TESTIMONY OF

Luke McCormack

Chief Information Officer

U.S. Department of Homeland Security

Before the

Senate Committee on Homeland Security and Governmental Affairs

Subcommittee on the Efficiency and Effectiveness of

Federal Programs and the Federal Workforce

June 10, 2014

Chairman Tester, Ranking Member Portman, and Members of the Subcommittee: Good afternoon, and thank you for the opportunity to speak to you about Information Technology (IT) at the Department of Homeland Security (DHS).

As the Chief Information Officer (CIO), I have oversight responsibility for more than 90 major IT programs across seven large operational components and Headquarters. I have more than 25 years of Federal IT experience, both within and outside of DHS, as well as private sector experience. I have served as DHS's CIO for fewer than six months, yet I can say with conviction that DHS has made great strides toward strong management of IT. This is critical to protecting our homeland and achieving our mission.

This is my first appearance before this committee. I appreciate this opportunity to discuss DHS's efforts to ensure effective delivery of IT programs to support DHS and the American public.

Today, I will describe what DHS is doing as an enterprise to support delivery of mission capabilities, and I will emphasize three areas in particular: how we govern IT infrastructure in DHS and across components; the efficiencies we can realize through appropriate and responsible enterprise-wide efforts; and the importance of recruiting, training, and retaining strong IT professionals.

Governing Our Infrastructure

Creating functional excellence requires every executive, manager, and employee in the Department to create an environment that rewards collaboration, promotes best practices, and shares accountability so that the Department can fulfill its mission. This concept of accountability mandates that both Component heads and key department functional experts are responsible for organizational excellence. In short, the Department and the IT community within it must work together.

In working with CIOs across the Department's Components to provide proper oversight, we have established a robust, tiered governance model that provides active oversight and ensures programs have the key executive stakeholders engaged to ensure alignment.

At the top of this governance structure is the Department's Acquisition Review Board (ARB), which has ultimate oversight over all large programs – those with a life cycle cost estimate of $300 million or more.

As CIO, I serve on the ARB, supporting the Acting Under Secretary for Management, who is also the Chief Acquisition Officer.

As an interim measure between ARBs for major acquisitions, the Department has created Executive Steering Committees (ESCs). ESCs are comprised of key executives who meet more regularly to ensure adequate oversight of major acquisitions. ESCs help to ensure programs stay or get back on the "right track," and are not going in "the wrong direction."

For IT programs, one of the most important processes to ensure we safeguard taxpayer dollars is our IT Acquisition Review, or ITAR. The ITAR process provides me with the opportunity to confirm that acquisitions comply with security, accessibility, and enterprise architecture requirements, as well as, align with DHS strategic direction on enterprise data centers, licenses, and services. One of the key elements of the ITAR process is that the DHS CIO approves every IT acquisition over $2.5M life cycle value. This is critical because it ensures that such high dollar expenditures comply with the Department's enterprise architecture, as well as our IT security standards.

A good example of how we have improved IT programs under this tiered governance model is how DHS successfully integrated the Acquisition Review Board (ARB), Executive Steering Committees (ESCs), Enterprise Architecture (EA), and the System Engineering Life Cycle (SELC) stage reviews into a defined, efficient governance process that is adaptable to the needs of each program. This has resulted in an improved program and project tracking and oversight.

Program performance is evaluated through a detailed review of program risk, human capital, cost and schedule, contract oversight, and requirements. These evaluation factors are based on OMB guidance. Since the implementation of the tiered governance model, approximately one third of DHS acquisition programs have improved from moderate to low risk, and half have improved from high to moderate risk, according to OMB performance assessment ratings.

In addition, we have established Centers of Excellence (COEs) in eight areas to support program management disciplines, including requirements engineering, cost analysis, and test and evaluation. The COEs work with programs to ensure they are using best practices in these disciplines and can provide guidance and even personnel and training materials to enable programs start and stay on track.

The COEs also support the TechStat process when we need to address a troubled program. TechStat Accountability Sessions allow the Department to review high risk IT projects, address systemic problems, and get programs back on track by addressing root causes and identifying when extra support is required. Based on the root causes that are documented, COEs provide support to programs to assist them in addressing their deficiencies, in areas such as requirements, configuration management, and accessibility.

Improving governance, making use of COEs, and addressing troubled programs in a consistent and timely manner ensure that we are good stewards of the tax payers' resources, both today and in the future, while we continuously meet our mission needs.

Strengthening Our Stewardship

As important as it is to achieve mission success, we must never lose sight of our fiscal responsibilities.

There remains potential for synergy across like functions. For instance, DHS Components perform standard business functions, such as human resources and finance. In addition, the

Components execute similar functions that support mission outcomes, such as screening, domain awareness, and incident response.

For efficiency and effectiveness, we are working to properly integrate, address duplication of effort, and streamline processes and systems through the use of the DHS Enterprise Architecture (EA), while leveraging existing governance structures.

In its most basic terms, the DHS EA is the roadmap for the implementation of business and technical models to drive improvement in the ways DHS meets its missions and carries out its business. We have divided DHS into 13 different functions that represent both the business (e.g., finance) and those that support the mission (e.g., screening, incident response). Looking at the Department from this perspective enables us to visualize areas that are natural opportunities for sharing and synergy across DHS.

To augment this work, we are in the process of establishing portfolio governance boards, in which senior executives from across DHS come together to drive decisions to affect better mission and business outcomes. For instance, significant work has been completed in the Information Sharing and Safeguarding portfolio. This function has a "segment" EA (a segment EA is specialized for use at the program or portfolio level) and a strong governance board (Information Sharing and Safeguarding Governance Board, or ISSGB) co-chaired by DHS's Under Secretary for Intelligence and Analysis and myself, as the CIO.

We are also achieving tremendous progress in integrating IT infrastructure across DHS, as well as establishing enterprise services and leveraging our size for purchasing power.

Last year, DHS completed a multi-year wide-area network consolidation to OneNet, which leverages the buying power of the Department for all network services. The consolidation of OneNet operations at Headquarters, combined with a management philosophy that increases transparency, works toward an economy of scale, and utilizes a cost recovery model, will result in average cost savings of 12 percent for operations and maintenance.

To enhance efficiencies, we have negotiated more than a dozen Enterprise License Agreements (ELAs) with major software and hardware vendors, resulting in more than $125 million in cost avoidance or direct savings per year. As of March 2014, this program participation saved the Department an estimated 36 percent off of the typical GSA licenses, for a cost avoidance of $509 million. These cost avoidances and savings are allowing the Department to more efficiently meet its needs and better utilize scarce funds for achieving the Department's mission.

In addition, we have consolidated 18 legacy data centers into our two state-of-the-art enterprise data centers. The data centers have become the foundation for the robust cloud services offerings by the Department, with 11 cloud service offerings in areas as diverse as e-mail, mobility, virtual desktops, and basic computing services. The DHS cloud computing business model will enable the Department to reduce IT capital expenditures, provide transparency into spending, and reduce the time-to-market for new capabilities.

Today, the Department is considered a leader in the Federal Government in leveraging cloud capabilities, focusing on eliminating duplication, and rationalizing the agency's information technology investments. Our commodity service offerings have the ability to drive significant integration along with cost savings. For e-mail, DHS has migrated over 136,000 users to our Email-as-a-Service cloud offering. DHS has capitalized on its size to demand efficiencies and has lowered the average email box cost per month from the benchmark industry standard of $24 per month to an average $7-$8 per month.

More recently, DHS has leveraged its cloud offerings to support the Digital Government Strategy, enhancing DHS's government-to-citizen services, enabling a mobile workforce, as well as reducing capital expenditures, and streamlining time-to-market for new services in Screening/Vetting, Benefits Administration, and Law Enforcement.

Managing Our Workforce

No matter how well we govern our programs, they are only as effective as our people. Attracting, training, and retaining quality DHS IT professionals are critically important to our long-term

success. Our workforce supports the Department's multiple missions to prevent terrorism and enhance security, secure and manage the nation's borders, and ensure resilience from disasters, amongst others.

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.

Over the past few years, we have been developing and implementing the DHS IT Human Capital Strategy, an approach that outlines IT career paths and enables us to more formally address how new workers can progress along a technical or managerial career track. We are currently working to leverage DHS developmental, mentoring, and rotational programs into this strategy. Additionally, we are partnering with the Office of the Chief Human Capital Officer on how to better market ourselves as a Department, both for IT and cyber security professionals.

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. I look forward to addressing your questions and concerns, as well as the opportunity to work with you, to ensure that DHS information technology remains strong, responsive, and secure.