STATEMENT BY

TERRY HALVORSEN
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE OVERSIGHT AND GOVERNMENT REFORM COMMITTEE

ON

FEDERAL AGENCIES' RELIANCE ON OUTDATED AND UNSUPPORTED INFORMATION TECHNOLOGY: A TICKING TIME BOMB

May 25, 2016

**NOT FOR PUBLICATION UNTIL
RELEASED BY THE HOUSE
OVERSIGHT AND GOVERNMENT
REFORM COMMITTEE**

Introduction

Good morning Mr. Chairman, Ranking Member, and distinguished Members of the Committee. Thank you for this opportunity to testify before the Committee today on the Department's legacy information technology (IT) spending, plans for modernization, and implications for IT acquisition reform and security. I am Terry Halvorsen, the Department of Defense (DoD) Chief Information Officer (CIO). As the senior civilian advisor to the Secretary of Defense for IT, I am responsible for all matters relating to the DoD information enterprise, including cybersecurity and IT modernization for the Department.

DoD has a long history of leaning forward on using and in some cases developing emerging and new technologies. We are one of the largest procurers of technology in the world. Our IT portfolio today has a mixture of inhouse-development, recently deployed, and older systems, and systems that are a mixture of all three.

GAO's report places great emphasis on Development, Modernization, and Enhancement, or DME, a construct used in budgetary and management reporting to categorize IT resources according to the life-cycle activities taking place in an IT investment. It is a longstanding and useful categorization, similar to how funds are categorized in the DoD budget. DME is one indicator of how well the Department is injecting new technology and systems into its inventory. DME is an indicator, not a goal. There are limitations to how well this and other budgetary constructs can be used to assess the technological currency of systems and portfolios.

Aging systems have risk. So does DME. The Department's approach is to balance our capacity to plan, architect, manage, coordinate, contract, build, document, test, train, and transition new systems into the portfolio with the need to manage, operate, and protect our installed base. In the last several years, DoD has modernized, replaced, updated, upgraded, enhanced, technologically "refreshed," consolidated, and retired hundreds of systems, whether coded as DME or as more routine technology replacements under "Operations and Maintenance."

In the past few years, DoD's focus has been on foundational changes that position the Department to move forward in a more enterprise, coordinated, secure and cost effective environment. These changes include consolidating data centers; making platform, backbone, and communications improvements; implementing common security constructs under the Joint Regional Security Stacks; moving to a standard operating systems and a common platform; rationalizing applications; and continuing the move to cloud environments.

This will improve the Department's IT infrastructure and processes for broad impact, and position even more systems to come into an enterprise or shared environment, in a more secure, mission effective and cost efficient way. Optimizing the DoD IT infrastructure in this way will help us meet the diverse missions of today, and support the strategic requirements of tomorrow. Supported by JRSS and leveraging the flexibility and interoperability of cloud computing, the future DoD IT environment will empower the Department to operate in a modern security environment that is highly connected and driven by data. We are working closely with our mission partners to make smart choices in how IT enables execution of the mission in the face of a persistent cyber threat.

DoD is striving to facilitate system improvements while lowering operating risks by increasing use of enterprise solutions, transforming the DoD IT to a more agile, innovative, and mobile thin client, cloud-based environment at less cost to the taxpayers. DoD's move to the enterprise and shared services model will reduce duplication, close performance gaps, and promote better security among government, industry, and mission partners. Enterprise solutions also provide current technologies to implement standardization, common design principles, responsive scalability, and repeatable architectures to foster more agile and useful planning, decision-making, and IT management.

The Department has some old systems and some cases of obsolete technology. We are making progress reducing obsolescence. Highlighting the oldest systems in our inventory does not represent the DoD technology portfolio as a whole. Some systems with older languages and older technologies exist like those that still use COBOL – the programming language DoD helped pioneer decades ago. Where it makes sense to re-code or upgrade those systems, we need to do that — with a priority on those systems with the greatest potential for cybersecurity vulnerabilities. It is critical that we focus on investing in system replacements, modernization, or upgrades when there is a clear and compelling operational need or business case to do so. Not everything old needs to be replaced.

Moving forward, the Department's IT strategies and policies will continue to evolve, including those related to the quality and quantity of evaluations to measure the ongoing effectiveness and technological profiles of the installed baseline of IT systems. As the DoD CIO, my goal is to ensure these strategies and policies are implemented by the DoD Components, who are ultimately responsible for funding, implementing, operating and modernizing the Department's IT systems, and to ensure that DoD IT investments continue to support mission critical and mission support operations of the Department.

To address obsolete IT investments in need of modernization or replacement, the GAO recommends that the Department identify and plan to modernize or replace legacy systems as needed and consistent with OMB's draft guidance, including timeframes, activities to be performed, and functions to be replaced or enhanced. The Department is already doing this using the principles described above, which leverage existing DoD policies and processes,

Conclusion

DoD recognizes the importance of modernization and the security implications that come with operating legacy systems. We have more work to do and are not where we want to be today. We are, however, making the right investments in our legacy systems and balancing modernization against the sustainment and improvement of systems that are critical to warfare mission and business mission success. The Department is actively pursuing modernization while operating within the confines of a constrained budget environment. We look forward to receiving final guidance from the Office of Management and Budget, as well as working with Congress on these matters. Thank you for the opportunity to testify today and I look forward to your questions.

Mr. Terry Halvorsen
Department of Defense Chief Information Officer

Terry Halvorsen assumed the duties as the Department of Defense Chief Information Officer effective March 8, 2015. He previously served as the Acting Department of Defense Chief Information Officer. Prior to that, he was the Department of the Navy Chief Information Officer.

As DoD CIO, Mr. Halvorsen is 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. He 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.

Before serving as the Department of the Navy CIO, Mr. Halvorsen was the deputy commander, Navy Cyber Forces. He began serving in that position in January 2010 as part of the Navy Cyber reorganization. Previous to that, Mr. Halvorsen served as the Deputy Commander, Naval Network Warfare Command. He was responsible for providing leadership for over 16,000 military and civilian personnel and supporting over 300 ships and approximately 800,000 globally dispersed computer network users. In this position he was responsible for the business performance of Navy network operations, space operations, information operations and knowledge management.

Mr. Halvorsen served as an Army intelligence officer in a variety of assignments, including Operations Just Cause and Desert Storm. He holds a bachelor's degree in history from Widener University, and a master's degree in educational technology from the University of West Florida. He is a Rotary International Paul Harris Fellow and an Excellence in Government Leadership Fellow.