OFFICE OF INSPECTOR GENERAL

Major Management and Performance Challenges Facing the Department of Homeland Security

Homeland Security

November 10, 2020

OIG-21-07

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

November 10, 2020

MEMORANDUM FOR: The Honorable Chad F. Wolf
Secretary *(Acting)*

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

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2020.11.10 17:54:34 -05'00'

SUBJECT: *Major Management and Performance Challenges Facing the Department of Homeland Security*

For your information is our annual report, *Major Management and Performance Challenges Facing the Department of Homeland Security*. Pursuant to the *Reports Consolidation Act of 2000*, the Office of Inspector General must issue an annual statement summarizing what the Inspector General considers the most serious management and performance challenges facing the Department of Homeland Security and assessing its progress in addressing them. This requirement is consistent with our duties under the *Inspector General Act of 1978*, as amended, to conduct audits, as well as provide leadership and recommend policies to promote economy, efficiency, and effectiveness in DHS programs and operations. We remain committed to conducting independent oversight and making recommendations to help the Department address these major management and performance challenges.

We acknowledge and appreciate your ongoing efforts during this unprecedented time to ensure that our Nation and its citizens are safe, secure, and resilient against terrorism and other hazards. In evaluating the challenges facing DHS, we again considered their importance relative to the *Department of Homeland Security's Strategic Plan for Fiscal Years 2020-2024* (DHS' FY 2020-2024 Strategic Plan), as well as its Enterprise Risk Management and Immigration Data Integration initiatives. Appendix A presents the goals and objectives in DHS' FY 2020–2024 Strategic Plan; elsewhere in this report, we cite specific examples of DHS' strategic progress. Several management challenges we identified last year remain outstanding for the Department. Appendix B contains the Department's response in its entirety.

Based on our recent and prior audits, inspections, evaluations, special reviews, and investigations, and the current coronavirus 19 (COVID-19) pandemic, we consider the most serious management and performance challenges facing DHS to be:

- Performing Fully and Effectively during COVID-19;
- Countering Terrorism and Homeland Security Threats;
- Ensuring Proper Financial Management;
- Ensuring Information Technology (IT) Supports Essential Mission Operations;
- Improving FEMA's Contracts and Grants Management, Disaster Assistance, and Fraud Prevention; and
- Strengthening Oversight and Management of Major Systems Acquisition.

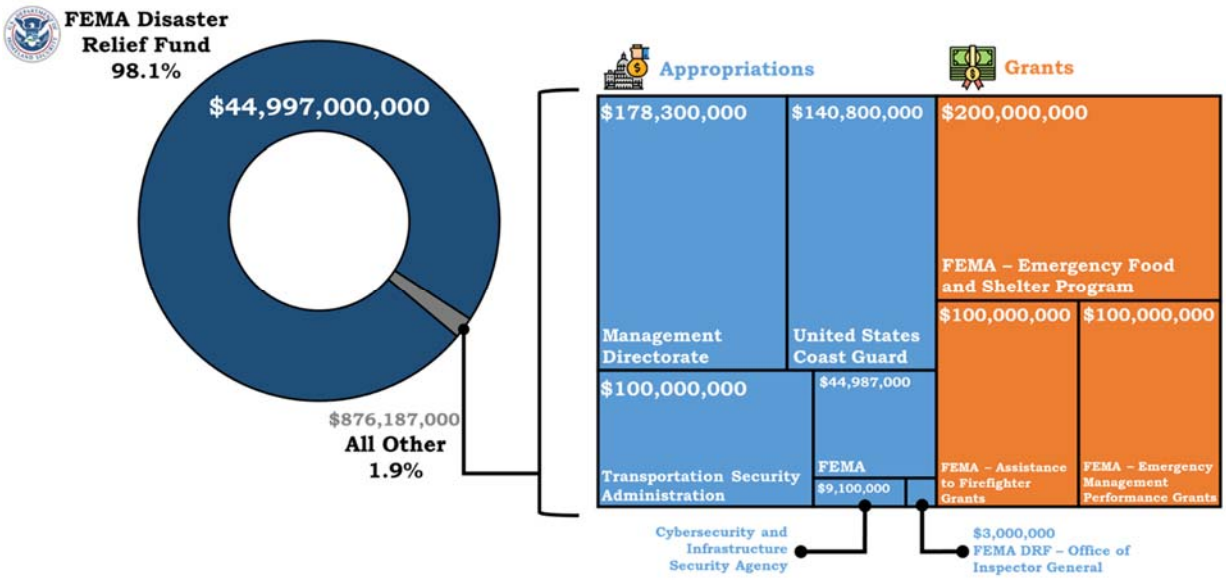
Meeting these challenges requires unity of effort, a commitment to mastering management fundamentals, and the identification and allocation of appropriate resources. As we have noted in previous Major Management and Performance Challenges reports, many of the Department's senior leadership positions still do not have permanent, Presidentially Appointed and Senate confirmed officials.[1]

Performing Fully and Effectively during COVID-19

The challenge to continue mission critical operations and programs relates to every aspect of DHS' mission but particularly the DHS FY 2020–2024 Strategic Plan at Goal 5: Strengthen Preparedness and Resilience, Objectives 5.1, Build a National Culture of Preparedness, and 5.2: Respond During Incidents.[2]
In response to outbreaks of the coronavirus disease in the United States, the Secretary of Health and Human Services declared a public health emergency on January 31, 2020, under section 319 of the *Public Health Service Act*.[3]

[1] As of October 16, 2020, acting officials filled over 20 percent of all DHS senior leadership positions. At FEMA, which bears central responsibility for coordinating the whole of government response to COVID-19, two of four lead positions are either vacant or filled by an acting official: the Deputy Administrator and the Deputy Administrator for Resilience, respectively. See https://www.dhs.gov/leadership.
[2] DHS' 2020-2024 Strategic Plan recognizes that the Department's diverse and complex mission requires integration across eight operational components, which execute the Department's operational activities: seven support components, which formulate guidance on policy, management, research, training, and intelligence and enable mission execution; and the Office of the Secretary, which coordinates and oversees the activities of the Department. See https://www.dhs.gov/sites/default/files/publications/19_0702_plcy_dhs-strategic-plan-fy20-24.pdf, p. 4.
[3] See https://www.hhs.gov/about/news/2020/01/31/secretary-azar-declares-public-health-emergency-us-2019-novel-coronavirus.html.

Soon thereafter, on March 11, 2020, the World Health Organization declared COVID-19 a pandemic, noting that it was not just a public health crisis, but also one that would affect every sector of society.[4] Two days later, President Donald Trump declared COVID-19 a national emergency, freeing $50 billion in Federal resources to combat the pandemic.[5] In March and April of 2020, Congress passed four funding bills to address the public health and economic crises caused by COVID-19.[6] Together, this legislation authorized approximately $2.4 trillion in Federal spending. The following OIG graphic displays allocations to DHS.



Given this funding and the range of associated mandates, the Department reported it has adopted a layered response to delivering critical supplies and services. According to DHS, it is working through U.S. Customs and Border Protection (CBP), the Countering Weapons of Mass Destruction Office (CWMD), United States Coast Guard, Transportation Security Administration (TSA), Federal Emergency Management Agency (FEMA), U.S. Immigration and Customs Enforcement (ICE), the Cybersecurity and Infrastructure Security

[4] See https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-COVID-19---11-march-2020.
[5] See https://www.whitehouse.gov/presidential-actions/proclamation-declaring-national-emergency-concerning-novel-coronavirus-disease-COVID-19-outbreak/.
[6] These include in order of passage the *Coronavirus Preparedness and Response Supplemental Appropriations Act, 2020*, Pub. L. No. 116-123, 134 Stat. 146 (2020); *Families First Coronavirus Response Act*, Pub. L. No. 116-127, 134 Stat. 178 (2020); *Coronavirus Aid, Relief, and Economic Security Act* (CARES Act), Pub. L. No. 116-136, 134 Stat. 281 (2020); and *Paycheck Protection Program and Health Care Enhancement Act*, Pub. L. No. 116-139, 134 Stat. 620 (2020).

Agency (CISA), and other operational and support components to protect the Nation.[7] CBP and CWMD, which houses the Department's Chief Medical Officer (CMO), reported providing direct support to the Centers for Disease Control and Prevention (CDC) by conducting enhanced health screenings at 15 major airports.[8]

In 2014 and 2016, we issued two reports on the preparedness of DHS' workforce to continue mission essential functions during a pandemic. In 2014, we reported that DHS did not adequately assess its needs before purchasing pandemic preparedness supplies and did not effectively manage its stockpile of pandemic personal protective equipment (PPE) and antiviral medical countermeasures.[9] In 2016, we reported that DHS may not have been able to effectively execute its preparedness plans during a pandemic.[10] We are currently assessing the adequacy and effectiveness of the corrective actions DHS took to address our report recommendations, through which we may identify ongoing challenges in this area. Since March 2020, we have initiated several audits and evaluations related to the Department's response to COVID-19, including audits of FEMA's Federal coordination efforts and medical supply chain.[11]

DHS has taken steps to protect its workforce by allowing remote performance, "any 80" hours,[12] and other flexibilities and support.[13] However, given the

[7] For additional details regarding the Department's effort to contain and prevent the spread of COVID-19, see https://www.dhs.gov/coronavirus?utm_source=hp_slideshow&utm_medium=web&utm_campaign=dhsgov/.
[8] *Id.* These screenings were in effect until September 14, 2020. As the Department lead for biodefense, CWMD's COVID-19 response activities also include coordinating DHS efforts with Federal interagency partners, decision support (e.g., intelligence analysis and biosurveillance activities), acquisition support (e.g., to acquire detection and reporting capability if needed). CWMD has further ensured internal access, maintenance, and support to classified systems and requested an exception to the rules regarding access to classified accounts to ensure users are not locked-out of their accounts due to non-use.
[9] *DHS Has Not Effectively Managed Pandemic Personal Protective Equipment and Antiviral Medical Countermeasures* (OIG-14-129), August 26, 2014.
[10] *DHS Pandemic Planning Needs Better Oversight, Training, and Execution* (OIG-17-02), October 12, 2016.
[11] See https://www.pandemicoversight.gov/oversight/reports?f[0]=report_type_taxonomy:89.

[12] This arrangement permits Federal employees to work outside normal duty hours during each pay period as long as their cumulative time and attendance totals 80 hours.
[13] DHS through its Office of the Chief Human Capital Officer (OCHCO) has also delivered more than 20 webinars and training sessions for supervisors, managers, and employees focused on updated or new human resources flexibilities issued by the Office of Personnel Management (e.g., on Telework, Leave Administration, and Performance Management) and the CARES Act,

nature of their work, certain DHS components and staff face heightened risk of exposure to COVID-19. In reviews conducted to determine how CBP and ICE were handling the COVID-19 pandemic at short- and longer-term detention facilities, we identified various actions taken to prevent and mitigate the pandemic's spread among staff.[14] Facilities noted decreases in current staff availability due to COVID-19, but reported having contingency plans to ensure continued operations. Personnel also expressed concerns with the availability of staff, as well as PPE, if there were an outbreak of COVID-19 in the facility. Overall, most facility responses show they were prepared to address COVID-19, but expressed concerns if the pandemic continued to spread.

In addition to possible DHS staff exposure to COVID-19, detained individuals also face a high risk of exposure due to the congregate nature of the facilities. In our reviews, we noted that facilities had taken actions to reduce the spread of COVID-19 among detained individuals, including increased cleaning and disinfecting of common areas, distribution of sanitizing materials, and quarantining new detainees, when possible, as a precautionary measure. However, personnel at facilities reported concerns with their inability to practice social distancing among detained individuals and to isolate or quarantine individuals who may be infected with COVID-19. Between the time we concluded our survey of ICE facilities and issued our report, the number of confirmed COVID-19 cases among ICE detainees increased significantly. We are currently conducting a more comprehensive review of ICE's response to the pandemic in detention facilities.

Finally, DHS faces a challenge to ensure stability and full and effective functioning of its components during COVID-19. For example, DHS recently faced the prospect of having to furlough almost 70 percent of its U.S. Citizenship and Immigration Services (USCIS) workforce reportedly due to decreased revenues related to COVID-19.[15] Although the component has been able to maintain operations through FY 2020, there is "no guarantee [USCIS] can avoid future furloughs. A return to normal operating procedures requires congressional intervention to sustain the agency through Fiscal Year 2021."[16]

---

which made available Emergency Paid Sick Leave. OCHCO also established a COVID-19 Workforce Protection Cell to provide guidance on how to protect the DHS workforce.

[14] *Early Experiences with COVID-19 at ICE Detention Facilities* (OIG-20-42), June 18, 2020, and *Early Experiences with COVID-19 at CBP Border Patrol Stations and OFO Ports of Entry* (OIG-20-69), September 4, 2020.

[15] See https://www.rollcall.com/2020/05/18/uscis-seeks-1-2-billion-from-congress/. The DHS OIG has not independently reviewed the circumstances leading to the potential furlough of USCIS workers.

[16] See https://www.uscis.gov/news/news-releases/uscis-averts-furlough-of-nearly-70-of-workforce.

We are conducting an audit to determine the effectiveness of USCIS' technology systems to provide timely and accurate electronic processing of immigration and naturalization benefit requests while field locations, asylum offices, and application support centers are closed or operating on a reduced workforce during the COVID-19 pandemic. We have previously reported that USCIS had made limited progress in transforming its paper-based processes into the new automated immigration benefits processing environment, known as the Electronic Immigration System (ELIS).[17] For example, ELIS did not havecritical functionality and internal controls needed to be fully operational for electronic benefits processing. Also, the underlying system design and architecture posed significant technical difficulties due to complex system interfaces and software coding defects, which led to slow processing time and frequent performance outages. USCIS subsequently addressed these issues and expanded electronic processing of immigration and naturalization benefits in ELIS.

Countering Terrorism and Homeland Security Threats

This challenge falls under the DHS FY 2020–2024 Strategic Plan's Goal 1: Counter Terrorism and Homeland Security Threats, Objectives 1.1, Collect, Analyze, and Share Actionable Intelligence; 1.2, Detect and Disrupt Threats; 1.3, Protect Designated Leadership Events, and Soft Targets; and 1.4, Counter Weapons of Mass Destruction and Emerging Threats.

DHS is challenged to properly plan, and provide adequate guidance, oversight, and monitoring of programs and operations to counter terrorism and homeland security threats. For example, a secure and resilient electoral process is a vital national interest and one of the Department's highest priorities.[18] Within DHS, CISA leads coordination efforts to manage risks to the Nation's 16 critical infrastructure sectors,[19] one of which — the government facilities sector — includes election infrastructure.[20] We believe that although DHS has improved

[17] *Management Alert: U.S. Citizenship and Immigration Services' Use of the Electronic Immigration System for Naturalization Benefits Processing, January 19, 2017, OIG-17-26-MA; USCIS Has Been Unsuccessful in Automating Naturalization Benefits Delivery, November 30, 2017, OIG-18-23; USCIS Automation of Immigration Benefits Processing Remains Ineffective*, OIG-16-48, 03/09/16.

[18] See www.dhs.gov/topic/election-security.

[19] The Nation's 16 critical infrastructure sectors include systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

[20] The remaining 15 critical infrastructure sectors include chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

coordination efforts to secure the Nation's systems used for voting, it should take additional steps to protect the broader election infrastructure, which includes polling and voting locations, election technologies, and related storage facilities. During our recent audit in this area,[21] CISA reported it has developed a set of plans and guidance aimed at securing election systems for the 2020 election cycle. However, the plans do not sufficiently mitigate risks associated with physical security, terrorism threats, and targeted violence to the election infrastructure, nor do they identify dependencies on external stakeholders that impede mission performance.

DHS senior leadership turnover and ongoing CISA reorganization have hindered CISA's ability to enhance planning and effectively monitor its progress in securing the Nation's election infrastructure. On election day, CISA officials stated there was no evidence of a major cyberattack on the elections, and CISA would continue to monitor hacking attempts and cyber intrusions and coordinate information sharing with state and local officials.

In addition, DHS continues to face challenges (1) mitigating threats posed by high-risk cargo from foreigh airports, (2) countering Unmanned Aircraft Systems (C-UAS), (3) using canines effectively, (4) executing successful covert testing, (5) protecting commercial facilities, and (6) defending food, agriculture, and veterinary systems against terrorism and other high-consequence events in the United States. In May 2020, we reported on the extent to which CBP's Air Cargo Advance Screening (ACAS) program prevents air carriers from transporting high-risk cargo from foreign airports into the United States.[22] Although CBP identified and targeted high-risk cargo shipments, the component did not always prevent air carriers from transporting high-risk air cargo from foreign airports into the United States. This occurred because neither CBP nor TSA developed adequate policies and procedures to ensure air carriers promptly and appropriately resolved referrals of cargo determined to be high-risk before transporting the cargo.

We also found that DHS' capability to counter illicit use of UAS is limited.[23] Specifically, the Office of Strategy, Policy, and Plans did not execute a uniform department-wide approach to expanding C-UAS capabilities because it did not request funding to obtain subject matter experts to fulfill the Secretary's

[21] *DHS Has Secured the Nation's Election Systems, but Work Remains to Protect the Infrastructure* (OIG-21-01), October 22, 2020.
[22] *CBP's ACAS Program Did Not Always Prevent Air Carriers from Transporting High Risk Cargo into the US* (OIG-20-34), May 11, 2020.
[23] *DHS Has Limited Capability to Counter Illicit Unmanned Aircraft Systems* (OIG-20-43), June 25, 2020.

requirements for such an approach, including developing a realistic work plan and issuing complete department-wide C-UAS guidance.

We identified deficiencies in TSA's use of passenger screening canine (PSC) teams. In April 2020, we reported TSA could not show that deployed PSC teams provide effective security at screening checkpoints.[24] Specifically, TSA did not:

- identify and document mission needs, capability gaps, and operational goals for deploying PSC teams;
- properly justify and document decisions on allocating PCS teams;
- justify the teams as the best, most cost-effective checkpoint security; or
- adequately oversee TSA management operations at airports.

We also found PSC teams have inherent limitations. As a result, our Nation's aviation system and the traveling public could be at risk of a catastrophic event caused by an undetected explosive device.

In May 2020, we reported that TSA did not monitor its Advanced Imaging Technology system (AIT) to ensure it continues to fulfill needed capabilities.[25] Although AIT met the requirement for system availability, TSA did not monitor the AIT system's probability of detection rate and throughput rate requirements set forth in TSA's operational requirements document. These issues occurred because TSA has not established comprehensive guidance to monitor AIT system performance. Without continuous monitoring and oversight, TSA cannot ensure AIT is meeting critical system performance requirements — a persistent weakness found in prior DHS OIG reports.[26]

We reported CBP does not comprehensively plan and conduct covert tests of its operations at Border Patrol checkpoints and ports of entry, use test results to address vulnerabilities, or widely share lessons learned.[27] In particular, CBP's two covert testing groups do not use risk assessments or intelligence to plan and conduct covert tests, plan coordinated tests, or design system-wide tests.

---

[24] *TSA Challenges with Passenger Screening Canine Teams (Redacted)* (OIG-20-28), April 28, 2020.
[25] *TSA Needs to Improve Monitoring of Deployed Advanced Imaging Technology Systems* (OIG-20-33), May 8, 2020.
[26] *TSA Penetration Testing of Advanced Imaging Technology*, (OIG-12-06), November, 2011; *Covert Testing of TSA's Passenger Screening and Technologies and Processes at Airport Security Checkpoints* (OIG-15-150), September 22, 2015; *Covert Testing of Access Controls to Airport Secure Areas* (OIG-19-21), February 13, 2019; *Covert Testing of TSA's Screening Checkpoint Effectiveness* (OIG-17-112), September 27, 2017.
[27] *CBP Needs a Comprehensive Process for Conducting Covert Testing and Resolving Vulnerabilities* (OIG-20-55), July 28, 2020.

This occurred because CBP does not provide adequate guidance on risk- and intelligence-based test planning, direct the groups to coordinate, give them the necessary authority, or establish performance goals and measures for covert testing. Following testing, CBP does not widely share covert test results, consistently make recommendations, or ensure corrective actions are taken. Results are not widely shared because CBP has not defined roles and responsibilities for such sharing. Covert testing groups do not make recommendations or ensure corrective actions are implemented due to insufficient authority and policies directing these actions. Finally, CBP does not effectively manage covert testing groups to ensure data reliability, completeness, and compliance with security requirements due to leadership changes and limited staff.

We also examined the extent of DHS' efforts to deter and prevent terrorism or physical threats within the commercial facilities sector.[28] CISA, which is primarily responsible for working with components and partners to defend against current threats to the commercial facilities sector and build a more secure and resilient infrastructure, does not effectively coordinate and share best practices to enhance security across the sector. This occurred because CISA does not have comprehensive policies and procedures to support its role as the commercial facilities' Sector-Specific Agency. Without such policies and procedures, CISA cannot effectively fulfill its responsibilities and limits its ability to measure the Department's progress toward accomplishing its sector-specific objectives. CISA may also be missing opportunities to help commercial facility owners and operators identify threats and mitigate risks, leaving the commercial facilities sector vulnerable to terrorist attacks and physical threats. Finally, DHS' CWMD — although required under the *Securing Our Agriculture and Food Act* (SAFA) — has not effectively implemented a program to coordinate the Department's efforts to defend food, agriculture, and veterinary systems against terrorism and other high-consequence events in the United States.[29] This occurred because CWMD believed it did not have clearly defined authority from the Secretary to carry out the requirements of the SAFA. In addition, since its establishment in December 2017, CWMD has not prioritized SAFA requirements but instead has focused its resources on other mission areas. As a result, CWMD has limited awareness of DHS' ongoing efforts and cannot ensure it is adequately prepared to respond to a terrorist attack against the Nation's food, agriculture, or veterinary systems.

[28] *DHS Can Enhance Efforts to Protect Commercial Facilities from Terrorist and Physical Threats* (OIG-20-37), June 11, 2020.
[29] *DHS Is Not Coordinating the Department's Efforts to Defend the Nation's Food, Agriculture, and Veterinary Systems against Terrorism* (OIG-20-53), July 16, 2020.

Ensuring Proper Financial Management

This challenge relates to every aspect of DHS' mission, and is captured in objectives listed under DHS' 2020–2024 Strategic Plan at Goal 6: Championing the Workforce and Strengthening the Department, Objectives 6.1, Strengthen Departmental Governance and Management and 6.3: Optimize Support to Mission Operations.

The Need for Modernization

Many key DHS financial systems do not comply with Federal financial management system requirements, as defined in the *Federal Financial Management Improvement Act of 1996*. Limitations in financial systems' functionality add substantially to the Department's challenges addressing systemic internal control weaknesses and restrict its ability to leverage IT systems to process and report financial data efficiently and effectively. These deficiencies may hinder DHS' ability to ensure proper financial planning payments and appropriate internal controls related to CARES Act funding.

Since its inception, DHS has made three major attempts to modernize and consolidate its financial systems. In 2017, DHS initiated its fourth attempt, the Financial Systems Modernization (FSM) TRIO program, to address the incompatible processes and antiquated financial management systems in use department-wide. The ultimate goal of this program is to improve the quality of financial information to support decision-making and improve the ability to provide timely and accurate reporting to ensure efficient stewardship of taxpayer dollars.

In accordance with DHS guidance, the Department developed a strategy to apply lessons learned from prior system updates to its current FSM TRIO effort. DHS indicated the program office had successfully identified 29 lessons from prior modernization efforts and has begun applying them to the FSM TRIO program. Our audit in this area highlights DHS' awareness of the importance of identifying and applying lessons learned and provides some assurance and a positive outlook for continued future progress of the FSM TRIO project.[30] Leveraging successful practices from prior efforts, and avoiding past errors, may help DHS use its resources wisely, mitigate risks, and achieve its goals for FSM TRIO.

[30] *DHS Confirmed It Has Applied Lessons Learned in the Latest Financial System Modernization Effort* (OIG-20-09), December 19, 2020.

Internal Control Deficiencies

DHS has continued to make strides in establishing certain management fundamentals, including by again obtaining an unmodified opinion (clean) on its financial statements.[31] The independent public accounting firm KPMG LLP (KPMG) noted that financial statements present fairly, in all material respects, DHS' financial position as of September 30, 2019 and 2018. At the same time, KPMG issued an adverse opinion on DHS' internal control over financial reporting as of September 30, 2019. KPMG identified material weaknesses in internal control in two areas and other significant deficiencies in three areas. KPMG also reported two instances of noncompliance with laws and regulations.[32]

KPMG found material weaknesses in information technology controls and financial systems, and in financial reporting. Other significant deficiencies were identified in property, plant, and equipment; custodial activities; entry processing, refunds and drawbacks, and seized and forfeited property; and grants management.[33]

In December 2019, we reported internal control deficiencies at CBP in processing drawback claims.[34] From 2011 to 2018, CBP processed an average of $896 million in drawback claims annually. We found that CBP:

- did not have appropriate documentation retention periods to ensure importers and claimants maintained support for drawback transactions;
- did not require drawback specialists to review an importer's prior drawback claims to determine whether, taken together, the importer claimed an excessive amount; and
- did not have effective automated controls in its legacy drawback system to prevent, or detect and correct, excessive drawback claims.

Finally, since our first audit in 2017, DHS has continued to make progress in meeting its *Digital Accountability and Transparency Act of 2014* (DATA Act)

[31] *Independent Auditors' Report on DHS' FY 2019 Financial Statements and Internal Control over Financial Reporting* (OIG-20-03), November 15, 2019.
[32] Specifically the *Federal Managers' Financial Integrity Act of 1982* and the *Federal Financial Management Improvement Act of 1996*.
[33] In February 2020, the DHS Office of the Chief Financial Officer (CFO) delivered risk and internal control training to more than 450 DHS employees and awarded over 1,000 continuing education units to attendees from the financial management, program office, and information technology fields. This effort was followed in July 2020 with an annual CFO symposium attended by more than 600 DHS employees that covered multiple tracts related to financial management.
[34] *Lack of Controls Could Affect CBP Drawbacks* (OIG-20-07), December 12, 2019.

reporting requirements, but challenges remain.[35] Our most recent audit focused on the completeness, accuracy, timeliness, and quality of DHS' FY 2019 first quarter spending data posted on USASpending.gov, and DHS' implementation and use of government-wide financial data standards. We found that to enable more effective tracking of Federal spending, DHS must continue to accurately align its budgetary data with the President's budget, reduce award misalignments across DATA Act files, improve the timeliness of financial assistance reporting, implement and use government-wide data standards, and address risks to data quality. Without these actions, DHS will struggle to meet its goal of achieving the highest possible data quality for submission to www.usaspending.gov.[36]

Ensuring IT Supports Essential Mission Operations

This challenge affects the Department's mission across all 22 components and is a necessary element for accomplishing all six goals in DHS' FY 2020–2024 Strategic Plan. Every day, employees across the Department rely on IT to carry out day-to-day mission operations. DHS continues to struggle when providing IT support for personnel, system functionality and integration, addressing deficiencies, and identifying and prioritizing systems for modernization.

Limitations in IT Functionality and Integration

DHS combined functions of 22 different Federal departments and agencies with broad responsibilities to collectively prevent attacks, mitigate threats, respond to national emergencies, preserve economic security, and preserve legacy agency functions. However, DHS faces ongoing challenges ensuring IT systems and infrastructure adequately support Department personnel. This year, we sought to determine the effectiveness of DHS' IT systems in tracking detainees and supporting efforts to reunify unaccompanied alien children with separated families.[37] We found that DHS did not have the IT system functionality needed to accurately track separated migrant families during the execution of the *Zero Tolerance Policy*.[38] DHS was also unable to reunify families as mandated by a

[35] *DHS Has Made Progress in Meeting DATA Act Requirements, But Challenges Remain* (OIG-20-62), August 13, 2020.
[36] The DHS DATA Act team in communication with OIG stated it will continue to reconcile misalignments, correct errors, correct unacceptable warnings, and adjust existing internal controls as needed to improve the overall quality of data published for public consumption.
[37] *DHS Lacked Technology Needed to Successfully Account for Separated Migrant Families* (OIG-20-06), November 25, 2019.
[38] On April 6, 2018, the U.S. Attorney General issued a memorandum directing all Federal prosecutors' offices along the Southwest Border to work with DHS to adopt a "Zero Tolerance Policy," which required criminal prosecution of DHS referrals of 8 U.S.C. § 1325(a) vioations, to the extent practicable.

Federal judge due to poor data tracking, information sharing, and IT systems capabilities.[39] Without the ability to track and share data on family separations and reunifications, CBP adopted various ad hoc methods to work around system limitations, but these methods led to widespread errors. These deficiencies also cost Border Patrol 28,000 hours and an additional $1.2 million in staff overtime. Because of these IT deficiencies, we could not confirm the total number of families DHS separated during the Zero Tolerance period. These conditions persisted because CBP did not address its known IT deficiencies, such as adding capability to track family separations, before implementing Zero Tolerance in May 2018.

We have highlighted similar technology challenges in prior reports.[40] For example, in 2017 we found ICE relied on myriad IT systems that lacked integration and information-sharing capabilities, forcing ICE personnel to laboriously piece together vital information from up to 27 distinct DHS information systems and databases to accurately determine an individual's overstay status. As a result, in some cases, it took months for ICE to determine a low priority visa holder's status and whether that person might pose a national security threat. ICE has since completed corrective actions that addressed our recommendations.

This year we sought to determine whether DHS had effectively identified and prioritized mission-critical legacy IT systems and infrastructure for modernization, identified associated challenges, and assessed related legislation and executive direction.[41] We found that 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 accomplish mission goals. However, not all components have complied with or fully embraced these efforts due to a lack of standard guidance and funding. Meanwhile, DHS continues to rely on deficient and outdated IT systems to perform mission critical operations. Additionally, DHS has not yet leveraged the *Modernizing Government Technology Act of 2017* mandate to accelerate ongoing IT modernization efforts, as DHS and its components questioned whether the benefits of the Act outweighed the additional effort needed to use the resources provided under the Act. Until DHS addresses these issues, it will

[39] *Ms. L. v. ICE*, 18-cv-428 (S.D. Cal. June 26, 2018).
[40] *DHS Tracking of Visa Overstays Is Hindered by Insufficient Technology* (OIG-17-56), May 1, 2017; *CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations* (OIG-17-114), September 28, 2017; and *FEMA Faces Challenges in Managing Information Technology* (OIG-16-10), November 20, 2015.
[41] *Progress and Challenges in Modernizing DHS' IT Systems and Infrastructure* (OIG-20-61), August 10, 2020.

continue to face significant challenges to accomplish mission operations efficiently and effectively.

Information Security

OIG's FY 2019 *Federal Information Security Modernization Act* (FISMA) evaluation of DHS' information security showed an overall reduction in the programs' effectiveness.[42] DHS' information security program was not effective for FY 2019 because the Department earned a maturity rating of "Ad Hoc" (Level 1) in three of five functions, compared to last year's higher overall rating of "Managed and Measurable" (Level 4).[43] We attributed DHS' regression in managing its information security program to a change in Coast Guard's cybersecurity and FISMA reporting.

Risks to the Nation's systems and networks continue to increase as security threats evolve and become more sophisticated. As such, the cyber threat information DHS provides to Federal agencies and private sector entities must be actionable to help better manage this growing threat. However, the Department still faces challenges to improving the quality of cyber threat information it shares across Federal and private sector entities.[44] CISA's lack of progress in improving the quality of information it shares was attributed to a number of factors, such as limited numbers of participants sharing cyber indicators with CISA, delays receiving cyber threat intelligence standards, and insufficient CISA office staff. The Department faced similar challenges in sharing cyber threat information across Federal and private sector entities, as noted in our 2019 report.[45] Until CISA improves the quality of its information sharing, participants remain restricted in their ability to safeguard their systems and the data they process from attack, loss, or compromise.

Improving FEMA's Contracts and Grants Management, Disaster Assistance, and Fraud Prevention

This challenge relates directly to DHS' 2020–2024 Strategic Plan at Goal 5: Strengthen Preparedness and Resilience, Objectives 5.1: Build a National Culture of Preparedness, and 5.2: Respond during Incidents.

[42] *Evaluation of DHS' Information Security Program for Fiscal Year 2019* (OIG-20-77), September 30, 2020.
[43] *Evaluation of DHS' Information Security Program for Fiscal Year 2018* (OIG-19-60), September 19, 2019.
[44] *DHS Made Limited Progress to Improve Information Sharing under the Cybersecurity Act in Calendar Years 2017 and 2018* (OIG-20-74), September, 25, 2020.
[45] *Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015* (OIG-18-10).

We have previously identified a pattern of FEMA management errors in overseeing procurements and reimbursing procurement costs; we continue to observe systemic problems and operational difficulties that contribute to FEMA not managing disaster relief grants and supplies adequately. At times, FEMA has not followed procurement laws, regulations, and procedures, nor has it ensured disaster grant recipients and subrecipients understand and comply with relevant authorities. FEMA has also proven susceptible to widespread fraud and made billions in improper payments, often due to lax oversight.[46]

Planning and Oversight Problems

In the aftermath of Hurricane Maria, we determined that FEMA did not maximize the use of advance contracts to address identified capability deficiencies and needs in Puerto Rico.[47] Specifically, we identified 49 of 241 new contracts issued for the same goods or services covered by existing advance contracts. In addition, FEMA did not issue any new advance contracts prior to Hurricane Maria and did not perform analysis to identify goods or services to obtain through advance contracts. We attributed FEMA's limited use of advance contracts to its lack of strategy and documented planning process for ensuring maximum use of advance contracts. Although FEMA reported to Congress in December 2007 it had a strategy in place, we determined it was a one-time strategy that did not meet the intent of the *Post-Katrina Emergency Management Reform Act of 2006*.[48] Without advance contracts to expedite acquisitions, goods and services for people in need may have been delayed or were more costly to the Government. Further, FEMA did not maintain contract files in accordance with Federal acquisition regulations and departmental or its own policy. This occurred because FEMA's Office of the Chief Procurement Officer did not have controls in place to ensure contract personnel follow Federal regulations and departmental or its own internal policy. As a result, FEMA's ability to hold contractors accountable for deliverables is hindered if contract files are not easily located.

We also determined that FEMA's Public Assistance grant to the Puerto Rico Electric Power Authority (PREPA) in the aftermath of Hurricane Maria did not comply with Public Assistance program guidelines.[49] Specifically, FEMA

[46] FEMA's Fraud Investigations and Inspections Division's (FIID) mission includes identifying, mitigating, deterring, and preventing fraudulent losses of Federal funds and assets through a variety of proactive efforts. In 2018, FIID requested and received permission to create and staff a new Program Review for the Inspections Branch (PRIB). To date, PRIB has conducted 3 program reviews that resulted in 156 recommendations and identified 59 best practices.
[47] *FEMA's Advance Contract Strategy for Disasters in Puerto Rico* (OIG-20-20), March 23, 2020.
[48] Pub. L. No. 109-295, § 691 (codified at 6 U.S.C. § 791).
[49] *FEMA's Public Assistance Grant to PREPA and PREPA's Contracts with Whitefish and Cobra Did Not Fully Comply with Federal Laws and Program Guidelines* (OIG-20-57), July 27, 2020.

reimbursed PREPA more than $852 million for a time and material contract before confirming PREPA provided a high degree of oversight of the contract. Furthermore, FEMA did not determine whether the time and material costs incurred by PREPA were reasonable and eligible for the Public Assistance grant program. This occurred because FEMA lacked guidance about how to verify a subrecipient's oversight of time and material contracts and how to assess reasonableness of time and material contract costs. As a result, FEMA may have reimbursed PREPA for time and material costs that are ineligible for PA funds.

This year we also contracted with public accounting firms to perform numerous FEMA capacity audits related to Hurricanes Irma and Maria,[50] as well as an audit of the Sewerage and Water Board of New Orleans.[51] This body of work demonstrates that FEMA did not always ensure disaster grant subrecipients established and implemented policies, procedures, and practices to account for and expend Public Assistance grant funds according to Federal regulations and FEMA guidance. At the same time, FEMA did not provide adequate oversight or instruction, which increased the risk of ineligible costs, substandard service delivery, unallowable costs, and fraudulent activities related to Public Assistance funds.

Supply Chain Weaknesses

In reviewing FEMA's response to Hurricanes Irma and Maria in Puerto Rico, we also noted significant deficiencies in its commodity distribution process.[52] FEMA lost visibility of approximately 38 percent of its life-sustaining

[50] *Capacity Audit FEMA Grants Awarded to Puerto Rico Department of Housing* (OIG-20-22), April 9, 2020; *Capacity Audit of FEMA Grant Funds Awarded to the Puerto Rico Aqueduct and Sewer Authority* (OIG-20-24), April 9, 2020; *Capacity Audit of FEMA Grant Funds Awarded to the Puerto Rico Department of Transportation and Public Works* (OIG-20-25), April 9, 2020; *Capacity Audit of FEMA Grant Funds Awarded to the Puerto Rico Department of Education* (OIG-20-26), April 9, 2020; *Capacity Audit of FEMA Grant Funds Awarded to the U.S. Virgin Islands Housing and Finance Authority* (OIG-20-29), May 4, 2020; *Capacity Audit of FEMA Grant Funds Awarded to the USVI Department of Education* (OIG-20-30), May 4, 2020; *Capacity Audit of FEMA Grant Funds Awarded to the USVI Water and Power Authority* (OIG-20-39), June 16, 2020; *Early Warning Audit of FEMA Public Assistance Grants to Collier County, Florida* (OIG-20-46), July 10, 2020; *Early Warning Audit of FEMA Public Assistance Grants to Lee County, Florida* (OIG-20-48), July 15, 2020; *Early Warning Audit of FEMA Public Assistance Grants to Polk County School Board, Florida* (OIG-20-50), July 20, 2020; and *Early Warning Audit of FEMA Public Assistance to Monroe County, Florida* (OIG-20-51), July 17, 2020.

[51] *Management of FEMA Public Assistance Grant Funds Awarded to the Sewerage and Water Board of New Orleans Related to Hurricanes Katrina, Isaac, and Gustav* (OIG-20-21), March 27, 2020.

[52] *FEMA Mismanaged the Commodity Distribution Process in Response to Hurricanes Irma and Maria* (OIG-20-76), September 25, 2020.

commodity shipments to Puerto Rico worth an estimated $257 million. Commodities successfully delivered to the Puerto Rico government took an average of 69 days to reach their final destinations. Consequently, FEMA could not provide reasonable assurance it provided sufficient life-sustaining commodities to Puerto Rico disaster survivors in a timely manner. Furthermore, FEMA's mismanagement included multiple contracting violations and policy contraventions that ultimately led to contract overruns of about $179 million and at least $50 million in questioned costs.

FEMA faced tremendous challenges meeting mission requirements because of the catastrophic nature of Hurricane Maria and multiple, concurrent, nationwide disasters. Although we understand FEMA's priority on expediting commodity shipments to disaster survivors, the extent of the deviations from established operating procedures significantly increased the risk for fraud, waste, and abuse. Some flexibility and adaptation of normal processes is expected during disaster responses, but controls necessary to safeguard commodities cannot be altogether ignored. FEMA's emphasis on delivering commodities to disaster survivors overrode the importance of following sound inventory management practices. To ensure this does not happen again, FEMA needs to develop a comprehensive strategy and implementation plans for improving asset tracking and in-transit visibility across all modes of transportation.

Ineligible and Questioned Costs, Improper Payments, and Potential Fraud Risks

FEMA's challenges to take additional, proactive steps to create and sustain a culture of fraud prevention and awareness will likely be exacerbated by the infusion of CARES Act funding.[53] Our work in FY 2020 shows FEMA continues to make ineligible payments from the disaster relief fund by not complying with Federal regulations and its own policies and guidelines.[54] Specifically, for ongoing rebuilding of schools in Louisiana from Hurricane Katrina, FEMA awarded $216.2 million in ineligible funding to repair or replace more than 292 Orleans Parish school facilities for the Recovery School District (RSD).[55] FEMA used a cost estimate rather than actual costs to determine how much to award RSD for schools that were already completed, thus awarding $156.6 million in

[53] *FEMA Must Take Additional Steps to Demonstrate the Importance of Fraud Prevention and Awareness in FEMA Disaster Assistance Programs* (OIG-19-55), July 24, 2019.
[54] *FEMA Should Recover $216.2 Million Awarded to the Recovery School District in Louisiana for Hurricane Katrina* (OIG-20-63), September 15, 2020.
[55] RSD is a statewide school district administered by the Louisiana Department of Education that intervenes in the management of chronically low-performing schools in Louisiana. Because of Orleans Parish public schools' poor performance, the Louisiana Legislature turned the majority of its schools over to RSD.

ineligible funding to RSD. FEMA duplicated benefits by not reducing the amount of the award by $57 million to account for other Federal grant funds RSD received. In addition, FEMA awarded $2.6 million in ineligible funding to replace portable school buildings that were not RSD's legal responsibility at the time of the hurricane.

In a different context, FEMA provides Federal funds through its Individuals and Households Program (IHP) for home repairs to applicants who claim to be underinsured or uninsured and for Small Business Administration (SBA) Dependent Other Needs Assistance (ONA) payments. From 2003 through 2018, FEMA paid $12.7 billion to individuals for home repair assistance and SBA Dependent ONA. We conducted two audits of FEMA's IHP — one related to home repairs and the other related to SBA ONA payments.[56] In both audits we identified weaknesses with FEMA's applicant eligibility determination and risk assessment processes. These weaknesses resulted in more than $6.3 billion in improper payments.

According to Office of Management and Budget (OMB) Circular A-123, Appendix C, when documentation or verification is non-existent to support eligibility payment decisions, payments must be considered improper. However, we found that FEMA through IHP does not collect sufficient supporting documentation or verify that applicants claiming to have no insurance are eligible for home repair assistance. Rather, according to FEMA, it relies on applicant self-certifications because no comprehensive repository of homeowner's insurance data exists and any additional verification processes would delay home repair payments. In the IHP SBA ONA program, FEMA did not collect sufficient income and dependent documentation or verify self-reported information to determine whether applicants below the income threshold, known as the Failed Income Test, were eligible for SBA Dependent ONA payments.

Additionally, FEMA has not adequately evaluated risk associated with not collecting or verifying homeowner's insurance or income and dependent information. Per Federal requirements, agencies must conduct risk assessments to determine whether programs are susceptible to improper payments. Rather, FEMA disregarded significant internal control deficiencies and prior audit findings when evaluating risk. Further, it assessed IHP at the overall program level and did not specifically evaluate each IHP form of assistance, such as SBA Dependent ONA. These weaknesses have allowed

[56] *FEMA Has Made More Than $3 Billion in Improper and Potentially Fraudulent Payments for Home Repair Assistance since 2003* (OIG-20-23), April 6, 2020; and *FEMA Has Paid Billions in Improper Payments for SBA Dependent Other Needs Assistance since 2003* (OIG-20-60), August 12, 2020.

applicants self-certifying homeowner's insurance, income, and dependent information to receive less oversight despite posing the greatest risks for improper payments. Without implementing changes to its home repair and SBA Dependent ONA processes, FEMA cannot ensure it is being a prudent steward of taxpayer dollars and adequately assessing its risks of improper payments and fraud.

Lastly, we noted risks related to fraud in our review of FEMA's Transitional Sheltering Assistance Program.[57] FEMA contracted with Corporate Lodging Consultants (CLC) to provide hotel rooms for disaster survivors. In 2017, FEMA spent about $642 million for more than 5 million hotel rooms. We determined FEMA did not properly award or oversee its contract with CLC to administer disaster survivors' hotel stays, which ultimately resulted in the improper release of personally identifiable information (PII) for about 2.3 million disaster survivors. This unauthorized release of PII increased survivors' risk of identity theft. Inadequate contractor oversight may have also increased the risk that unacceptable lodging conditions were used.

Strengthening Oversight and Management of Major Systems Acquisition

This challenge relates to every aspect of DHS' mission, and is captured in objectives listed under DHS' 2020–2024 Strategic Plan at Goal 6: Championing the Workforce and Strengthening the Department, Objectives 6.1: Strengthen Departmental Governance and Management and 6.3: Optimize Support to Mission Operations.

Systems acquisitions are a key part of DHS' annual budget and are fundamental to the Department's ability to accomplish its mission.[58] A successful systems acquisition process requires an effective acquisition management infrastructure. Acquisition management is a complex process that goes beyond simply awarding a contract. It begins with the identification of a mission need; continues with the development of a strategy to fulfill that need while balancing cost, schedule, and performance; and concludes with contract closeout after satisfactorily meeting the terms. Acquisition management includes managing operational and life cycle requirements — from formulating concepts of operations, developing sound business strategies,

[57] *FEMA Did Not Properly Award and Oversee the Transitional Sheltering Assistance Contract* (OIG-20-58), August 5, 2020.
[58] In FY 2020, DHS budget included about $5 billion for Procurement, Construction and Improvements, to fund planning, operational development, engineering, purchase, and deployment of assets to support component missions; and an additional $546 million for Research and Development, to provide resources needed to identify, explore, and demonstrate new technologies and capabilities to support component missions.

and exercising prudent financial management to assessing tradeoffs and managing program risks. The Department has generally made progress in its acquisition oversight processes and controls through implementation of a revised acquisition management directive. However, it continues to face challenges.

In our second of two audit reports concerning the acquisition of the Department's Performance and Learning Management System (PALMS), we determined that DHS' funding and payments for PALMS violated Federal appropriations law.[59] Specifically, DHS violated the bona fide needs rule, the purpose statute, and the *Antideficiency Act* when the DHS Working Capital Fund used component funds for PALMS implementation. The Department also violated the statutory prohibition on advance payments when it made upfront payments for annual PALMS subscriptions that exceeded the value of the subscription services received. The Department misspent more than $4.6 million in fees for more than 200,000 paid subscriptions that expired before the contractor provided any subscription services.

In July 2020, we reported CBP did not demonstrate the acquisition capabilities needed to execute the Analyze/Select Phase of the Southern Border Wall Acquisition Program effectively.[60] Specifically, CBP did not:

- conduct an Analysis of Alternatives to assess and select the most effective, appropriate, and affordable solutions to obtain operational control of the southern border as directed, but instead relied on prior outdated border solutions to identify materiel alternatives for meeting its mission requirement; or
- use a sound, well-documented methodology to identify and prioritize investments in areas along the border that would best benefit from physical barriers.

We also found the Department did not complete the required plan to execute the strategy to obtain and maintain control of the southern border, as required by its Comprehensive Southern Border Security Study and Strategy. Without an Analysis of Alternatives, a documented and reliable prioritization process, or a plan, the likelihood CBP will be able to obtain and maintain complete operational control of the southern border with mission effective, appropriate, and affordable solutions is diminished.

[59] *PALMS Funding and Payments Did Not Comply with Federal Appropriations Law* (OIG-20-19), March 24, 2020.
[60] *CBP Has Not Demonstrated Acquisition Capabilities Needed to Secure the Southern Border* (OIG-20-52), July 14, 2020.

We also reported that CBP did not have a comprehensive strategy for meeting its Large-Scale Non-Intrusive Inspection (LS-NII) equipment needs at all CBP locations.[61] Instead, CBP uses multiple plans, such as its Multi-Year Investment and Management Plan, and individual acquisition plans for each type of LS-NII equipment it may purchase. At times, these acquisition plans contained conflicting information and did not align with the program's approved lifecycle cost estimate. This occurred because DHS and CBP acquisition officials did not provide effective oversight of CBP's fragmented acquisition planning efforts and did not confirm acquisition plans aligned with LS-NII program objectives. Without improvements, CBP cannot ensure that its multi-million dollar investments in LS-NII technology and equipment will help the component fulfill its mission of protecting U.S. borders.

The Way Forward

As the Department coordinates the Federal response to COVID-19, we urge it to address these other major management and performance challenges. Achieving progress requires steady leadership, unity of effort, and a commitment to mastering management fundamentals. By establishing a strong, overarching internal control structure to reinforce established goals and objectives, the Department will be better able to assign roles and responsibilities, promote coordination of resources and cooperation among programs and operations, promulgate necessary policies and procedures, and ensure compliance and accountability.

[61] *CBP Does Not Have a Comprehensive Strategy for Meeting Its LS-NII Needs* (OIG-20-75), September 28, 2020.

Appendix A

GOAL 1: COUNTER TERRORISM AND HOMELAND SECURITY THREATS
OBJECTIVE 1.1: COLLECT, ANALYZE, AND SHARE ACTIONABLE INTELLIGENCE
OBJECTIVE 1.2: DETECT AND DISRUPT THREATS
OBJECTIVE 1.3: PROTECT DESIGNATED LEADERSHIP, EVENTS, AND SOFT TARGETS
OBJECTIVE 1.4: COUNTER WEAPONS OF MASS DESTRUCTION AND EMERGING THREATS

GOAL 2: SECURE U.S. BORDERS AND APPROACHES
OBJECTIVE 2.1: SECURE AND MANAGE AIR, LAND, AND MARITIME BORDERS
OBJECTIVE 2.2: EXTEND THE REACH OF U.S. BORDER SECURITY
OBJECTIVE 2.3: ENFORCE U.S. IMMIGRATION LAWS
OBJECTIVE 2.4: ADMINISTER IMMIGRATION BENEFITS TO ADVANCE THE SECURITY AND PROSPERITY OF THE NATION

GOAL 3: SECURE CYBERSPACE AND CRITICAL INFRASTRUCTURE
OBJECTIVE 3.1: SECURE FEDERAL CIVILIAN NETWORKS
OBJECTIVE 3.2: STRENGTHEN THE SECURITY AND RESILIENCE OF CRITICAL INFRASTRUCTURE
OBJECTIVE 3.3: ASSESS AND COUNTER EVOLVING CYBERSECURITY RISKS
OBJECTIVE 3.4: COMBAT CYBERCRIME

GOAL 4: PRESERVE AND UPHOLD THE NATION'S PROSPERITY AND ECONOMIC SECURITY
OBJECTIVE 4.1: ENFORCE U.S. TRADE LAWS AND FACILITATE LAWFUL INTERNATIONAL TRADE AND TRAVEL
OBJECTIVE 4.2: SAFEGUARD THE U.S. TRANSPORTATION SYSTEM
OBJECTIVE 4.3: MAINTAIN U.S. WATERWAYS AND MARITIME RESOURCES
OBJECTIVE 4.4: SAFEGUARD U.S. FINANCIAL SYSTEMS

GOAL 5: STRENGTHEN PREPAREDNESS AND RESILIENCE
OBJECTIVE 5.1: BUILD A NATIONAL CULTURE OF PREPAREDNESS
OBJECTIVE 5.2: RESPOND DURING INCIDENTS
OBJECTIVE 5.3: SUPPORT OUTCOME-DRIVEN COMMUNITY RECOVERY
OBJECTIVE 5.4: TRAIN AND EXERCISE FIRST RESPONDERS

GOAL 6: CHAMPION THE DHS WORKFORCE AND STRENGTHEN THE DEPARTMENT
OBJECTIVE 6.1: STRENGTHEN DEPARTMENTAL GOVERNANCE AND MANAGEMENT
OBJECTIVE 6.2: DEVELOP AND MAINTAIN A HIGH PERFORMING WORKFORCE
OBJECTIVE 6.3: OPTIMIZE SUPPORT TO MISSION OPERATIONS

Source: Department of Homeland Security's Strategic Plan for Fiscal Years 2020–2024 (undated)
Table of Contents

Appendix B
DHS Comments to the Draft Report

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

Homeland Security

November 3, 2020

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

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

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2020.11.03 16:12:13 -05'00'

SUBJECT: Management Response to the Office of Inspector General's (OIG) Draft Report: "Major Management and Performance Challenges [MMPC] Facing the Department of Homeland Security" (Project No. 21-006-IQO-DHS)

Thank you for the opportunity to comment on this draft report. As Acting Secretary of Homeland Security Chad Wolf remarked during his "2020 State of the Homeland" address on September 9, 2020:

> "The Department of Homeland Security [DHS or the Department] is bound by one mission, one creed. Answering the call, often times in the most arduous of environments and difficult circumstances, to safeguard the American people, our homeland, and our values from all threats, all the time—both today, tomorrow, and in the years to come … we stand—ready to rise and ready to face the next challenge that threatens our homeland."

The Acting Secretary also highlighted that during the past year the Department was:

- Leading the Federal Government's response to a global pandemic;
- Protecting federal buildings and federal law enforcement officers from an emerging threat of violent rioters;
- Combatting crises at the Southern Border, including human trafficking, drug smuggling, and unprecedented illegal migration flows;
- Fortifying our economic security by tightening our immigration system, preserving free and fair trade, and thwarting the growing threats posed by China now and in the future; and
- Identifying and preventing malign foreign actors and nation states from interfering in our elections and protecting our election infrastructure.

Against each of these challenges, DHS has marshaled its resources, tapped its authorities, and unified its efforts to safeguard the American people and our way of life. Yet, as Acting Secretary Wolf also stated, "We will not rest on yesterday's success. Our eyes are on the horizon. On the future."

DHS recognizes the Office of Inspector General's (OIG) perspective on the most serious management and performance challenges facing the Department and our progress in addressing these challenges. DHS is also mindful of its responsibility to be a good steward of taxpayer dollars.

Senior DHS leadership, however, is concerned that in developing the challenges identified in this year's MMPC report, OIG (1) understated the vast responsibility the Federal Emergency Management Agency (FEMA) has had to assume in response to the coronavirus (COVID-19) pandemic, and (2) focused on highlighting the findings and conclusions its auditors, evaluators, and inspectors summarized in previously published reports without including almost any Departmental perspective on these issues. It is important to recognize that various DHS leaders, program officials, and subject matter experts expressed significant concerns about and disagreement with many of OIG's findings and conclusions at the time the original reports were published.

Without this context, OIG's MMPC report is extremely misleading and, frankly, does a disservice to end users of the report (including Congress and the public) by providing a skewed discussion about the challenges OIG believes DHS faces, challenges with which the Department does not necessarily disagree. We note that the Departmental concerns and disagreements were discussed in the referenced individual final reports and subsequent communications; however, it is unlikely that end users of OIG's MMPC report will seek or access all of this information in order to obtain the missing Departmental perspectives.

Additional information about FEMA's significantly increased responsibilities and examples of specific contextual concerns with selected audits the OIG highlighted in its various challenge areas is provided below:

- **Performing Fully and Effectively during COVID-19**

OIG's MMPC report tremendously understates the magnitude of new responsibilities FEMA assumed in the face of the COVID-19 pandemic, a historic challenge that has tested federal response capabilities. For the first time in our Nation's history, all 55 states and territories, as well as District of Columbia were declared under the same nationwide Emergency Declaration. On March 19, 2020, FEMA was designated to lead federal COVID-19 pandemic response operations, while keeping up with all of

2

its other responsibilities at the same time. The scale and scope of this pandemic necessitated a collaborative interagency response. There have been more than 46,000 personnel from over 40 agencies—such as the Department of Defense, Department of Health and Human Services (HHS), Centers for Disease Control and Prevention, Department of Veterans Affairs, U.S. Army Corps of Engineers, Defense Logistics Agency — embedded within FEMA's National Response Coordination Center and ten Regional Response Coordination Centers to coordinate response and recovery efforts at both the national and local levels.

FEMA has obligated $54 billion in support of COVID-19 efforts, including $42 billion for the Lost Wages Assistance Program to ease the economic burden for those struggling with lost wages due to the COVID-19 pandemic pursuant to a Presidential authorization. Additionally, as of October 30, 2020, FEMA, HHS, and the private sector coordinated delivery of or are currently shipping: 309.2 million N95 respirators, 1.3 billion surgical and procedural masks, 66.9 million face and eye shields, 571.4 million surgical gowns and coveralls, 33.3 billion gloves, and more than 15,000 ventilators. FEMA also supported HHS efforts to drastically expand COVID-19 testing capabilities.

While COVID-19 has affected all of the Agency's operations, the men and women of FEMA never lost sight of ongoing recovery efforts or need to posture for future incidents. Since March 13, 2020, there have been 35 non-COVID major disaster declarations across 21 states, including declarations for flooding, hurricanes, tornadoes, and wildfires. FEMA deployed more than 8,300 staff to these and other non-COVID active disasters operating out of physical and virtual Joint Field Offices, Joint Recovery Offices, and Regional Offices across the nation. Furthermore, FEMA actively worked to ensure sustained resilience of its operations. The Agency has enhanced facility redundancy, increased robust staffing options, deepened its interagency partnerships, and drafted new guidance to ensure prioritization of life safety, life sustainment, and workforce protection while maintaining delivery of FEMA programs to the highest level possible.

- **Countering Terrorism and Homeland Security Threats**

  - "TSA Challenges with Passenger Screening Canine [PSC] Teams (Redacted)," OIG-20-28, dated April 28, 2020.

  OIG reported the Transportation Security Administration (TSA) could not show that deployed PSC teams provide effective security at screening checkpoints and thus our Nation's aviation system and the traveling public could be at risk of a catastrophic event caused by an undetected explosive device. However, TSA

3

strongly disagreed with the report's conclusions, including the statement that "TSA could have redirected the nearly $77 million it spent on PSC teams to other security programs and activities to better protect the aviation system." TSA leadership stated: "The OIG audit team has not completed any analysis with the level of methodological rigor necessary to support these conclusions."

- "CBP Needs a Comprehensive Process for Conducting Covert Testing and Resolving Vulnerabilities (Redacted)," OIG-20-55, dated July 28, 2020.

OIG reported that U.S. Customs and Border Protection (CBP) did not comprehensively plan and conduct covert tests of its operations at Border Patrol checkpoints and ports of entry, use test results to address vulnerabilities, or widely share lessons learned. The OIG report took nearly two years to complete and in its management response, CBP stated its concern that the report contains several inaccurate and misleading representations. These included the definition of "risk" OIG applied to CBP's program methodologies, which could seemingly only be explained by OIG fundamentally misunderstanding Homeland Security risk management doctrine and CBP's covert testing program. CBP contests the OIG's conclusion that CBP does not comprehensively plan and conduct covert testing or use its test results to address vulnerabilities as a false understanding of the process.

Ensuring Proper Financial Management

- "DHS Confirmed It Has Applied Lessons Learned in the Latest Financial System Modernization Effort," OIG-20-09, dated December 19, 2020.

With regard to "The Need for Modernization" portion of this challenge, the OIG referenced only one report highlighting DHS's awareness of the importance of identifying and applying lessons learned as the Department continues to implement the Financial Systems Modernization (FSM) TRIO program. OIG's narrative then went on to mention avoiding past errors and using resources wisely. While the Department appreciates OIG's recognition of the progress made to modernize DHS financial systems, the narrative did not mention senior DHS leadership's disappointment with the report because (1) the scope and objectives of the report varied so greatly from those OIG originally announced, resulting in a much less value-added report for the Department, and (2) the report's conclusion that money spent on the FSM program could have been better spent had more focused attention been dedicated to identifying and applying lessons learned through the years lacked context and, as such, was misleading. More specifically, the report did not provide any context concerning the value received from prior FSM efforts (i.e., investments). In fact, DHS realized significant benefits from

these efforts, which was outlined in the Department's management response to OIG's report.

The referenced OIG report also took nearly two years to complete and is now almost a year old, meaning that the information contained therein is extremely dated. The TRIO program, which is overseen by a Headquarters Joint Program Management Office (JPMO) and is part of a broader FSM program, managed by the JPMO, includes three DHS Components: (1) Countering Weapons of Mass Destruction (CWMD), (2) TSA, and (3) the United States Coast Guard (USCG). CWMD has used the Financial Systems Modernization Solution (FSMS) for several years and successfully underwent a technical refresh in 2019. DHS is proud to report that TSA was migrated to FSMS in October 2020. The implementation and cutover activities were very successful in large part due to the reliance on FSM lessons learned. The JPMO maintains a repository with over 700 lessons learned and leverages these lessons across all FSM programs, including Trio and future efforts for FEMA, U.S. Immigration and Customs Enforcement, and other Components. Lessons are gathered in the following categories, in alignment with Project Management Institute standards: (1) Change Management, (2) Communications, (3) Cost, (4) Documentation, (5) Governance, (6) Human Resources, (7) Procurement, (8) Project Management, (9) Quality, (10) Risk, (11) Schedule, (12) Scope, and (13) Systems Engineering.

It is also important to note the OIG's MMPC report does not recognize that the Department continues to make significant progress ensuring proper financial management as evidenced by having now earned an unmodified (clean) audit opinion on its financial statements for the past eight years and greatly reducing its' material weaknesses and significant internal control deficiencies. USCG and FEMA, the two primary drivers of remaining weaknesses, are both scheduled to move to modern systems in fiscal years 2022 and 2024, respectively.

- **Ensuring Information Technology (IT) Supports Essential Mission Operations**

  - "DHS Lacked Technology Needed to Successfully Account for Separated Migrant Families," OIG-20-06, dated November 25, 2019.

OIG reported, in part, that DHS was unable to reunify families as mandated by a federal judge due to poor data tracking, information sharing, and IT systems capabilities. Not disclosed in the MMPC report was DHS's concern, among others, that OIG's inflated numbers that will lead to misunderstandings and misperceptions as to the Department's operational efforts and compliance with court orders. Specifically, OIG's report inaccurately characterized the level of

5

certainty to which DHS and the Department of Health and Human Services (HHS) identified separated parents and children. OIG's conclusions were based on a flawed analysis of DHS data systems in an attempt to try to confirm the numbers of "potentially separated minors who were not included in DHS's numbers." The OIG's data analysis did not include information from the full range of sources and methods used by DHS, HHS, and the Department of Justice to identify and verify the numbers of separated children. As a result, the degrees of certainty between the multi-agency reunification effort and the OIG's limited analysis were not remotely comparable.

- "Evaluation of DHS' Information Security Program for Fiscal Year 2019," OIG-20-77, dated September 30, 2020.

OIG reported an overall reduction in the program's effectiveness. The Department disagreed with OIG's overall assessment that DHS regressed in the management of its information security program due to the decision made by a former DHS Chief Information Officer (CIO) permitting the USCG to submit their cybersecurity and Federal Information Security Modernization Act (FISMA) reports to the Department of Defense. OIG's conclusion seemed to primarily derive from an incorrect legal assessment that the CIO lacked the authority to make such a decision, despite the Department reiterating the DHS CIO is afforded *statutory authority* to accept cybersecurity risk for the Department. DHS previously demonstrated in meetings and with supporting documentation that the CIO acted appropriately to accept risk and confirmed this decision with the Office of Management and Budget and Federal Chief Information Security Officer.

- **Improving FEMA's Grant Management, Disaster Assistance, and Fraud Prevention.**

  - "FEMA Mismanaged the Commodity Distribution Process in Response to Hurricanes Irma and Maria," OIG-20-76, dated September 25, 2020.

With regard to the "Supply Chain Weakness" portion of this challenge, the OIG referenced a single report highlighting "significant deficiencies" in FEMA's commodity distribution process. In its management response to this report, FEMA leadership disagreed with OIG's conclusion. FEMA explained that while the response to Hurricanes Irma and Maria in Puerto Rico posed a number of logistical challenges, FEMA delivered a historic quantity of 63.6 million (M) meals and 74.1 M liters of water to the Commonwealth of Puerto Rico government from September 2017 through April 2018. FEMA also explained how it recognized the opportunity for, and taken actions to improve staffing, training, processes, tools, and accounting for meals and water.

6

- "FEMA Has Made More Than $3 Billion in Improper and Potentially Fraudulent Payments for Home Repair Assistance since 2003," OIG-20-23, dated April 6 2020, and "FEMA Has Paid Billions in Improper Payments for SBA [Small Business Administration] Dependent Other Needs Assistance since 2003," OIG-20-60, dated August 12, 2020.

With regard to the "Improper Payments and Fraud Prevention" portion of this challenge, the OIG reported weaknesses in FEMA's applicant eligibility determination and risk assessment processes resulting in more than $6.3 billion in improper payments. The OIG did not report that FEMA leadership strongly disagreed with the OIG's conclusions. For example, FEMA believes the OIG overstates the amount of questionable home repair assistance FEMA provided by categorically questioning assistance payments made to applicants who self-certified a lack of homeowner's insurance. FEMA has exhaustively researched potential ways to reliably and expeditiously verify whether an applicant has homeowner's insurance. FEMA also has significant concerns with the methodology that was used to project the improper payment figure provided within the home repair report. Of the $3 billion of assistance payments questioned by the OIG, the OIG's report raises potential questions about 2 percent of the limited sample of payments reviewed.

Concerning OIG-20-60, FEMA also did not agree with the OIG's assessment that a five percent deviation in income reporting necessarily indicated an error on FEMA's part. The U.S. Census Bureau reported that the U.S. median household income during 2017 was $60,336, five percent of which is $3,017. FEMA does not regard a $3,000 reporting differential to automatically indicate error or malintent. A multitude of reasons could explain why an applicant's reported income immediately after a disaster is $3,000 less or more than what they report at the end of the year, such as income fluctuation. Many applicants—US citizens, noncitizen nationals, or qualified aliens—do not have a standard and predictable annual salary, so comparing reported income at different points in the same year could produce discrepancies that are not attributable to the applicant purposefully misrepresenting their income in an attempt to qualify for disaster aid.

FEMA believes that it is unlikely that all these income reporting differentials were incorrect and not, at least in some cases, due to actual income differences between the time reported to FEMA and the time reported to the IRS. However, even if all applications had a reporting differential due to an error on the part of the applicant, FEMA does not believe such errors warrant slowing the delivery of potentially life-saving disaster assistance for the other nearly 80 percent of the applicant's in order to eliminate that reporting error.

7

- **Strengthening Oversight and Management of Major Systems Acquisition**

  - "PALMS [Performance and Learning Management System] Funding and Payments Did Not Comply with Federal Appropriations Law," OIG-20-19, dated March 24, 2020.

The OIG highlights its belief that DHS's funding and payments for PALMS violated federal appropriations law, and a statutory prohibition on advance payments resulting in more than $4.6 million being misspent. The MMPC report, however, does not disclose that many DHS program officials, subject matter experts (including counsel), and others disagreed with the OIG's conclusions, which they viewed as significantly flawed and inaccurate factual representations, despite numerous meetings and the thousands of pages of technical comments and supporting documentation provided to the audit team during the two and a half years it took to complete this audit.

In addition, DHS viewed the OIG's findings and recommendations as inconsistent with the legislative framework governing the DHS Working Capital Fund and argued that these findings contravened longstanding interpretations of those governing provisions and the administrative practices and policies that effectuate those interpretations. DHS also non-concurred with the nine recommendations in the report, disagreements which remain open and unresolved.

  - "CBP Has Not Demonstrated Acquisition Capabilities Needed to Secure the Southern Border," OIG-20-52, dated July 14, 2020.

In a report that took nearly three years to complete, the OIG concluded DHS and CBP inadequately analyzed and incompletely documented the decision-making processes. In its management response, DHS expressed strong disagreement with the OIG's analysis and expressed concerns about the apparent misalignment of purpose and product with the OIG's report, specifically: (1) regarding the role of an Executive Branch agency, (2) conflation and confusion of "Operational Control" and "Impedance and Denial," and (3) the proper use of an Analysis of Alternatives versus an Alternatives Analysis. The OIG made three recommendations, two with which DHS non-concurred and one with which it agreed based on the belief DHS had already completed it. The OIG asserted what DHS viewed as an appropriate response to the third recommendation was inadequate, resulting in all recommendations remaining open and unresolved.

8

- "CBP Does Not Have a Comprehensive Strategy for Meeting Its LS-NII [Large Scale Non-Intrusive Inspection] Needs," OIG-20-75, dated September 20, 2020.

The OIG reported that CBP did not have a comprehensive strategy for meeting its LS-NII equipment needs at all CBP locations. DHS and CBP strongly disagreed with the OIG's conclusion that acquisition officials did not provide effective oversight of CBP's acquisition planning efforts and did not confirm acquisition plans aligned with LS-NII program objectives. In fact, the LS-NII program's acquisition planning was consistent with the Department's Management Directive 102-01, "Acquisition Management," dated February 25, 2019, and its implementing instructions. For example, the OIG's draft report did not address the program's demonstrated compliance with required acquisition activities, including recognizing that the program: (1) had an approved Acquisition Program Baseline, (2) was exempt from having a Test and Evaluation Master Plan, and (3) was actively pursuing acquisition management activities to address future program requirements. The report instead suggests that CBP is not acting in accordance with DHS acquisition policies.

In addition, the OIG did not disclose Departmental concerns that the OIG's findings reflected in the draft report were not timely or current. For example, the OIG announced the LS-NII audit on April 24, 2018 and released its draft report for technical and management comments on June 23, 2020. During this 26-month audit period, however, DHS' acquisition policies were revised, and the OIG's findings did not fully account for these policy revisions.

Looking forward to next year's MMPC report, DHS leadership would appreciate receiving the OIG's draft in August or September (as has occurred in some past years) to begin the review, comment, and final publication process. Receiving the report in October or November, as occurred this year and in some prior years, places an undue burden on both DHS and the OIG to finalize the report for inclusion as part of the Department's Annual Financial Report by mid-November, as required by statute.

Again, thank you for the opportunity to review and comment on this draft report. DHS strives to maintain a culture where all its employees and contractors understand that audits help make us better and both auditors and auditees must be engaged throughout the audit lifecycle. DHS will continue to be open and transparent with the OIG and responsive to the OIG's requests for information, devoting an appropriate level of attention among competing mission-related priorities and demands to the OIG's work. DHS will also remain committed to actively following up on recommendation implementation. Please feel free to contact me if you have any questions. We look forward to working with you during the coming year.

9

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