U.S. Department of Homeland Secu
Washington, DC 20528

Homeland Security

The Honorable Margaret Wood Hassan
United States Senate
Washington, DC 20510-6250

Dear Senator Hassan:

This is in response to your letter, dated June 3, 2020, urging the Department of Homeland Security (DHS) to modernize its information technology (IT) systems to improve security, increase efficiency, and reduce wasteful spending associated with the maintenance of legacy IT systems.

We appreciate your interest and engagement with our modernization efforts here at DHS. We share your desire to modernize DHS's IT systems for all the same beneficial reasons you cited. Enclosed you will find individual responses to your questions regarding our implementation of and adherence to the Federal Information Technology Acquisition Reform Act (FITARA), as well as our general modernization plans and efforts.

We appreciate your continued support of DHS. Should you wish to discuss this matter further, please do not hesitate to contact us.

Sincerely,

TROY D EDGAR
Digitally signed by TROY D EDGAR
Date: 2020.07.30 14:49:44 -04'00'

KAREN S EVANS
Digitally signed by KAREN S EVANS
Date: 2020.07.30 16:26:19 -04'00'

The Honorable Troy D. Edgar
Chief Financial Officer
Department of Homeland Security

The Honorable Karen S. Evans
Chief Information Officer
Department of Homeland Security

Enclosures:
DHS Briefing Cloud and Data Center Consolidation Strategy
Enterprise Infrastructure Solutions Transition and Modernization Plan

Responses to Questions from the Senate Homeland Security and Governmental Affairs Committee Subcommittee on Federal Spending Oversight

1. Does your agency have a comprehensive IT modernization plan?
Yes.

a. If so, please attach it to your response.

- Enclosure titled, "DHS Briefing Cloud and Data Center Consolidation Strategy;" and
- Enclosure titled, "Enterprise Infrastructure Solutions Transition and Modernization Plan."

Modernizing the network is a top priority for the Office of the Chief Information Officer (OCIO) due to the following:

- a network architecture has been the same for roughly 16 years; and
- an outdated infrastructure that makes it difficult to keep the network operational and protected against today's threat landscape.

DHS oversees the modernization of the Department's wide area network (WAN) which is underway and incorporates many technological, architectural and cybersecurity improvements.

The DHS WAN core infrastructure provides numerous services for DHS end users, such as secure internet access, routing information for remote routers, trust zone separation for the different DHS Components and enterprise cloud access.

DHS will provide new network capabilities such as Software Defined Networking (SDN) and Software Defined Wide Area Network (SD-WAN) capabilities while increasing cloud connectivity and security enhancements from the DHS Headquarters (HQ) Zero Trust Architecture initiative including Cloud Access Security Broker (CASB), Cloud Security Gateway (CSG), and Trusted Internet Connection (TIC) 3.0. In addition, DHS is moving the core network infrastructure to a co-location facility which provides for direct network connectivity to the cloud service providers (CSPs), improved performance and a reduction in network latency.

DHS HQ is enhancing the security of its networks and cloud assets through the Zero Trust Architecture initiative and has implemented several aspects already. The Zero Trust architecture will provide DHS with targeted security enhancements to reduce the risk to our enterprise while limiting access to departmental resources and those residing on external networks, such as cloud providers and vendor data centers. CASB and CSG work together to manage and secure access to resources such as Microsoft Office 365, external vendor software-as-a-service offerings, and other DHS assets residing in the cloud. The DHS TIC 3.0 implementation provides network inspection, monitoring and response in a much higher performing and better distributed manner than prior implementations. TIC 3.0 provides the ability to migrate applications from the data center while retaining the network performance

characteristics, traffic inspection, and monitoring that were previously required to be on-site for performance reasons.

These capabilities enable central management of the network infrastructure and lowers costs for network access circuits. Another feature of the DHS WAN network modernization is to increase bandwidth to the CSPs and the internet, allowing for more applications to migrate to the cloud environment and provide optimal performance. The virtualized network infrastructure will provide rapid scalability and flexibility to adapt to emerging requirements from our customers, as well as improving resilience and mean time to restore.

DHS implemented the Cloud Smart strategy in its Data Center (DC) consolidation planning for DC1 and DC2 to include elements of the enterprise conversion of email-as-a-service. To facilitate cloud computing adoption, DHS OCIO implemented its own cloud solution platforms as a cost-effective option for system owners to migrate to the cloud.

DHS continues to coordinate with each of the operational Components to establish specific goals for the number of Component-owned systems that should be migrated to the cloud. Coordination also includes ensuring the alignment of IT portfolios and other strategies with the DHS IT Strategic Plan 2019-2023.

b. If not, please provide a comprehensive IT modernization plan for your agency.

N/A

2. What are the top five modernization priorities for your agency? For each, please provide or describe:

1. **Network and Security Modernization** – Migrate from an equipment-based network to a software defined network to provide flexibility and resiliency;
2. **DC2 Exit** - Migrate legacy systems out of Data Center 2 in Clarksville, Virginia through cloud migration, system retirement, and colocation;
3. **DC1 Acquisition/Optimization** - Continue to optimize within an enterprise data center. Integrate operations with the cloud through a new acquisition – Data Center and Cloud Optimization (DCCO);
4. **Security Operations Center (SOC) Optimization** – Implement modern cybersecurity tools and engineering enhancements, standardization of SOC accreditation standards, and optimization of current shared-services model; and
5. **Cybersecurity Talent Management System (CTMS)** – Implementation of a skills-based recruitment and retention process to transform the Department's cybersecurity skillset, achieve cybersecurity talent parity with the private sector, and support the SOC optimization priority.

a. the modernization plan for the priority;

These are summarized above and outlined in more detail within the Enclosures.

b. the expected cost of modernization and any anticipated cost-savings as a result of modernization;

1. Increased bandwidth at field sites via broadband and Ethernet WAN circuits without additional cost;
2. Improved performance by reducing network connections and latency to Cloud Service Providers;
3. Improved performance by increasing DHS WAN network bandwidth at core infrastructure, Internet gateway and Enterprise Cloud Access Point (ECAP);
4. More efficient and responsive security operations services; and
5. An optimized government-contractor cybersecurity workforce balance.

c. the expected completion date of the modernization; and

1. DHS is pursuing a phased approach to network modernization, which runs through FY 2023.
2. DC2 Exit is targeted for Q1 2021.
3. DC consolidation and optimization will run through 2021.
4. DHS SOC optimization commences in FY20 with the first assessments, and optimization efforts will be ongoing through FY24.
5. DHS plans to use the Cybersecurity Talent Management System (CTMS) under the Title 6 authority to recruit DHS Cybersecurity Service employees to support SOC optimization in FY 2021. Initially, DHS plans to use CTMS to hire and manage approximately 40 new DHS Cybersecurity Service employees for the enterprise 24 hour-per-day security operations site outside the National Capital Region. This effort will provide a roadmap for program implementation by Components, and associated CTMS hiring will expand beginning in FY 2022.

d. the reason(s) for any schedule delays or cost overruns to date.

None currently for all five priorities.

3. What is the status of the modernization of the legacy system identified by GAO and described in this letter?

OCIO collaborated with 12 Components within DHS, including the Federal Emergency Management Agency (FEMA), to finalize the DHS Enterprise Infrastructure Solutions Transition and Modernization Plan. The Plan details each Component's strategy to complete modernization efforts and dispose of legacy systems. Deputy Chief Information Officer (DCIO) Elizabeth A. Cappello approved the finalized plan and it has progressed to the implementation phase via the Office of Management and Budget.

4. Please describe your efforts to phase out the use of legacy systems that are physically outdated and do not support current software capabilities, are no longer supported by the vendor or manufacturer, or require specialized employees or contractors to operate and maintain. For example, have you conducted a survey of your IT systems based on use and determined which systems can be eliminated to reduce waste?

In keeping with the *Federal Information Technology Shared Services Strategy* guidance emphasizing and encouraging the use of enterprise IT services, such as email, to help reduce duplication and provide common capabilities at defined service levels and with greater efficiency, DHS has moved from email-as-a-service to cloud-based email services. All Components, except for the U.S. Secret Service and the U.S. Coast Guard, have either migrated to or are in the process of migrating to Microsoft Office 365.

5. Please describe the coordination between the Office of the Chief Information Officer and the Office of the Chief Financial Officer on IT acquisitions.

a. In particular, how has the implementation of FITARA changed the way your agency acquires, maintains, and organizes its IT investments?

The DHS Office of the Chief Financial Officer (OCFO) and OCIO continue to collaborate and partner to ensure continuous improvement of the Planning, Programming, Budgeting and Execution (PPBE) processes. OCIO, Office of Policy, and OCFO have leveraged a strong working relationship to ensure Chief Information Officer (CIO) involvement in all stages of PPBE. Over the last several years of budget cycles, OCIO and OCFO collaborated on the Resource Allocation Plan (RAP) instructions and associated Component roadshows. This effort helps to ensure inclusion of the CIO at the beginning of the programming process. The CIO also regularly participates in the monthly CFO Council meetings as well as all prep sessions for the Deputy's Management Action Group, the body that determines what is included within the annual DHS budget submission.

DHS ensures the CIO plays a key role in all aspects of IT investment decisions. For the last two years, OCIO worked with Component CIOs to review and validate any funding changes to IT resources to ensure alignment with DHS IT enterprise strategy and reduce potential duplicative efforts. OCIO also continues to review all IT-related program changes for compliance with the IT priorities outlined within the Resource Planning Guidance (RPG) and Under Secretary for Management (USM) strategic guidance.

The Department continues to explore ways to ensure the CIO has full visibility into IT planned expenditure reporting. To date, CIO oversight of planned IT expenditures has been accomplished through the Capital Planning and Investment Control (CPIC) process. Project data is collected and tracked to inform IT investment reporting and enhance decision-making.

In addition, the Department has completely revised its process for acquiring and developing IT investments through the Acquisition Transformation effort and the Streamlined Software Acquisition Process (SSAP). The Acquisition Transformation effort and resulting SSAP were created in full partnership and alignment with other DHS CXOs, the Joint Requirements Council (JRC), the office of Program Accountability and Risk Management (PARM), and the Science and Technology Directorate (S&T). The updated processes were piloted, and action plans resulting from the pilot discoveries were produced and completed. This includes significant changes to the policies and procedures that govern the IT Acquisition and Systems Engineering Life Cycles. These updated policies are being finalized and implemented in FY20.

b. How can your offices' coordination under FITARA be improved to better address IT modernization across the agency, especially for legacy systems?

The Department recently completed an FY 2020 FITARA self-assessment that revealed strong ongoing coordination among the Component IT organizations across all OMB baseline measures but revealed an opportunity to increase the visibility of Component CIOs into planned IT expenditures occurring within Component non-IT organizations. This increased visibility can enable the potential identification or optimization of additional modernization opportunities across the Department.

OCIO is undertaking an effort to analyze and revise the Program Health Assessment process to provide a more accurate rating of the current level of Program risk in its ability to accomplish its mission. This robust, holistic, evidence-based assessment includes several key OMB categories and has resulted in increased accuracy of the Risk ratings on the Federal IT Dashboard. OCIO also is analyzing its Operational Analysis (OA) process for IT programs that have transitioned to Operations and Maintenance (O&M). This is being done to ensure there is an equal amount of rigor placed in the decision to continue to fund legacy systems as there is in the initial decision to fund IT capabilities. To accomplish this, OCIO is partnering with DHS Components to update its metrics and analytics in this space and to implement Technology Business Management (TBM) concepts. The Department also hosts a monthly High Visibility review, which provides a forum for DUSM and CXO principals to review major acquisition programs of interest.

6. Finally, how can Congress better facilitate or oversee the modernization of government IT systems to achieve greater system reliability, security, and fiscal efficiency?

- ***Is there a Congressional requirement (e.g., burdensome reporting) that is impeding an agency's ability to modernize? See, for example, the Council's recommendations on updating the elements of the FITARA Scorecard.***
- ***Burden reduction. The Administration wants to work with Congress to provide information about our operations in a way that is meaningful, informative, and timely, while reducing the burden on agencies. In general, we prefer to produce machine-readable data files for public consumption, rather than time-intensive narrative reports or custom data pulls.***

To effectively manage and modernize IT, DHS plans to stand up an IT Working Capital Fund (WCF) per the Modernizing Government Technology (MGT) Act. A WCF increases DHS's ability to quickly respond to technology needs such as those required during the COVID-19 pandemic. If a WCF were available, DHS would have tapped into that fund to bolster our virtual private network (VPN) capability and increase network bandwidth, while putting in place the proper security measures.

DHS intends to use the CIO and CFO Councils to make decisions on the projects that are funded by the IT WCF. Recommendations would go to these Councils from the IT Modernization Leadership Council (established upon implementation of an IT WCF), the primary interface to the Chief Financial Officer (CFO) Council and the Chief Information Officer (CIO) Council, and its determinations will serve as the joint recommendations of both Councils for funding proposals to be approved by USM.

Modernization efforts proposed through the IT WCF must meet the following criteria: (1) the improvement, retirement, or replacement of existing IT systems; (2) the transition of legacy information databases to commercial cloud and other innovative technologies; (3) improve IT modernization strategy with a strong project management approach that aligns to industry best practices and incorporates, to the greatest extent practicable, commercial technology solutions.

Because no appropriations have been enacted previously for this purpose, the Department currently does not have statutory authority to establish an ITMF and transfer funds into and from the account as envisioned by the MGT Act. Legislative language was proposed as part of the Department's FY 2020 President's Budget. The Department intends to permanently establish the Governance Board and ITMF once enacted, and begin considering project proposals.

An IT WCF reduces the risk for agencies engaging in IT modernization projects, because it increases the likelihood that funding will be available throughout the entire lifecycle of a project. We hope that Congress considers our proposed transfer authority language.