OFFICE OF INSPECTOR GENERAL

Progress and Challenges in Modernizing DHS' IT Systems and Infrastructure

Homeland Security

August 10, 2020

OIG-20-61

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

August 10, 2020

MEMORANDUM FOR: Karen Evans
Chief Information Officer
Department of Homeland Security

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI

Digitally signed by JOSEPH V CUFFARI
Date: 2020.08.07 14:12:09 -04'00'

SUBJECT: *Progress and Challenges in Modernizing DHS' IT Systems and Infrastructure*

Attached for your action is our final report, *Progress and Challenges in Modernizing DHS' IT Systems and Infrastructure*. We incorporated the formal comments provided from your office in the final report.

This report contains three recommendations aimed at improving DHS implementation of cloud technology, data center migration, and oversight of legacy IT systems and infrastructure. The Department concurred with all three recommendations. Based on the information provided in response to the draft report, we consider each recommendation open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may review the recommendations for closure. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Sondra McCauley, Assistant Inspector General for Audits at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

Progress and Challenges in Modernizing DHS' IT Systems and Infrastructure

August 10, 2020

Why We Did This Audit

Information technology (IT) is critical to accomplishing DHS' vast mission. Prior DHS Office of Inspector General (OIG) work highlighted ongoing challenges to ensuring IT systems and infrastructure adequately support DHS personnel. We conducted this audit to determine whether DHS has effectively identified and prioritized mission-critical legacy IT systems and infrastructure for modernization, to identify major challenges and operational impact associated with using and modernizing out-of-date IT, and to assess how recent legislation and executive direction may help address these challenges.

What We Recommend

We are making three recommendations to the DHS Office of the Chief Information Officer to improve its ongoing modernization efforts and establish a risk rating process for major legacy IT investments.

For Further Information:
Contact our Office of Public Affairs at 202-981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

The DHS Chief Information Officer (CIO), and most component CIOs, conducted strategic planning activities to help prioritize legacy IT systems or infrastructure for modernization to better accomplish mission goals. The DHS 2019–2023 IT strategic plan included two distinct department-wide IT modernization initiatives: to adopt cloud-based computing and to consolidate data centers. However, not all components have complied with or fully embraced these efforts due to a lack of standard guidance and funding. Without consistent implementation of these efforts, DHS components remain hindered in their ability to provide personnel with more enhanced, up-to-date technology.

In the meantime, DHS continues to rely on deficient and outdated IT systems to perform mission-critical operations. We identified three legacy IT systems with significant operational challenges that negatively affected critical DHS functions, such as human resources and financial management, as well as disaster recovery mission operations. DHS has not made sufficient progress in replacing or augmenting these IT systems due to ineffective planning and inexperience in executing complex IT modernization efforts. Additionally, the DHS CIO has not performed mandated oversight of legacy IT to mitigate and reduce risks associated with outdated systems. Until DHS addresses these issues, it will continue to face significant challenges to accomplish mission operations efficiently and effectively.

DHS has not yet leveraged the *Modernizing Government Technology Act* to accelerate its IT modernization efforts. DHS and its components questioned whether the benefits of the Act outweighed the additional effort needed to use the resources the Act provided. Without pursuing such funding, DHS may be further hindered in accomplishing its objective of reducing reliance on outdated, legacy IT.

DHS Response

DHS concurred with all three recommendations.

Table of Contents

Appendixes

Abbreviations

CAS	Core Accounting System
CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
Coast Guard	United States Coast Guard
FEMA	Federal Emergency Management Agency
FITARA	*Federal Information Technology Acquisition Reform Act*
GAO	Government Accountability Office
HRIT	Human Resources Information Technology
ICE	Immigration and Customs Enforcement
IT	information technology
OCHCO	Office of the Chief Human Capital Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
Secret Service	United States Secret Service
TMF	Technology Modernization Fund
TSA	Transportation Security Administration
USCIS	U.S. Citizenship and Immigration Services
WCF	Working Capital Fund

Background

The Federal Government relies heavily on information technology (IT) to carry out critical processes, procedures, and tasks vital to America's security and prosperity. The Federal Government invests nearly $90 billion annually to provide required IT capabilities to support essential day-to-day operations. However, despite this substantial investment, Federal legacy IT investments are becoming increasingly obsolete.[1] According to the Government Accountability Office (GAO), agencies are reportedly using systems that are, in some cases, at least 50 years old.[2] In fiscal year 2019, the Federal Government planned to spend more than 80 percent of the total amount budgeted for IT on operations and maintenance of legacy systems. This would equate to the Department of Homeland Security spending approximately $5.6 of its $7 billion FY 2019 IT budget on maintaining and operating outdated legacy IT, instead of improving and developing new IT capabilities.

DHS requires effective and up-to-date technology to accomplish its broad mission of ensuring the homeland is safe, secure, and resilient against terrorism and other hazards. DHS has seven major operational components[3] that work to accomplish the Department's front-line missions, including border security, emergency response, and immigration processing, among others. The seven operational components and their respective missions are as follows:

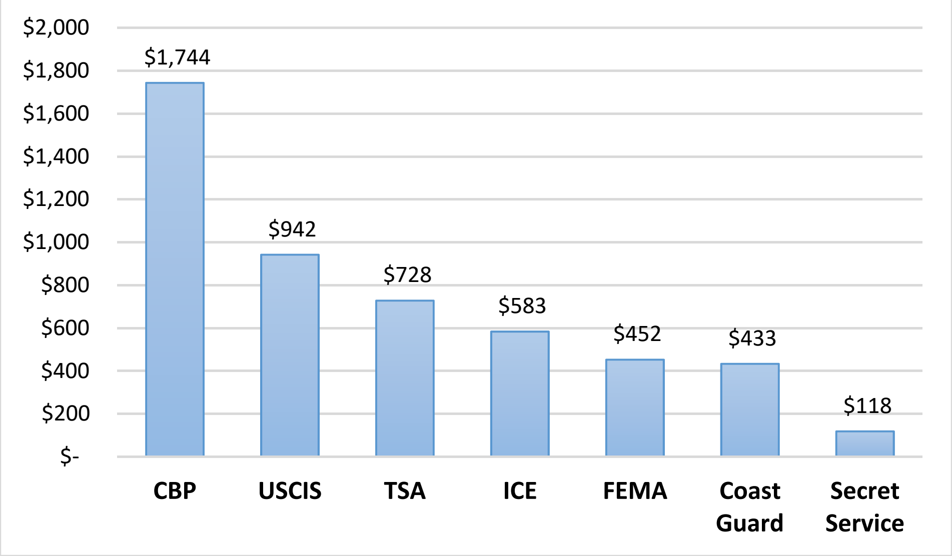
- U.S. Customs and Border Protection (CBP) safeguards the United States' borders by protecting the public from dangerous people and materials, while also facilitating legitimate trade and travel.
- Federal Emergency Management Agency (FEMA) coordinates Federal Government activities to prepare for, prevent, respond to, and recover from domestic disasters.
- Immigration and Customs Enforcement (ICE) protects America from cross-border crime and illegal immigration through immigration enforcement operations.
- Transportation Security Administration (TSA) protects the Nation's transportation systems to ensure freedom of movement for people and commerce.

[1] According to Federal IT legislation, the term "legacy information technology system" means an outdated or obsolete system of information technology.
[2] Many agencies use outdated and inefficient software and hardware that are no longer supported by the vendor. GAO-16-468, *Federal Agencies Need to Address Aging Legacy Systems*, May 2016 (https://www.gao.gov/assets/680/677436.pdf)
[3] We are defining the seven *major* operational components as those with front-line missions with a distributed public-facing workforce and an IT investment budget over $100 million.

- United States Coast Guard (Coast Guard) ensures our Nation's maritime safety, security, and stewardship.
- U.S. Citizenship and Immigration Services (USCIS) administers the Nation's lawful immigration system by adjudicating requests for immigration benefits.
- United States Secret Service (Secret Service) ensures the security of the President, Vice President, national and visiting world leaders, former Presidents, and events of national significance.

To support these mission operations, DHS' FY 2019 IT budget represents approximately 14 percent, or $7 billion, of DHS' overall budget of approximately $49 billion.[4] Each operational component maintains a significant investment in IT, ranging from $118 million to $1.7 billion. Yet, DHS still maintains and operates many legacy IT systems that are too outdated or deficient to perform critical functions effectively. Figure 1 identifies the IT budgets for each of the seven operational components.

Figure 1. DHS 2019 IT Budget by Component (in millions)



Source: Office of Management and Budget's IT Dashboard

By law, each Federal agency must designate a Chief Information Officer (CIO) to promote the effective and efficient design and operation of its major IT systems and infrastructure.[5] The *Homeland Security Act of 2002*, as amended, established the position of the DHS CIO to govern and manage IT across components to ensure technologies and services are in place and appropriately

[4] The total IT budget for DHS' seven operational components for 2019 is approximately $5 billion. DHS also has seven support components with a total IT budget of approximately $2 billion.
[5] *Clinger-Cohen Act of 1996*, February 10, 1996

managed to meet the Department's mission needs.[6] The CIO reports to the Under Secretary for Management and is supported by the Office of the CIO (OCIO), which specifically administers the Department's IT infrastructure, applications, services, and management functions. The OCIO is responsible for ensuring DHS' approximately 240,000 employees remain connected to the Department's IT infrastructure environment and receive required IT operational support. DHS' current organization chart is depicted in appendix C.

One of the DHS CIO's primary responsibilities is to review the Department's IT portfolio, including how well IT supports the Department's programs and aligns to mission needs, and make recommendations for modernizing IT systems. To do this, DHS has issued a number of policies, procedures, and standards to guide IT modernization efforts. For example, DHS issued the following directives during the past 3 years to promote effective management and optimization of department-wide IT:

- DHS Directive 142-02, *Information Technology Integration and Management*, April 2018, identifies the DHS CIO as the authority over IT policy and DHS-wide programs.

- DHS Delegation 04000, *Delegation to the Chief Information Officer*, April 2018, delegates department-wide responsibility to the CIO for the approval, management, and oversight of the Department's IT resources.

- DHS Directive 262-09, *Enterprise Information Technology Service Management*, May 2017, establishes policy for the DHS CIO and components to leverage enterprise IT services where appropriate.

- DHS Directive 138-03, *Information Technology Asset Management and Refresh*, March 2018, provides policy regarding IT management to ensure IT infrastructure assets are secure, trustworthy, efficient, and resilient in support of missions and business operations.

However, during the past 9 years, we have issued at least 10 reports on DHS' ongoing challenges with information technology systems. In addition, we have reported all seven DHS' operational components rely heavily on outdated technology for increasingly complex mission operations. We emphasized the inherent consequences of DHS' dependence on numerous legacy IT systems in the following reports beginning in 2010:

- In 2010 and 2017, we reported ICE had not finalized its information technology strategic plan to ensure IT capabilities were aligned with

[6] Public Law 107-296, November 25, 2002

mission requirements. Further, ICE's legacy IT systems were not integrated to effectively support visa-tracking operations.[7]

- In 2011, we reported Coast Guard's aging systems and infrastructure were insufficient to support mission requirements and needed improvement.[8]
- In 2011, 2015, and 2018 we reported FEMA's IT infrastructure did not effectively support emergency disaster-response mission operations.[9]
- In 2011, we reported Secret Service had made progress in implementing a modernization program, but encountered challenges in reaching its objectives.[10]
- In 2013, we reported TSA CIO faced challenges in ensuring TSA's IT environment fully supported TSA's mission needs.[11]
- In 2014 and 2016, we reported USCIS struggled to modernize its stove-piped, paper-based immigration benefits processing to a more centralized and automated environment.[12]
- In 2017, we reported CBP's IT systems and infrastructure did not fully support its border security objectives. The slow performance of a critical pre-screening system reduced the ability to identify passengers who may have posed security concerns. Additionally, frequent system outages required CBP officers to rely on backup systems that weakened the screening process.[13]

[7] *Immigration and Customs Enforcement Information Technology Management Progresses But Challenges Remain*, OIG-10-90, May 28, 2010; *DHS Tracking of Visa Overstays Is Hindered by Insufficient Technology*, OIG-17-56, May 1, 2017

[8] *Coast Guard Has Taken Steps to Strengthen Information Technology Management, but Challenges Remain*, OIG-11-108, September 7, 2011

[9] *Federal Emergency Management Agency Faces Challenges in Modernizing Information Technology*, OIG-11-69, April 1, 2011; *FEMA Faces Challenges in Managing Information Technology*, OIG-16-10, November 20, 2015; *Management Alert – Inadequate FEMA Progress in Addressing Open Recommendations from our 2015 Report, "FEMA Faces Challenges in Managing Information Technology" (OIG-16-10)*, OIG-18-54, February 26, 2018

[10] *U.S. Secret Service's Information Technology Modernization Effort (Redacted)*, OIG-11-56, March 15, 2011

[11] *Transportation Security Administration Information Technology Management Progress and Challenges*, OIG-13-101, June 24, 2013

[12] *U.S. Citizenship and Immigration Services Information Technology Management Progress and Challenges*, OIG-14-112, July 3, 2014; *USCIS Automation of Immigration Benefits Processing Remains Ineffective*, OIG-16-48, March 9, 2016

[13] *CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations*, OIG-17-114, September 28, 2017

Likewise, GAO reported in 2019 the need to develop IT modernization plans to address critical legacy systems across the Federal Government.[14] Specifically, GAO found many legacy IT systems had unsupported hardware and software and were operating with known security vulnerabilities. GAO reported that without complete modernization plans, agencies will be at an increased risk of cost overruns, schedule delays, and project failures. GAO recommended Federal agencies identify and document modernization plans for legacy systems, including milestones, a description of the work necessary, and details on the disposition of legacy systems.

During the last 10 years, an increasing number of initiatives and legislation have established IT modernization as a top priority across the Federal Government. Notably, the *Modernizing Government Technology Act* was enacted as part of the FY 2018 *National Defense Authorization Act* and called for agencies to modernize IT systems to mitigate existing operational and security risks. The Act also established the Technology Modernization Fund, authorizing up to $250 million in appropriations for each of fiscal years 2018 and 2019 for Federal technology modernization projects. Specifically, this Act authorizes agencies to establish IT modernization and working capital funds to:

- improve, retire or replace existing IT systems to enhance cybersecurity and increase efficiency and effectiveness;
- transition legacy IT systems to commercial cloud computing and other innovative commercial platforms and technologies, including consolidating services across multiple agencies; and,
- assist and support efforts to provide adequate, risk-based, cost-effective IT capabilities that address evolving cybersecurity threats.

Additionally, the following recent legislation and initiatives play a key role in promoting IT modernization and accountability for CIO's across the Federal Government:

- IT Dashboard: The Office of Management and Budget (OMB) requires performance updates and supporting data for major IT investments to be published on the IT Dashboard, which was launched in 2009.[15] The IT Dashboard displays agency CIO evaluations and data from agency IT

[14] *Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-471, June 2019

[15] *Open Government Directive,* December 8, 2009, required Federal agencies to comply with reporting requirements for the IT Dashboard, launched on June 1, 2009 (https://www.itdashboard.gov/). IT investments are determined to be a major investment if the investment has significant program or policy implications; has high executive visibility; has high development, operating, or maintenance costs; or requires special management attention because of its importance to the mission or function of the agency.

Portfolio and Business Case reports to provide the public the ability to track Federal IT investments over time.

- *Federal Data Center Consolidation Initiative*: The OMB established this initiative in 2010 to reduce redundancy and inefficiency among the growing number of data centers across the Federal Government.[16]

- *25-Point Implementation Plan to Reform Federal Information Technology Management*: The Federal CIO implemented this initiative in 2010 to improve IT acquisitions and operational efficiencies, and to deliver more IT value to the taxpayer.[17]

- The *Federal Information Technology Acquisition Reform Act* (FITARA): This legislation, passed in December 2014, mandated the agency CIO oversee information technology investments to help find opportunities for IT efficiencies.[18]

- *Data Center Optimization Initiative*: This 2016 initiative requires agencies to optimize and consolidate data centers to deliver better services to the public while increasing return-on-investment to taxpayers. Specifically, agencies are instructed to consolidate and close existing data centers and transition to shared services and cloud technology. A 2019 update to the *Data Center Optimization Initiative* established targets, metrics, and requirements for agencies to report progress to OMB.[19]

- *Executive Order Enhancing the Effectiveness of Agency CIOs*: In 2018, the President issued this order emphasizing the power of agency CIOs to ensure agency IT systems are secure, efficient, accessible, and effective, and to modernize IT infrastructure.[20] Each agency is required to take necessary and appropriate action to ensure the CIO reports directly to the agency head and serves as the primary strategic advisor for all IT matters. This will better position agencies to modernize IT systems and execute IT programs more efficiently.

- OMB's *Federal Cloud Computing Strategy*: OMB published this long-term strategy in June 2019 to accelerate agency adoption of cloud-based

[16] Federal CIO Memorandum, *Federal Data Center Consolidation Initiative,* February 26, 2010

[17] Federal CIO, *25-Point Implementation Plan to Reform Federal Information Technology Management*, December 9, 2010

[18] Public Law 113-291, December 19, 2014

[19] *Data Center Optimization Initiative*, August 1, 2016 and *Update to Data Center Optimization Initiative*, June 25, 2019

[20] *Executive Order Enhancing the Effectiveness of Agency Chief Information Officers*, May 15, 2018

solutions.[21] This cloud strategy will support agencies in achieving additional savings, security, and will deliver faster services.

We conducted this audit to determine whether DHS has effectively identified and prioritized mission-critical legacy IT systems and infrastructure for modernization; to identify major challenges and operational impact associated with using and modernizing out-of-date IT; and to assess how recent legislation and executive direction may help to address these challenges.

Results of Audit

The DHS CIO, and most component CIOs, conducted strategic planning activities to help prioritize legacy IT systems or infrastructure for modernization to better accomplish mission goals. The DHS 2019–2023 IT strategic plan included two distinct department-wide IT modernization initiatives: to adopt cloud-based computing and to consolidate data centers. However, not all components have complied or fully embraced these efforts due to a lack of standard guidance and funding. Without consistent implementation of these efforts, DHS components remain hindered in their ability to provide personnel with more enhanced, up-to-date technology.

In the meantime, DHS continues to rely on deficient and outdated IT systems to perform mission-critical operations. We identified three legacy IT systems with significant operational challenges that negatively affected critical DHS functions, such as human resources and financial management, as well as disaster recovery mission operations. DHS has not made sufficient progress in replacing or augmenting these IT systems due to ineffective planning and inexperience in executing complex IT modernization efforts. Additionally, the DHS CIO has not performed mandated oversight of legacy IT to mitigate and reduce risks associated with outdated systems. Until DHS addresses these issues, it will continue to face significant challenges to accomplish mission operations efficiently and effectively.

DHS has not yet leveraged the *Modernizing Government Technology Act* to accelerate its IT modernization efforts. DHS and its components questioned whether the benefits of the Act outweighed the additional effort needed to use the resources the Act provided. Without pursuing such funding, DHS may be further hindered in accomplishing its objective of reducing reliance on outdated, legacy IT.

[21] OMB's *Federal Cloud Computing Strategy*, June 24, 2019; The term "cloud" is used broadly in the Federal Government for any technology solution provided by an outside vendor.

DHS Made Progress to Identify and Prioritize Legacy IT for Modernization, but Implementation Needs Improvement

The DHS CIO and component CIOs met Federal mandates to develop IT strategic plans, analyze legacy IT infrastructure requirements, and identify modernization needs. The DHS CIO's 2019–2023 IT strategic plan included two major modernization initiatives: to adopt cloud-based computing and consolidate data centers. However, DHS and its components have made varied progress in completing these efforts due to a lack of standard guidance and funding. Without more consistent implementation of these department-wide modernization efforts, DHS components may not realize the intended benefits of the cloud technology and consolidation.

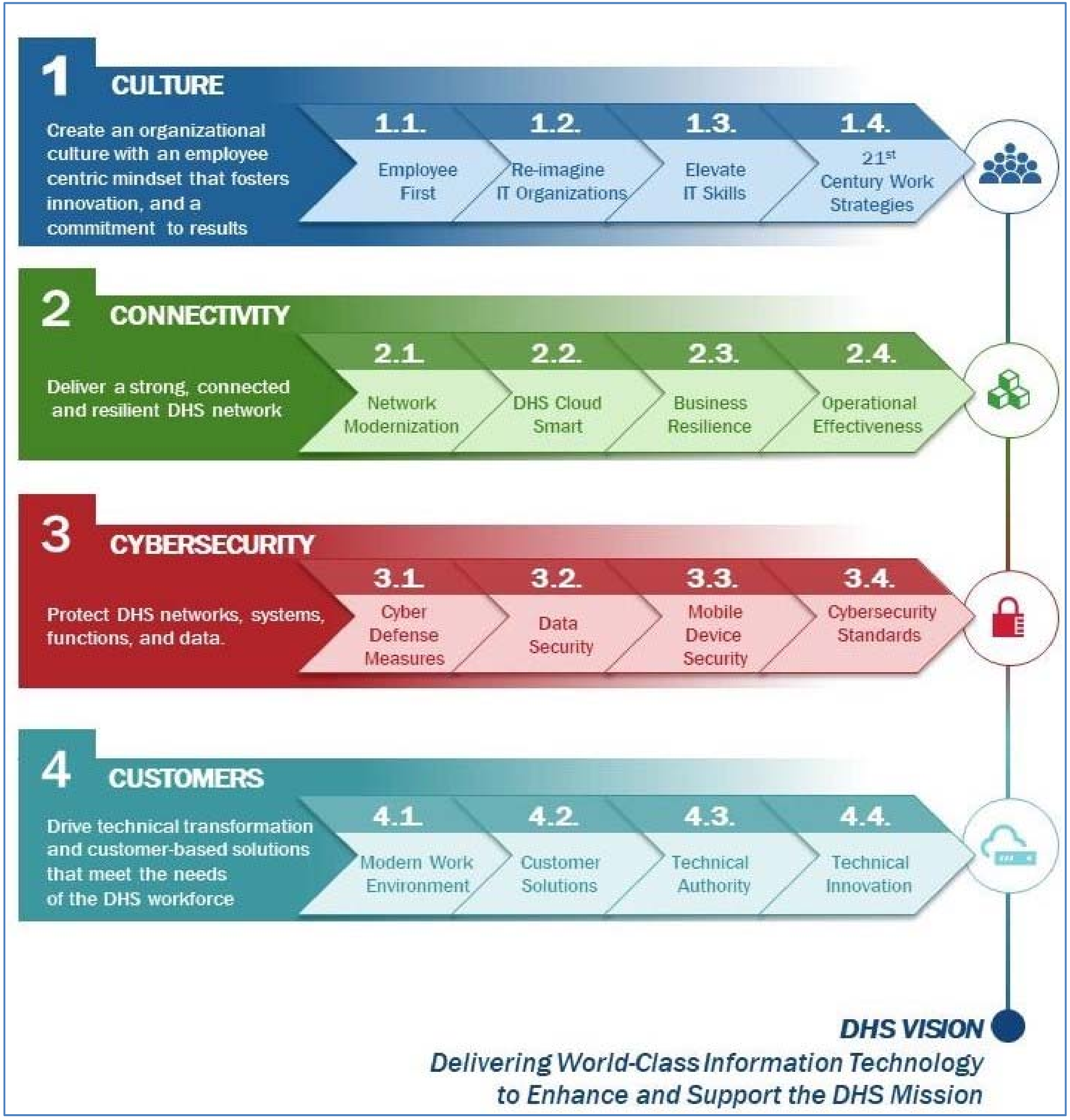
Strategic Planning Conducted to Identify IT Modernization Priorities

Federal agency CIOs are required to conduct strategic planning to identify and document how IT will be used to effectively accomplish the agency's mission. The *Government Performance and Results Act Modernization Act of 2010* holds Federal agencies responsible for strategic planning to ensure efficient and effective operations and use of resources to achieve mission results.[22] As stated in this guidance, the strategic plan should define the agency mission, long-term goals, planned strategies, and approaches it will use to monitor progress in addressing specific problems, needs, challenges, and opportunities related to its mission. Additionally, the *Clinger Cohen Act of 1996* instructs agency CIOs to create strategic plans that demonstrate how information resources will be used to improve the productivity, efficiency, and effectiveness of Government programs.[23]

To accomplish these mandates, the DHS CIO published the FYs 2019–2023 IT Strategic Plan in March 2019. The DHS IT Strategic Plan identifies an IT vision to "deliver world class IT to enhance and support the DHS mission." To do this, the plan includes four goals focusing on rebuilding foundations and driving innovation by outlining specific objectives and IT improvement initiatives. Figure 2 depicts the four goals in the DHS IT Strategic Plan.

[22] Public Law 111-352, January 4, 2011
[23] Public Law 104-106, February 10, 1996

Figure 2. DHS IT Strategic Plan Goals


1 CULTURE
Create an organizational culture with an employee centric mindset that fosters innovation, and a commitment to results
1.1. Employee First
1.2. Re-imagine IT Organizations
1.3. Elevate IT Skills
1.4. 21st Century Work Strategies
2 CONNECTIVITY
Deliver a strong, connected and resilient DHS network
2.1. Network Modernization
2.2. DHS Cloud Smart
2.3. Business Resilience
2.4. Operational Effectiveness
3 CYBERSECURITY
Protect DHS networks, systems, functions, and data.
3.1. Cyber Defense Measures
3.2. Data Security
3.3. Mobile Device Security
3.4. Cybersecurity Standards
4 CUSTOMERS
Drive technical transformation and customer-based solutions that meet the needs of the DHS workforce
4.1. Modern Work Environment
4.2. Customer Solutions
4.3. Technical Authority
4.4. Technical Innovation
DHS VISION
Delivering World-Class Information Technology to Enhance and Support the DHS Mission

Source: DHS FY 2019–2023 IT Strategic Plan documentation

As part of Goal #2 "Connectivity," the plan includes four Department objectives to accomplish key modernization initiatives:

- Network Modernization – to simplify network management and deliver high quality performance that ensures information flows smoothly across all DHS missions and devices.

- DHS Cloud Smart – to develop a plan of action for migration to a safe and secure cloud network that aligns with the OMB Cloud Smart strategy.

- Business Resilience – to optimize the reliability of the DHS network.

- Operational Effectiveness – to develop policy, modernize standards, and introduce digital business solutions to enable optimal IT service delivery.

In order to inform its broader agency-wide modernization planning efforts and to meet Federal mandates, the DHS OCIO initiated an effort called the "IT Infrastructure Study" in October 2016 to help provide a centralized approach to gather IT infrastructure data and establish performance measures across the Department. The DHS OCIO used the information gathered from these studies to define IT performance standards, assess risks, and develop plans to reduce long-term risks.

A DHS OCIO official said the Business Management Office is responsible for completing the IT Infrastructure Study annually. The office conducts this analysis by collecting data on IT infrastructure and systems from each operational component. These studies have expanded each year to include additional infrastructure used to support systems across the Department. For example, when the study first started in 2016, it included infrastructure used to support 134 systems. In comparison, the most recent 2018 study encompassed infrastructure supporting 580 systems and cloud migration for 456 systems. Examples of content from each study include:

- IT Infrastructure Study of FY 2016 – Evaluated upgrades needed to refresh and sustain infrastructure that supports 134 mission essential systems. The study implemented a scorecard to identify priorities for refresh and sustainment.

- IT Infrastructure Study of FY 2017 – Assessed 256 systems and cataloged the DHS IT Infrastructure Portfolio, defined common IT performance standards, and assessed the current state and risks of the IT infrastructure. DHS OCIO used this information to develop IT infrastructure management approaches and inform funding decisions.

- IT Infrastructure Study of FY 2018 – Assessed the IT infrastructure supporting 580 systems to recommend investment needed for older or at risk equipment. The study also provided technical and business cost data analysis to help accelerate cloud migration for 456 systems.

To ensure strategic planning activities are conducted across the Department, DHS issued a directive in 2018 to require component-level CIOs to develop, implement, and maintain IT strategic plans annually.[24] The component IT strategic plans should directly align to current department-wide strategic goals and objectives for supporting DHS mission operations. To identify IT modernization needs that best support mission goals and activities, IT strategic plans are critical for DHS components with aging and overly complex IT environments.

We found that most component CIOs complied with this requirement by developing IT strategic plans to assist in prioritizing IT modernization efforts. Five of seven DHS operational components developed IT strategic plans in the past year.[25] For example, CBP developed an IT Modernization Plan in October 2018 focused on modernizing its IT applications, infrastructure, and data management capabilities. ICE, Coast Guard, USCIS, and Secret Service also developed IT strategic plans in the past 2 years that identified overarching IT modernization plans to help enhance mission capabilities. Although FEMA and TSA did not develop separate IT strategic plans within this timeframe, leadership within both components recently documented broad component-wide strategic goals that contained IT related initiatives.[26]

Implementation of Key Modernization Initiatives Has Been Inconsistent Due to Inadequate Guidance, Funding, and Incentive

While DHS and most operational components maintained documented plans to identify and prioritize IT modernization requirements, the key modernization efforts identified in the 2019–2023 DHS IT Strategic Plan are not being effectively implemented across the Department. Specifically, Goal #2 outlined 4 key objectives and 16 priority focus areas, some of which are also mandated government-wide. Notably, the DHS CIO outlined initiatives in the 2019–2023 IT Strategic Plan to accomplish cloud migration and optimize DHS data centers. However, DHS components have been slow to achieve these IT modernization goals, due in part to a lack of standard guidance and funding.

Migrating DHS IT Systems to the Cloud

OMB's *Federal Cloud Computing Strategy* requires Federal agencies to regularly evaluate and update applications and migrate them to the cloud as needed to reduce risks and better allocate resources. Additionally, the strategy requires Federal agencies to evaluate their IT portfolios in order to drive cloud adoption to reduce unnecessary redundancy and obsolete IT applications. The strategy defines cloud computing as solutions exhibiting five essential characteristics:

[24] DHS Directive 142-02 Rev. 01, *Information Technology Integration and Management*, April 12, 2018

[25] CBP, ICE, Coast Guard, USCIS, and Secret Service developed IT Strategic Plans for Fiscal Years 2018, 2018–2021, 2020–2025, 2019–2024, and 2018–2023, respectively.

[26] *2018–2022 Strategic Plan, Federal Emergency Management Agency; TSA Strategy, 2018–2026*

on-demand service, broad network access, resource pooling, rapid elasticity, and measured service. The benefits of cloud-based technology include lower maintenance costs and increased capacity to meet IT requirements. For example, migration to cloud-based applications will reduce the amount of on-premises IT infrastructure, such as servers, required to support departmental operations.

As part of the 2019–2023 DHS IT Strategic plan, IT Strategic Goal #2 represents the OCIO's commitment to the adoption of cloud technology. Objective 2.2 outlines DHS' "Cloud Smart" approach for adopting a plan for migration to a safe and secure cloud network that aligns with the OMB Cloud Smart strategy proposal. To execute this plan, the DHS OCIO established a goal to migrate approximately 30 percent of components' IT systems to the cloud. The OCIO coordinated with each of the seven operational components to establish specific goals for the number of component-owned systems that should be migrated to the cloud by the end of the first quarter of 2019. Secret Service did not commit to migrating any of its systems to the cloud, and thus did not have a specific goal established by the DHS OCIO. The remaining six components signed "Cloud Commitment Memorandums" that were established by the DHS OCIO to outline the terms and the number of systems agreed upon by each component.

As of April 2019, each of DHS' six operational components (excluding Secret Service) were in various stages of investing and migrating their systems to the cloud. Specifically, six components had met the DHS OCIO's cloud migration goals, while Secret Service performed its own internal evaluation and determined that it would not commit to migrating any of its systems to the cloud. Table 1 shows cloud migration goals and progress by each component.

Table 1. System Cloud Migration Goals and Results (Q1 CY 2019)

Component	Total Systems	Cloud Migration Goal for Q1 CY 2019	Systems Using or Adopting Cloud as of April 2019	Achieved Goal
CBP	120	27	47	Yes
FEMA	105	19	34	Yes
ICE	65	38	48	Yes
TSA	78	24	38	Yes
Coast Guard	64	4	5	Yes
USCIS	40	28	30	Yes
Total	**472**	**140**	**202**	

Source: DHS OCIO Business Management Office

Although migration goals were met, DHS has struggled to ensure systems remain operational at the same level of performance in the cloud. The majority of the component system migrations completed thus far are classified as "lift and shift," meaning the systems are being migrated to the cloud as-is, without taking steps to conduct specific modernization efforts which may be needed to optimize system performance and functionality in the new cloud environment. This approach has resulted in systems not being configured to maximize the benefits of cloud technology, which can negatively impact performance and stability. To illustrate, at the time of this audit, DHS officials reported approximately 41 percent of the seven operational components' systems were migrated to the cloud; but, only about 24 percent of these systems were actually operational in the cloud. Table 2 provides the number of migrated component systems that are actually operational in the cloud.

Table 2. Migrated Systems Operational in the Cloud as of April 2019

DHS Component	Systems Using or Adopting Cloud	Number of Operational Systems in the Cloud
CBP	47	13
FEMA	34	9
ICE	48	10
TSA	38	6
Coast Guard	5	1
USCIS	30	10
Secret Service	0	0
Total	**202**	**49**

Source: DHS OCIO Business Management Office

DHS' challenges in cloud migration stems from inadequate departmental guidance regarding cloud implementation activities. Specifically, DHS has not developed detailed guidance or best practices on how to mitigate performance risks or manage potential enterprise-wide challenges associated with cloud migration. For example, "lift and shift" cloud migrations add complexity to cybersecurity, as these systems may not adhere to specific standards and technical controls needed to meet security and operational requirements.

The DHS OCIO anticipates that if the Department continues its current cloud migration effort in the same manner, DHS will likely be faced with increased complexity, operational costs, and instability. The DHS OCIO also recognizes the need to further document and standardize technical processes and mission support metrics for cloud migration. To address these concerns, DHS established a Cloud Steering Group in May 2018 that is focused on implementing a more comprehensive cloud environment across the Department.

DHS Data Center Consolidation

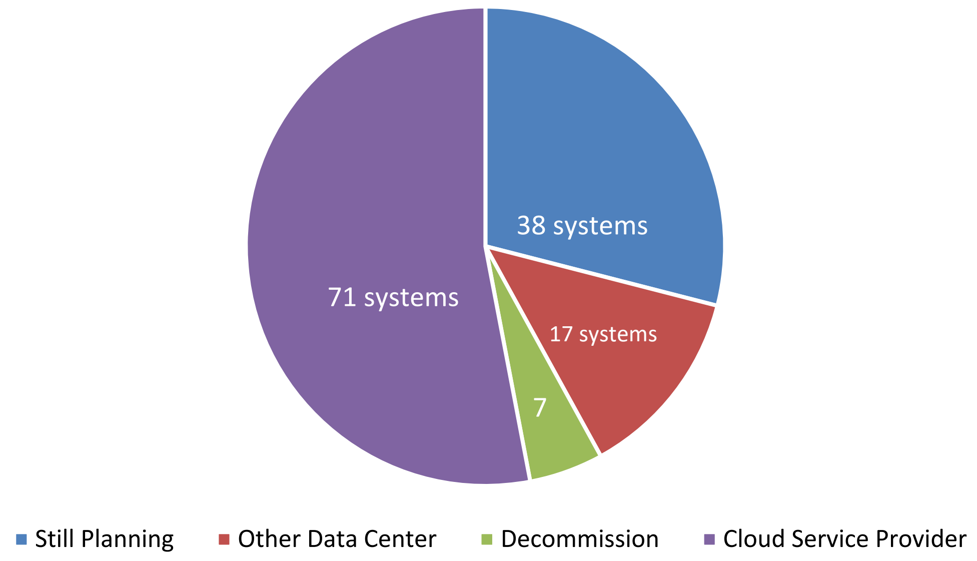
Adoption of shared data centers promotes greater collaboration and standardization, reducing physical footprint and reliance on distributed legacy IT infrastructure. As part of DHS IT Strategic Goal #2, the OCIO has prioritized the consolidation of its data centers to meet Federal mandates, such as FITARA. DHS established two enterprise data centers: Data Center 1 (DC1) at Stennis Space Center, Mississippi, and Data Center 2 (DC2) in Clarksville, Virginia. DHS recently optimized its DC1 facility, but faces challenges executing its current plan to vacate the DC2 location.

DHS OCIO made progress optimizing its existing enterprise data centers at DC1 by reducing its footprint in the Stennis facility. DHS vacated DC1 zones A and B by accelerating migration to the cloud for specific applications. OCIO officials reported the Department's continued implementation of cloud-based applications has reduced the amount of on-site IT infrastructure required at DC1, such as physical email servers.

According to DHS, modernizing network components at DC1 has improved overall network stability, connection, and security. An OCIO official stated network availability has benefited from the modernized network components installed at DC1. As of March 2019, the OCIO had modernized DC1 network components by replacing approximately 300 legacy IT hardware elements such as routers and switches. DHS reported its network service uptime availability, an indicator of overall reliability in providing continuous service to personnel on the network, was at 99 percent.

Although DHS OCIO made progress at DC1, it struggled to consolidate and optimize its DC2 facility in Clarksville, Virginia, as planned. Systems hosted in DC2 are required to migrate to a new hosting environment by June 2020, due to impending expiration of DHS' contract with its DC2 vendor. OCIO hopes to accomplish this goal through its ongoing cloud migration efforts, converting IT systems from a server environment to an internet-based platform. As of summer 2018, DHS planned to migrate 53 percent of component systems supported at DC2 to the cloud. However, OCIO officials expect 25 percent of DC2 systems may not meet the June 2020 target date to vacate DC2. The status of the DC2 system migration-plan as of summer 2018 is outlined in figure 3.

Figure 3. Plans for DC2 System Migration – as of Summer 2018



Source: DHS

DHS OCIO reported DC2 migration challenges stem from a lack of funding and the complexity of the move. Although DHS OCIO is coordinating the overall effort, components must identify their own funding to complete system migrations. In March 2019, 79 percent of DHS DC2 occupants identified a lack of funding as a challenge to vacate by the required deadline.

DHS OCIO stated the need to consider each system's unique operational requirements for migration increases the overall complexity of planning the move to meet the June 2020 DC2 evacuation deadline. Such complexity makes it difficult for components to develop an effective strategy for system migration that can be completed in less than 1 year. As of summer 2018, DHS officials had not yet developed transition plans for 29 percent of the systems affected by the DC2 evacuation.

Lastly, some Department officials said that historically they have favored hosting their own IT systems in-house rather than moving them to DHS-shared data centers. For example, one component official expressed reluctance to invest the necessary time and money required to move systems due to the lack of long-term vision and potential benefits for DHS data centers and cloud-based computing.

Inconsistent Implementation of Modernization Initiatives Increases Costs and Poses Operational Risks

DHS' inconsistent migration of systems to the cloud may increase the likelihood of incurring higher implementation and maintenance costs and disruption to IT services. Further, DHS' current "lift and shift" approach to cloud migration may potentially increase the Department's overall costs in maintaining its systems. At the time of this audit, DHS had not conducted a formal study to determine the specific costs resulting from its current implementation approach. However, OCIO provided an industry example that determined lift and shift cloud migration can potentially increase costs by up to 22 percent for migrating 105,000 servers and 20 terabytes of data to the cloud. By comparison, taking steps to modernize systems before cloud migration would have reduced backend IT costs by 36 percent. Additionally, DHS OCIO identified industry examples that reduced IT overhead costs by 30 to 40 percent by fully embracing modern cloud-native architectures rather than migrating IT systems in their existing platforms without modification.

DHS' decentralized approach for migrating systems to the cloud has resulted in varying approaches and timelines for cloud migration and increases the risk that the Department does not receive the intended benefits of cloud technology, including:

- removal of fixed costs (i.e., data centers) and other liabilities associated with operating and refreshing government-owned infrastructure and other assets;
- increased efficiency, resiliency, agility, and speed through automation;
- improved business process reengineering and optimized resource utilization; and
- timely and effective mission and administrative decision support.

Moreover, DHS officials reported they face increased risk of business disruption if Data Center 2 systems are not migrated by the required June 2020 deadline. This may result in systems being temporarily unavailable or operating at reduced capacity, negatively affecting the Department's mission capabilities. Additionally, DHS' lack of planning for its DC2 migration may force components to migrate systems to temporary, non-enterprise IT solutions to avoid systems disruptions if the June 2020 deadline cannot be met. Migrating systems to temporary or non-enterprise solutions could potentially require systems to be migrated more than once, unnecessarily increasing costs and wasting personnel resources.

By not appropriately planning and executing these major, department-wide modernization efforts, DHS components remain hindered in their ability to provide personnel with more enhanced, up-to-date technology. In turn, the Department remains dependent on costly and maintenance-challenged legacy IT to perform its mission operations.

DHS Has Not Reduced Its Dependency on Legacy Technology

While DHS established a strategic objective in its 2019–2023 strategic plan to reduce dependency on legacy technology, it continues to rely on deficient and outdated IT systems to perform mission critical operations. We identified three legacy IT systems with significant operational challenges negatively affecting critical DHS functions, such as human resources and financial management, as well as disaster recovery mission operations. DHS has not made sufficient progress in replacing or augmenting these legacy IT systems due to ineffective planning and inexperience in executing complex and broadly scoped modernization efforts. Additionally, the DHS CIO has not performed mandated oversight of all legacy IT to mitigate and reduce risks associated with outdated systems. Until DHS addresses these issues, the Department will continue to face significant risks of legacy IT system deficiencies threatening mission operations and system security.

Components Rely on Outdated IT Systems for Critical Mission Functions

DHS personnel require adequate, up-to-date IT systems to support their critical mission operations. According to the 2018 *Executive Order Enhancing the Effectiveness of Agency Chief Information Officers,* CIOs are empowered to modernize IT infrastructure, improve IT management and oversight, and ensure agency IT systems enable missions.[27] Yet, DHS' IT environment includes numerous outdated IT systems that lack key functionality to support its vast mission operations.

Based on our review of DHS component IT system documentation, we identified three legacy IT systems with significant operational challenges negatively affecting critical DHS mission operations including human resources, financial management, and disaster recovery, as shown in table 3.

[27] *Executive Order Enhancing the Effectiveness of Agency CIOs*, May 15, 2018

Table 3. At Risk Legacy IT Systems

IT System	Purpose	Age of System (years)
(1) DHS-wide Human Resources IT (HRIT)	Facilitates the hiring, training, servicing, evaluation, and improvement of DHS' workforce.	17
(2) DHS Legacy Major IT Financial System[28]	Serves as Coast Guard and TSA's financial system of record.	21
(3) FEMA Grants Management Mission Domain and Operational Environment	Facilitates the awarding of Federal assistance and grants for disaster-related events.	Up to 22

Source: DHS IT system documentation

DHS-wide Human Resources System

DHS employs more than 240,000 staff across 14 components, and currently relies on more than 120 disparate HRIT systems to hire, train, and service its workforce. The DHS Office of the Chief of Human Capital (OCHCO) was unable to provide a complete inventory of all legacy HRIT systems during this audit, but we determined there are approximately 124 legacy human resources IT programs across the Department. Some of the legacy HRIT systems were at least 17 years old, pre-dating the creation of DHS in 2002.[29] However, despite DHS' repeated efforts over the past decade, or more, to modernize its Human Resources IT environment, its systems remain fragmented, with distinct capabilities performed by separate legacy systems. This environment does not allow for department-wide information gathering or reporting to inform programmatic decisions. Currently, reporting and analyzing enterprise human capital data are time-consuming, labor-intensive, and challenging because the Department's data management largely consists of disconnected, standalone systems, with multiple data sources for the same content.

The DHS OCHCO intends to modernize these systems through the HRIT investment. DHS initiated the HRIT effort in 2003 to consolidate, integrate, and modernize the human resources IT infrastructure across all components. However, the date for completing these efforts has continued to be pushed out due to delays. To illustrate, DHS initially estimated HRIT modernization would be completed in 2016, but subsequently changed the completion date to FY 2032. At the time of this audit, DHS had actually removed the completion date

[28] Our audit scope included the Core Accounting System, DHS' only legacy IT financial system classified as a major IT investment.
[29] The 17-year-old age estimate is based on documentation of legacy HRIT systems that existed when 22 agencies merged to form DHS in 2002.

all together. Rather than set a date to integrate and modernize the entire portfolio of HRIT systems, the Department decided to prioritize HRIT systems most in need of modernization and set completion dates for these specific systems. DHS does not currently have a date when all HRIT systems will be modernized.

Further, in a 2016 internal memo, the DHS OCIO reported the Department's HRIT investment priorities were not well-developed due to the complexity and broad scope of business requirements across the Department. DHS OCIO officials indicated without adequate IT system priorities to guide HRIT modernization, the overall modernization effort became misaligned with the Department's strategic goals. This misalignment resulted in DHS OCIO developing an ineffective HRIT modernization plan and the investment priorities being restructured in 2017.

To address previous challenges in defining HRIT's priorities and outcomes, DHS recently returned the program to the OCHCO and reprioritized areas where improvement was possible. Specifically, the Department transferred responsibility for DHS IT system modernization from the OCIO to OCHCO, which is responsible for the Department's human resources systems, policies and programs, to improve oversight of ongoing modernization efforts. Additionally, the OCHCO reduced the number of strategic improvement opportunities and organized them into 14 categories.[30] OCHCO advised that the Department plans to continue to rely on legacy IT until the strategic improvement opportunities are completed and DHS' human resource IT capabilities have been modernized. Until HRIT modernization is completed, the Department will continue to rely on disparate and fragmented systems for performing critical HR functions such as workforce data gathering and reporting.

DHS Financial Management System

Two DHS components rely on a 21-year-old Core Accounting System (CAS), which serves as the Coast Guard's and TSA's official financial system of record. The CAS is DHS' only legacy IT financial system designated as a major investment. This designation is intended to place special emphasis on the system's importance to DHS' overall mission. However, despite its importance, the CAS has presented the Coast Guard with numerous challenges. Most

[30] The 14 Strategic Improvement Opportunities are as follows: Position Classification and Position Management; Talent Acquisition Management; Applicant Screening, Reciprocity and Investigation Request; New Hire in Processing and Onboarding; Talent Development and Training; Employee Performance Management; Compensation Management; Retirement Planning and Processing; Out Processing and Off Boarding; Administrative Grievances and Third Party Proceedings; Labor Management Relations; Workforce and Performance Analytics; Workforce and Performance Reporting; and Personnel Action Request Processing.

concerning, Coast Guard reported it expects vendor support for security patches to end in December 2020.[31] Due to security concerns, Coast Guard was required to obtain a waiver in lieu of an Authority to Operate[32] on the Coast Guard network. In addition to security vulnerabilities, the system does not provide required functionality to meet evolving mission needs within Coast Guard. For example, the system cannot be updated to meet DHS accounting classification structure changes, increasing the risk financial transactions are not recorded accurately.

Although DHS has made CAS modernization a priority, efforts to do so dating back to 2013 have been unsuccessful. DHS established an interagency agreement with the Department of the Interior in 2013 to act as a Federal Shared Service Provider to modernize the CAS.[33] Despite a $122 million investment, DHS terminated the project in July 2017 due to challenges with the Department of Interior managing a modernization effort of this size and complexity properly. DHS established a new effort, the Financial Systems Modernization (referred to as TRIO) in 2017, to replace the CAS. At the time of this audit, the estimated completion year of this effort was September 2021.

Amid the ongoing challenges in modernizing DHS-wide human resource and accounting systems, the DHS CIO must maintain adequate oversight of its major IT investments, as federally mandated.[34] Namely, Federal agency CIOs are required to periodically evaluate and assign risk ratings to major IT investments.[35] Such oversight would be beneficial to proactively address the security concerns and technical challenges associated with relying on outdated systems for everyday functions. Per DHS' internal assessment schedule (dictated by FITARA), DHS should have conducted nine evaluations of HRIT and four evaluations of CAS between June 2018 and June 2019.[36] However, the DHS CIO only evaluated and assigned a risk rating to each system on one occasion, February 2019.

[31] *Core Accounting System Operational Analysis Report*, August 2018

[32] An information system must be granted an Authority to Operate (ATO) before it first becomes operational, and must be re-authorized at least every three years and whenever changes are made that affect the potential risk level of operating the system.

[33] The interagency agreement was established to modernize CAS and the financial systems of record for the Transportation Security Administration and the Countering Weapons of Mass Destruction Office.

[34] *Federal Information Technology Acquisition Reform Act* (FITARA) Public Law 113-291, December 19, 2014

[35] These assessments include assigning a score based on a rating scale of 1 to 5 to demonstrate overall risk.

[36] The DHS OCIO performs Program Health Assessments to help meet FITARA mandates. The rating schedules are "living schedules," meaning they may be reviewed more or less often depending on the results of the last review.

Until these mission-critical systems are updated, the Department may not be able to effectively recruit and retain the staff needed to perform vital missions. Additionally, DHS' reliance on legacy financial IT systems increases IT security risks, as the CAS vendor will end security patches in December 2020. Without vendor-provided security patches, DHS' network is at increased risk of malicious activity and network compromises. Coast Guard reported if DHS is unable to replace the CAS with a modernized system before 2021, the system could lose functionality, security, and reliability, resulting in business process disruptions for Coast Guard and its customers.

FEMA's Disaster Management Capabilities

FEMA has a primary mission to secure and manage the majority of Federal disaster and non-disaster-based financial assistance and grants. FEMA's current grants management IT portfolio is composed of nine systems. FEMA reported these systems are outdated, overly complex, and difficult to maintain.[37] Moreover, the multiple systems operate on multiple platforms, each utilizing different technologies that are non-standard and not integrated.

The current grants management IT portfolio's lack of integration with agency financial management capabilities and insufficient intuitive, user-friendly tools (business and systems) across regional and field operations has resulted in grants personnel developing a number of manual processes. For example, in a recent 2019 audit, the DHS OIG identified FEMA grants personnel had adopted a manual process to track grant event information, such as notifications to FEMA's comptroller office on funding allocations.[38] To ensure complete information on an individual grant, FEMA personnel had to continually monitor progress separately in multiple systems and manually notify stakeholders when additional actions were required because systems did not send out automated alerts. Duplicate IT capabilities and reliance on manual processes have increased costs and placed a significant administrative burden on FEMA disaster-support personnel and grant recipients.

Although FEMA initiated its Grants Management Modernization effort in October 2015 to modernize its disparate grant systems, the agency has faced challenges managing the project's cost and technical requirements. For example, in March 2019 FEMA reported it would exceed its cost estimate by $140 million due to FEMA's insufficient understanding of the project's scope and complexity, and inexperience in performing major modernization efforts. According to a 2019 GAO audit, FEMA has not yet fully established plans for

[37] FEMA Capability Development, January 29, 2016
[38] *FEMA's Longstanding IT Deficiencies Hindered 2017 Response and Recovery Operations*, OIG-19-58, August 27, 2019

implementing new business processes or established complete traceability of IT requirements.[39]

FEMA's continued reliance on its legacy grants management systems increases the risk critical funding needed to help communities and individuals recover from disasters may not be processed timely, potentially leaving disaster victims without vital assistance.

DHS Has Evaluated, but Not Leveraged the Modernizing Government Technology Act to Address IT Modernization Challenges

DHS has not yet leveraged the *Modernizing Government Technology Act* to accelerate its IT modernization efforts. DHS lacked authority to leverage one key benefit of the Act, and its components questioned whether the Act's other potential benefits outweighed the additional effort needed to use the resources. Without pursuing the Act's funding, DHS may be further hindered to accomplish its strategic objective of reducing reliance on legacy IT.

DHS Took Steps to Establish Internal Processes to Leverage the Modernizing Government Technology Act

The Act enables agencies to obtain funds from the Technology Modernization Fund (TMF) to improve or replace existing legacy IT.[40] The TMF provides agencies with an additional source of funding to pay for IT modernization projects. Specifically, Congress authorized a total of $250 million for each fiscal year in 2018 and 2019 for the TMF. While the Act encourages agencies to apply for funding to help reduce outdated or duplicative systems through modernization, agencies are required to repay the funding within 5 years. Additionally, the Act authorizes agencies to establish an IT working capital fund to improve and modernize legacy IT systems to improve security or system effectiveness. The IT Working Capital Fund (WCF) allows agencies to reprogram existing funds to fund IT modernization efforts and to reimburse the TMF for funding received.

OMB issued a memorandum in February 2018 identifying how the Act funding may be applied to modernization projects. This included guidance for submitting project proposals for consideration. For example, in preparing project proposals, agencies are encouraged to consider how the proposed projects could leverage commercial capabilities and industry best practices,

[39] *FEMA Grants Modernization: Improvements Needed to Strengthen Program Management and Cybersecurity,* GAO-19-164, April, 2019
[40] The Technology Modernization Fund is administered by the General Services Administration.

reduce outdated or duplicative systems, and deliver common solutions within agencies or with external partners.

Based on OMB's guidance, DHS OCIO performed actions to evaluate the Act's applicability and benefits. In August 2018, DHS OCFO provided the Department's leadership with the Act, OMB guidance, and the Deputy Under Secretary for Management's direction for implementing the Act. Additionally, the DHS CIO and CFO Councils proposed the establishment of the DHS' Information Technology Modernization Leadership Council. The mission and purpose of the council is to provide recommendations to DHS' Under Secretary for Management on Act proposals generated by DHS components and headquarters offices. At the time of our audit, the charter for the council was in draft and pending approval.

DHS took initial steps to leverage the Act's authorization to establish an IT WCF. However, according to one DHS OCIO official, the Department currently does not have transfer authority to repurpose expiring or lapsed appropriated funds into such a fund. While the Act authorizes the creation of an IT working capital fund, it does not grant transfer authority. DHS requested fund transfer authority for its FY 2019 budget in an attempt to leverage the Act.

DHS Component Officials' Uncertainty of the Modernizing Government Technology Act Benefits

Although Federal agencies may be able to obtain funding to modernize legacy IT through the Act, officials from multiple operational components had concerns related to the Act's benefits. Specifically, some officials expressed concerns over the Act's 5-year payback period for funds received. For example, at least three component OCIOs viewed the Act funding as a loan with unreasonable payback terms. At the time of our audit, CBP was the only component that was in the process of submitting a proposal for the Act's funding.[41]

Department officials' concerns over the Act's benefits resulted in the conclusion that the legislation was not an immediately attractive option for meeting modernization needs. Additionally, DHS officials advised that since the use of the Act's funding for IT modernization is optional, implementing new processes for non-mandatory legislation was a low priority. For example, we identified one component official who viewed leveraging the Act's processes to obtain additional funding as a lower priority than meeting requirements set forth by other Federal mandates and departmental policy such as network modernization.

[41] In May 2019, CBP was in the process of developing a proposal to modernize and integrate its Automated Commercial Environment Collections system.

Conclusion

DHS needs to overcome its longstanding IT deficiencies to ensure its technology systems and infrastructure support 24 x 7 mission-critical operations and timely response to evolving threats. To accomplish its mission efficiently and effectively, DHS must modernize its IT systems and infrastructure in line with key Federal mandates and guidance. DHS should also establish a concrete long-term vision for leveraging and gaining value from ongoing modernization efforts, such as cloud migration and data center optimization. Otherwise, the Department's strategic modernization initiatives may be ineffectively developed and executed, further increasing reliance on legacy IT and decentralized IT operations.

Without adequate progress in modernizing legacy IT, DHS personnel will remain dependent on outdated and unintegrated legacy systems, inadequate equipment, and manual workarounds to accomplish critical mission operations. Continued use of legacy IT systems also increases maintenance and operations costs. To the extent DHS is not able to access available IT modernization funding, the Department may continue to face difficult decisions on which modernization efforts to prioritize based on funds available. This may result in ongoing IT capability gaps that negatively affect the Department's ability to efficiently secure the Homeland.

Recommendations

Recommendation 1: We recommend the DHS OCIO develop department-wide guidance for implementing cloud technology and migrating legacy IT systems to the cloud.

Recommendation 2: We recommend the DHS OCIO coordinate with components to develop and finalize a data center migration approach to accomplish strategic goals for reducing the footprint of DHS IT infrastructure.

Recommendation 3: We recommend the DHS OCIO establish a process to assign risk ratings for major legacy IT investments, as required by the *Federal Information Technology Acquisition Reform Act.*

OIG Analysis of DHS Comments

We obtained written comments on a draft of this report from the Departmental GAO-OIG Liaison Office. In the comments, the Director, Departmental GAO-OIG Liaison Office, provided details on DHS' efforts to identify and prioritize mission-critical legacy IT systems and infrastructure for modernization. We have included a copy of the comments in their entirety in appendix B.

We reviewed DHS' comments, as well as the technical comments submitted by DHS under separate cover, and made changes to the report as appropriate. The Director, Departmental GAO-OIG Liaison Office, concurred with all of our recommendations. The following is our evaluation of DHS' response to our recommendations.

Recommendation 1: We recommend the DHS OCIO develop department-wide guidance for implementing cloud technology and migrating legacy IT systems to the cloud.

Management Comments

The Department concurred and stated that DHS is committed to adhering to the OMB's Cloud Smart strategy for migrating assets to a safe and secure cloud network. To achieve this goal, the DHS OCIO continues to coordinate with operational components to establish goals for system cloud migrations. The DHS OCIO established a department-wide Cloud Action Officer Forum to share best practices and guidance for implementing cloud technology and legacy IT system migrations. Furthermore, the DHS OCIO implemented its own cloud solution platform for cost-effective options for cloud migration. DHS OCIO requested this recommendation be considered closed and resolved, as implemented.

OIG Analysis

We recognize the DHS OCIO's efforts as positive steps toward addressing this recommendation. While the Cloud Action Officer Forum should help DHS share guidance and best practices for cloud technology, this recommendation will remain open until DHS has developed and disseminated department-wide guidance for implementing cloud technology and migrating legacy IT systems to the cloud. This recommendation is open and resolved.

Recommendation 2: We recommend the DHS OCIO coordinate with components to develop and finalize a data center migration approach to accomplish strategic goals for reducing the footprint of DHS IT infrastructure.

Management Comments

The Department concurred and stated that it continues to prioritize consolidation of its data centers and has taken steps to develop a coordinated approach to reducing the DHS IT infrastructure footprint. Specifically, DHS is managing components' progress in exiting DC2, for which the contract was set to expire on June 26, 2020, but a new contract was awarded through December 18, 2021. Additionally, the DHS OCIO is supporting components as they migrate IT systems from DC1 to cloud environments. DHS OCIO plans to transform legacy IT capabilities from an asset-based model to a service-based model to reduce the DHS infrastructure footprint. DHS OCIO requested this recommendation be considered closed and resolved, as implemented.

OIG Analysis

We recognize DHS OCIO's efforts to coordinate with components to develop and finalize data center migration and reduce the DHS IT infrastructure footprint. Due to the Department's ongoing efforts for vacating DC2 and the extension of the DC2 contract to December 2021, this recommendation will remain open until a finalized DC2 exit plan has been developed to demonstrate that DHS is on schedule to meet the updated timeline. This recommendation is open and resolved.

Recommendation 3: We recommend the DHS OCIO establish a process to assign risk ratings for major legacy IT investments, as required by the *Federal Information Technology Acquisition Reform Act*.

Management Comments

The Department concurred and stated that the DHS OCIO and Program Accountability and Risk Management determined the planned transition of the Risk Rating process for legacy IT programs to the Program Accountability and Risk Management's Acquisition Program Health Assessment was not feasible within the current organizational and resource constraints. As a result, DHS OCIO reconstructed its previous Risk Rating process, Program Health Assessments, to more accurately determine risk ratings for major legacy IT programs as mandated by OMB. Beginning in June 2020, DHS OCIO commenced submitting updated risk ratings for IT programs, including legacy programs, to the Federal IT Dashboard. The estimated completion date for this recommendation is September 30, 2020.

OIG Analysis

We recognize DHS OCIO's efforts to update risk ratings as a positive step toward addressing this recommendation. We look forward to receiving these plans following the anticipated September 30, 2020 completion date. This recommendation is open and resolved.

Appendix A
Objective, Scope, and Methodology

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107−296) by amendment to the *Inspector General Act of 1978*.

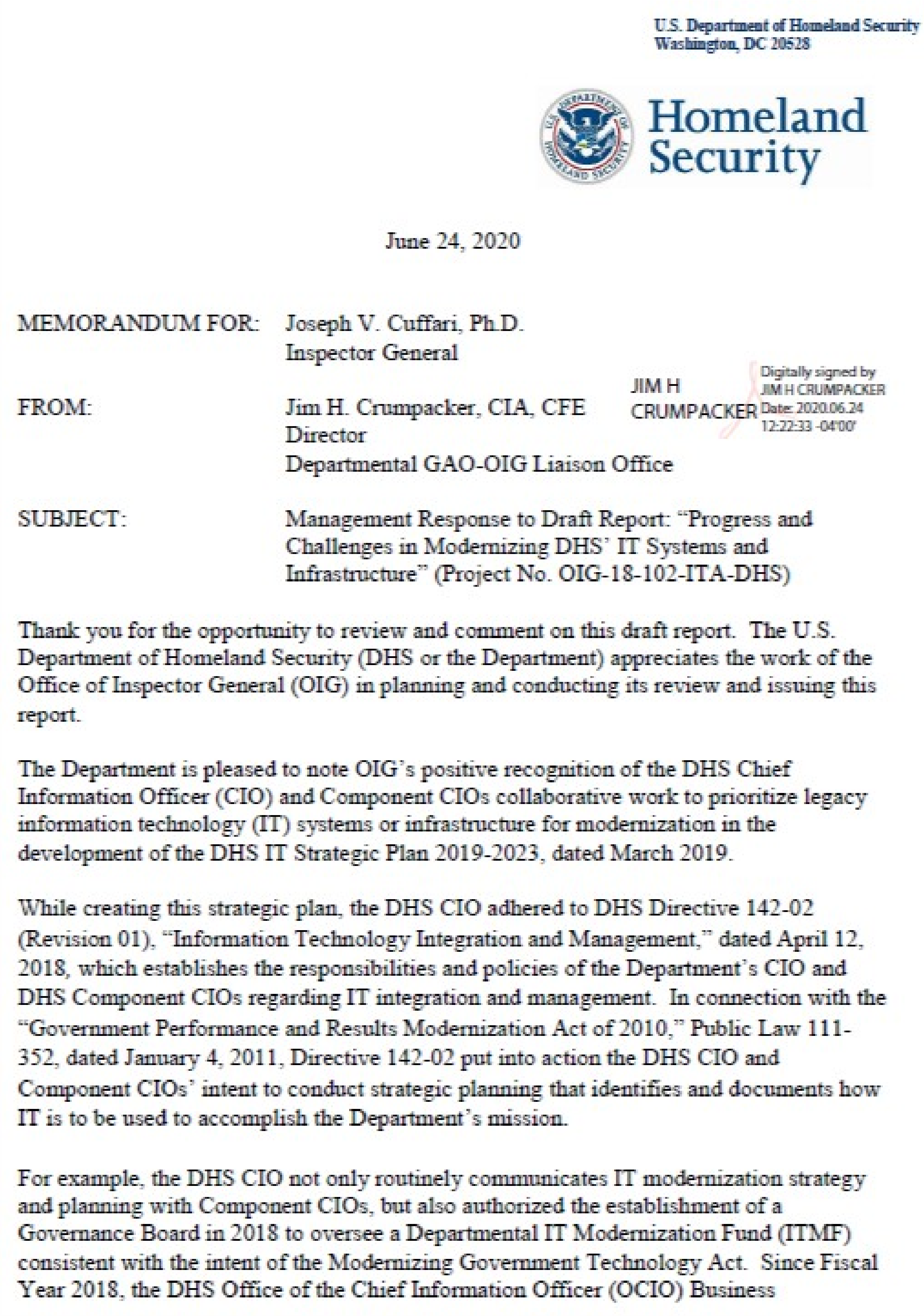
Our audit objectives were to determine whether DHS has effectively identified and prioritized mission-critical legacy IT systems and infrastructure for modernization, to identify major challenges and operational impact associated with using and modernizing out-of-date IT, and to assess how recent legislation and executive direction may help address these challenges.

To accomplish our audit objectives, we examined Federal, departmental, and agency criteria related to IT modernization, management, and oversight. We also obtained and analyzed published reports, testimonial transcripts, and prior GAO and DHS OIG audit reports related to IT modernization.

During our audit testing, we conducted more than 30 interviews of DHS OCIO, component OIT, and specific IT system management personnel to identify processes and information significant to our audit. We used our professional judgment to identify IT systems and infrastructure included in the scope of our audit testing. Specifically, we identified all 1) legacy major IT investments, 2) major IT modernization investments designed to address legacy IT gaps, and 3) significant legacy non-major IT investments related to ongoing modernization investments. For IT systems included in our audit scope, we reviewed risk assessments, gap analyses, operational analysis reports, acquisition documentation, and other IT system performance information. We did not use or rely on computer processed data for this audit.

We conducted this performance audit between July 2018 and April 2019 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

Appendix B
DHS Comments to the Draft Report



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

Homeland Security

June 24, 2020

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2020.06.24 12:22:33 -04'00'

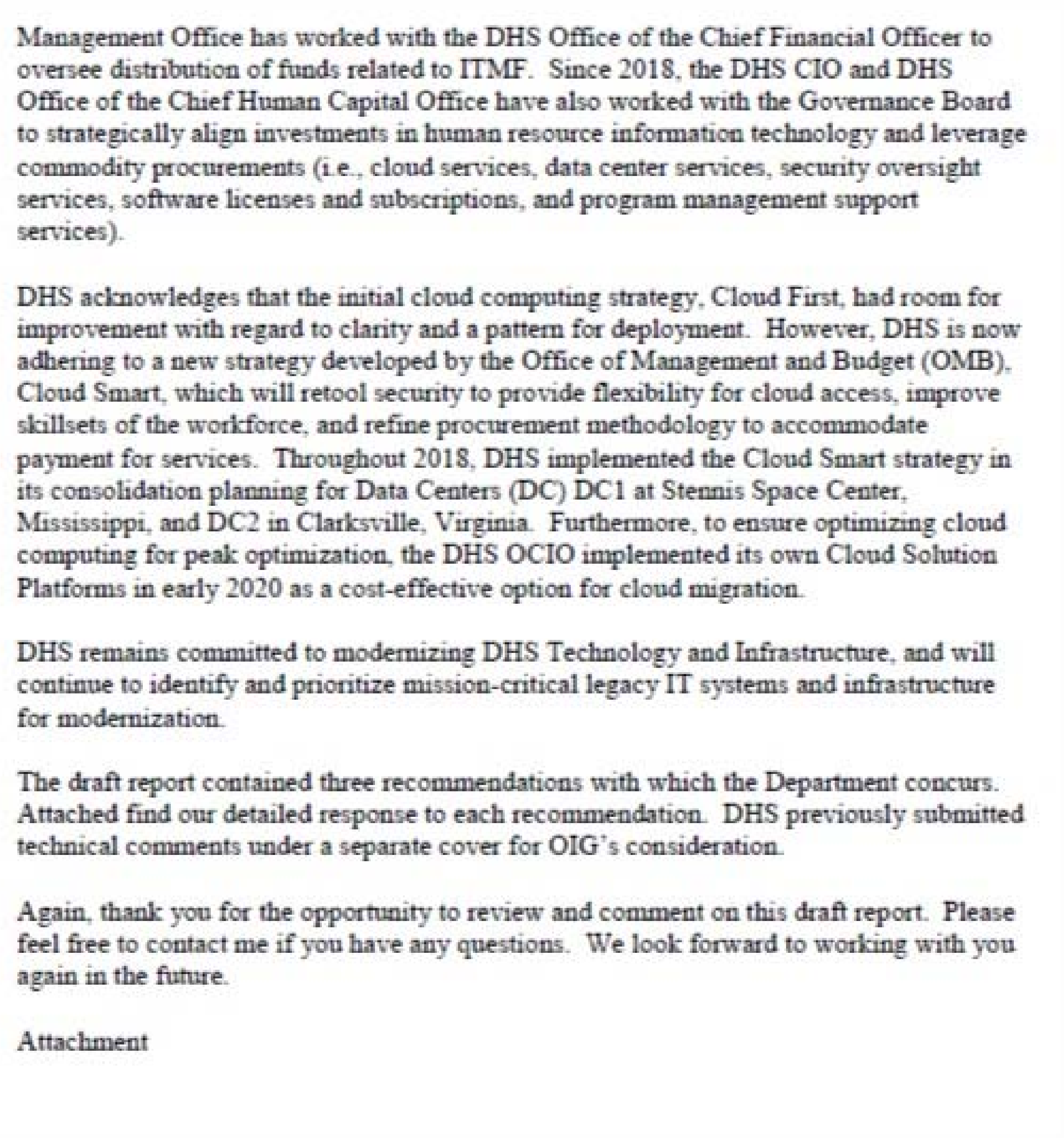
SUBJECT: Management Response to Draft Report: "Progress and Challenges in Modernizing DHS' IT Systems and Infrastructure" (Project No. OIG-18-102-ITA-DHS)

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

The Department is pleased to note OIG's positive recognition of the DHS Chief Information Officer (CIO) and Component CIOs collaborative work to prioritize legacy information technology (IT) systems or infrastructure for modernization in the development of the DHS IT Strategic Plan 2019-2023, dated March 2019.

While creating this strategic plan, the DHS CIO adhered to DHS Directive 142-02 (Revision 01), "Information Technology Integration and Management," dated April 12, 2018, which establishes the responsibilities and policies of the Department's CIO and DHS Component CIOs regarding IT integration and management. In connection with the "Government Performance and Results Modernization Act of 2010," Public Law 111-352, dated January 4, 2011, Directive 142-02 put into action the DHS CIO and Component CIOs' intent to conduct strategic planning that identifies and documents how IT is to be used to accomplish the Department's mission.

For example, the DHS CIO not only routinely communicates IT modernization strategy and planning with Component CIOs, but also authorized the establishment of a Governance Board in 2018 to oversee a Departmental IT Modernization Fund (ITMF) consistent with the intent of the Modernizing Government Technology Act. Since Fiscal Year 2018, the DHS Office of the Chief Information Officer (OCIO) Business



Management Office has worked with the DHS Office of the Chief Financial Officer to oversee distribution of funds related to ITMF. Since 2018, the DHS CIO and DHS Office of the Chief Human Capital Office have also worked with the Governance Board to strategically align investments in human resource information technology and leverage commodity procurements (i.e., cloud services, data center services, security oversight services, software licenses and subscriptions, and program management support services).

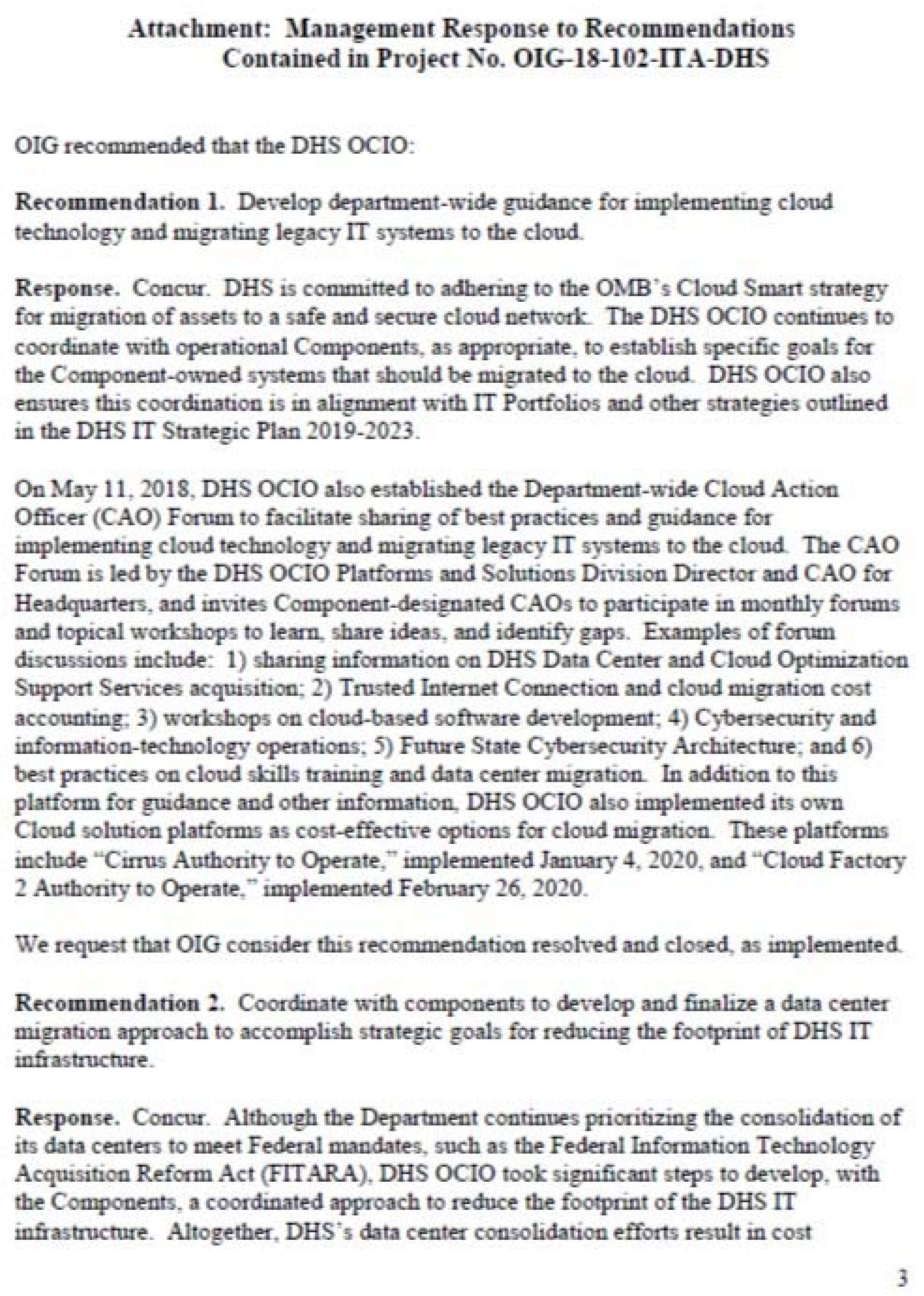
DHS acknowledges that the initial cloud computing strategy, Cloud First, had room for improvement with regard to clarity and a pattern for deployment. However, DHS is now adhering to a new strategy developed by the Office of Management and Budget (OMB), Cloud Smart, which will retool security to provide flexibility for cloud access, improve skillsets of the workforce, and refine procurement methodology to accommodate payment for services. Throughout 2018, DHS implemented the Cloud Smart strategy in its consolidation planning for Data Centers (DC) DC1 at Stennis Space Center, Mississippi, and DC2 in Clarksville, Virginia. Furthermore, to ensure optimizing cloud computing for peak optimization, the DHS OCIO implemented its own Cloud Solution Platforms in early 2020 as a cost-effective option for cloud migration.

DHS remains committed to modernizing DHS Technology and Infrastructure, and will continue to identify and prioritize mission-critical legacy IT systems and infrastructure for modernization.

The draft report contained three recommendations with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment



Attachment: Management Response to Recommendations Contained in Project No. OIG-18-102-ITA-DHS

OIG recommended that the DHS OCIO:

Recommendation 1. Develop department-wide guidance for implementing cloud technology and migrating legacy IT systems to the cloud.

Response. Concur. DHS is committed to adhering to the OMB's Cloud Smart strategy for migration of assets to a safe and secure cloud network. The DHS OCIO continues to coordinate with operational Components, as appropriate, to establish specific goals for the Component-owned systems that should be migrated to the cloud. DHS OCIO also ensures this coordination is in alignment with IT Portfolios and other strategies outlined in the DHS IT Strategic Plan 2019-2023.

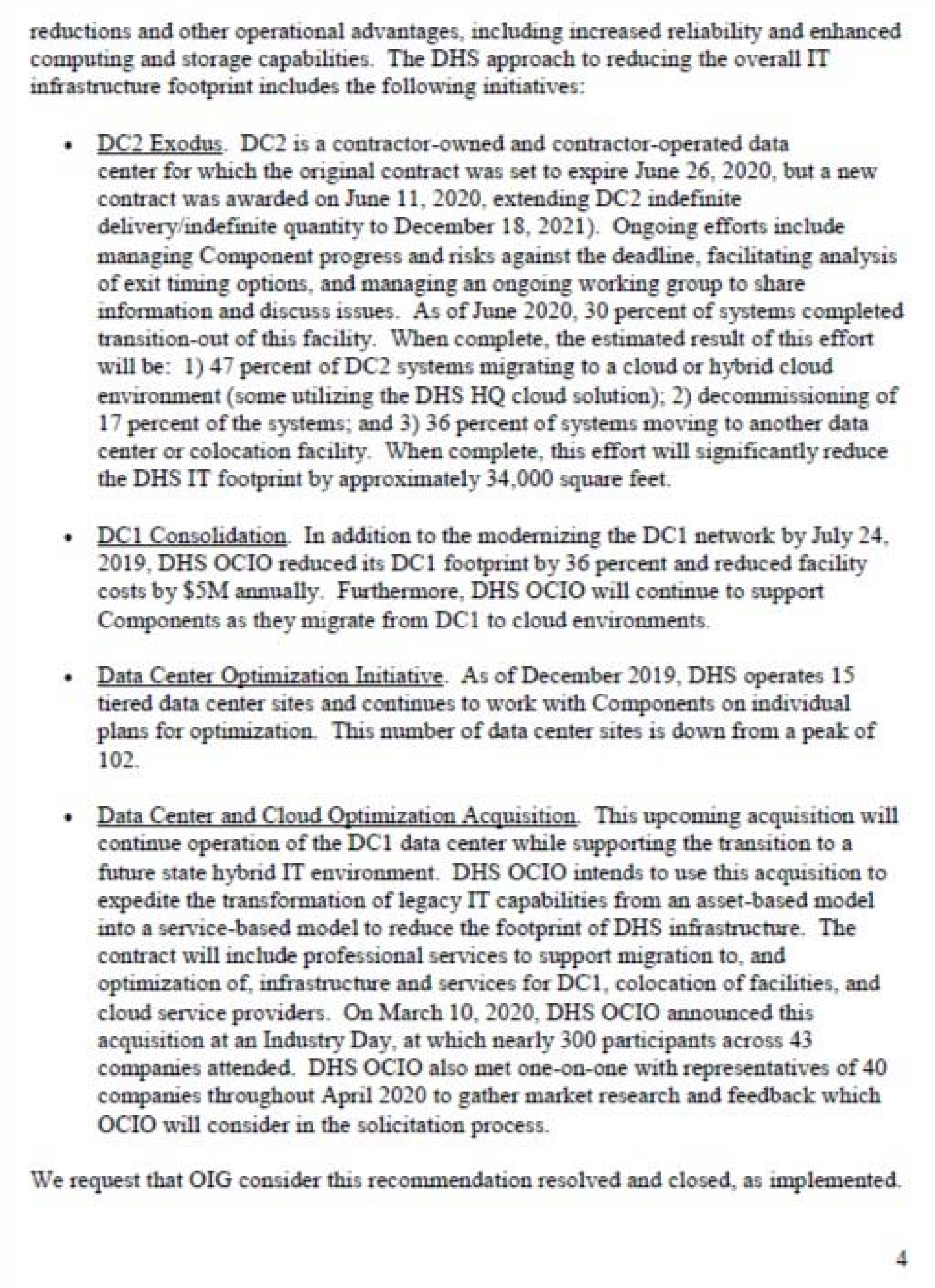
On May 11, 2018, DHS OCIO also established the Department-wide Cloud Action Officer (CAO) Forum to facilitate sharing of best practices and guidance for implementing cloud technology and migrating legacy IT systems to the cloud. The CAO Forum is led by the DHS OCIO Platforms and Solutions Division Director and CAO for Headquarters, and invites Component-designated CAOs to participate in monthly forums and topical workshops to learn, share ideas, and identify gaps. Examples of forum discussions include: 1) sharing information on DHS Data Center and Cloud Optimization Support Services acquisition; 2) Trusted Internet Connection and cloud migration cost accounting; 3) workshops on cloud-based software development; 4) Cybersecurity and information-technology operations; 5) Future State Cybersecurity Architecture; and 6) best practices on cloud skills training and data center migration. In addition to this platform for guidance and other information, DHS OCIO also implemented its own Cloud solution platforms as cost-effective options for cloud migration. These platforms include "Cirrus Authority to Operate," implemented January 4, 2020, and "Cloud Factory 2 Authority to Operate," implemented February 26, 2020.

We request that OIG consider this recommendation resolved and closed, as implemented.

Recommendation 2. Coordinate with components to develop and finalize a data center migration approach to accomplish strategic goals for reducing the footprint of DHS IT infrastructure.

Response. Concur. Although the Department continues prioritizing the consolidation of its data centers to meet Federal mandates, such as the Federal Information Technology Acquisition Reform Act (FITARA), DHS OCIO took significant steps to develop, with the Components, a coordinated approach to reduce the footprint of the DHS IT infrastructure. Altogether, DHS's data center consolidation efforts result in cost

3



reductions and other operational advantages, including increased reliability and enhanced computing and storage capabilities. The DHS approach to reducing the overall IT infrastructure footprint includes the following initiatives:

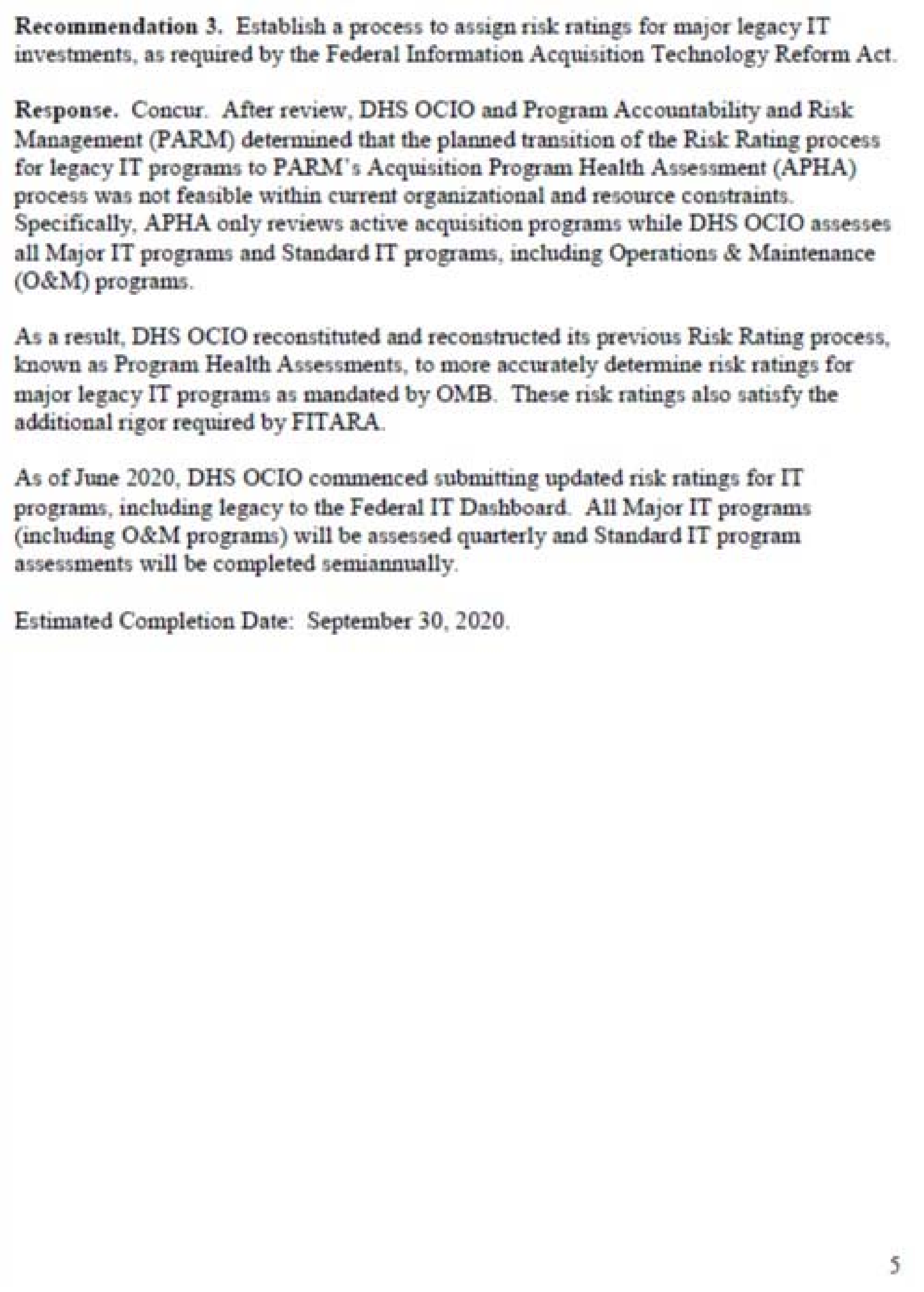
- DC2 Exodus. DC2 is a contractor-owned and contractor-operated data center for which the original contract was set to expire June 26, 2020, but a new contract was awarded on June 11, 2020, extending DC2 indefinite delivery/indefinite quantity to December 18, 2021). Ongoing efforts include managing Component progress and risks against the deadline, facilitating analysis of exit timing options, and managing an ongoing working group to share information and discuss issues. As of June 2020, 30 percent of systems completed transition-out of this facility. When complete, the estimated result of this effort will be: 1) 47 percent of DC2 systems migrating to a cloud or hybrid cloud environment (some utilizing the DHS HQ cloud solution); 2) decommissioning of 17 percent of the systems; and 3) 36 percent of systems moving to another data center or colocation facility. When complete, this effort will significantly reduce the DHS IT footprint by approximately 34,000 square feet.

- DC1 Consolidation. In addition to the modernizing the DC1 network by July 24, 2019, DHS OCIO reduced its DC1 footprint by 36 percent and reduced facility costs by $5M annually. Furthermore, DHS OCIO will continue to support Components as they migrate from DC1 to cloud environments.

- Data Center Optimization Initiative. As of December 2019, DHS operates 15 tiered data center sites and continues to work with Components on individual plans for optimization. This number of data center sites is down from a peak of 102.

- Data Center and Cloud Optimization Acquisition. This upcoming acquisition will continue operation of the DC1 data center while supporting the transition to a future state hybrid IT environment. DHS OCIO intends to use this acquisition to expedite the transformation of legacy IT capabilities from an asset-based model into a service-based model to reduce the footprint of DHS infrastructure. The contract will include professional services to support migration to, and optimization of, infrastructure and services for DC1, colocation of facilities, and cloud service providers. On March 10, 2020, DHS OCIO announced this acquisition at an Industry Day, at which nearly 300 participants across 43 companies attended. DHS OCIO also met one-on-one with representatives of 40 companies throughout April 2020 to gather market research and feedback which OCIO will consider in the solicitation process.

We request that OIG consider this recommendation resolved and closed, as implemented.



Recommendation 3. Establish a process to assign risk ratings for major legacy IT investments, as required by the Federal Information Acquisition Technology Reform Act.

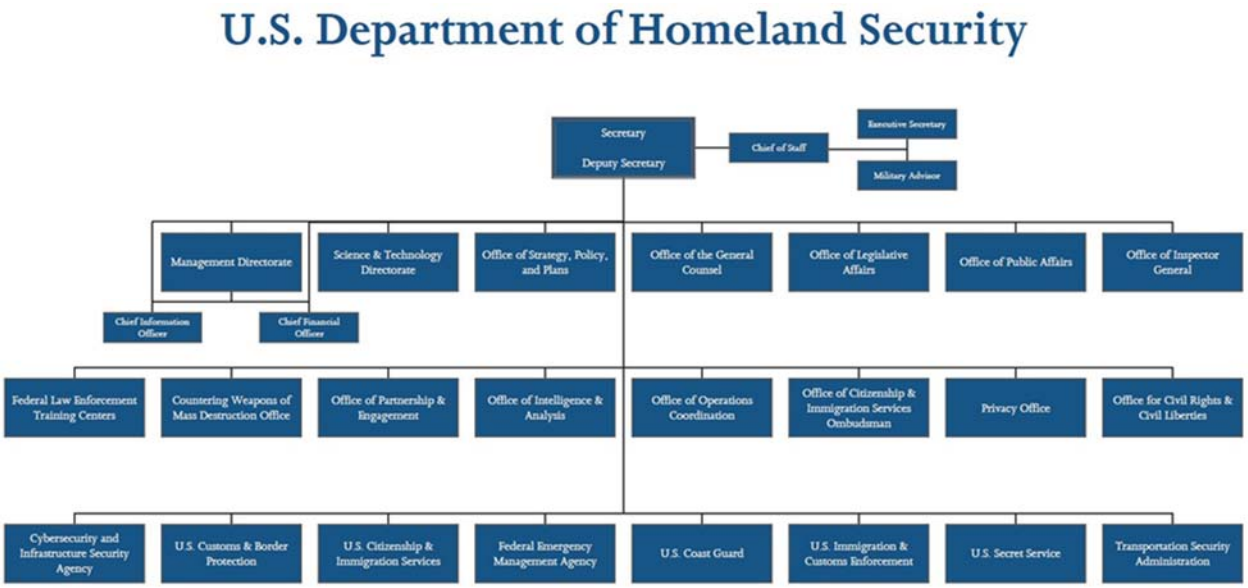
Response. Concur. After review, DHS OCIO and Program Accountability and Risk Management (PARM) determined that the planned transition of the Risk Rating process for legacy IT programs to PARM's Acquisition Program Health Assessment (APHA) process was not feasible within current organizational and resource constraints. Specifically, APHA only reviews active acquisition programs while DHS OCIO assesses all Major IT programs and Standard IT programs, including Operations & Maintenance (O&M) programs.

As a result, DHS OCIO reconstituted and reconstructed its previous Risk Rating process, known as Program Health Assessments, to more accurately determine risk ratings for major legacy IT programs as mandated by OMB. These risk ratings also satisfy the additional rigor required by FITARA.

As of June 2020, DHS OCIO commenced submitting updated risk ratings for IT programs, including legacy to the Federal IT Dashboard. All Major IT programs (including O&M programs) will be assessed quarterly and Standard IT program assessments will be completed semiannually.

Estimated Completion Date: September 30, 2020.

Appendix C
DHS Organization Chart


U.S. Department of Homeland Security
Secretary
Deputy Secretary
Chief of Staff
Executive Secretary
Military Advisor
Management Directorate
Chief Information Officer
Chief Financial Officer
Science & Technology Directorate
Office of Strategy, Policy, and Plans
Office of the General Counsel
Office of Legislative Affairs
Office of Public Affairs
Office of Inspector General
Federal Law Enforcement Training Centers
Countering Weapons of Mass Destruction Office
Office of Partnership & Engagement
Office of Intelligence & Analysis
Office of Operations Coordination
Office of Citizenship & Immigration Services Ombudsman
Privacy Office
Office for Civil Rights & Civil Liberties
Cybersecurity and Infrastructure Security Agency
U.S. Customs & Border Protection
U.S. Citizenship & Immigration Services
Federal Emergency Management Agency
U.S. Coast Guard
U.S. Immigration & Customs Enforcement
U.S. Secret Service
Transportation Security Administration

Appendix D
Office of Audits Major Contributors to This Report

Kristen Bernard, Deputy Assistant Inspector General
Craig Adelman, Director
Kristen Gearhart, Audit Manager
Alexander Stewart Jr, Auditor in Charge
Nasanjargal Zana, Auditor
Deborah Mouton-Miller, Communications Analyst
Michael Staver, Independent Reference Reviewer

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
DHS OIG Liaison
DHS Chief Information Officer
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Acting Commissioner, U.S. Customs and Border Protection
U.S. Customs and Border Protection Audit Liaison
Administrator, United States Coast Guard
United States Coast Guard Audit Liaison
Administrator, Federal Emergency Management Agency
Federal Emergency Management Agency Audit Liaison
Acting Director, Immigration and Customs Enforcement
Immigration and Customs Enforcement Audit Liaison
Director, Secret Service
Secret Service Audit Liaison
Administrator, Transportation Security Administration
Transportation Security Administration Audit Liaison
Acting Director, U.S. Citizenship and Immigration Services
U.S. Citizenship and Immigration Services Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305