

STATEMENT BY
TERRY HALVORSEN
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE
HOUSE OVERSIGHT AND GOVERNMENT REFORM COMMITTEE

ON
SECURITY CLEARANCE REFORM: THE PERFORMANCE
ACCOUNTABILITY COUNCIL'S PATH FORWARD

FEBRUARY 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NOT FOR PUBLICATION UNTIL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 Information Technology and Cybersecurity support to the National Background Investigation Bureau. 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 for the Department. In this capacity, I look forward to expanding this role with this opportunity to oversee IT systems for the National Background Investigations Bureau (NBIB). This is an opportunity for the Federal Government to truly capitalize on established DoD technology and expertise to improve the security of the IT infrastructure for the vital federal background investigation systems process. DoD has substantial experience in the development of systems with strong cybersecurity, and has worked to integrate commercial and government developed cyber defense and detection tools into the DoD networks, which gives the Department unique cyber defense capabilities.

The DoD CIO is driving cultural, business, and technical innovation in the DoD by better integrating our IT infrastructure, streamlining business processes, and supporting agile and innovative IT acquisition. The Department's cybersecurity workforce is well trained to protect against and respond to cyber intrusions. DoD cybersecurity operations and procedures are mature and reinforced by policy and regulations across the entire Department. DoD's IT development process requires the inclusion of cybersecurity in every step of the development lifecycle of all systems, even after the system is fielded. The Department's processes, systems, and security architecture are well-integrated and continuously improving to ensure that future attacks are deterred or detected quickly and effectively. DoD will use these same processes to build IT support for the NBIB.

As the lead for building the new background investigation IT system, I will bring together the Department's full range of resources and expertise. LTG Alan Lynn, Director of the Defense Information Systems Agency (DISA), will oversee his organization's efforts to provide the majority of IT services and security to the NBIB, under DoD CIO oversight. The Department's 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. Ensuring continuous operations for the vital background investigations system, even as we build and transition to the new IT infrastructure, is paramount.

DoD has been working closely with OPM since the incident was discovered. Recent collaboration has focused on getting the Department's team prepared to begin the process of designing, building, operating, securing, and defending these IT systems. DoD will support OPM as they continue to operate the current system. DoD will cooperatively conduct a full cybersecurity assessment of the current background investigation

infrastructure. This joint assessment will 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 better defend the current system. It will also inform DoD's design and instantiation of the new investigation system IT infrastructure. DISA will lead this assessment, with support from the NSA and the Deputy CIO for Cybersecurity. Planning for this assessment is ongoing, with on-site work at OPM expected to begin within the next 60 days.

In mid-December, DoD CIO formed a multi-organizational IT Task Force with members from OPM, DISA, NSA, USD(I), and DMDC to build the foundation for future program office and acquisition activities. This IT Task Force has six work streams to articulate the detailed requirements and design of the new information system and the supporting operations. The work streams are: Data Strategy; Application Migration / Business Process Reengineering; Architecture; Governance; Operations; and Resource Management/Program Management. The IT Task Force will analyze the current OPM system and all of its dependencies in detail, scope the new system architecture requirements, and draft implementation and operations plans with metrics for the new system.

As the organization responsible for providing the majority of the IT support directly to the NBIB, DISA will lead development and deployment of the new information system. DISA also will operate and defend the system, under the operational control of USCYBERCOM. The full scope of DoD cyber tools, including those that integrate government and commercial technology, such as the Joint Regional Security Stacks, will protect the systems as they are developed and fielded within the DoD network. DISA cyber operations personnel will conduct monitoring, incident detection, diagnostics, and adversary containment. Then, DISA – supplemented as necessary by USCYBERCOM Cyber Protection Teams – will handle incident response and remediation. The alignment of NBIB systems under the DoD will assure that we leverage all of this national security systems expertise and capability to protect the background investigation data.

Conclusion

In closing, the Department is excited about this opportunity to design, develop, secure, and operate, and defend the new background investigation IT systems for the NBIB. This is an important opportunity for the Federal Government to truly capitalize on established DoD technology, expertise, and information technology systems to improve the security of the IT infrastructure for the vital federal background investigations process. I want to thank you for your interest in our plans to support NBIB, 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.