STATEMENT FOR THE RECORD

Elizabeth Cappello
Acting Chief Information Officer
U.S. Department of Homeland Security

BEFORE THE

United States House of Representatives
Committee on Oversight and Reform
Subcommittee on Government Operations

"FITARA 9.0"

December 11, 2019

Introduction

Chairman Connolly, Ranking Member Meadows, and distinguished Members of the Subcommittee, thank you for the opportunity to appear before you today to share the Department of Homeland Security's (DHS) progress on implementation of the *Federal Information Technology Acquisition Reform Act* (FITARA). I would also like to thank you for your continued support and commitment to achieving the goals of FITARA.

Over the past five years since the passage of FITARA, DHS has made significant progress in enhancing and strengthening the role and authority of the Department's Chief Information Officer (CIO). I look forward to talking about this success and others we have had here at DHS, and the improvements we are making around specific FITARA Scorecard metrics and related areas. In keeping with the tenets of FITARA, we are committed to efficiently and effectively overseeing information technology (IT) resources across the Department.

The CIO's Role at DHS Headquarters

DHS includes 14 Operational and Support Components with varied mission sets, operational tempos, and technology complexities spread out across the globe working together in support of securing the Homeland. This condition requires a federated IT model implemented with necessary governance and oversight, allowing for sharing of information, best practices, solutions, and other important services to achieve efficiencies, transparency, and accountability.

The CIO enhances the DHS mission, ensuring that information flows securely and effectively across the broad mission space. As Acting CIO, I am responsible for collaborating with Component CIOs and staff of the Department's Components, so they can execute their vital missions. My office operates the enterprise-wide area network that connects DHS federal employees, contractors, and dozens of networks and IT systems. We do this with our enterprise Security Operations Center (SOC) scanning for and mitigating the risk of attack from both foreign and domestic hostile cyber actors, as well as ensuring routine cyber hygiene.

The principles and authority provided in FITARA have strengthened collaboration with the DHS Component CIOs and the DHS Management Directorate Lines of Business Chiefs (CXOs), particularly with the Chief Financial Officer (CFO), Chief Human Capital Officer (CHCO), and Chief Procurement Officer (CPO). Each CXO provides a critical function. The CIO develops, operates, and secures IT; the CFO prepares the annual budget request; the CPO provides contract services; the CHCO supports the workforce needs; and the Executive Director of Program Accountability and Risk Management provides oversight of the entire acquisition process. These CXOs work closely together, ensuring alignment of IT resources with the Department's mission to reduce duplicative IT spending, improve speed to deliver capability, grow the skillset of our workforce, and enhance transparency.

These partnerships help the CIO Office (OCIO) to navigate a complex environment and continue to build on this progress of improving the management of IT resources – a core theme across the four pillars of our IT strategy – 1) advance the mission, 2) optimize the organization, 3) enhance service delivery, and 4) institutionalize cybersecurity.

The CIO's Important Role in Budget and Acquisition

As Acting CIO, I am committed to ensuring sound IT investments for the DHS enterprise. The Department's comprehensive investment management approach addresses all levels of IT investment from initiation to termination and provides the ability to analyze the IT portfolio from multiple perspectives. I have visibility into potentially duplicative IT investments and opportunities for consolidation across DHS through the budget review process, IT Acquisition Review, the Acquisition Review Board (ARB), and the Joint Requirements Council (JRC).

One key element of FITARA is defining IT resources for future years. OCIO does this through engagement in the Planning, Programming, Budgeting, and Execution process. We provide investment recommendations in a timely and meaningful manner to influence IT elements of Resource Allocation Plans and critical decision making in the Program Budget Review. These activities are the foundation for building the Secretary's budget.

In conjunction with our counterparts in OCFO and OCPO, we are working to expand OCIO visibility into all IT expenditures. As a first step, we are using the Technology Business Management (TBM) taxonomy as a mechanism to enhance visibility. To date, the Department has completed an alignment of its IT investments through the Capital Planning and Investment Control process to the TBM taxonomy to provide more transparency into IT planned spending for Fiscal Year (FY) 2021. This was submitted to the Office of Management and Budget (OMB) on September 20. This alignment will enable DHS to better track all IT spending across the Department and benchmark spending, identify opportunities for improvement, and help increase the taxpayer value of IT.

FITARA requires CIOs to review IT acquisitions. DHS accomplishes this through the IT Acquisition Review (ITAR) process. The DHS CIO reviews and approves any IT procurement request with a lifecycle cost of more than $500,000 that are aligned with our major IT investments. OCIO has allowed Component CIOs additional flexibility to review even smaller lifecycle values. In 2019, OCIO reviewed over 530 ITARs submitted by the Components.

The CIO is integrated into all areas of the acquisition process, including the Department's ARB. The ARB works in concert with the other DHS CXOs, including the CPO and CFO. The board is chaired by the Deputy Under Secretary for Management. It is the primary forum to address concerns and recommendations regarding troubled projects from remediation up to and including recommendation for termination. When significant issues are encountered, the CIO has proposed several different remediations, as well as recommendations for pausing projects. Another avenue to engage in the acquisition process is the Department's JRC. As a member of this Council, I review the identification of all new requirements within DHS on a regular basis. As is required by FITARA, I have a seat at the table and a strong voice in the process.

Using FITARA to Build the IT Workforce

FITARA and other relevant authorities include requirements for the IT workforce at all levels — ranging from my position as Acting CIO to the staff level. As a major first step, OCIO successfully implemented the Strategic Workforce Planning (SWP) Initiative aimed at enhancing the workforce. We developed the SWP Initiative in collaboration with OCHCO as a repeatable, four-step process for assessing the current IT skills of employees and identifying future needs. The analysis performed to date includes building IT competency models, conducting competency

assessments, categorizing training opportunities for each role, and identifying gaps.

One success to date is our collaboration with OCHCO to develop the Cyber Talent Management System, or CTMS, to manage the entry and training of cyber talent within DHS. The system will pay personnel at a level requisite with the experience and education they have acquired, including in the private sector. To develop and retain needed IT workforce skills, OCIO also implemented a cyber-retention pay program for FY 2019, as well as a cyber-internship program aimed at identifying potential cybersecurity talent. Both initiatives have been successful for the Department to date and show promise moving forward. OCIO will continue to engage with Components to oversee IT workforce skillsets, share methodologies and best practices, and align with the Office of Personnel Management competencies and National Institute of Standards and Technology cybersecurity methodologies. We will also conduct outreach to stakeholders outside of the government. For example, DHS IT personnel held numerous engagements this summer with educational institutions, such as George Mason University, as part of an ongoing strategic outreach campaign to bring innovation and current IT trends into the Department and increase collaboration with the private sector.

Looking internally, strategic workforce development is essential. Key training areas across the Department include application rationalization, Cloud adoption and management, and the Agile development methodology. This skills enhancement training is occurring across DHS, which has collected best practices from our own Components. For example, U.S. Citizenship and Immigration Services (USCIS) has trained more than 4,000 employees from DHS and other federal agencies in Agile development, and U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP) have also trained their staff in Agile.

OCIO seeks to continue DHS's excellence in the field of Agile development by conducting several services to enhance the Agile skill set of our employees. Our Agile Center of Excellence gathers all DHS Components monthly and conducts an annual Agile Expo, which pulls together the best projects using Agile from all Components into one place.

I am confident that FITARA will be a useful tool to help build upon our progress and confront any roadblocks as we further enhance our IT workforce to meet the needs of an evolving IT environment.

The Department's Approach to Data Consolidation and Cloud Migration

I understand that one of the top priorities for the Chairman and the Ranking Member of this Subcommittee is Data Center consolidation. I agree with the focus given to this matter and am pleased to report on our progress to date, especially among our Components. OCIO prioritizes Data Center consolidation and is actively looking for ways to further consolidate through existing technologies and innovative uses of IT.

At the enterprise level, DHS is consolidating its data centers and reducing the footprint within its two enterprise data centers (DC1 and DC2). These centers provide major service capabilities. For DC1, DHS is consolidating or migrating to the Cloud, which has reduced the DHS footprint by 36 percent. We are also making progress with DC2. In FY 2019 to date, 20 percent of systems have completed their transition out of this facility, and 65 percent of DC2 systems have migrated or plan to migrate to the Cloud.

DHS is a leader in Cloud adoption using a federated, hybrid multi-Cloud approach. We recognize the need to evolve our enterprise security model, policy, and architecture to remove barriers and support our modernization and migration to the Cloud while accounting for the tactical needs of our missions. To do this, DHS is focused on removing barriers to support optimized "Compute and Storage" environments that enable DHS Components to move to the Cloud at the speed fitting their mission. This means starting with network modernization, driving towards a new Trusted Internet Connection (TIC 3.0), streamlining the Authority to Operate (ATO) processes, and finding the best way to procure Cloud services.

Data center consolidation and Cloud migration are the future in IT – a future envisioned by FITARA. The Department will continue to move towards this future in partnership with Congress and especially this Subcommittee.

Enabling FITARA Advancements Through Robust Cybersecurity

As definitive perimeter boundaries dissolve, DHS is following Zero Trust principles to drive an evolution from traditional approaches to security, and further enhance the security and defense of our users, devices, networks, applications, and data. We are also moving our risk assessment and authorization processes from compliance-based to risk-based. Understanding risk and mitigating it requires a more thoughtful approach than compliance alone. Fighting cyber-attacks is a multi-dimensional challenge.

OCIO is seeking to implement a Zero Trust Security Architecture to help protect DHS IT assets from compromise and to improve monitoring and access control. This is a set of security architecture principles that treats all requests for IT resources as untrusted and requires verified policy enforcement at each stage of access. Using this approach, everything is evaluated against a set of conditional security policies before access is granted. This enables enforcement at every point.

OCIO provides enterprise security operations, designs and engineers technical solutions, measures compliance, and develops and enforces policies. We measure via a Cybersecurity Maturity Model and evaluate progress against the *Federal Information Security Management Act* (FISMA) Compliance Scorecard.

To standardize and advance SOC accreditation and assure baseline cyber capability, DHS borrowed best practices from the Department of Defense (DOD) Cyber Security Service Provider, a tried-and-tested federal approach to accreditation. DHS implemented its Cybersecurity Service Provider program this year by tailoring the DOD platform to DHS requirements. The Defense Information Systems Agency assessed the ICE SOC this past year, and then the DHS CIO accredited it. DHS will continue to inspect the remaining Component security operations this fiscal year to enable a common and shared awareness during critical events and ensure uniform application of security functions across Components. Looking ahead, we plan to follow up this work by creating a Center of Excellence and an integrated approach across the tool sets.

I am proud to note that the Department's improved cybersecurity posture is evident from our increased FISMA scorecard grades, Cross-Agency Priority cybersecurity goals, and annual Inspector General assessment.

Building on Foundational Success to Enhance IT

I believe the Department has a strong foundation for implementing FITARA, but there is certainly room for more progress. DHS is implementing several key initiatives to make additional strides, including establishing Authority to Proceed (ATP), Zero Trust, TIC 3.0, Wide Area Network (WAN) Modernization, and other innovations. I regard each of these elements as essential to making important gains in areas of consequence for FITARA – Cloud adoption, data center consolidation, and managing cyber risk.

OCIO is adopting the ATP as a method to expedite the ATO process, establish ongoing authorization, and improve the Department's cyber risk management. We aim to streamline the ATO process by implementing the ATP. This cumulative assessment method allows for rapid deployment of selected low and moderate impact information systems and helps Components start using the latest technologies. For example, if a commercial Cloud provider has satisfied most of its security issues, an interim approval, or their ATP, may be provided. The idea behind this process is to increase compliance and have the Components be more nimble in their advancements in modernizing systems through the Cloud and emerging technologies.

The Department's Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with OCIO, is conducting a range of activities to implement the "Update to the Trusted Internet Connections Initiative Memorandum" issued by OMB. We will work with the CISA TIC Program to ensure alignment and compliance with pending changes in federal standards. Advances in TIC are necessary for further advances in the Cloud. We will integrate Cloud Security Gateway services and functionality with the capabilities provided by a Cloud access security broker service and Cloud-native visibility and enforcement services. The integration of these functions will meet the Department's visibility and enforcement needs in the Cloud and enhance our abilities to defend DHS networks and data. The implementation of TIC 3.0 will further support our efforts around Cloud migration, better enabling future data center consolidation efforts.

I am sensitive to the challenges with the current WAN from bandwidth cost to reliability as well as the constraints of our operating environment. There are a variety of improved networking technologies such as Ethernet, SD-WAN, and 5G technologies that support better performance and management. One of the steps we are taking is to prepare to transition from the existing Networx contract to the General Services Administration's Enterprise Infrastructure Services (EIS) contract vehicle. This transition will help to modernize our networks and support our other on-going initiatives. However, many of these technologies are not yet available in the geographic areas where DHS operates. We must address capacity demand necessary to support Cloud adoption, enhanced applications, mobility, and resiliency for all our networks.

A simplified, federated network architecture that is easier to manage and more responsive to Component mission requirements and Department priorities is needed. Keeping pace with technology means we must modernize our architecture. We are actively identifying ways to do this to support DHS operations across the globe.

In addition to modernizing our architecture, we strive to keep pace with the latest capabilities available through emerging technology. We are adopting Artificial Intelligence and Robotic Process Automation to enhance cybersecurity, procurement, budget, and human resource management. Our Components are leading the way in some of these technology areas. It speaks

to the maturity of our federated structure that we can capitalize on best practices and leverage successes across the Department. As a new leader in Headquarters with an immediate past in one of the Department's Components, I will actively look to Components for innovative ways to improve our enterprise and FITARA implementation.

Conclusion

DHS Headquarters and the Components need a Department Network that runs 24/7 and is secure. They want the delivery of their mission capabilities and security for all their technology, and I am committed to making this happen. This means that my organization will provide strategic guidance, facilitation among Components, and enterprise technical solutions where they make sense.

All the advances and steps outlined in this testimony ensure fundamental IT resources are available to the Department. From budget, to infrastructure, to the workforce, these pieces play a critical role in how we successfully move forward in a federated model. As Acting CIO, I will continue to ensure that each Component and mission space is able to respond to their tactical technology requirements and emerging operational needs.

Against this backdrop, I use the FITARA Scorecard the same way this Committee does – to demonstrate my commitment to continuously improving IT and as a measure of progress for the Department. In important aspects, we know that we still have more work to do. Nevertheless, I am looking forward to the successes we will realize for Cloud, Cyber, Workforce, and the overall FITARA agenda through our ongoing improvements. I thank you again for the opportunity to testify and for your continued support of this important work. I look forward to your questions.