OFFICE OF INSPECTOR GENERAL

Major Management and Performance Challenges Facing the Department of Homeland Security

Homeland Security

October 27, 2022

OIG-23-01

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, D.C. 20528 / www.oig.dhs.gov

October 27, 2022

MEMORANDUM FOR: The Honorable Alejandro N. Mayorkas
Secretary
Department of Homeland Security

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

JOSEPH V CUFFARI

Digitally signed by JOSEPH V CUFFARI
Date: 2022.10.27 15:36:06 -07'00'

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

For your information is our final report, *Major Management and Performance Challenges Facing the Department of Homeland Security*. This annual publication, required by the *Reports Consolidation Act of 2000*, summarizes what the OIG considers the most serious management and performance challenges facing the Department of Homeland Security and assesses its progress addressing them. It is intended to help the Department improve program performance and ensure the effectiveness of its operations.

These challenges are based on OIG's independent research, assessment, and judgment. They also relate to the three major priorities you identified as you assumed leadership of DHS (immigration, cybersecurity, and targeted violence/terrorism); the Department's operations under its six strategic goals in the *Department of Homeland Security's Strategic Plan for Fiscal Years 2020–2024*[1]*;* and the 12 strategic priorities in *DHS' 2022 Priorities*[2].

In this edition, OIG identifies eight challenges that reflect overarching issues affecting multiple DHS programs and responsibilities. They are not the only challenges confronting DHS - OIG's reports highlight specific opportunities to improve programs and operations. These eight challenges include:

- Countering Terrorism and Homeland Security Threats;
- Coordinating Border Security Efforts and Managing Migrant Surges and Resettlements;
- Managing Detention Conditions;
- Securing Cyberspace and Critical Infrastructure;
- Ensuring Proper Financial Management and Oversight;

[1] https://www.dhs.gov/sites/default/files/publications/19_0702_plcy_dhs-strategic-plan-fy20-24.pdf. See Appendix A
[2] https://www.dhs.gov/2022-priorities. See Appendix B

- Ensuring Technology Supports Essential Mission Operations;
- Improving FEMA's Disaster Assistance and Fraud Prevention; and
- Strengthening Oversight and Management of Major Systems Acquisition and Procurement.

In this report, we describe each challenge and potential associated risks, summarize actions DHS has taken or is taking to address each challenge, and summarize steps DHS needs to take to further address each challenge. OIG received technical comments on a draft of this report and made revisions as appropriate.

Countering Terrorism and Homeland Security Threats

THE CHALLENGE

DHS is challenged to effectively plan and provide adequate guidance, oversight, and monitoring of programs and operations to counter terrorism and homeland security threats and leverage law enforcement unity of effort. In addition, DHS seeks to achieve specific objectives related to countering terrorism and homeland security threats in strategic goal 1 as well as strategic priority 7.

WHY IS THIS A CHALLENGE?

Domestic and international actors abroad pose dangers to our Nation and at its borders. The threats are dynamic and becoming more complex. Threats are more interconnected, technologically advanced, targeted, and close to home.

Countering Terrorism:

Following the breach of the U.S. Capitol building in Washington, D.C. on January 6, 2021, we found DHS identified specific threat information prior to January 6 but did not issue any intelligence products about these threats until 2 days later. DHS was unable to provide its many state, local, and Federal partners with timely, actionable, and predictive intelligence.[3] Additionally, DHS did not adequately follow its internal processes and comply with applicable Intelligence Community policy standards and requirements when editing and disseminating an Office of Intelligence and Analysis (I&A) intelligence product regarding Russian interference in the 2020 U.S. Presidential election,[4] which put I&A at risk of creating a perception of politicization. We also determined DHS has not completed, as planned, 70 percent of the goals under its strategic framework for countering domestic

[3] *I&A Identified Threats prior to January 6, 2021, but Did Not Issue Any Intelligence Products before the U.S. Capitol Breach*, OIG-22-29, Mar. 2022.
[4] *DHS Actions Related to an I&A Intelligence Product Deviated from Standard Procedures (REDACTED)*, OIG-22-41, Apr. 2022.

terrorism, and can improve how it identifies domestic terrorism threats, tracks trends for future risk-based planning, and informs partners and the public about domestic terrorism.[5]

We continue to identify challenges DHS faces countering improvised explosive devices. DHS needs to improve its management of component activities to comply with implementation of *Presidential Policy Directive 17: Countering Improvised Explosive Devices* within DHS. OIG continues to review DHS' countering terrorism efforts including DHS' response to the events of January 6, 2021, and DHS' procedures and technology systems to safeguard and share terrorist screening data.

Law Enforcement Unity of Effort:

We continue to identify law enforcement missions where DHS would benefit from better collaboration, sharing and leveraging processes, data collection, and best practices across components. We have identified inadequate oversight of DHS' law enforcement components to ensure proper DNA collection[6] and preparation for cross-component protection of Federal facilities.[7] We found that U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations investigated less than 1 percent of U.S. Customs and Border Protection's (CBP) Intellectual Property Rights seizures annually from fiscal years 2017 to 2020 because CBP did not prioritize reporting investigative referrals to ICE, nor did it establish guidance or a system to do so.[8] Further, we found opportunities for the Cybersecurity and Infrastructure Security Agency (CISA), Office for Bombing Prevention to improve its oversight of components' input for countering improvised explosive devices and to better lead DHS and nationwide capability efforts to address these threats.[9] Finally, DHS component collaboration on law enforcement virtual training is limited.[10]

[5] *DHS Could Do More to Address the Threats of Domestic Terrorism*, OIG-22-49, July 2022.
[6] *DHS Law Enforcement Components Did Not Consistently Collect DNA From Arrestees*, OIG-21-35, May 2021.
[7] *DHS Had Authority to Deploy Federal Law Enforcement Officers to Protect Federal Facilities in Portland, Oregon, but Should Ensure Better Planning and Execution in Future Cross-Component Activities*, OIG-21-31, Apr. 2021.
[8] *DHS and CBP Should Improve Intellectual Property Rights Management and Enforcement (REDACTED)*, OIG-22-52, July 2022.
[9] *The Office for Bombing Prevention Needs to Improve Its Management and Assessment of Capabilities to Counter Improvised Explosive Devices*, OIG-22-33, Mar. 2022.
[10] *DHS Component Collaboration on Law Enforcement Virtual Training Is Limited*, OIG-22-67, Sep. 2022.

WHAT PROGRESS HAS DHS MADE?

Countering Terrorism:

DHS has developed strategies and taken other steps to help the U.S. counter terrorism, and has made progress countering domestic terrorism. For example, DHS implemented redundant capabilities to disseminate intelligence products addressing departmental threats. Additionally, DHS will initiate a needs assessment to identify staffing and budget requirements to counter domestic terrorism. The Department's Counterterrorism Coordinator will work with other program offices to evaluate the oversight and coordination of efforts to counter domestic terrorism following the conclusion of the needs assessment.

Law Enforcement Unity of Effort:

DHS continues its efforts to develop and update internal controls, directives, policies, procedures, and training plans, as well as improve its integration of data sources and modernize its reporting systems to generate real-time automated reports. These actions are designed to strengthen collaboration among its components and Federal law enforcement partners. For example, on September 29, 2021, the Secretary established the Law Enforcement Coordination Council that coordinates department-wide law enforcement related matters on training and policy.

WHAT DHS STILL NEEDS TO DO

DHS needs to remain committed to effective threat assessment methods and law enforcement collaboration, as well as internal control development, including useful and relevant goals, performance indicators, metrics, measures, corrective action plan implementation, and deliberate improvement. In addition, DHS needs to enhance and provide intelligence training and guidance and improve its processes for timely reviews of open source intelligence products. DHS could also improve how it identifies domestic terrorism threats, tracks trends for future risk-based planning, and informs partners and the public about domestic terrorism. DHS needs to better manage its counter-improvised explosive devices (C-IED) efforts, as well as its assessment of national, regional, and state C-IED capabilities. Finally, DHS needs to address multiple unresolved and open recommendations from OIG's previous reports.[11]

[11] *ICE Faces Challenges to Screen Aliens Who May Be Known or Suspected Terrorists*, OIG-18-36, Jan 2018; *A Joint Review of Law Enforcement Cooperation on the Southwest Border between the Federal Bureau of Investigation and Homeland Security Investigations*, OIG-19-57, July 2019; and *HSI Effectively Contributes to the FBI's Joint Terrorism Task Force, But Partnering Agreements Could Be Improved (REDACTED)*, OIG-20-59, Aug 2020.

Coordinating Border Security Efforts and Migrant Surges

THE CHALLENGE

Migrant and refugee surges continue to pose significant challenges for DHS. Meanwhile, DHS seeks to achieve specific objectives related to securing U.S. borders and approaches in strategic goal 2 as well as strategic priority 9.

WHY IS THIS A CHALLENGE?

CBP apprehended more than 1.6 million migrants illegally crossing the Southwest Border in FY 2021. This trend continued in FY 2022. Migrant surges require a whole-of-government approach. DHS manages a major part of the border security and immigration enforcement mission set, but in prior surges multi-component planning between CBP and ICE and a coordinated response ultimately did not occur. These surges in immigration have exposed technology challenges which impede CBP and ICE personnel from tracking migrants from apprehension to release or transfer. Technology deficiencies also meant that data was not consistently documented in DHS' systems of record, which can delay DHS from uniting children with families and sponsors, or cause migrants to remain in DHS custody longer than legally allowed.[12]

The United States also experienced a sudden influx of Ukrainian and Afghan citizens requesting entry into the country under unprecedented circumstances. This change in immigration patterns reconfirmed longstanding staffing issues at CBP. Sufficient staffing is needed to ensure complete and accurate processing of all individuals requesting entry into the United States. However, screening, vetting, and inspecting all evacuees during the recent Afghanistan crisis was a challenge, and OIG continues to evaluate CBP's access to critical data to fully vet individuals trying to enter the United States. OIG continues to conduct reviews in this area, such as DHS' preparations to receive and expedite requests from Afghan evacuees for long-term legal status, and the effectiveness of DHS' technology, procedures, and coordination to screen and vet non-citizens entering or resettling in the United States.

WHAT PROGRESS HAS DHS MADE?

Corrective action plans submitted to OIG show that DHS is updating its technology platforms to enhance information sharing across its components and with external partners, including the U.S. Department of Health and Human Services. DHS is also updating internal guidance to ensure staff fully

[12] *DHS Technology Systems Do Not Effectively Support Migrant Tracking at the Southwest Border*, OIG 22-66, Sep. 2022; *ICE and CBP Should Improve Visa Security Program Screening and Vetting Operations*, OIG-22-70, Sep. 2022; and *U.S. Border Patrol Screened Migrants at the Southwest Border but Could Strengthen Processes*, OIG-22-71, Sep. 2022.

understand processes, procedures, technology systems, and the value of robust controls.

WHAT DHS STILL NEEDS TO DO

DHS should continue to address internal fragmentation affecting border security and immigration processing. DHS should work on improving consistent application of standard procedures to fully document migrant apprehensions and to enhance timely and orderly processing to identify security threats. DHS should also develop a comprehensive contingency plan to handle evacuation efforts in the future and thoroughly account for, screen, vet, and inspect all individuals during unprecedented events when limited biographic data is available.[13] Additionally, DHS needs to address multiple unresolved and open recommendations from OIG's previous reports.[14]

Managing Detention Conditions

THE CHALLENGE

Managing its detention system and safe, orderly, and humane immigration processes continues to be a significant challenge for DHS, particularly given recent surges at the Southwest border. In addition, DHS seeks to achieve specific objectives related to enforcing immigration law in strategic goal 2 and strategic priority 10.

WHY IS THIS A CHALLENGE?

Surges result in prolonged detention in short-term facilities, overcrowding, capacity issues, and inconsistent compliance with standards for care at Border Patrol stations. According to CBP officers, the lack of bed space at ICE detention facilities also contributes to the challenges CBP is experiencing managing migrants at its facilities. Additionally, DHS continues to struggle with contractor performance and overall compliance with detention standards such as segregation,[15] medical care, and access to legal services.[16] For example, in March 2022, OIG issued a Management Alert[17] recommending the immediate removal of all detainees from the Torrance County Detention Facility

---

[13] *DHS Encountered Obstacles to Screen, Vet, and Inspect All Evacuees during the Recent Afghanistan Crisis (Redacted)* OIG-22-64, Sep. 2022.
[14] *DHS Missing Data Needed to Strengthen Its Immigration Enforcement Efforts*, OIG-15-85, May 2015; *Border Patrol Needs a Better Plan For Hiring More Agents*, OIG-19-23, Feb 2019; *CBP Has Taken Steps to Limit Processing of Undocumented Aliens at Ports of Entry*, OIG-21-02, Oct 2020;
[15] *ICE Needs to Improve Its Oversight of Segregation Use in Detention Facilities*, OIG-22-01, Oct. 2021.
[16] *Capping Report: CBP Struggled to Provide Adequate Detention Conditions During 2019 Migrant Surge*, OIG-20-38, June 2020.
[17] *Management Alert – Immediate Removal of All Detainees from the Torrance County Detention Facility*, OIG-22-31, Mar. 2022.

in Estancia, New Mexico due to safety risks and unsanitary living conditions. In April 2022, we made several recommendations aimed at improving care of detainees at the South Texas ICE Processing Center.[18] We continue to perform unannounced inspections of ICE adult detention facilities and CBP holding facilities.

WHAT PROGRESS HAS DHS MADE?

CBP has taken steps to increase coordination and planning, enhance existing infrastructure to add capacity, and expand access to medical care through improved screening. According to DHS, ICE continues to improve conditions at its detention facilities and completing any identified repairs from internal or OIG inspections. In addition, ICE has updated its request tracking system and enhanced its documentation of commissary and mail services for detainees at the South Texas ICE Processing Center. Further, DHS recently announced it is creating a new Office of Health Security to coordinate and provide oversight for public health, medical, and safety activities for both its own workforce and those in its care.

WHAT DHS STILL NEEDS TO DO

DHS should work on improving consistent application of standards for treatment and care of migrants and timely, orderly, and humane processing. Additionally, DHS needs to address OIG recommendations including one unresolved and open recommendation from a previous report.[19]

Securing Cyberspace and Critical Infrastructure

THE CHALLENGE

DHS must provide a high level of cybersecurity for the information and systems supporting day-to-day operations for its approximately 240,000 personnel. DHS' mission in this area, providing enterprise-wide security solutions to protect the Department and partnering with industry and government, is multi-faceted and vast. This persistent challenge relates to every aspect of DHS' mission and relates to all of DHS' strategic goals as well as strategic priority 8 to increase cybersecurity. Additionally, multiple administrations have issued executive orders to improve the Nation's cybersecurity and to secure the critical infrastructure underlying our Nation's economy and way of life.

[18] *Violations of ICE Detention Standards at South Texas ICE Processing Center*, OIG-22-40, Apr. 2022.
[19] *Violations of Detention Standards Amidst COVID-19 Outbreak at La Palma Correctional Center in Eloy, AZ*, OIG-21-30, Mar. 2021.

WHY IS THIS A CHALLENGE?

Recent breaches have shown that cyber attacks pose a serious threat against the Nation's cyberspace and critical infrastructure, and why preventing such attacks will remain a major management challenge. These attacks have been designed to gain unauthorized access to sensitive data stored and processed by DHS systems, infiltrate U.S. Government computers and networks to slow or halt operations, access intellectual property and research, and gather useful intelligence. In addition to Nation-state sponsored Advanced Persistent Threats,[20] recent attacks include the SolarWinds Orion breach, Microsoft Exchange attacks, and the Colonial Pipeline ransomware victimization. As cyber threats evolve, securing U.S. technology systems and networks from unauthorized access and potential exploits will become more challenging.

WHAT PROGRESS HAS DHS MADE?

The DHS Secretary has made operationalizing cybersecurity and increasing cybersecurity awareness a top priority for DHS. Within DHS, CISA leads cybersecurity and critical infrastructure security programs, operations, and associated policy; and carries out DHS' antiterrorism efforts[21]. Other priorities include strengthening the integrity of elections, protecting government networks, applying new technologies to supply chain security, and preparing for the challenges of new, emerging technology. DHS has made some progress to address the threats of cyberattacks and reduce the likelihood of exploitation of critical weaknesses. For example, DHS implemented specific tools and technologies to detect and prevent security events on component systems and to help protect DHS' network communication and data. DHS has also made progress improving cybersecurity collaboration and coordination with the Department of Defense (DoD) in accordance with the Cyber Action Plan and memorandums. DHS continues to participate in critical infrastructure programs, improve cyber situational awareness, co-locate DHS and DoD liaisons, and conduct cybersecurity readiness training. DHS has also continued to provide oversight of the department-wide intelligence system and has implemented programs to monitor ongoing security practices. It is also working to update relevant plans, address identified vulnerabilities, and continues to improve configuration and patch management.

DHS concurred with recent OIG recommendations aimed at helping the Department improve upon its efforts to implement its critical infrastructure

[20] According to the National Institute of Standards and Technology (NIST), an Advanced Persistent Threat is an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors including cyber, physical, and deception.
[21] In addition to CISA, ICE, CBP, and other DHS components and agencies have significant roles in counterterrorism efforts for the Department.

strategy and programs. CISA is working to improve oversight for Dams Sector security and resilience.[22] Additionally, OIG is reviewing DHS' efforts to improve Energy Sector resilience.

WHAT DHS STILL NEEDS TO DO

OIG has issued numerous recommendations to DHS to address cybersecurity weaknesses and improve its information security program functions to identify, detect, respond, and recover from cybersecurity incidents.[23] DHS needs to revise its policies and procedures to reflect the latest NIST standards. The DHS Chief Information Officer should develop a change management process to identify and implement Policy Directives. DHS also needs to improve its Cybersecurity Awareness Training Program to ensure all DHS users receive a comprehensive, baseline level of cybersecurity education. Additionally, DHS needs to address weaknesses in access controls, patching procedures, and configuration settings. DHS needs to address recent recommendations to improve the Department's information security program.[24]

OIG will continue to monitor DHS' cybersecurity coordination efforts by partnering with the National Security Agency (NSA) to review DHS and NSA's efforts to assess the actions taken by DHS in advance of, and in connection with, recent intrusions into U.S. Government and private networks. OIG is also reviewing CISA's ability to detect and mitigate risks from major cyberattacks based on lessons learned after the SolarWinds breach.

CISA needs to improve its oversight, coordination, and communication to better support the Dams Sector security and resilience. Also, DHS is receiving approximately $8 billion from the *Infrastructure Investment and Jobs Act* (IIJA) to strengthen critical infrastructure. The Department will need to create new programs, and a strategy for spending IIJA funds.

Ensuring Proper Financial Management and Oversight

THE CHALLENGE

Ensuring strong financial management principles and results is foundational to every aspect of DHS' mission and supports all of DHS' strategic goals and strategic priorities. Proper financial management and resulting data are commonly viewed as important strategic assets.

---

[22] *CISA Can Improve Efforts to Ensure Dam Security and Resilience*, OIG-21-59, Sept. 2021.
[23] *USCIS Should Improve Controls to Restrict Unauthorized Access to its Systems and Information*, OIG-22-65, Sep. 2022.
DHS Can Better Mitigate the Risks Associated with Malware, Ransomware, and Phishing Attacks, OIG-22-62, Aug. 2022.
[24] *Evaluation of DHS' Information Security Program for Fiscal Year 2021*, OIG-22-55, Aug. 2022.

WHY IS THIS A CHALLENGE?

DHS has shown it has strong financial principles, but notable financial deficiencies can undermine the public's confidence in DHS and its ability to make strategic investments using taxpayer dollars. For FY 2022, Congress provided funding of $57 billion, an increase of $5.1 billion compared with FY 2021. It provided total funding of $94.8 billion, including $18.8 billion for major disaster response and recovery and $19 billion offset by fee collections.

Independent auditors issued an adverse opinion on DHS' internal controls over financial reporting because of material weaknesses. Specifically, auditors found weaknesses in Information Technology Controls and Information Systems and Financial Reporting. Auditors identified significant deficiencies in Custodial Activities: Drawbacks and Seized and Forfeited Property; Grants Management and Other Needs Assistance Programs; Insurance Liabilities; and Journal Entries. They also noted noncompliance with the *Federal Managers' Financial Integrity Act of 1982* and *Federal Financial Management Improvement Act of 1996.*[25]

OIG found DHS did not fully comply with the *Payment Integrity Information Act of 2019* (PIIA) in FY 2021.[26] OIG also found the Department continues to make progress meeting *Digital Accountability and Transparency Act of 2014* (DATA Act) requirements, but system limitations hinder the Federal Emergency Management Agency's (FEMA) ability to track spending associated with the Department's response to the pandemic.[27] FEMA received 98 percent (approximately $45.4 billion) of the Department's COVID-19 funding.

In August 2020, the President directed FEMA to expend as much as $44 billion from the Disaster Relief Fund for a Lost Wages Assistance (LWA) program. FEMA is challenged to ensure State Workforce Agencies (SWA) report suspected or identified LWA fraud to DHS OIG, as many agencies' plans lacked required procedures to report.[28] Further, FEMA did not implement controls to prevent SWAs from paying more than $3.7 billion in potentially fraudulent and

---

[25] *Independent Auditors' report on DHS' FY 2021 Financial Statements and Internal Control over Financial Reporting*, OIG-21-08, Nov. 2021.
[26] *Department of Homeland Security's FY 2021 Compliance with the Payment Integrity Information Act of 2019 and Executive Order 13520, Reducing Improper Payments*, OIG-22-45, June 2022.
[27] *DHS Continues to Make Progress Meeting DATA Act Requirements, but Challenges Remain*, OIG-22-04, Nov. 2021.
[28] *Management Alert – Reporting Suspected Fraud of Lost Wages Assistance*, OIG-22-28, Feb. 2022.

improper payments through its LWA program.[29] FEMA relied on weak underlying Unemployment Insurance program controls, such as self-certifications, to determine eligibility and prevent fraud. This also allowed ineligible and potentially ineligible DHS employees, or individuals using their identities, to receive LWA. The Department also did not contain the necessary controls in its Unemployment Compensation for Federal Employees program to ensure SWAs had accurate information to determine claim eligibility. Consequently, FEMA and the Department significantly increased DHS employees' risk of fraud and exposure to identity theft.

CBP's revenue collection efforts focus on enforcing trade laws, facilitating legitimate trade, and collecting lawfully owed duties, taxes, and fees. Revenue Collection is designated as a Priority Trade Issue due to the high risk of significant revenue loss, harm to the U.S. economy, or threats to the health and safety of the American people. Importers may illicitly attempt to avoid paying duties, taxes, and fees and circumvent trade practices, defrauding the Federal Government and undermining lawful business. CBP implemented its Centers of Excellence and Expertise (Centers), in part, to centralize trade enforcement and facilitation. The absence of performance standards has made it difficult to determine to what extent establishing the Centers improved the assessment, collection, and protection of trade revenue.[30]

WHAT PROGRESS HAS DHS MADE?

DHS continued to improve its financial management in FY 2021 and achieved its nineth consecutive unmodified (clean) opinion on all financial statements. DHS continues to make progress meeting its reporting requirements under the DATA Act. DHS implemented actions to improve the completeness of budgetary and award data in its DATA Act submission to make the spending information more transparent.

DHS is working to improve compliance with requirements set forth in laws, regulations, directives, and policies by strengthening oversight, internal control, data quality, and transparency. For example, DHS demonstrated through corrective action plans, its intent to address OIG recommendations to develop or enhance various performance measures, procedures, and internal controls.

[29] *FEMA Did Not Implement Controls to Prevent More than $3.7 Billion in Improper Payments from the Lost Wages Assistance Program*, OIG-22–69, Sep. 2022, and *The Identities of DHS Employees Were Linked to More than $2.6 Million in Potentially Fraudulent Lost Wages Assistance*, OIG-22-73, Sept. 2022.

[30] CBP Needs Improved Oversight for Its Centers of Excellence and Expertise, OIG-22-34, Mar. 2022.

DHS has taken steps toward remediating other issues OIG previously reported, including in Financial Statement Audit reports. DHS has undertaken a Financial Systems Modernization program which is intended to replace outdated systems across the Department. To date, DHS has deployed a modernized financial management system to the Countering Weapons of Mass Destruction Office, the Transportation Security Administration, and United States Coast Guard. DHS is also planning to modernize financial management systems at other components. DHS officials have stated that this modernization effort will help mitigate many of the underlying causes of the Information Technology Controls and Information Systems and Financial Reporting material weaknesses identified in previous audit reports.

WHAT DHS STILL NEEDS TO DO

DHS must thoughtfully execute its role as steward of taxpayer investment in its programs, making continued progress toward full compliance with applicable laws, regulations, directives, policies, prevailing guidance, and internal control standards. DHS needs to sustain a clean opinion on its financial statements and obtain a clean opinion on its internal control over financial reporting. In addition, DHS needs to implement and consistently use the government-wide financial data standards to improve the accuracy of reporting for certain data elements to fully achieve the DATA Act's objective. Further, FEMA needs to strengthen its fraud preventive controls when determining claimant eligibility. Its reliance on self-certifications continues to lead to billions of dollars in potentially fraudulent and improper payments. Also, CBP needs to improve its compliance with the *Trade Facilitation and Trade Enforcement Act of 2015*, its procedural guidance for its Centers of Excellence and Expertise, and the reliability of trade import and enforcement data in its information systems.

Ensuring Technology Supports Essential Mission Operations

THE CHALLENGE

Providing technology support for personnel, maintaining system functionality and integration, addressing deficiencies, identifying and prioritizing systems for modernization, and ensuring data is accurate and reliable for strategic decision makers continues to be a major management challenge. In addition, DHS seeks to achieve specific objectives related to improving workforce capability and strengthening governance in strategic goal 6 as well as innovating and harnessing technology to advance mission delivery in strategic priority 5.

WHY IS THIS A CHALLENGE?

DHS continues to struggle with aligning DHS technology, personnel, resources, assets, systems, and infrastructure to support its mission. State-of-the-art technology and services remain critical tools to that end. It is important for

DHS to mitigate risks to operational performance before they become issues and to deploy capability timely.

Systems and Applications:
OIG continues to identify control deficiencies, outdated or incorrectly configured systems, and inadequate operator training. In addition, issues with technology and applications continue to be identified as underlying features of many of the OIG's recommendations for improvement in oversight work not primarily focused on technology. Further, independent auditors identified material weaknesses in Information Technology Controls and Information Systems.[31]

Data Management:
Significant challenges hinder DHS' day-to-day use of some of the Nation's largest and most diverse databases to support its vast mission operations.[32] DHS needs to improve the collection and management of data across its components to better serve and safeguard the public. We continue to identify data access, availability, accuracy, completeness, and relevance issues which present numerous obstacles for DHS personnel as they make decisions or carry out day-to-day mission operations. In addition to data quality problems in the National Flood Insurance Program system,[33] shortcomings exist in systems supporting DHS' open source intelligence operations.[34]

WHAT PROGRESS HAS DHS MADE?

Systems and Applications:
Responses to OIG's recommendations show that DHS continues to dedicate necessary resources to oversight, controls, configuration management, modernization, increased automation, and strategic capability deployment.

Data Management:
As noted previously, DHS has taken steps to remediate issues OIG previously reported, including in Financial Statement Audit reports. The Department has taken corrective actions to implement recommendations in prior reports and

[31] *Independent Auditors' report on DHS' FY 2021 Financial Statements and Internal Control over Financial Reporting*, OIG-21-08, Nov. 2021.
[32] *Summary Report: Persistent Data Issues Hinder DHS Mission, Programs, and Operations*, OIG-21-37, May 2021.
[33] *FIMA Made Progress Modernizing Its NFIP System, but Data Quality Needs Improvement*, OIG-21-04, Nov. 2020.
[34] *The Office of Intelligence and Analysis Needs to Improve Its Open Source Intelligence Reporting Process*, OIG-22-50, July 2022.

has developed various plans and strategies to improve the quality and management of its data.[35]

WHAT DHS STILL NEEDS TO DO

OIG's recommendations show that DHS still needs to increase and sustain its focus and effort to: (1) improve oversight, (2) ensure consistent configuration management, (3) prioritize systems and applications modernization, and (4) remediate the internal control issues that underlie data deficiencies. Additionally, DHS needs to address a remaining unresolved and open recommendation from OIG's evaluation of DHS' information security program for FY 2019.[36]

Improving FEMA's Disaster Assistance and Fraud Prevention

THE CHALLENGE

FEMA continues to struggle to reimburse procurement costs and continues to experience systemic problems and operational difficulties contributing to inadequate management of disaster relief grants. According to DHS, COVID-19 response and recovery is the largest relief assistance program in American history. FEMA, as the lead response agency, has been charged with administering and overseeing $45 billion in Coronavirus Aid, Relief, and Economic Security (CARES) Act funding. Further, FEMA has recently been charged with administering $6.8 billion in IIJA funding. In addition, DHS seeks to achieve specific objectives related to strengthening preparedness and resilience in strategic goal 5 and strategic priority 11.

WHY IS THIS A CHALLENGE?

FEMA struggles with ensuring disaster grant recipients and subrecipients understand and comply with relevant authorities governing grants and assistance. FEMA has also proven susceptible to widespread fraud and made billions in improper payments.[37]

Grants Management:

[35] *Independent Auditors' report on DHS' FY 2021 Financial Statements and Internal Control over Financial Reporting*, OIG-21-08, Nov. 2021.
[36] *Evaluation of DHS' Information Security Program for Fiscal Year 2019 (REDACTED)*, OIG-20-77, Sept. 2020.
[37] *Success of Future Disaster Response and Recovery Efforts Depends on FEMA Addressing Current Vulnerabilities*, OIG-21-25, Mar. 2021; FEMA Did Not Implement Controls to Prevent More than $3.7 Billion in Improper Payments from the Lost Wages Assistance Program, OIG-22-69, Sep. 2022.

OIG continues to identify grantee and subgrantee oversight weaknesses, insufficient systems to process information and data, inadequate policies and guidance, and improper payments.

Disaster Assistance:
OIG continues to identify persistent, systemic shortcomings in FEMA's disaster response and recovery efforts. OIG has published a significant body of work recommending improvements in Federal disaster response and recovery efforts. We remain committed to examining FEMA's disaster response and recovery programs, including program oversight and management, authorities, and data for decision making.[38] OIG also continues to examine FEMA's management of contracts, including FEMA's contracting practices during national disaster declarations.

Oversight of Pandemic Funding and Fraud Prevention:
OIG has received a substantial number of COVID-19 fraud complaints nationwide and continues to investigate COVID-19 fraud perpetrated by companies and individuals seeking to exploit DHS-affiliated programs, notably relief programs that FEMA administers. Further, as of July 31, 2022, OIG had received more than 7,500 complaints and initiated more than 300 investigations related to COVID-19, including allegations that fraud networks have secured pandemic-related benefits.

WHAT PROGRESS HAS DHS MADE?

Grants Management:
FEMA's corrective action plans show FEMA continues to strengthen adherence to Federal regulations and its own policy, oversight, risk assessment, and training.

Disaster Assistance:
Responses to OIG's recommendations show that FEMA continues efforts to augment staff and systems to improve oversight, and develop resources, tools, and procedures to support more effective programs.

Oversight of Pandemic Funding and Fraud Prevention:

[38] *FEMA Needs to Improve Oversight and Management of Hazard Mitigation Grant Program Property Acquisitions*, OIG-22-46, June 2022; *FEMA's Waiver Authority under the Disaster Recovery Reform Act of 2018*, OIG-22-43, May 2022; *Assessment of FEMA's Public Assistance Alternative Procedures Program*, OIG-22-51, July 2022; *FEMA Did Not Prevent More than $3.7 Billion in Improper Payments from the Lost Wages Assistance Program*, OIG-22-69, Sep. 2022 and *DHS Employees Were Linked to More than $2.4 Million in Potentially Fraudulent and Ineligible Lost Wages Assistance*, OIG-22-73, Sep. 2022.

FEMA continues to collaborate with OIG and others to leverage multi-disciplinary expertise to identify fraud schemes.

WHAT DHS STILL NEEDS TO DO

While DHS and FEMA continue to address OIG recommendations, they need to analyze systemic weaknesses across the spectrum of disaster-related funding and services and make overarching improvements in risk assessment, controls, policies, systems and applications, resources, training, data to support equitable assistance distribution, and collaboration with stakeholders.[39] FEMA also needs to address multiple unresolved and open recommendations from previous reports.[40]

Strengthening Oversight and Management of Major Systems Acquisition and Procurement

THE CHALLENGE

Acquiring major acquisition systems is a key part of DHS' annual budget and fundamental to accomplishing its many critical missions. This challenge relates to every aspect of DHS' mission and relates to all DHS strategic goals and strategic priorities. In addition, enhancing mission capabilities is included as a priority in the Office of the Chief Procurement Officer's annual report for FY 2021.[41]

WHY IS THIS A CHALLENGE?

Oversight of major acquisition programs is critical to obtaining the new capability that DHS needs to combat evolving threats. As reported by the U.S. Government Accountability Office (GAO), each year, DHS invests billions of dollars in a diverse portfolio of major acquisition programs to help execute its many critical missions. DHS and its components are acquiring capabilities to help secure the border, increase marine safety, screen travelers, enhance cybersecurity, improve disaster response, and execute a wide variety of other operations. In FY 2021, DHS planned to spend more than $7 billion on major

[39] *Lessons Learned from Prior Reports on Disaster-related Procurement and Contracting*, OIG-18-29, Dec. 2017; *Lessons Learned from FEMA's Initial Response to COVID-19*, OIG-21-64, Sept. 2021; *Summary and Key Findings of Fiscal Year 2015 FEMA Disaster Grant and Program Audits*, OIG-17-13, Nov. 2016.

[40] *FEMA Has Made More than $3 Billion in Improper and Potentially Fraudulent Payments for Home Repair Assistance since 2003*, OIG-20-23, Apr. 2020; *FEMA Has Paid Billions in Improper Payments for SBA Dependent Other Needs Assistance since 2003*, OIG-20-60, Aug. 2020; *FEMA Has Not Prioritized Compliance with the Disaster Mitigation Act of 2000, and Hindering Its Ability to Reduce Repetitive Damages to Roads and Bridges*, OIG-21-43, July 2021.

[41] DHS' Office of the Chief Procurement Officer Fiscal Year 2021 Annual Report, Priority 3 – Enhance Mission Capabilities.

acquisition programs. In FY 2022, DHS plans to spend more than $5 billion on major acquisition programs, and, ultimately, the Department plans to invest more than $240 billion over the life cycle of these programs. Most of DHS' major acquisition programs have lifecycle costs of at least $300 million and take multiple years to acquire.[42]

We continue to identify issues with poorly defined operational requirements for assets being acquired, adherence to the DHS Acquisition Lifecycle Framework, contract oversight, and reporting.[43] Without effective oversight and plans, DHS cannot ensure systems are meeting critical system performance requirements or mitigating future vulnerabilities. Additionally, the Department may fund future systems without accurately defining capability needs.

WHAT PROGRESS HAS DHS MADE?

DHS continues to make progress in its acquisition program oversight processes and controls through implementation of a revised acquisition management directive and a revised acquisition instruction.[44] DHS continues to update acquisition management policy and guidance, including specific guidance on developing operational requirements and sharing lessons learned across acquisition programs.

WHAT DHS STILL NEEDS TO DO

DHS needs to continue to grow and mature the Joint Requirements Council and its requirements process the Joint Requirements and Integration Management System as well as other requirements determination guidance. DHS' Office of Program Accountability and Risk Management needs to continue to strengthen oversight of acquisitions programs to ensure they follow all key steps in the Acquisition Lifecycle Framework. DHS also needs to reinforce the use of the checklists, job aids, and guides developed by the DHS Office of the Chief Procurement Officer. DHS and its components also need to address multiple unresolved and open recommendations from OIG's previous reports.[45]

---

[42] *GAO's DHS Annual Assessment, GAO-21-175* and *GAO-22-104684.*

[43] For example, *CBP and CWMD Need to Improve Monitoring and Maintenance of Radiation Portal Monitor Systems (Redacted)*, OIG-22-39, Apr. 2022.

[44] DHS 102-01 Rev. 03.1 approved in February 2019; DHS 102-01-001 Rev. 01.3 approved in January 2021.

[45] *CBP Has Not Demonstrated Acquisition Capabilities Needed to Secure the Southern Border*, OIG-20-52, July 2020; *DHS Grants and Contracts Awarded through Other Than Full and Open Competition, FYs 2018 and 2019*, OIG-21-17, Feb. 2021; *U.S. Customs and Border Protection's Acquisition Management of Aviation Fleet Needs Improvement to Meet Operational Needs*, OIG-21-53, Aug. 2021.

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

Building the Department You Deserve: DHS's 2022 Priorities

Every day, our Department interacts more frequently with the public than any other federal agency. Building on a strong year of progress in 2021 and seeking to enhance our capabilities in key mission areas, **Secretary Mayorkas and the leadership team across all DHS components developed 12 priorities to guide our Department's strategic focus this year.**

Each of you play a vital role in accomplishing these priorities. As we approach our Department's 20th anniversary next year, these priorities will complement your individual office and agency goals and meaningfully advance our critical mission.

Organizational Advancement

1. **Increase our effectiveness** through transformational, cross-cutting initiatives: Strengthen our workforce, enhance our incident management capabilities, bolster our operational management, and better integrate the work of our component agencies and personnel so that we are drawing on our best resources to prepare for and respond to complex and dynamic events
2. **Champion our workforce and a culture of excellence** internally and externally: Enhance employee engagement, build and maintain a culture of recognition, and champion the successes of our dedicated workforce
3. **Increase openness and accountability:** Build and maintain trust with the communities we serve through improved data transparency, robust

external communication, and strengthened oversight and disciplinary systems

4. **Advance Diversity, Equity, Inclusion, and Accessibility (DEIA)** in our workforce and **protect the privacy, civil rights, civil liberties, and human rights** of the communities we serve: Ensure our Department reflects the diversity of the communities we serve and ensure that our programs, policies, and operations improve equity and protect privacy, civil rights, and civil liberties
5. **Innovate and harness technology** to advance mission delivery: Adopt innovative approaches to optimize our operations and mission fulfillment and improve the customer experience
6. **Maximize our international impact** and strength: Leverage our international footprint and relationships to advance homeland security objectives, and unify and fortify Department efforts to counter threats from China

Mission-Specific Advancement

7. **Combat all forms of terrorism and targeted violence:** Counter all forms of terrorism, including through enhancing domestic and international information sharing, empowering communities, strengthening screening and vetting, and addressing new and emerging threats such as unmanned aerial vehicles
8. **Increase cybersecurity** of our nation's networks and critical infrastructure, including election infrastructure: Lead federal efforts to increase nationwide resilience across the public and private sectors, and continue playing a lead role in responding to major cybersecurity incidents
9. **Secure our borders and modernize ports of entry:** Harness technology at and between ports of entry, improve intelligence and information capabilities, and give our dedicated workforce the tools they need to secure our nation’s borders, including interdicting irregular migration and illicit flows of drugs, weapons, and other contraband
10. **Build a fair, orderly, and humane immigration system:** Develop and implement regional migration solutions, lawful pathways as alternatives

to irregular migration, and enhanced policies and processes to expeditiously and fairly administer our nation's laws and uphold our values as a nation of immigrants

11. **Ready the nation to respond to and recover from disasters and combat the climate crisis:** Increase our investments in community resilience and adaptation and improve our disaster readiness capabilities
12. **Combat human trafficking, labor exploitation, and child exploitation:** Apply our resources and personnel to identify and protect victims, bring perpetrators to justice, and prevent the entry into the U.S. of products made with forced labor

***

Appendix C

Management Comments

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

Homeland Security

October 17, 2022

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: 2022.10.17 13:58:59 -04'00'

SUBJECT: Management Response to Draft Report: "Major Management and Performance Challenges Facing the Department of Homeland Security" (Project No. 23-003-NONE-DHS)

Thank you for the opportunity to comment on this draft report. Senior U.S. Department of Homeland Security (DHS or the Department) leadership appreciates the Office of Inspector General's (OIG's) independent research, assessment, and judgment identifying what the OIG considers the most serious management and performance challenges facing the Department, and DHS's progress in addressing these challenges.

DHS leadership, program officials, and subject matter experts throughout the Department will give appropriate consideration to the OIG perspectives offered in this report as part of continuing efforts to improve the effectiveness and efficiency with which the Department carries its mission of safeguarding the American people, our homeland, and our values.

Leadership, however, is concerned that OIG's major management and performance challenges (MMPC) report could be misleading to some readers about Departmental efforts to successfully carry out its mission. This is because of inaccurate, contextually incomplete, and confusing statements in the draft report resulting in misinformation, which calls into question the quality control processes OIG has in place to ensure its reporting can be relied upon by others. Selected examples include:

- The enacted funding and other dollar figures OIG references as part of the "Ensuring Proper Financial Management and Oversight" challenge in the draft report are not accurate. For example, it appears OIG used the fiscal year (FY)

2022 U.S. House of Representatives "mark up" version of legislation instead of the enacted values from the actual appropriations law[1] when stating:

> "For FY 2022, Congress provided funding of $52.81 billion, an increase of $934 million compared with FY 2021. It provided total funding of $76.15 billion, including $18.8 billion for major disaster response and recovery and $4.57 billion offset by fee collections."

However, for FY 2022, Congress actually provided Adjusted Net Discretionary funding of $58 billion, an increase of $6.1 billion compared with FY 2021. In total, the final bill provided total funding of $94.8 billion, including $18.8 billion for major disaster response and recovery and $18 billion from "Fees, Mandatory, & Rescissions."

Also, it is unclear from where OIG sourced information that DHS received $19 billion from the "Infrastructure Investment and Jobs Act" (referenced as part of the "Securing Cyberspace and Critical Infrastructure" challenge) when DHS actually received $8 billion.

- The Department is concerned that the "Strengthening Oversight and Management of Major Systems Acquisition and Procurement" challenge does not clearly differentiate procurement, acquisition, and requirements oversight roles, thus creating an opportunity for confusion about these activities in the minds of readers of OIG's report. For example, after focusing on acquisition budgets, acquiring assets, and the acquisition lifecycle framework (ALF) as to "Why Is This A Challenge," OIG references DHS's Office of the Chief Procurement Officer "checklists, job aids, and guides" as part of "What DHS Still Needs To Do." This leaves the impression that this office supports acquisitions, which it does not. In addition, OIG's narrative mentions specific guidance on operational requirements development as part of updated acquisition policy and guidance, but omits the relevant fact that operational requirements development policy and guidance is governed by the Joint Requirements Council (JRC), which works closely with, but is independent from, the DHS Office of Program Accountability and Risk Management.

  The Department also does not believe the report adequately recognizes the strides DHS has made overseeing capability needs and operational requirements, especially as regards OIG's statement that "the Department may fund future systems without accurately defining capability needs." To the contrary, the JRC effectively governs the Department's requirements process through the Joint Requirements Integration and Management System (JRIMS), which ensures:

[1] Public Law 117-103, "Consolidated Appropriations Act, 2022"

(1) transparency across the Department;
(2) that capability needs are valid and traceable to strategic goals;
(3) that operational requirements are well-defined; and
(4) that opportunities for common efforts are identified.

JRC's actions and the JRIMS process also ensure the appropriate level of visibility and oversight on Component activities well before program establishment to deliver or field a new product or capability.

DHS also noted that only 1 of the 6 reports (i.e., OIG-22-39, "CBP and CWMD Need to Improve Monitoring and Maintenance of Radiation Portal Monitor Systems") referenced in footnote 42 and used to support "Why Is This A Challenge" arguably pertained to OIG's major systems acquisition-related statements regarding the ALF and operational requirements. The other reports addressed contract/procurement issues. Specifically, conducting an operational analysis to ensure that a system is meeting mission is part of the ALF, but assessing a fielded capability does not correlate directly with future funding of systems without accurately defining capability needs, which is a separate and thorough process which takes place before acquiring/fielding.

- As part of several challenges, OIG's draft report states that "DHS and its Components also need to address multiple unresolved and open recommendations from OIG's previous reports," but in doing so creates what the Department believes is a fragmented and misleading presentation of the issue. For example, as part of the "Strengthening Oversight and Management of Major Systems Acquisition and Procurement" challenge, the aforementioned statement was linked to the four previously published reports referenced in footnote 44. However, only 2 of 18 (11 percent) recommendations in these reports are currently "open and unresolved." Of the other 89 percent, 13 of the 18 (72 percent) have already been closed **with OIG agreement**, and 3 of 18 recommendations (17 percent) are currently "open and resolved" (i.e., no disagreement exists). In addition, two of the four reports (50 percent) OIG cites in this footnote as having "open and unresolved" recommendations do not.[2]

  Department officials understand the value of minimizing the number of open and unresolved recommendations to the greatest extent possible, but having no such recommendations is an aspirational goal, as some level of efforts to resolve disagreements will likely always take place between DHS and OIG, as well as the U.S. Government Accountability Office (GAO), for that matter. DHS leadership is proud that its program officials and others have reduced the number of open and

[2] OIG-20-19, "PALMS Funding Did Not Comply with Federal Appropriations Law," dated March 24, 2020; and OIG-21-53, "U.S. Customs and Border Protection's Acquisition Management of Aviation Fleet Needs Improvement to Meet Operational Needs," dated August 9, 2021.

unresolved OIG recommendations more than 6 months old from a high of 691 during FY 2011 to the current number of about 35, only two of which involve acquisition or procurement-related issues. That said, some of DHS's currently open and unresolved recommendations represent "hard non-concurrences," from a Component-level perspective, which program office and OIG staff have been unsuccessful at reaching agreement on despite holding numerous follow-up meetings and discussions in the months and years after the original audit reports were issued.

Of significance, although not noted in OIG's draft MMPC report, DHS continues to strictly adhere to a self-imposed practice of not closing any open OIG or GAO recommendations without first reaching agreement with respective audit staff to do so. This provides Congress and the public added confidence that the Department has taken appropriate actions to implement these recommendations or otherwise resolve any disagreements.

In addition, it is important to note that, in accordance with Office of Management and Budget Circular A-50, "Audit Follow-up," the Secretary of Homeland Security has established a process whereby the Inspector General can elevate any open and unresolved recommendation to the Under Secretary for Management for a final resolution determination (i.e., whether to implement or not implement). However, the OIG has not taken advantage of this process since January 2018, nearly 5 years ago.

- Many of the examples cited in the OIG's draft MMPC report focus on highlighting the findings and conclusions of OIG auditors, evaluators, and inspectors summarized in previously published reports, generally without including 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 these reports were issued, as discussed in those reports.

  For example, under the "Managing Detention Conditions" challenge, OIG referenced a Management Alert issued recommending the immediate removal of all detainees from the Torrance County Detention Facility (TCDF) due to safety risks and unsanitary living conditions.[3] However, no reference was made to U.S. Immigration and Customs Enforcement (ICE) leadership's disagreement with OIG's recommendation and concerns about the accuracy and integrity of this report, and whether it met the "Quality Standards for Inspection and Evaluation" issued by the Council of Inspectors General on Integrity and Efficiency (i.e., the

[3] OIG-22-31, "Management Alert – Immediate Removal of All Detainees from the Torrance County Detention Facility," dated March 16, 2022.

"Blue Book"), dated December 2020. In a number of instances, it appeared the OIG had mischaracterized evidence and ignored facts presented to it. This included, according to ICE El Paso field office personnel, disconcerting and unprofessional behavior by an OIG inspector during the TCDF inspection.

ICE is also concerned that corrective actions have not been acknowledged by the OIG. The TCDF completed a majority of the repairs to address conditions identified prior to the conclusion of the OIG's inspection and the remaining repairs were completed by April 30, 2022. ICE provided documentation to OIG demonstrating completion of these repairs.

In another example under the "Coordinating Border Security Efforts and Managing Migrant Surges and Resettlements" challenge, OIG references a report questioning the processes used to screen, vet, and inspect all Afghan evacuees arriving in the United States as part of Operation Allies Refuge/Operation Allies Welcome (OAW).[4] However, many of OIG's claims are not accurate, which DHS program officials, subject matter experts, and others repeatedly relayed to OIG during the audit through significant efforts and multiple attempts to provide the OIG a comprehensive understanding of the extensive details related to the numerous facts and nuances of the unprecedented OAW vetting process.

For example, OIG's draft report did not adequately reflect the *interagency* and *multi-layered* vetting process that started overseas, continued at the U.S. Port of Entry (POE), and is currently ongoing with recurrent vetting. OIG claimed that U.S. Customs and Border Protection (CBP) was unable to appropriately "screen, vet, and inspect" all Afghan nationals during the recent operation, when CBP was only one part of an interagency screening and vetting process and did, in fact, screen, vet, and inspect all Afghan nationals at the POE.

OIG's draft report also used specific examples to allege that the vetting system does not work, when in fact, these examples highlight how the process worked as intended. Specifically, the report stated that two individuals were paroled into the United States with derogatory information in their vetting records, which is incorrect. In March 2022, DHS provided the OIG with information on these two individuals, clarifying that they were cleared by the interagency vetting process at the time of travel, and no derogatory information was reported prior to their parole into the United States. Although DHS provided information to the OIG on multiple occasions to clarify the end-to-end screening and vetting processes and the specifics about the two referenced individuals, this information was not

[4] OIG-22-64, "DHS Encountered Obstacles to Screen, Vet, and Inspect All Evacuees during the Recent Afghanistan Crisis," REDACTED, dated September 6, 2022.

included in the final report, and the mistakes and omissions are repeated in the OIG's draft MMPC report.

- The "Law Enforcement Unity of Effort" sub-challenge under the "Countering Terrorism and Homeland Security Threats" challenge does not mention the significant progress DHS has made to better manage and coordinate DHS law enforcement with creation of the Law Enforcement Coordination Council (LECC) in October 2021. Comprised of the leadership of the operational law enforcement Components and offices, as well as relevant headquarters support and oversight offices, the LECC has three subcommittees focusing on use of force policy, training, and law enforcement administration. In FY 2022, the LECC was successful in implementing new use of force reporting, updating the use of force policy, reviewing law enforcement training programs, and beginning to address several requirements related to Presidential Executive Order 14074, "Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety," dated May 25, 2022.

- The Department notes that the draft MMPC report does not include an "Objective, Scope, and Methodology" section like most OIG reports. Such a section would provide readers of the report important insights about the independent research OIG undertook to identify the challenges highlighted, thus facilitating a better understanding of OIG's perspective.

Again, thank you for the opportunity to review and comment on this draft report. DHS also submitted technical comments addressing several accuracy, contextual and other concerns under a separate cover for OIG's consideration.

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