STATEMENT BY

DAVID DEVRIES
PRINCIPAL DEPUTY
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE OVERSIGHT AND GOVERNMENT REFORM COMMITTEE'S INFORMATION TECHNOLOGY SUBCOMMITTEE AND THE VETERANS' AFFAIRS COMMITTEE'S OVERSIGHT AND INVESTIGATIONS SUBCOMMITTEE

ON

"VA and DoD IT: Electronic Health Records Interoperability"

OCTOBER 27, 2015

NOT FOR PUBLICATION UNTIL RELEASED BY HOUSE OVERSIGHT AND GOVERNMENT REFORM COMMITTEE'S INFORMATION TECHNOLOGY SUBCOMMITTEE AND THE VETERANS' AFFAIRS COMMITTEE'S OVERSIGHT AND INVESTIGATIONS SUBCOMMITTEE

Introduction

Good afternoon Chairmen, Ranking Members, and distinguished Members of both Subcommittees. Thank you for the opportunity to testify today on the Department's cybersecurity posture and information technology (IT) policies. I am David DeVries, the Department of Defense Principal Deputy Chief Information Officer (DoD CIO). I serve as the deputy 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, guidance and oversight of the Department's information technology and cybersecurity efforts. As the Principal Deputy DoD CIO, I have one imperative – to ensure 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

Today I would like to provide you with an overview of the Department's efforts to secure our information and networks, and to ensure DoD can execute its missions in the face of increasing cyber threats. My office is working closely with partners across the U.S. government, industry, and international partners to accomplish our cybersecurity mission, and we are improving our ability to share with industry and the public. DoD has astoundingly complex challenges. The Department has over 1.4 million active-duty men and women, 718,000 civilians, and 1.1 million National Guard and Reserve members. More than 450,000 of our employees are overseas. We have several hundred thousand buildings, and structures located in more than 5,000 different locations or sites, and on 30 million acres of land. We have four million computers on our unclassified networks alone. We are enormous on the enterprise network scale. By our numbers, we have the world's biggest enterprise network. Our IT/Cyber budget was nearly $40 billion in fiscal year 2014, with nearly $5 billion invested in cybersecurity. If we were included in the Fortune 500, the Defense Department would be at the top of the list.

The Department's IT is complicated. We are in the business of defense, but that requires us to be integrated in almost every discipline you can think of: acquisitions, health, logistics, real estate, food distribution, industrial control systems, and more. The DoD CIO's office is striving to

improve information sharing and justified access as well as data strategies and storage across all of these diverse communities of interest, including across the Services, Defense Agencies, Combatant Commands, and our international partners; all while trying to do this in a more secure manner. While our top goal is to deliver capabilities more effectively and efficiently, we also need to maximize security in a budget constrained environment worldwide. Our cyber adversaries are agile, diverse and sophisticated and we must be able to maneuver in the cyber world at unprecedented speeds to protect our nation's assets. Adapting the ability to innovate rapidly and soundly presents a challenge to our process oriented Department of Defense. However, we are driving our leaders to evolve.

IT/Cyber Budget

The Department's Fiscal Year (FY) 16 IT budget request is $36.9 billion. As the DoD CIO testified before the House Armed Services Committee Emerging Threats and Capabilities Subcommittee last February, 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, as well as 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 while reducing the costs of these efforts and accomplishments. These cyber efforts continue to receive the highest-level attention and support of the Department.

Last year Congress passed the Federal IT Acquisition Reform Act (FITARA) as part of the FY15 National Defense Authorization Act. DoD applauds the intent of FITARA to increase the stature of agency CIOs in the decision-making processes of their respective agencies, and improve the overall management of IT investments government-wide. For those agencies that lack the long-standing requirements, acquisition and budgeting processes the DoD has, FITARA provides a structure that can help improve how government buys, implements and manages IT products,

systems and services. The Department recently completed its implementation plan which describes how DoD will use its existing processes and procedures to satisfy those portions of FITARA that apply to the Department and the Office of Management and Budget (OMB)'s "Management and Oversight of Federal Information Technology," guidance. FITARA re-enforces current DoD CIO authorities and responsibilities for DoD's IT investments.

Department's Cybersecurity Strategy – Cybersecurity Discipline Implementation Plan

As you know, adversaries are becoming increasingly aggressive in their cyber-attacks on the Department's and Federal computer systems. These attacks put all of us and our missions and information at risk. The Office of Personnel Management breach and Joint Staff unclassified network attacks are recent examples that underscore the importance of cybersecurity. To address the Secretary's top priority - cybersecurity, I am working very closely with the Under Secretary of Defense for Acquisition, Technology and Logistics (USD (AT&L)), Commander of U.S. Cyber Command (USCYBERCOM) and Under Secretary of Defense for Policy, as well as the Combatant Commands, Services and Agencies on an aggressive, multifaceted DoD Cybersecurity Campaign. This Cybersecurity Campaign is in direct alignment with the Department's Cybersecurity Strategy and is being executed as we speak via two synchronized efforts: 1) The DoD Cybersecurity Discipline Implementation Plan and 2) the DoD Cybersecurity Scorecard. Nearly every single one of the successful network exploitations that DoD has had to deal with can be traced to one or more human errors that allowed entry into the network. So raising the level of individual cybersecurity awareness in performance is absolutely paramount. Accordingly, we're working to transform our cybersecurity culture by improving human performance and accountability. Both are critical to achieving the strategic goal of defending information networks, security data, and mitigating risks to missions established in the Cyber Strategy. We are working with support of the highest levels of the Department to create a cyber culture and advance cyber discipline through leadership, accountability, and transparency.

The DoD Cybersecurity Campaign, Cybersecurity Discipline Implementation Plan, and Cybersecurity Scorecard are critical to achieving the strategic goal of defending DoD information networks, securing DoD data, and mitigating risks to DoD missions as set forth in the 2015 DoD Cyber Strategy. As part of the DoD Cybersecurity Campaign, I have asked my staff to clarify where the Department must have "zero tolerance" for failure to implement these

basic disciplines, and to prioritize our efforts so we collectively focus on doing the most important things first. The Cybersecurity Discipline Implementation Plan lists the four identified "most exploited" basic disciplines, establishes the priorities for correcting these deficiencies, and directs compliance reporting to responsible commanders as well as the Secretary of Defense and Deputy Secretary on a monthly basis. This includes things like configuring all computers to the DoD security standard; ensuring that every computer is defended by an operational organization and that nothing in our enormous, global infrastructure has fallen through the operational cracks; and eliminating the use of passwords by all systems administrators, and replacing these passwords with the cryptographic identity credentials issued by the DoD Public Key Infrastructure. This list became the Cybersecurity Discipline Implementation Plan.

An important measurement of maintaining the Department's cyber defenses is the annual FISMA report. DoD's FY14 Report, which was submitted last March, reflected the Department's commitment to continuously improving information security and privacy management. Our assessments, along with those of the DoD Senior Official for Privacy, reflect areas in which the Department has shown improvements when measured by the OMB metrics.

Joint Regional Security Stacks (JRSS)

Our top priority at DoD CIO is implementing the Joint Regional Security Stacks, which is the first or foundational phase of the Department's Joint Information Environment (JIE). Today, the Department has numerous disparate security suites facilitated by separate, individualized, localized Service and Agency systems, and thousands of firewalls that must be configured the same way. This is expensive and difficult to secure. Weak configuration management can cause Denials of Service to ourselves when fielding new capabilities or making major changes to the network. The pace of the ever-changing threat will drive JRSS to remain fluid as technology and the adversary mature. Transitioning to the regionally based, centrally managed suite of security appliances known as JRSS will simplify and secure this environment while simultaneously reducing the number of internal and mission owner access points. JRSS goals are to reduce costs, improve configuration management, increase our cyber situational awareness, and enhance functionality across our networks. In particular, JRSS will be the baseline for a more coherent, singular security architecture for our cyber defenders. It will normalize security for data and networks across the Services, and consolidate the Department's security posture across its

infrastructure. Critically, it will also improve overall cyber situational awareness by enabling better data integrity and creating a common operating picture of the cyber environment, as well as improving the capacity for immediate action and predictive planning. The Deputy Director of CYBERCOM, Lt. Gen. James McLaughlin, has said that achieving cybersecurity will require visibility across all of our networks, and JRSS is critical to accomplishing this visibility.

As JRSS is our top priority at the DoD CIO, we are making progress on its implementation. Despite each Service being at a different stage of technology (driven by unique mission requirements), our plan is to have the security stacks fully operational by the end of FY17. In addition, we are focused on how we securely, reliably, and affordably share information with external partners. Our second priority is focused on appropriately facilitating safe information sharing with our mission partners.

IT Acquisition and Government/Industry Partnerships

As I mentioned earlier, we are working with industry and international partners on our cyber guidelines and improving our cyber alignment with industry. Well beyond cloud security, the Internet of Things presents new dimensions for our cyber threat environment, and USD(AT&L) Frank Kendall is also updating the Department's acquisition guidelines to accommodate the cyber threat to our weapons systems. This threat of cyberattack to our weapons systems is incredibly serious, and we are taking very aggressive action to counter those threats. Aligning to industry environment, when appropriate, will decrease costs, increase the speed to deployment, and offer potentially insightful and tested solutions. In this business process research, we are also evaluating the values of public/private networks; commercial networks garner the benefits of physical security within DoD facilities. We are producing a guidebook to help program managers balance the costs and risks with new weapons programs, and help make them more secure, and we are also issuing new acquisitions rules. Our goal is to have a completely unclassified acquisition guidebook and acquisition rules released later this year. I'm confident these guidebook and rules will help industry help us secure our weapons systems from cyberattack. This too will help raise the defensive basics of cybersecurity and the broader understanding of the threat environment. In addition, USD(AT&L)'s recent release of Better Buying Power 3.0 (BBP 3.0) supports the Department's commitment to continuous

improvements in the defense acquisition system, focusing attention on the overriding concern that our nation's technological superiority is at risk.

Beyond sharing with industry, we collaborate broadly with specific industry sectors to raise the national level of cybersecurity, as applicable to the Department's specific areas of focus. I'd like to mention specifically our Defense Industrial Base Cybersecurity / Information Assurance program as well as our Supply Chain Risk Management efforts. Initiated in 2007 and established as a permanent DoD program in 2013, the DIB CS/IA program improves the capabilities of the more than 100 participating cleared defense contractors to safeguard DoD information that resides on, or transits, Defense Industrial Base information systems. These participating member companies include groups from industries like aerospace, cybersecurity and IT solutions, geospatial, engineering, and transportation. This voluntary public-private partnership enables the Department and these participating companies to share unclassified and classified cyber threat information with each other. This allows them to identify and respond to adversary activity through the program's operational focal point, the DoD Cyber Crime Center.

In addition to closely sharing cybersecurity information with other defense contractors, we consider our Supply Chain Risk Management (SCRM) efforts to be a model for partnerships across government and industry. Our SCRM efforts truly are a best practice example of intergovernmental collaboration. SCRM is a multi-disciplinary challenge that requires contributions and collaborations among many disciplines, including systems engineering, system security engineering, information security, software development, and others. DoD has been working closely with the intergovernmental partners for years to improve U.S. Government SCRM capabilities for trusted systems and National Security Systems. This important work continues today with these partners and others, like the White House Office of Science and Technology Policy and the National Science Foundation. Through reaching out to industry and constantly seeking new ways to capitalize on the joint intellectual capital such as employee exchange programs, we are working to raise the national level of cybersecurity across DoD, our industrial partners and the nation. The cyber threat has no geographic boundaries and is rapidly evolving to affect every aspect of our business. Being able to take advantage of state of the art innovation across government and industry is critical to our ability to address this threat. As well as pushing forward hard on our new efforts to raise the defensive basics of cybersecurity, we

need to take every opportunity to partner with industry as we tackle this daunting challenge together.

Conclusion

Thank you for the opportunity to testify before you today. I look forward to your questions.

David DeVries

Principal Deputy Chief Information Officer

David DeVries became the Department of Defense Principal Deputy Chief Information Officer on March 22, 2015 after serving as the Acting Department of Defense Principal Deputy Chief Information Officer since May 2014.

As the Principal Deputy, Mr. DeVries assists the DoD CIO as the principal advisor to the Secretary of Defense for Information Management / Information Technology and Information Assurance, as well as non-intelligence space systems; critical satellite communications, navigation, and timing programs; spectrum; and telecommunications.

Mr. DeVries joined the DoD CIO in May 2009 as the Deputy CIO for Information Enterprise, where he was responsible for integrating DoD policies and guidance to create information advantages for department personnel and organizations, and DoD mission partners. Since August 2010, Mr. DeVries has been deeply

involved in several efforts including moving the department towards adopting a Joint Information Enterprise (JIE) based on a single, secure, reliable DoD-wide IT architecture; realizing Secretary of Defense IT efficiencies; creating the way ahead for improved DoD - Veterans Affairs electronic health record exchange capability; expanding cloud adoption and mobile communications capabilities; and establishing key enabling capabilities to achieve the DoD Information Enterprise.

Mr. DeVries holds a Bachelor of Science from the United States Military Academy, and a Master of Science in Electrical Engineering from the University of Washington in Seattle, Washington. He is also a graduate of the Army Senior Service College and served as a Corporate Fellow with IBM Business Consulting Services while participating in the Secretary of Defense Corporate Fellowship Program.