseeing the modernization of the DoD's nuclear command, control and communications capabilities, as well as senior leader communications. DoD, with many Government and industry partners, just completed the most successful spectrum auction ever conducted, raising $43 billion for the U.S. Government, and providing commercial industry access to critical spectrum. My office continues to lead efforts to maximize spectrum access for Government and industry, engaging with industry and partners to develop and exploit technologies that support spectrum sharing and ensure a win-win. In the area of satellite communications (SATCOM), we are driving down costs by better managing requirements at the enterprise level, and by consolidating leases at DISA. Collaboration with the commercial SATCOM industry offer opportunities to identify new business models that will help us further drive down costs, and to take advantage of emerging technologies that will increase capabilities for the Warfighter and for our senior leadership.

In addition, I continue to partner with the Deputy Chief Management Officer to review the DoD's business processes and the supporting IT systems. Our common 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.

Conclusion

I want to emphasize the importance of our partnerships with Congress, the Federal CIO and Industry. As the importance of cyber and information technology more generally continues to increase these partnerships are essential for our continued success and improvement. The mission and operational impact of our portfolio issues like information sharing, cybersecurity, spectrum management, positioning, navigation, and timing, nuclear command and control and mobility cannot be overstated in today's strategic environment. The role of the CIO in government and industry will continue to evolve and I believe that role will become even more critical as Cyber/IT continues to play an increasingly important role in almost every aspect of our lives.

Thank you for your time and for your continued support of this increasingly critical component of the DoD budget, and I look forward to your questions.