TESTIMONY OF

Luke McCormack

Chief Information Officer

U.S. Department of Homeland Security

Before the

Senate Committee on Appropriations

Subcommittee on

Homeland Security

April 15, 2015

INTRODUCTION

Chairman Hoeven, Ranking Member Shaheen, and Members of the Subcommittee: Thank you for this opportunity to speak to you about cybersecurity at the Department of Homeland Security. As you are aware, it is vital for our Department and the Federal Government to defend our systems against cyber-attacks. The Office of the Chief Information Officer (CIO), in close coordination with the National Protection and Programs Directorate (NPPD) ensures that our Nation is secure and able to stay ahead of cyber threats.

In the following remarks, I will focus on the roles and responsibilities of the Office of the Chief Information Officer to ensure the Department's information is safe from cyber-attacks, and how the nation's cybersecurity is strengthened through ongoing collaboration with our components, with NPPD, and across-government. I will also highlight some of the Department's ongoing and future cybersecurity initiatives.

THE ROLE OF CIO AT DHS

As the DHS Chief Information Officer, my role is to implement information security programs at the Department level. My office's mission is to develop and maintain a single, Department-wide information technology (IT) infrastructure that is reliable, scalable, flexible, maintainable, accessible, and secure. I provide oversight to over 90 major IT programs across the Department's seven operational components and Headquarters offices. Because of our size and mission diversity, we have some unique challenges and opportunities for success.

DHS OCIO AND COMPONENTS

The Department's leadership recognizes the importance of strengthening a collaborative environment and culture within DHS, especially across programming, budgeting, and acquisition oversight processes. On April 22, 2014, the Secretary signed a memo entitled *Strengthening Departmental Unity of Effort*. Through this Unity of Effort initiative, we are:

- Actively supporting the Joint Requirements Council (JRC) – a body that develops recommendations for investment, as well as changes to training, organization, legislation, and operational processes and procedures;
- Enhance the Department's programming and budgeting process; and
- Actively collaborating with our component counterparts to drive efficiencies and improve effectiveness.

Using Unity of Effort as our foundation, the Councils of the CFO and CIO – bodies comprised of the chief financial and chief information officers from across DHS –worked collaboratively to clearly define budgetary needs for cybersecurity efforts in 2016 and into the near future. It is because of these efforts that the President's budget includes $31.7 million for essential cybersecurity remediation initiatives in Fiscal Year 2016.

The Unity of Effort also resulted in updating the DHS IT Strategic Plan. It is a focused, mission-driven, achievable plan that positions our technology environment to address the critical areas of people and culture, innovative technologies, cybersecurity, and governance and accountability.

As part of that IT Strategic Plan, the CIO Council developed a specific cybersecurity goal: to "*Empower DHS and its partners to operate secure IT systems and networks, keeping ahead of evolving cyber threats*." Additionally the CIO Council is supported on all matters of cybersecurity by another cross-Department council comprised of the Chief Information Security Officers from Headquarters and our components.

PARTNERING WITH NPPD

NPPD's role is to enhance the security, resilience, and reliability of the nation's cyber and communications infrastructure. NPPD coordinates the federal response to cyber incidents, and leads efforts to protect the federal ".gov" domain, and collaborates with the ".com" domain to increase the security of critical networks. Due to our partnership with NPPD we are able to internally implement and collaborate on many federal cybersecurity programs, sometimes while they are still in development. By taking on the role of an early adopting agency, we provide valuable feedback to NPPD on products and programs before they are more widely implemented across government. For example, we are currently working with NPPD to test the Continuous Diagnostics and Mitigation (CDM) dashboard. Through collaboration of this nature, DHS strengthens its cybersecurity posture across government to serves as an initiator and leader in federal cybersecurity efforts.

CROSS-GOVERNMENT EXPERTISE AND COLLABORATION

In addition, my office contributes cybersecurity expertise to the federal IT community. Two of the areas where we are working with colleagues across government are to enhance security of mobile applications and standardizing the approach for assessing and monitoring the security of cloud products and services.

Secure Mobility

Directly related to the Presidential memorandum issued on May 23, 2012, entitled, Building a 21st Century Digital Government, the Federal CIO Council has been charged with identifying solutions to challenges that prevent progress in IT delivery. One such challenge is ensuring the rapid adoption of mobile technologies while maintaining a security posture appropriate to the agency's mission. To address this, the Federal CIO Council established a Mobile Technology Tiger Team. DHS co-chairs the tiger team, which recently unveiled a set of criteria to be used in validating security for mobile applications. This effort provides consistency across the Federal Government and allows industry to better meet the needs of federal customers. As additional federal agencies adopt the criteria, mobile application development will be more secure and predictable.

The Federal Risk and Authorization Management Program (FedRAMP)

DHS is a major partner in the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP provides a standardized approach for assessing and monitoring the security of cloud products and services and will significantly reduce the time-to-market for Departments and Agencies as they implement cloud computing. Testing and authorizing a cloud provider is performed once and is shared multiple times across the government. This reduces

both time and cost by reusing the authorization of a cloud provider, and introduces competition in the cloud market.

DHS was engaged in FedRAMP from its inception, contributing to the development of its security standards. Along with the Department of Defense and the General Services Administration, DHS serves as one of the tri-chairs of the FedRAMP Joint Authorization Board, the primary governance and decision-making body for the program. DHS provides technical reviews of cloud service provider proposals for the board. As more of government moves to cloud services and our engagement intensifies, we see an expected program increase of $2.6 million in Fiscal Year 2016 to support FedRAMP.

DHS CYBERSECURITY INITIATIVES

As you know, Congress passed two key pieces of legislation that greatly enhances our ability to shape and resource cybersecurity initiatives. Both the 2014 Federal Information Security Modernization Act (FISMA) and the Federal Information Technology Acquisition Reform Act (FITARA) will strengthen our ability, as a Department, to respond and establish stronger guidance and controls.

- The 2014 Federal Information Security Modernization Act allows for more nimble and risk-based security assessments and compliance. It defines roles and responsibilities for cybersecurity within the Federal Government. FISMA frames information security in a more modern and efficient fashion.

- FITARA strengthens the role of Departmental CIOs. It ensures that all IT investments are be reviewed by the CIO prior to acquisition. This is vital to reduce duplication of IT systems, provide high-value services, and ensure the continued ability to proactively combat cyber-attacks.

Continuous Diagnostics and Mitigation Program

The Department was the first agency to contract Continuous Diagnostics and Mitigation. As an early adopter, the Department expects to see positive impacts to how we detect and counteract cyber threats. CDM uses real-time data to provide stakeholders with the tools needed to protect their networks and enhance their ability to detect and counteract day-to-day cyber threats. The CDM capabilities feed into agency-level dashboards that alert us to critical cyber risks in near real time.

DHS is currently testing the CDM dashboard in two operational instances. This enables the system stakeholders to readily identify which network security issues to address first, enhancing the overall security posture of agency networks in hours instead of days. The CDM dashboard will provide extensive visibility across the DHS enterprise.

Ongoing Authorization

Originally, a system's Authority to Operate was granted every three years after a large paper-based security controls review. This triennial paper-based process will evolve to the Ongoing

Authorization (OA) program. OA uses real-time event-driven data from CDM sensors to alert on dynamic, risk-based events. OA delivers effective, timely, event-driven security services to federal IT systems.

DHS is a role model for the implementation of OA across the federal government. Our OA program continues to expand. Seventy systems were enrolled in the program before the end of Fiscal Year 2014, exceeding the goal of 50. Currently, 82 systems are enrolled.

Security Operations Center

Like other Departments, DHS uses a federated architecture that relies on mission-focused components leveraging their intimate knowledge of their missions to police their networks. The DHS Security Operations Center (SOC) aggregates these data feeds to create a holistic view of the DHS enterprise. The Department's SOC monitors the enterprise network and reports all cyber incidents to the United States Computer Emergency Readiness Team (US-CERT) under NPPD. Additionally, the DHS Chief Information Security Officer provides advanced threat investigation services.

As our adversaries continue to evolve and become more sophisticated, we must evolve as well. To do this, we anticipate additional investment in cyber counterintelligence services like Focused Operations.

Intrusion Defense Chain

Cyber attacks are more than isolated activities. They often occur in phases, in a chain of offensive events that are repeated, reused, and predictable. In 2013, we began implementing and refining the Intrusion Defense Chain (IDC) into our security operations. The DHS IDC methodology uses the attackers' tactics against them. It hardens the Department's defenses based on what we learn from evaluating all the links of their previous attacks.

The IDC allows us to use what we learn from past attacks to bolster our defenses and identify areas that might need future investment. Defending the Department is a full-time effort and the IDC helps to provide us with an advantage tactically and financially.

Strengthening the IT Workforce

Workforce planning at DHS is an inclusive process involving top management support with input from human resources, program management, budget, acquisition, and legal partners. It is the responsibility of every DHS component to support and ensure that effective workforce plans are prepared, implemented with action plans, monitored, and evaluated.

Attracting, training, and retaining quality IT professionals is critical to the long-term success of our mission. To attract IT professionals with cutting-edge skills in emerging technologies necessary to address cybersecurity future needs, DHS has developed and implemented a number of initiatives:

- The CyberSkills Management Support Initiative develops and executes Department-wide human capital strategies, policies, and programs that will create, enhance, and support a top-notch DHS cyber workforce.

- The DHS IT Human Capital Strategy outlines IT career paths and enables DHS to more formally address how new workers can progress along a technical or managerial career track. As part of this strategy, DHS is leveraging developmental, mentoring, and rotational programs.

- The DHS IT Immersion Program provides newly-hired employees with a formal path to learning about IT across DHS components, and to engage with senior leadership and colleagues about career management, component activities, and working in DHS IT. This supports a true IT culture, including mentoring and educational opportunities.

The Department continues to explore possibilities to collaborate on ways to create a community of high-performing IT professionals.

CONCLUSION

I appreciate your time and attention, and I look forward to addressing your questions and concerns.