Major Management and Performance Challenges Facing the Department of Homeland Security

November 8, 2024
OIG-25-04

OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

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

November 8, 2024

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: 2024.11.08 12:13:27 -07'00'

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

The Office of Inspector General supports the Department of Homeland Security's (Department) mission by conducting investigations, audits, evaluations, and inspections on behalf of the American public. The *Reports Consolidation Act of 2000* requires OIG to complete an annual report on what it determines to be the top management challenges facing the Department. These challenges highlight the need for enhanced management attention to ensure the effective operation of Department programs and the advancement of its strategic goals.

The four overarching challenges identified in last year's Major Management and Performance Challenge report — *transparency*, *accountability*, *efficiency*, and *sustainability* — continue to affect a broad spectrum of the Department's program and operation responsibilities that may hinder its ability to advance essential missions and protect the Nation and its citizens.

This year, we took a different approach[1] by aligning the four overarching challenges with the Department's operations under its seven strategic missions, as outlined in the *Department of Homeland Security Annual Performance Report for Fiscal Years 2023-2025,*[2] and its updated 12 cross-functional priorities.[3]

[1] Last year, we aligned the four overarching challenges with the Department's operations under its six strategic goals outlined in the Department of Homeland Security's Strategic Plan for Fiscal Years (FY) 2020-2024. However, the Department's Strategic Plan sunsets at the end of FY 2024. Based on discussions with the Department's Strategic Integration and Policy Planning staff and subsequent review of the Department's drafted Strategic Plan for FY 2023-2027, scheduled for release around the beginning of FY 2025, the Department will align its strategic goals with the strategic missions listed in its latest annual performance report. For a crosswalk between the Department's strategic goals and objectives for FY 2020-2024 and its strategic missions and objectives for FY 2023-2025, see Appendix A. For a description of sunsetting strategic goals, see Appendix B.

[2] Department of Homeland Security Annual Performance Report for Fiscal Years 2023-2025

[3] Department Priorities, see Appendix C

The Department's seven strategic missions are:

- Counter Terrorism and Prevent Threats;
- Secure and Manage our Borders;
- Administer the Nation's Immigration System;
- Secure Cyberspace and Critical Infrastructure;
- Build a Resilient Nation and Respond to Incidents;
- Combat Crimes of Exploitation and Protect Victims; and
- Enable Mission Success by Strengthening the Enterprise.

Additionally, we described potential risks associated with each of the four challenges and summarized actions the Department has taken, is taking, or should take to further address these challenges. Recent Progress sections in this report reflect progress reported by the Department and its components in the latest annual performance report and have not been validated by OIG.

The challenges outlined in this report are based on our judgment and independent research, including discussions with internal and Department component Senior Leaders. We also considered prior audit, inspection, and investigative oversight work, our analyses of data and risks, Congressional testimony, U.S. Government Accountability Office reports, and the Department's Strategic Plan and annual performance reports.

These challenges are not wholly representative of the vulnerabilities confronting the Department. We publish reports throughout the year that highlight specific opportunities to improve programs and operations. We remain committed to conducting independent oversight and making recommendations to help the Department address these major management and performance challenges and ensure the effectiveness of its operations.

Consistent with our responsibility under the *Inspector General Act of 1978*, as amended, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department. We will post the report on our website for public dissemination.

Please contact me with any questions, or your staff may contact Chief of Staff, Kristen Fredricks, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

Major Management and Performance Challenges Facing the Department of Homeland Security

November 8, 2024

Why We Did This Report

This annual publication required by the *Reports Consolidation Act of 2000*, summarizes what the Office of Inspector General considers the most serious management and performance challenges facing the Department of Homeland Security (Department) and assesses its progress in 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 of prior work, and professional judgment and are aligned to the Department's seven strategic missions and 12 cross-functional priorities.

For further information, contact our Office of Public Affairs at (202) 981-6000 or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

OIG identified four overarching challenges — *transparency*, *accountability*, *efficiency*, and *sustainability* — that reflect vulnerabilities affecting a broad spectrum of the Department's programs, operations, and responsibilities. These challenges may hinder its ability to advance essential missions and protect the Nation and its citizens.

We aligned the four overarching challenges to the Department's seven strategic missions. We assessed the potential impact to program operations and the Department's ability to meet its latest annual performance report's mission objectives. The Department's seven strategic missions are:

- Counter Terrorism and Prevent Threats
- Secure and Manage our Borders
- Administer the Nation's Immigration System
- Secure Cyberspace and Critical Infrastructure
- Build a Resilient Nation and Respond to Incidents
- Combat Crimes of Exploitation and Protect Victims
- Enable Mission Success by Strengthening the Enterprise

We also summarized actions the Department has taken, is taking, or should take to further address the overarching challenges. Recent Progress sections in this report reflect progress reported by the Department and its components in the latest annual performance report and have not been validated by OIG. These challenges are not wholly representative of all vulnerabilities confronting the Department. OIG publishes reports throughout the year that highlight specific opportunities to improve programs and operations.

Office of Inspector General
U.S. Department of Homeland Security

Table of Contents

Abbreviations

APR	Annual Performance Report
CBP	U.S. Customs and Border Patrol
CBP One™	CBP One™ mobile and web application
CCTV	closed-circuit television
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
COVID-19	coronavirus disease 2019
Coast Guard	United States Coast Guard
CPC	Central Processing Centers
critical repairs	priority, critical, and life safety repairs
CSEA	child sexual exploitation and abuse
DOJ	Department of Justice
DRRA	Disaster Recovery Reform Act of 2018
EDS	Evidence-Based Data Strategy
ERO	ICE Enforcement and Removal Operations
Evidence Act of 2018	The Foundations for Evidence-Based Policymaking Act of 2018
FCA	Facility Condition Assessments
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Modernization Act of 2014
FLETC	Federal Law Enforcement Training Centers
GAO	United States Government Accountability Office
GPRA Modernization Act of 2010	Government Performance and Results Act Modernization Act of 2010
HHS	United States Department of Health and Human Services
HQ	DHS Headquarters
HSI	ICE Homeland Security Investigations
I&A	Office of Intelligence and Analysis
ICE	United States Immigration and Customs Enforcement
IG	Inspectors General
IG Act	Inspector General Act of 1978
IHSC	ICE Health Service Corps
IIJA	Infrastructure Investment and Jobs Act
IT	Information Technology
JTFA	Joint Task Force Alpha
LMS	learning management systems
LPOE	land port of entry
MTS	Marine Transportation System
NTA	Notice to Appear
OAW	Operation Allies Welcome

Abbreviations (continued)

OMB	Office of Management and Budget
PBNDS 2011	Performance-Based National Detention Standards 2011
PII	personally identifiable information
PIIA	Payment Integrity Information Act of 2019
POE	port of entry
R&D	research, development, testing, and evaluation
S&T	Science and Technology Directorate
SA	Special Agent
Secret Service	United States Secret Service
STT	state, territorial, and tribal
TEDS	National Standards on Transport, Escort, Detention, and Search
TSA	Transportation Security Administration
UC	unaccompanied migrant children
USCIS	United States Citizenship and Immigration Services

Background

In the wake of the September 11, 2001, terrorist attacks, Congress passed the *Homeland Security Act*, which established the Department of Homeland Security (Department) and combined the functions of 22 Federal departments and agencies with broad responsibilities to secure the Nation from threats. Since its inception, the Department has matured its mission areas to collectively prevent attacks, mitigate threats, respond to national emergencies, and preserve economic security. However, the Nation faces an ever-changing threat landscape, which presents a multitude of complex risks for the Department.

A clear strategic plan is an essential element in achieving and advancing the Department's mission to protect the American people from threats to their security. The Department's 2020 — 2024 Strategic Plan established a common framework to analyze and inform management decisions, and included strategic guidance for mission execution, operational requirements, and annual performance reporting. The Department's complex security mission requires close coordination and collaboration across components, and with other government and private entities, to execute strategic objectives and achieve strategic goals. As of the date of this publication, the Department's 2023-2027 Strategic Plan has not been issued; however, based on our review of the draft strategic plan, the Department is realigning its goals to the missions outlined in its latest annual performance report.

The Department relies on strategic guidance that outlines specifics, such as roles, responsibilities, policies, procedures, and reportable measures focused on efficient and effective operations, and sustainability of future operations. Implementing strategic planning foundational principles, such as *transparency, accountability, efficiency,* and *sustainability*, helps the Department ensure effective operations; however, deficiencies in these areas may result in the inability to effectively execute programs and advance the organization's missions.

"*Implementing strategic planning foundational principles, such as* ***transparency, accountability, efficiency****, and* ***sustainability,*** *helps the Department ensure effective operations.*"

Office of Inspector General
U.S. Department of Homeland Security

Summary of Major Management Challenges

*"…the overarching major management challenges — **transparency, accountability, efficiency,** and **sustainability** — span across multiple Department mission areas, impact day to day operations, and its ability to secure the Nation from threats."*

The challenges outlined in this report are a culmination of our judgment, independent research, including discussions with internal and Department component Senior Leaders, and review of our own audits, inspections, and evaluations, as well as relevant U.S. Government Accountability Office (GAO) reports. We further analyzed recent Congressional testimony and the Department's Strategic Plan and Annual Performance Reports (APR). Based on our assessment, the overarching major management challenges identified in last year's Major Management and Performance Challenge report — *transparency, accountability, efficiency,* and *sustainability* — continue to span across multiple Department mission areas, impact day-to-day operations, and its ability to secure the Nation from threats. We identified a pattern of weaknesses in key operational and programmatic impact areas that, when coupled with barriers to adaptation, impair the Department's ability to provide *efficient* and effective programs now and in the future, and have cascading effects on whole-of-government strategies.

In this report, we aligned the overarching major management challenges with the Department's seven strategic missions and 12 cross-functional priorities. Additionally, we described potential risks associated with each of the four challenges and summarized actions the Department has taken, is taking, or needs to take to further address the foundational challenges, including the status of previous OIG recommendations.[1]

[1] A recommendation is considered "open" when an agreed-upon corrective action has not been implemented. Open recommendations may be unresolved or resolved. "Open and unresolved" recommendations occur when a management decision has not been received by OIG, or if received, has not been agreed to by OIG. A recommendation is considered "open and resolved" when Department or Component officials and OIG agree on (1) the reported finding and recommendation; (2) the corrective actions to be taken; and (3) target completion dates. A recommendation is considered "closed" if a resolved management decision has been implemented.

The Department's seven strategic missions are:

- Counter Terrorism and Prevent Threats
- Secure and Manage Our Borders
- Administer the Nation's Immigration System
- Secure Cyberspace and Critical Infrastructure
- Build a Resilient Nation and Respond to Incidents
- Combat Crimes of Exploitation and Protect Victims
- Enable Mission Success by Strengthening the Enterprise

The overarching major management challenges, *transparency, accountability, efficiency,* and *sustainability*, weave throughout program performance outlined in the Department's APRs. When considering the self-reinforcing nature of these foundational challenges, incremental adjustments to improve *transparency*, *accountability*, *efficiency*, and *sustainability* in the Department's programs and operations can result in a force multiplying effect that advances the Department's missions and secures the Nation from threats.

Transparency is the Department sharing information with citizens and stakeholders. Policy, budget, and programmatic information allow stakeholders to make informed decisions and, if appropriate, hold officials *accountable* for their conduct and decisions.

Accountability is the Department's obligation to report, explain, or justify actions and decisions it makes regarding performance, deficiencies, services, and costs. *Accountability* ensures stakeholders have the information (*transparency*) and ability to hold Department officials responsible for program *efficiencies*, or *inefficiencies*, including actions to promote *sustainability.* Strategic guidance should clearly outline roles and responsibilities (*accountability*).

Efficiency is the Department's ability to reduce waste in resources, cost, time, and effort while still producing the intended outcome, product, or service. *Efficiency* requires a clearly defined and measurable objective. The Department's *efficiency* is bolstered by formal and sufficient strategic guidance (*transparency*), including roles and responsibilities (*accountability*), adequate resources, such as reliable and accessible data (*transparency*), modernized technology and proper workforce support, and the capacity to adapt to new and emerging threats, as necessary (*sustainability*).

Figure 1: Effective Operations

Sustainability is the Department's ability to support organizational needs and processes, as well as the overarching mission, both now and into the future. The Department achieves *sustainability* through implementing *efficient* practices. Tracking and reporting program execution (*transparency*) ensures stakeholders can hold Department officials *accountable* for proper implementation and program *sustainability*.

Figure 2: Barriers to Effective Operations

Figure 3: Analysis of Department Mission Areas by OIG; images included in the graphic are from the DHS Multimedia Library

Mission 1: Counter Terrorism and Prevent Threats

Figure 4: Uniformed Division Officer protecting White House and grounds
Source: U.S. Secret Service

Mission 1 Overview:

One of the Department's top priorities is to protect Americans from terrorism and other homeland security threats by preventing domestic and international actors who engage in terrorist or criminal acts from threatening the homeland.

Related Strategic Goal: 1

Related Strategic Priority: 7

Components Impacted: All

Recent Mission-Related OIG Reports

- DHS Needs to Improve Its Screening and Vetting of Asylum Seekers and Noncitizens Applying for Admission into the United States - (REDACTED) (OIG-24-27)
- TSA Could Not Assess Impact of Federal Air Marshal Service Personnel Deployed to Support Southwest Border Security - (REDACTED) (OIG-24-35 revised)
- The Secret Service's Preparation for, and Response to, the Events of January 6, 2021 - (REDACTED) (OIG-24-42)
- TSA Made Progress Implementing Requirements of the 9/11 and TSA Modernization Acts but Additional Work Remains (OIG-24-50)

APR Challenges

The Department's recent APRs include numerous challenges and risks its components face relating to their ability to counter terrorism and homeland security threats, including but not limited to:

- Impending retirements, retention challenges, increases in personnel demands from expansion of non-traditional protectees, and limited throughput of hiring activities constraining the number of trained personnel to execute the investigative mission
- Transnational criminals continuing to innovate new ways to commit fraud, such as through their digital assets, requiring resourcing for training and tools to keep pace
- Adapting to evolving adversary capabilities to support the ability to detect, deter, and investigate evolving financial crimes

Recent Progress as Reported in the APR

- The Office of Intelligence and Analysis (I&A) collaborated with Wisconsin state partners to release an eLearning module titled *Foundations of Targeted Violence Prevention*. This training educates the public to recognize threats or potentially concerning behaviors, where to report information of concern, and how reported information is used to keep their communities safe. According to I&A, since its release in 2023, over 16,000 community members have participated in the training.
- In 2023, Transportation Security Administration (TSA) invested in over $1.4 billion in contracts for critical screening technology. These investments will help enhance airport security screening by substantially improving identity verification, validating the authenticity of a passenger's identification, confirming pre-screening status, and validating flight reservations. Additionally, the contracted technology will help officers detect explosives and prohibited items.

Figure 5: The possible application of robots to perform routine autonomous tasks could potentially reduce dangers to Secret Service personnel

Source: U.S. Secret Service

The *Government Performance and Results Act Modernization Act of 2010* (GPRA Modernization Act of 2010) holds Federal agencies *accountable* for establishing management processes, performance goals, and objectives. Developing outcome-oriented goals and describing how to achieve them allows agencies to assess results compared to their intended purpose and contributes to the agencies' *transparent* delivery of program results to the American taxpayer.

In FY 2024, we made one recommendation to TSA to assess risks and measure operational impacts when deploying air marshals to the Southwest border. As of September 18, 2024, OIG considers this recommendation open and resolved.

Vulnerabilities Resulting from Transparency Challenges

Assess Program Results

Although the *GPRA Modernization Act of 2010* requires the Department to develop objective, quantifiable, and measurable performance goals, TSA could not assess the operational impacts to its primary mission of safeguarding the Nation's transportation system while it deployed air marshals to assist U.S. Customs and Border Patrol (CBP) at the Southwest border. TSA did not establish baseline quantifiable goals to measure the effectiveness of its primary, day-to-day operations. Additionally, TSA did not perform a risk assessment to determine the operational impact of air marshal border deployments on transportation security. Establishing performance measures and assessing risks related to deploying air marshals would increase *transparency* by providing TSA the capability to report to stakeholders how deployments impact the Federal Air Marshal Service's mission to mitigate potential risks and threats to our Nation's transportation system. (OIG-24-35)

Figure 6: Federal Air Marshal Escorting Migrants
Source: OIG-24-35

Figure 7: Federal Air Marshal Training to Mitigate Potential Risks and Threats
Source: Law Enforcement/Federal Air Marshal Service Roadmap, June 2023, TSA

The Department's strategic mission to counter terrorism and homeland security threats focuses on instituting actions to detect, disrupt, mitigate, and guard against homeland security threats, as well as inform decision makers. To meet these desired outcomes, the Department and its partners need a proactive response to identify, detect, and prevent attacks against the United States. Developing and implementing best practices, formalizing after-action reports, and collaborating with stakeholders may aid in operational *efficiency* to the Homeland Security Enterprise.

As of September 18, 2024, we made 14 recommendations to the Department and its components in FY 2024 regarding *efficiency* challenges that impair the ability to counter terrorism and prevent threats. Of the 14 recommendations, OIG considers 12 open and resolved and 2 open and unresolved.

Further, based on our review, 7 of the recommendations pertain to improving coordination with internal and external stakeholders to better respond, support, address, and resolve issues related to protecting the Nation. The Department may avoid future challenges by developing and implementing or reviewing and updating protocols and agreements with stakeholders at the program level.

Vulnerabilities Resulting from Efficiency Challenges

Collaborate with Stakeholders

The *Intelligence Reform and Terrorism Prevention Act of 2004*[2] requires all agencies that store or use intelligence or terrorism information to implement Government-wide information sharing. However, CBP could not access all biometric data held in the Department of Defense's Automated Biometric Identification System. This information is vital for CBP to make a fully informed decision regarding traveler admissibility. Additionally, CBP officers may not always query every traveler against law enforcement databases to identify whether derogatory information exists. Without querying all noncitizens entering the country through available systems and databases, CBP negates *efficiencies* these technologies provide for determining admissibility and risks, allowing criminals, suspected terrorists, or other nefarious actors to enter the United States. Improving collaboration with stakeholders, including the use of databases that share intelligence and terrorism information would advance CBP's ability to execute the Department's mission to counter terrorism and prevent threats *efficiently*. (OIG-24-27)

Figure 8: CBP processes pedestrians and vehicles entering and leaving the United States
Source: CBP Visual Communications Division

[2] Pub. L. No. 108-458 (2004).

Vulnerabilities Resulting from Efficiency Challenges (continued)

Develop and Implement Best Practices and Formalize After-action Reports

The U.S. Secret Service (Secret Service) planned and conducted protective operations at several sites affected by the January 6 events. Although it did not anticipate or plan for the level of violence that ultimately occurred, Secret Service took actions to respond to and mitigate the threats it encountered, ultimately avoiding any harm to its protectees, while also assisting U.S. Capitol Police. These were unprecedented events; however, OIG identified opportunities for Secret Service to improve future *efficiencies*. For example, the process used to identify personnel available for deployment to the Capitol resulted in an 80-minute delay and fewer personnel deploying than Secret Service leadership anticipated. Secret Service personnel who took part in the response to the Capitol said they participated in after-action discussions but not in any formal documented reviews. Some Secret Service staff felt that, given their level of training and equipment, they could have been better utilized to directly engage rioters rather than secure static positions. Other officers expressed concerns with the lack of coordination. A formal after-action review by Secret Service would have been invaluable for its own institutional knowledge and to help external reviewers determine the true happenings of the day. Proper planning and preparation are vital for protecting leadership, events, and soft targets and could help the Department to *sustain* its mission and mitigate against *inefficient* practices.

Secret Service did not concur with two of OIG's recommendations, which are still open and unresolved. For example, we recommended the Director of the Secret Service develop and implement protocols for providing Civil Disturbance Unit support to law enforcement partners in the event of an emergency such as occurred on January 6 to ensure appropriate and timely response. Secret Service stated its primary mission limits its ability to provide emergency support to other law enforcement partners. The recommendation does not assert that Secret Service should enter into an agreement with other law enforcement partners to provide mutual aid. However, the review identified that Secret Service offered and provided assistance but did not have protocols in place for this rare emergency. Without such protocols, Secret Service could not identify available officers in a timely manner. (OIG-24-42)

Recent Reviews Announced by OIG

Following the assassination attempt that injured former President Donald Trump, we announced reviews of the Secret Service Process for Securing Trump Campaign Events on July 13, 2024, Secret Service Counter Sniper Preparedness, and Secret Service Planning and Implementation Activities for Protective Operations.

Mission 2: Secure and Manage Our Borders

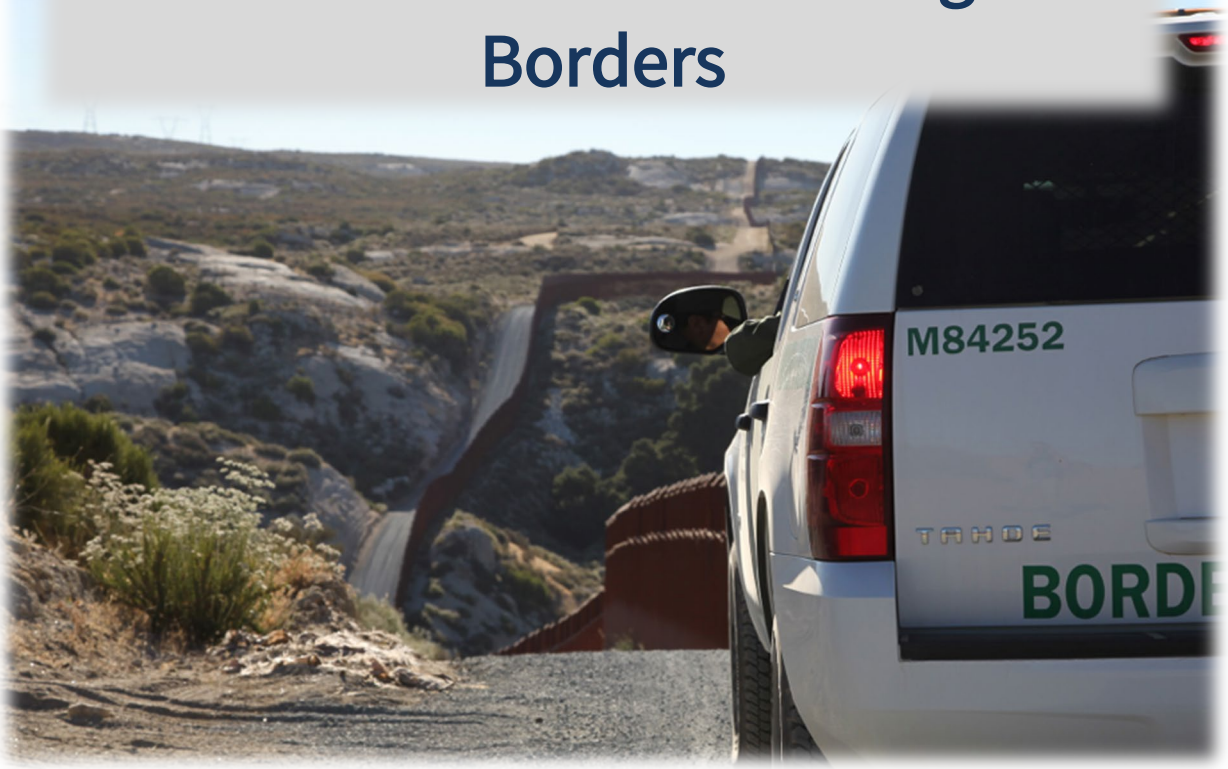


Figure 9: U.S. Border Patrol agents guarding the Southwest border
Source: U.S. Border Patrol, 2024-2028 Strategy, CBP

Mission 2 Overview:

Across the world, more people are displaced from their homes than at any time since World War II, and over the past decade there has been a fundamental change in migratory patterns that has far-reaching impacts for DHS and the broader U.S. immigration system. The Department's mission to secure and manage our borders has been bolstered by our investments and reinvigoration of the legal immigration system, as well as our work to leverage an all-of-DHS approach and collaboration with our partners across the federal government. We have shown that we can both enforce our laws and treat those in our custody with dignity and respect, while also improving logistics, coordination, technology, innovation, intelligence, consequence delivery, and accountability.

Related Strategic Goal: 2 and 4

Related Strategic Priority: 9

Components Impacted: CBP, United States Immigration and Customs Enforcement (ICE), TSA, United States Citizenship and Immigration Services (USCIS), United States Coast Guard (Coast Guard), DHS Headquarters (HQ)/Support

Figure 10: CBP Uniform Patch
Source: DHS, Photo by Benjamin Applebaum

Recent Mission-Related OIG Reports:

- Limited-Scope Unannounced Inspection of Mesa Verde ICE Processing Center in Bakersfield, California (OIG-24-03)
- Results of Unannounced Inspections of CBP Holding Facilities in the Miami Area (OIG-24-04)
- Results of Unannounced Inspections of CBP Holding Facilities in the San Diego Area (OIG-24-07)
- Summary of Previously Issued Recommendations and Other Insights to Improve Operational Conditions at the Southwest Border (OIG-24-10)
- ICE Major Surgeries Were Not Always Properly Reviewed and Approved for Medical Necessity (OIG-24-16)
- Results of July 2023 Unannounced Inspections of CBP Holding Facilities in the Rio Grande Valley Area (OIG-24-20)
- Results of an Unannounced Inspection of ICE's Krome North Service Processing Center in Miami, Florida (OIG-24-21)
- Results of an Unannounced Inspection of ICE's Golden State Annex in McFarland, California (OIG-24-23)
- Results of an Unannounced Inspection of ICE's Denver Contract Detention Facility in Aurora, Colorado (OIG-24-29)
- ICE's Risk Classification Assessment Process Was Not Consistently Used to Prevent the Release of High-Risk Individuals (OIG-24-31)
- Management Alert - CBP Has Limited Information to Assess Interview-Waived Nonimmigrant Visa Holders - (REDACTED) (OIG-24-33)
- Results of October 2023 Unannounced Inspections of CBP Holding Facilities in the El Paso Area (OIG-24-39)
- Results of January 2024 Unannounced Inspections of CBP Holding Facilities in the Del Rio Area - (REDACTED) (OIG-24-44)
- CBP Did Not Thoroughly Plan for CBP One™ Risks, and Opportunities to Implement Improvements Exist (OIG-24-48)
- CBP Conducts Individualized Assessments but Does Not Comprehensively Assess Land Port of Entry Operations (OIG-24-51)
- Summary of Unannounced Inspections of ICE Facilities Conducted in Fiscal Years 2020-2023 (OIG-24-59)

APR Challenges

The Department's recent APRs include numerous challenges and risks its components face relating to their ability to secure and manage U.S. borders, including but not limited to:

- Responding to elevated levels of irregular migration at the Southwest border putting a strain on Department-wide resources and personnel
- Diverting assets to respond to other priorities
- Challenging work locations, evolving job requirements, and shifting policies
- Maintaining operational availability and capability of many assets at the end of their service life being costly

Recent Progress as Reported in the APR

- CBP announced a dramatic expansion of non-intrusive inspection technology at U.S. ports of entry (POEs). These large-scale scanners will advance CBP's inspection capacity for passenger vehicles to 40 percent and for cargo vehicles to 70 percent.
- CBP is identifying workforce management solutions to close critical gaps in recruiting and retention efforts and is focused on developing incentives that improve the retention of skilled and experienced agents and establishing training for law enforcement and mission support personnel across career lifecycles.

Managing the flow of people and goods into the United States is critical to maintain national security. As such, the Department performs operations to safeguard the Nation from terrorism and illegal entry of persons. The Department may detain people who are inadmissible, deportable, or subject to criminal prosecution in short- and long-term detention facilities, as appropriate; ultimately, repatriating, releasing, or transferring detainees to other agencies.

Maintenance and availability of accurate records are vital when informing partners, such as Congress, of program efforts. The Department's inability to provide data and information to its stakeholders to ensure compliance with applicable standards related to securing U.S. borders highlights a critical challenge to *transparency.*

As of September 18, 2024, we made 8 recommendations to the Department and its components in FY 2024 regarding *transparency* challenges impacting its ability to protect detainees in custody. Of the 8 recommendations, OIG considers 3 open and resolved and 5 closed.

Further, 6 of the recommendations pertain to improving data integrity, including ensuring the Department documents custodial, use of force, and medical approvals accurately. The Department may avoid future *transparency* challenges by developing and implementing a quality assurance plan across department-wide detention facilities.

Vulnerabilities Resulting from Transparency Challenges

Provide Accurate, Complete, and Consistent Records

CBP operates the "e3" portal to collect and transmit data related to law enforcement activities. According to the *National Standards on Transport, Escort, Detention, and Search* (TEDS), "[a]ll custodial actions, notifications, and transports that occur after the detainee has been received into a CBP facility must be accurately recorded…as soon as practicable." While accurate, complete, and consistent records are critical for CBP to monitor the care of detainees, data integrity issues remain a recurring theme for CBP. For example, TEDS requires staff to provide detainees with food at regularly scheduled mealtimes and to document these meals in the appropriate electronic system of record. Although CBP agents reported detainees receive three meals per day at the facilities, some of the CBP logs did not reflect this. We highlighted unreliable data and inaccurate reporting of CBP holding facility conditions in last year's review of the Department's top management and performance challenges. Based on FY 2024 reviews, this issue remains a barrier to *transparency*. CBP generally met other applicable standards to provide or make available amenities such as food, water, sleeping mats, and medical care to detainees. (OIG-24-04, OIG-24-07, OIG-24-20, OIG-24-39, OIG-24-44)

Figure 11: Border Patrol Agent provides Migrant with Drink, Food, and Clothing
Source: OIG-24-04

Vulnerabilities Resulting from Transparency Challenges (continued)

Support Decisions Appropriately

ICE Health Service Corps (IHSC) medical staff administer health care at ICE facilities and oversee the care of detained non-citizens at contracted facilities. In some cases, an offsite medical provider may examine a detainee and recommend a surgical procedure. To ensure medical necessity, only IHSC physicians designated as Regional Clinical Directors and Clinical Directors can review and approve surgeries to be performed on detained non-citizens. However, in a statistical sample of 227 cases from FY 2019 through FY 2021, IHSC was not able to provide supporting documentation to demonstrate that appropriately designated IHSC staff reviewed and approved 72 major surgeries (32 percent). Without this documentation to determine medical necessity, these major surgeries were not properly reviewed or approved, and therefore were unauthorized. These findings show a lack of *transparency* and *accountability* in the IHSC approach to noncitizen health care, especially as it pertains to authorizing critical surgical procedures. (OIG-24-16)

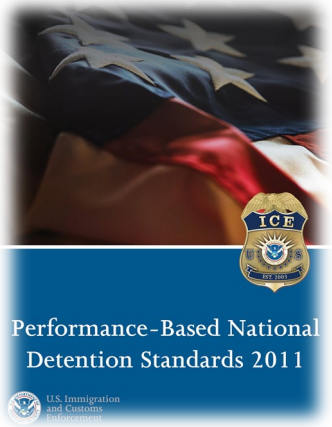


Figure 12: PBNDS 2011
Source: ICE

Ensure Appropriate Documentation of Any Use of Force Incidents

The *Performance-Based National Detention Standards 2011* (PBNDS 2011), revised in 2016, requires facility staff to use physical force only when necessary and reasonable and requires appropriate documentation of any use of force incidents, including use of audio-visual recordings. Facility staff must also notify the ICE Field Office Director of any use of force incident as soon as practical and in writing within 2 business days. Although one ICE facility claimed no use of force incidents occurred in the past 2 years, detainee interviews revealed a recent event when facility staff removed four detainees from their dorm using tactics classified in PBNDS 2011 as a use of force. Our review of the facility's closed-circuit television (CCTV) system and written accounts showed the facility and ICE staff used an appropriate amount of force to remove detainees, but the facility did not report the incident to the ICE Field Office Director appropriately. Additionally, the facility's CCTV system captured the incident, but it did not provide an audio record. CCTV footage remains preserved for 90 days. Had this incident occurred more than 90 days before our visit, we would have had to rely solely on facility and ICE staff's written documentation and interviews of detainees involved in the incident, which may confuse or impede *transparency* related to appropriate use of force. (OIG-24-03)

Enforcing immigration laws focused on protecting national security is critical. To ensure the Department delivers immigration processes and systems in a safe, orderly, and humane manner, upholding civil rights, civil liberties, and privacy, the Department issues standards to guide the safety, security, and care for detainees while in custody.

CBP is responsible for short-term holding of noncitizens encountered at the border who are inadmissible or deportable from the United States, as well as individuals at the border who are subject to criminal prosecution. TEDS standards incorporate best practices and reflect key legal and regulatory requirements, including provisions for transport, escort, detention, search, care of at-risk individuals in custody, and personal property, among many others. Similarly, when ICE detains noncitizens pending their immigration proceedings, PBNDS 2011 sets expectations for various services ICE is required to provide to detainees, such as medical and mental health services, legal access services, communication services for noncitizens with limited English proficiency, a grievance process, and more. Although the Department is *accountable* for complying with these standards, CBP and ICE did not consistently meet some requirements put in place to ensure the safety, security, and care for detainees and facility staff.

As of September 18, 2024, we made 36 recommendations to the Department and its components in FY 2024 regarding *accountability* challenges impacting its ability to care for detainees. Of the 36 recommendations, OIG considers 12 open and resolved and 24 closed.

Further, 24 of the recommendations pertain to ensuring consistent compliance with standards of care for detainees. Components have performed the actions required to close 18 of these recommendations in FY 2024, the same year OIG reports related to these reviews and recommendations were published. To avoid future *accountability* challenges, the Department, its components, and detainees may benefit from the development, implementation, and regular monitoring of quality assurance mechanisms across department-wide detention facilities to ensure detainees are treated safely, securely, and humanely.

Figure 13: Crowded Cell at CBP Holding Facility
Source: OIG-24-07

Figure 14: Crowded Cell at CBP Holding Facility
Source: OIG-24-20

Vulnerabilities Resulting from Accountability Challenges

Comply with TEDS Requirements

We previously reported that detainees in CBP custody experienced prolonged detention and overcrowding; OIG inspection results published in FY 2024 confirm these issues continue. For example, TEDS generally limits detention to 72 hours (3 days), as operationally feasible. However, 668 of the 1,187 (56 percent) detainees in custody in the facilities OIG inspected were held over 72 hours, including one detainee in custody over 34 days while USCIS and Department of Justice (DOJ) considered a fear claim.[3] Additionally, two facilities exceeded maximum facility capacity. There were additional instances of non-compliance related to medical support, hygiene, bedding, and temperature below the minimum standard. (OIG-24-07, OIG-24-20, OIG-24-39, OIG-24-44)

Figure 15: Detainees in Holding Cell Without Sleeping Mats
Source: OIG-24-39

Comply with PBNDS 2011 Requirements

ICE facilities OIG inspected did not comply with some PBNDS 2011 requirements, such as Staff-Detainee Communication and Grievance System requirements. Table 1 provides a sample of non-compliance with detention standards published in some of OIG's FY 2024 Inspection Reports.

Table 1: PBNDS 2011 Total Requirements Violated by ICE Facilities Inspected

Mesa Verde ICE Processing Center	Krome North Service Processing Center	Golden State Annex	Denver Contract Detention Facility
3	6	6	10

Source: Based on analysis of ICE data in OIG Reports (OIG-24-03, OIG-24-21, OIG-24-23, OIG-24-29)

Ensure Sufficient Contract Support

Contract medical providers at CBP facilities can diagnose medical conditions and prescribe medication, while assistant-level providers deliver medical support. However, some CBP holding facilities were understaffed to deal with the number of detainees encountered. CBP's inability to ensure the contract medical provider meets the staffing requirements could reduce the quality of medical support provided to detainees while in CBP custody. (OIG-24-20, OIG-24-44)

[3]Individuals subject to expedited removal who indicate an intention to apply for asylum, express a fear of persecution or torture, or a fear to return to their home country are referred to asylum officers to determine whether they have credible fear of persecution or torture.

Holding Bad Actors Accountable

Fighting Against Human Smuggling

The Department has recently expanded safe pathways for migrants to lawfully enter the United States; however, there are some who attempt to circumvent immigration processes and systems through illegal means, such as human smuggling. Human smuggling is the importation of noncitizens into the United States by deliberately evading immigration laws, as well as unlawfully transporting and harboring noncitizens who have already crossed the border into our Nation. To mitigate human smuggling, Homeland Security Investigations (HSI) is *accountable* for identifying, tracing, and dismantling criminal networks, alongside domestic and international partners.

For example, in July 2021, DOJ's Office of Attorney General established the Joint Task Force Alpha (JTFA), in partnership with the Department, including HSI, Border Patrol, and OIG, and others to strengthen efforts to combat the rise in prolific and dangerous smuggling coming from Central America and affecting border communities. Joint efforts of the JTFA resulted in the indictment of a woman who pled guilty along with 10 others of money laundering and human smuggling.[4]

As an additional example, in December 2023, an investigation led by OIG, with assistance from HSI, CBP, and other partners, resulted in the indictment of two individuals illegally present in the United States on conspiracy to forge and distribute I-551 stamps[5] as part of a broader human smuggling scheme.[6]

Figure 16: JTFA Encountered 81 Migrants in the back of a tractor trailer
Source: DOJ, Office of Public Affairs

[4] Operation leader and 10 others plead guilty in prolific human smuggling and money laundering case,
[5] The Department issues I-551 stamps on foreign passports as temporary evidence of permanent resident status, which can be used for travel, identity verification, and employment authorization.
[6] Mexican men indicted for forging federal documents related to human smuggling scheme

Combatting Department Workforce Trafficking and Bribery

The Department is *accountable* for handling high level corruption investigations involving significant smuggling organizations and bribery. To *sustain* mission operations at the border, Department investigators must foster relationships with Federal partners and other stakeholders, including sharing real-time information and deconflicting, to ensure the Department gathers appropriate evidence and investigations result in subsequent convictions of corrupt officers.

During FY 2024, several CBP officers were convicted in federal court on charges such as accepting bribes to allow vehicles containing unauthorized individuals or illicit drugs to pass through the border into the United States or to provide immigration paperwork that would permit an individual to remain in the United States. For example, one former CBP officer conspired to allow entry without inspection or documentation of passengers. Additionally, he accepted $6,000 to smuggle "sham" cocaine across the POE. Another former CBP officer admitted to opening restricted border fences to allow people to enter the United States illegally in exchange for cash payments of $5,000 per opening. Additionally, unbeknownst to him, as part of a sting operation, he picked up a bag of narcotics in exchange for $20,000, after which, he was arrested. Agents searched his residence and found over $130,000 in cash and 7.7 grams of cocaine.[7]

Countering Department Workforce Corruption

An OIG Special Agent (SA) was recently recognized by HSI as its Law Enforcement Partner of the Year. HSI noted the SA's impeccable reputation and work ethic helped to build bridges between OIG and HSI, as well as the Drug Enforcement Administration and the Federal Bureau of Investigation. Additionally, the SA's ability to creatively investigate corruption, in one case, resulted in the location, identification, and ultimate arrest of two CBP officers that fled to Mexico. In a separate case, the SA led a thorough corruption investigation that resulted in the conviction of a corrupt CBP officer, as well as the arrests and convictions of several targets of investigation. HSI noted the SA played a significant role in furthering the Department's mission.

[7] Former federal officer admits to smuggling aliens and receiving bribes to allow cocaine across the border, Former U.S. Border Patrol Agent Sentenced to 87 Months in Prison for Attempting to Distribute Methamphetamine and Receiving Bribes, Former Border Patrol Agent Sentenced on Bribery Charges; and Customs and Border Protection Officer Convicted by Federal Jury of Receiving Bribes, Allowing Drug-Laden Vehicles to Enter the U.S.

The ability to staff programs and provide resources are key to advancing the Department's mission. However, the Department struggles to staff program functions properly, supply resources, advance technology, and minimize waste, hampering its efforts to *efficiently* maintain the safety and security of U.S. borders. The overall rising number of migrant encounters has resulted in increased workloads and the need for additional or advanced resources.

As of September 18, 2024, we made 7 recommendations to the Department and its components in FY 2024 regarding *efficiency* challenges it faces when securing the U.S. borders, including but not limited to its ability to provide or obtain services timely for detainees. Of the 7 recommendations, OIG considers 4 open and resolved and 3 closed.

Vulnerabilities Resulting from Efficiency Challenges

Accrue and Advance Resources

While migrant encounters have increased since FY 2021, there was no corresponding increase in transport vehicles for one of the sectors OIG inspected. The shortage of transportation vehicles and holding capacity limitations prevent CBP from *efficiently* facilitating migrants' progress through the immigration system. CBP has taken initial steps to increase its transportation resources, but without proper follow through, the Department risks not providing appropriate care and conditions for migrants in detention. Since our review, CBP took steps to increase transportation resources. (OIG-24-04)

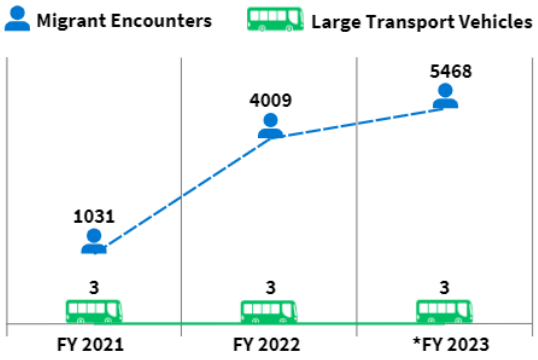


Figure 17: Border Patrol's Miami Sector Encounters Compared to the Number of Large Transport Vehicles, FY 2021-2023
Source: OIG-24-04

Plan for Migrant Surges and Dedicate Sufficient Staff

We previously reported that CBP could not sufficiently staff one of its sector's Central Processing Centers (CPC) during migrant surges and made staffing recommendations to the Sector Chief, accordingly. CBP conducted corrective actions and OIG closed the recommendation; however, during an October 2023 inspection, we found CBP continued to experience challenges staffing CPCs during migrant surges. This occurred because CBP did not dedicate staff to the three CPCs commensurate with the increased migrant holding capacity created in the sector. Subsequently, agents could not effectively manage the processing and supervision of detainees at two of its facilities and could not open a third facility to accommodate the influx of detainees due to current sector staffing levels. Ultimately, insufficient staffing resulted in delays and *inefficiencies* in immigration enforcement actions and contributed to prolonged time in custody for detainees. (OIG-24-39)

Vulnerabilities Resulting from Efficiency Challenges (continued)

Eliminate Waste

ICE's Enforcement and Removal Operations (ERO) Division oversees detention facilities, which are managed in conjunction with private contractors, state, or local governments. These ICE-established facility contracts require a guaranteed minimum payment for a fixed number of detainees, regardless of unused bed space. During our unannounced inspection of one ICE facility, we determined ICE paid approximately $25.3 million for unused bed space in the 12 months preceding our inspection. ICE may need to reassess facility contracts to avoid excessive payment for unused bed space and ensure *efficient* operations. (OIG-24-23)

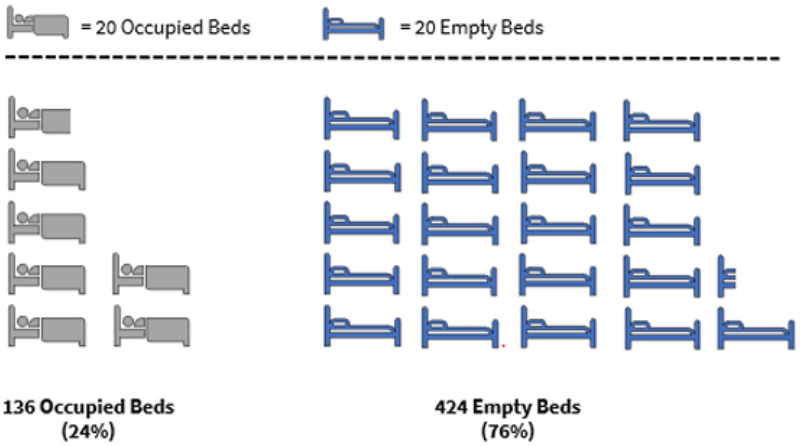


Figure 18: Monthly Average of Occupied vs. Empty Beds Based on the Guaranteed Minimum of 560 Detainees between April 20, 2022, and April 19, 2023
Source: OIG-24-23

Taking Crime Off the Streets

Adopting a Government-wide Approach

Fourteen indictments were handed down in federal court charging 47 alleged members of an Imperial Valley-based, Sinaloa Cartel-linked fentanyl and methamphetamine operation network with drug trafficking, firearms, and money laundering offenses. "[We] are unrelenting in our work to keep deadly fentanyl off our streets and bring those who traffic in it to justice," said Secretary of Homeland Security Alejandro N. Mayorkas. "Together, we are preventing fentanyl and other deadly drugs from being produced, distributed, or consumed, and saving countless lives."[8]

[8] Forty-Seven Defendants Charged in HSI-led Drug Trafficking Investigation Linked to Sinaloa Cartel

Mission 3: Administer the Nation's Immigration System

Figure 19: Naturalization Ceremony
Source: DHS, Photo by Benjamin Applebaum

Mission 3 Overview:

DHS has combined an expansion of lawful pathways with significantly strengthened consequences to reduce irregular migration. At the same time, we have worked to support improvements to the legal immigration system, which has enabled DHS to respond to humanitarian crises, respond to U.S. labor needs, and reunify families.

Related Strategic Goal: 2

Related Strategic Priority: 10

Components Impacted: CBP, ICE, TSA, USCIS, Coast Guard, HQ/Support

Recent Mission-Related Reports:

- DHS Has a Fragmented Process for Identifying and Resolving Derogatory Information for Operation Allies Welcome Parolees (OIG-24-24)
- CBP and ICE Did Not Have an Effective Process for Detaining and Removing Inadmissible Travelers at an International Airport - (REDACTED) (OIG-24-30)
- USCIS Faces Challenges Meeting Statutory Timelines and Reducing its Backlog of Affirmative Asylum Claims (OIG-24-36)

APR Challenges

The Department's recent APRs include numerous challenges and risks its components face relating to their ability to administer the Nation's immigration system, including but not limited to:

- Processing and detaining individuals seeking protection
- Lengthy approval processes for regulatory changes and paperwork reduction processes hindering efforts to digitize paper forms
- Unprecedented workforce stressors due to mission changes from new populations coming to the United States and funding constraints
- Addressing regulatory actions in a timely manner to fulfill CBP's travel mandate
- Increasing immigration court docket litigation due to limited resources
- Defending ICE's enforcement authorities and policies

Recent Progress as Reported in the APR

- In 2023, USCIS awarded approximately $22 million in grants to 65 organizations in 29 states to help prepare lawful permanent residents for naturalization.
- USCIS continues to expand its online presence, increasing the number of forms available to file online, delivering on an agency priority to make operations more efficient and effective for the agency and its stakeholders, applicants, petitioners, and requestors. To help manage this process, the USCIS Contact Center has online tools and resources to give users the same information they would get by speaking to a representative. This information is available 24 hours a day, 7 days a week, from a cell phone, tablet, or computer.

Figure 20: Homeland Security Secretary Alejandro Mayorkas participated in a USCIS Naturalization Ceremony
Source: DHS, Photo by Benjamin Applebaum

Holding Bad Actors Accountable

Fighting Immigration Fraud

Violations of immigration law include benefit fraud and document fraud. Benefit fraud is committed by an individual who knowingly and willfully misrepresents material fact on a petition or application to gain an immigration benefit. Most detection of immigration fraud occurs during adjudications of request for immigration benefits by USCIS. The USCIS Fraud Detection and National Security Directorate conducts administrative investigations which often result in the denial of immigration benefit requests because of fraud.

According to the Department, the most serious cases of fraud are referred by USCIS to HSI for criminal investigation. Document fraud refers to the general manufacturing, counterfeiting, alteration, sale, or use of identity documents and other fraudulent documents to evade immigration laws or for other criminal activity. HSI identifies sources of identity and benefit fraud and refers these criminals who prey on people and systems for illegal access to benefits to the U.S. Attorney for prosecution. In essence, the USCIS Fraud Detection and National Security Directorate and HSI are *accountable* for holding perpetrators of fraud both civilly and criminally liable for their fraudulent activities.

- A Chicago attorney was indicted on federal fraud charges for allegedly providing false and fraudulent information to U.S. authorities to obtain immigration benefits for his noncitizen clients. For example, he allegedly advised clients to enter sham marriages with U.S. citizens or lawful permanent residents to obtain benefits, helped clients cheat on oral civics exams, falsified claims of spousal abuse purportedly suffered by clients, and fictionalized job offers from U.S. companies who would supposedly sponsor clients for residency. The indictment charges the attorney with one count of conspiracy to commit immigration fraud and 5 individual counts of falsifying applications for immigration benefits. Each count of visa fraud carries up to 10 years in federal prison, while the conspiracy count carries a maximum sentence of 5 years.[9]
- In 2014, a Maryland woman married a Ghanaian national, who subsequently obtained legal permanent residence status. From 2014 through 2021, the couple conspired to obtain U.S. passports for the man's children through false statements and fraudulent identity documents. In July 2024, the woman was sentenced to 30 months in federal prison for passport fraud, among other types of fraud. Additionally, she was ordered to pay over $128,000 in restitution. The man previously pled guilty to a series of fraud charges, including conspiracy to commit passport fraud and was sentenced to 28 months in federal prison and ordered to pay restitution of nearly $128,000.[10]

[9] Chicago Attorney Indicted on Immigration Fraud Charges

[10] Maryland Woman Convicted After Five-Day Trial for a Series of Fraud Schemes, Including Passport Fraud, Wire Fraud, and Bankruptcy Fraud
Maryland Woman Sentenced To 30 Months For A Series Of Fraud Schemes, Including Passport Fraud, Wire Fraud, And Bankruptcy Fraud

USCIS developed an operational planning model to determine how hypothetical shifts in staff levels and workload priorities impact the backlog of affirmative asylum cases. For instance, USCIS can enter resource inputs into the planning model to run different resource allocation scenarios and determine how different resource configurations affect its backlog reduction. After applying the operational planning model to affirmative asylum cases, USCIS projects its backlog to increase to over 2 million cases by FY 2030. The rise in asylum claims without a corresponding increase in resources may have a domino effect on program *efficiencies*.

As of September 18, 2024, we made 4 recommendations to the Department in FY 2024 regarding *efficiency* challenges it faces when administering the Nation's immigration system, including developing and implementing a multi-year operational plan that includes clear priorities and goals and submitting a budget request in line with the plan and improving risk management. Of the 4 recommendations, OIG considers 3 open and resolved and 1 open and unresolved.

Vulnerabilities Resulting from Efficiency Challenges

Adjudicate Affirmative Asylum Applications Timely and Reduce Caseload Backlog

USCIS is responsible for administering lawful immigration and adjudicating affirmative asylum applications per the applicable mandates. The Immigration and Nationality Act requires completion of final administrative adjudication of these applications within 180 days of filing, absent exceptional circumstances. However, USCIS did not timely adjudicate affirmative asylum applications, impacting its ability to reduce its existing backlog.[11] As of the end of FY 2023, USCIS had more than 786,000 asylum cases pending determination for over 180 days. This occurred because USCIS did not have sufficient funding, staffing, and planning to complete its affirmative asylum caseload. Without an increase in resources, USCIS cannot meet statutory timelines which will result in growth of the affirmative asylum case backlog. If USCIS continues to postpone adjudication of asylum claims, it will delay eligible affirmative asylum applicants' ability to obtain asylum and related immigration benefits, such as lawful permanent residency and citizenship. USCIS will likely experience increased litigation from individuals filing lawsuits due to adjudication delays. This would require diverting USCIS' already limited resources from production efforts. Without sufficient resources to perform *efficient* review and adjudication of asylum applications, the ever-growing backlog of cases may become a mission *sustainability* challenge. (OIG-24-36)

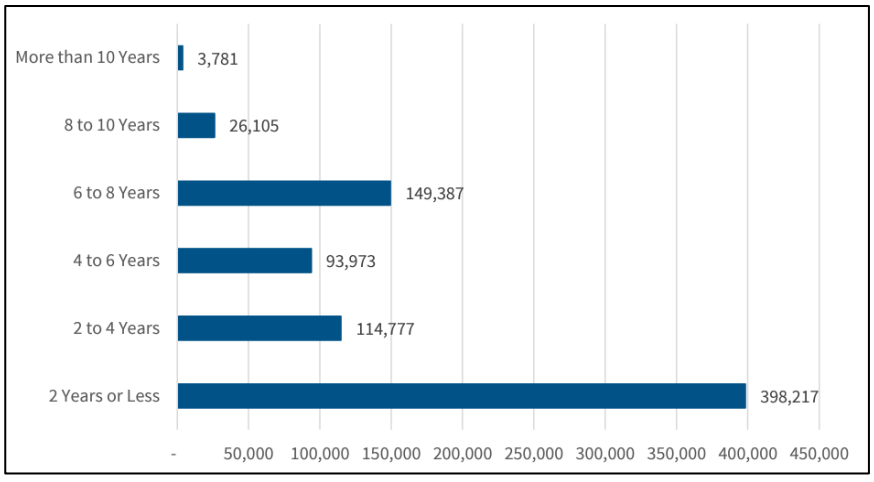


Figure 22: Affirmative Asylum Claims Pending More than 180 days as of FY 2023
Source: OIG-24-36

[11] *Immigration and Nationality Act, Title II § 208, 8 United States Code, § 1158 (d)(5)(A)(iii).*

Congress established the Department to consolidate the Nation's approach to homeland security, combining the functions of 22 different Federal departments and agencies with broad responsibilities to secure the Nation from threats. Since its inception over 20 years ago, the Department has matured its mission areas to collectively prevent attacks, mitigate threats, respond to national emergencies, and preserve economic security. However, Department components still use fragmented approaches to execute enterprise-wide missions. The Department can do more to strengthen enterprise governance and advance operational *sustainability,* such as ensuring the Department's vision consists of actionable goals, objectives, and operational activities through strategic planning documents. To advance organizational governance effectively, Components must work together to align strategic guidance to resources and operational outcomes across the enterprise. In July 2018, GAO issued *Better Guidance for Strategy Development Could Help Agencies Align Their Efforts* (GAO-18-499), identifying key elements that help ensure agencies align strategies without fragmenting planning efforts. Addressing interagency coordination, strategic integration, and assessment of progress consistently may help the Department to better manage fragmentation in strategic planning to *sustain* enterprise-wide missions, such as administering the Nation's immigration system.

As of September 18, 2024, we made 8 recommendations to the Department in FY 2024 regarding *sustainability* challenges it faces when administering the Nation's immigration systems, including but not limited to its ability to coordinate across components. Of the 8 recommendations, OIG considers 7 open and resolved and 1 open and unresolved. Formalizing a cohesive, enterprise-wide approach to achieving critical homeland security objectives may improve the Department's ability to mitigate risks and *sustain* program operations.

Figure 23: Department Components

Source: Department of Homeland Security Annual Performance Report for Fiscal Years 2023-2025

Vulnerabilities Resulting from Sustainability Challenges

Identify and Resolve Derogatory Information for Operation Allies Welcome Parolees

Three Department components—CBP, USCIS, and ICE—have separate but interconnected processes to identify and resolve derogatory information for individuals evacuated from Afghanistan and paroled into the United States under Operation Allies Welcome (OAW). For each evacuee,[12] Components and Federal partners review derogatory information, which includes any information that prompts a request for additional investigation or clarification and may ultimately lead to an unfavorable decision by a reviewing entity. While the Department has a multifaceted approach to identify and resolve issues for noncitizens with derogatory information, the process is fragmented. The siloed approach creates gaps in Components' responsibility for terminating parole, initiating removal proceedings, and monitoring parole expiration. The process has been complicated by litigation on the Department's immigration law enforcement policies, as well as factors such as considering derogatory information in the re-parole and parole extension processes. To *sustain* the Department's mission to administer the Nation's immigration system, it must consider how to address these vulnerabilities in USCIS and ICE processes for resolving derogatory information and to establish processes for managing the end of parole. (OIG-24-24)

Detain and Remove Inadmissible Travelers

CBP inspects international travelers at POEs, including airports, to determine admissibility. If CBP determines a traveler arriving at an international airport is inadmissible, a CBP officer may arrange to return the traveler to their country of residence on the next available flight. If a return flight for an inadmissible traveler is unavailable on the same day, CBP contacts ICE to detain the individual until a return flight can be arranged. However, at the location reviewed, CBP and ICE did not have an effective process for detaining and removing inadmissible travelers from custody. Between FY 2021 and 2023, CBP officials at this location released at least 383 inadmissible travelers from custody; 168 (44 percent) of these travelers did not return for their removal flight. Additionally, CBP did not issue Notices to Appear (NTA) to 77 inadmissible travelers who did not return for their flights. As such, the inadmissible travelers at the location reviewed were not placed in removal proceedings or subject to ICE monitoring. Without a coordinated approach between CBP and ICE, CBP will continue to release inadmissible travelers, many of whom do not return for removal flights as required. This results in ICE offices nationwide assigning personnel and using funds to locate and arrest inadmissible travelers, litigate cases in removal proceedings, and arrange repatriation flights, which is an *inefficient* use of resources. Additionally, if CBP does not issue NTAs to transfer these cases to ICE, ICE officers may not be aware that these travelers remain in the United States and are potentially subject to removal proceedings, impacting mission *sustainability*. (OIG-24-30)

[12] An evacuee is any individual, regardless of immigration status, who the U.S. Government evacuated from Afghanistan during Operation Allies Refuge and OAW.

Mission 4: Secure Cyberspace and Critical Infrastructure

Figure 25: Understanding infrastructure system operations and dependency relationships, such as physical, cyber, geographical, and logical, supports identification of resilience issues
Source: Marine Transportation System Resilience Assessment Guide, CISA

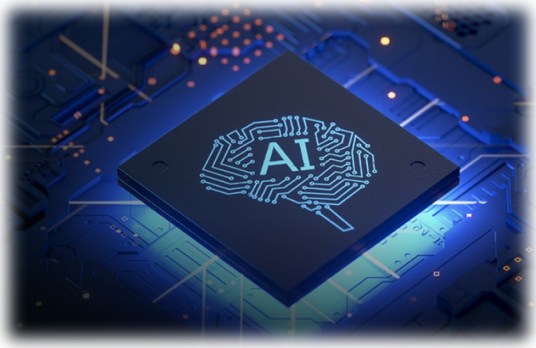
Mission 4 Overview:

DHS will continue to protect the American people by preventing and mitigating active cyber threats, strengthening the nation's cyber resilience, driving a "security-by-design" approach with partners, and developing a cybersecurity workforce with the size, skills, diversity, and training necessary to meet our mission, protect our businesses and families, defend critical infrastructure, and forge a more secure future.

Related Strategic Goal: 3

Related Strategic Priority: 8

Components Impacted: CBP, Cybersecurity and Infrastructure Security Agency (CISA), Federal Emergency Management Agency (FEMA), ICE, TSA, Coast Guard, Secret Service, HQ/Support



Recent Mission-Related OIG Reports:

- Management Alert - ICE Management and Oversight of Mobile Applications - (REDACTED) (OIG-24-02)
- CISA Needs to Improve Collaboration to Enhance Cyber Resiliency in the Water and Wastewater Sector (OIG-24-09)
- Summary of Selected DHS Components that Did Not Consistently Restrict Access to Systems and Information (OIG-24-11)
- CISA's Use of Infrastructure Investment and Job Act Funds (OIG-24-22)
- Evaluation of DHS' Information Security Program for Fiscal Year 2023 (OIG-24-26)
- (U) Evaluation of DHS' Compliance with Federal Information Security Modernization Act Requirements for Intelligence Systems for Fiscal Year 2023 (OIG-24-28)
- Infrastructure Investment and Jobs Act Funding: CBP Must Improve Processes for Addressing Critical Repairs at CBP-owned Land Ports of Entry (OIG-24-32)
- Coast Guard Should Take Additional Steps to Secure the Marine Transportation System Against Cyberattacks (OIG-24-37)
- Management Alert - CISA and FLETC Did Not Take Action to Protect Personally Identifiable Information and Sensitive Law Enforcement Training Curricula (OIG-24-40)
- S&T Inconsistently Managed Critical Infrastructure Security and Resilience Research and Development Activities (OIG-24-47)
- CBP Did Not Thoroughly Plan for CBP One™ Risks, and Opportunities to Implement Improvements Exist (OIG-24-48)
- DHS Improved Election Infrastructure Security, but Its Role in Countering Disinformation Has Been Reduced (OIG-24-52)
- ICE Did Not Fully Implement Effective Security Controls on Selected High Value Asset Systems (OIG-24-53)
- I&A Needs to Improve Its Security Inspection Program to Reduce the Risk of Unauthorized Access to Classified Information (OIG-24-55)
- Coast Guard Needs to Implement Effective Planning for Infrastructure Investment and Jobs Act Projects (OIG-24-56)
- CISA Faces Challenges Sharing Cyber Threat Information as Required by the Cybersecurity Act of 2015 (OIG-24-60)
- ICE Did Not Always Manage and Secure Mobile Devices to Prevent Unauthorized Access to Sensitive Information (OIG-24-61)

APR Challenges

The Department's recent APRs include numerous challenges and risks its components face relating to their ability to secure cyberspace and critical infrastructure, including but not limited to:

- Identifying and improving stakeholder-specific, defensible architectural needs
- Hiring technology-proficient staff
- Funding gaps between demand and capabilities
- Challenges related to staffing subject matter expert positions, such as cybersecurity experts, operations research, and risk and data analysts
- Lacking necessary authorities for CISA's Infrastructure Security program to legally execute its mission due to a lapse of current authorities or failure to codify necessary authorities. Additionally, insufficient resources to execute its mission, inadequate contracting capabilities, and inefficient hiring processes impact the security, safety, and resilience of the Nation's infrastructure
- Improving TSA's ability to collaborate with partners to meet cybersecurity requirements for Transportation Security Equipment or it will be unable to maintain integrity of the aviation security infrastructure and address cyber vulnerabilities
- Maintaining situational awareness of persistent and evolving cybersecurity threats and ensuring the capability and capacity to respond with agility
- Growing cybersecurity risk (exploitation, misuse, or failure of maritime-based technologies) to the maritime transportation system significantly impacts the Nation's security and economy

Recent Progress as Reported in the APR

- CISA's updated Continuous Diagnostics and Mitigation Federal Dashboard enabled CISA analysts to quickly detect vulnerable systems related to a recent exploit on federal agency networks. Within minutes, CISA leveraged this host-level visibility into federal agency infrastructure to confirm potential risks, alert affected agencies, and actively track mitigation — preventing an active exploit from causing widespread harm across agency systems and impacting essential services upon which Americans depend.
- Components have leveraged the Department's Cyber Talent Management System to act more quickly than possible under traditional federal hiring authorities; compete with private sector compensation; and hire applicants based on skills and aptitude. Components whose core missions have a cyber nexus — like CISA, ICE, and Secret Service — continue to engage with the Cyber Community through conferences, coordinated in-person hiring and job fairs, and joined efforts to reach key talent pools.

The Department achieves its missions and protects its cyber systems and critical infrastructure by modernizing efforts, deploying protective capabilities, engaging with stakeholders, prioritizing risk management activities, and responding to emerging risks. Cyberattacks disrupt and can impair the *sustainability* of mission-essential operations. Executive Order 13800 holds executive departments and agencies *accountable* for managing cybersecurity risk to their enterprises. Maintaining *accountability* in the Department through the implementation and monitoring of internal controls safeguards against unauthorized access to systems, decreases the risk of cyberattacks, and reduces exposure of sensitive information.

As of September 18, 2024, we made 20 recommendations to the Department and its components in FY 2024 regarding *accountability* challenges it faces when securing cyberspace and critical infrastructure. Strengthening enterprise-wide oversight to ensure components adhere to Department policies and prioritizing information security weaknesses, both at the Department-level and component level, may help the Department better achieve optimal mission execution across the enterprise. Of the 20 recommendations, OIG considers 18 open and resolved and 2 open and unresolved.

Vulnerabilities Resulting from Accountability Challenges

Protect Sensitive Information

In 2023, the Department's Chief Information Security Officer (CISO) concluded the contractor for a specific online Learning Management System (LMS) — DHSLearning — had poor cybersecurity practices and did not comply with federal monitoring requirements leading to multiple hard drive failures, a service outage, and loss of Department data. The CISO issued a denial of authorization to operate and ordered all employees to stop using DHSLearning. Additionally, the CISO notified all component CISOs about the denial and shared the results of the investigation since some components also used this contractor's services to provide its LMS — including the Federal Law Enforcement Training Centers (FLETC) and CISA. According to its June 2017 Privacy Assessment, FLETC's LMS collects, maintains, uses, and disseminates personally identifiable information (PII) from law enforcement officers who are registered users of the system. CISA's LMS also serves as a privacy-sensitive system for members of the public, Department personnel, and other Federal employees. Although *accountable* for securing sensitive systems and information, FLETC and CISA did not take action to protect PII and sensitive law enforcement training curricula after being notified of the denial of authorization by the Department CISO. Additionally, the Department is *accountable* for ensuring CISA and FLETC mitigate the risk of using a contractor with poor cybersecurity practices that put users' PII at risk and expose sensitive courses housed on the systems. As of July 2024, the Department reported CISA and FLETC have taken action to proactively replace their LMSs and mitigate the control deficiencies identified in the Management Alert. CISA estimates completion by December 31, 2024; FLETC estimates completion by June 30, 2025. (OIG-24-40)

Vulnerabilities Resulting from Accountability Challenges (continued)

Improve the Cyber Posture of the Marine Transportation System

Coast Guard is *accountable* for strengthening the Marine Transportation System (MTS) against cyberattacks, mitigating the impact of cyberattacks on it, and preparing industry stakeholders for the future to protect the supply chain, U.S. ports, and U.S. waterways. The MTS facilitates the flow of trillions of dollars of U.S. imports and exports, making it a target for both adversary nations and cybercriminals. Coast Guard Cyber Command observed attacks targeted at companies providing logistics or technology services to the MTS. Such attacks could affect industry software and impact a large portion of the MTS at once. However, limited regulatory authority to enforce industry stakeholder compliance with cybersecurity measures combined with inadequate training and subject matter expertise across Coast Guard sectors impede the Component's ability to secure the MTS against cyber threats.

While Coast Guard concurred with the four recommendations made to improve its cyber readiness and precautions to secure the U.S. supply chain, two recommendations remain open and unresolved. For example, OIG recommended that Coast Guard's Assistant Commandant for Prevention Policy complete and publish cybersecurity-specific regulations providing enforcement authority for facility and vessel inspections. In February 2024, Coast Guard published a Notice of Proposed Rulemaking to seek public comment on proposed regulations specifically focused on establishing minimum cybersecurity requirements for U.S. flagged vessels, Outer Continental Shelf facilities, and U.S. facilities subject to Marine Transportation Security Act regulations. OIG believes the Notice of Proposed Rulemaking adheres to the intent of the recommendation. According to the Department, public comment on the Notice of Proposed Rulemaking closed in May 2024. As of October 2024, Coast Guard's estimated publication date for that final rule is December 31, 2024. (OIG-24-37)

Collaborate and Coordinate with Stakeholders

CISA supports the Environmental Protection Agency to reduce the risk of cyber threats and increase the Water Sector's resiliency. Although it offers an extensive portfolio of products and services to mitigate cybersecurity threats to Water Sector stakeholders, CISA did not consistently collaborate with the Environmental Protection Agency and the Water Sector to leverage and integrate its cybersecurity expertise with stakeholders' water expertise. Additionally, CISA did not effectively coordinate internally to share critical information. Although CISA is *accountable* for ensuring it communicates cyber risks appropriately to stakeholders and that stakeholders are aware of CISA's products and services, inconsistent collaboration with external stakeholders and ineffective internal coordination limit its ability to help improve resiliency against cyber threats. (OIG-24-09)

The *FY 2024-2026 Cybersecurity Strategic Plan* guides CISA's efforts in pursuit of a new vision for cybersecurity: a vision grounded in collaboration, in innovation, and in *accountability*.

Vulnerabilities Resulting from Accountability Challenges (continued)

Mitigate Data Exploitation

CBP developed CBP One™ mobile and web application (CBP One™) with the Advance Submission and Appointment Scheduling feature for undocumented noncitizens to schedule an appointment at select POEs. According to CBP, the Appointment functionality was implemented to facilitate safe and orderly travel into the POE, to reduce the administrative burden of manually entering information into systems of record, and to help the process of vetting undocumented noncitizens prior to their arrival, an *efficient* measure to save time and allow better use of its staff. However, when launched, the application experienced crashes, frequent error messages, language barriers, and discrepancies with appointment distribution that could be misused to gain an advantage in seeking an appointment. The difficulties with the appointment scheduling application were attributable, in part, to CBP not performing a technology risk assessment prior to implementing the application, and consequently, its inability to remediate problems before the application was released. Additionally, OIG testing identified vulnerabilities in the CBP One™ mobile application and supporting infrastructure operating systems that could compromise the integrity of sensitive systems and information. CBP One™ data could be susceptible to potential exploitation and expose the confidentiality, integrity, and availability of information to bad actors.

Although CBP acknowledged its shortcomings in planning, CBP is *accountable* for protecting this information by implementing a corrective action plan.[13] The corrective plan, estimated to be completed in October 2024, addresses both the *inefficiencies* of the scheduling application performance and the vulnerabilities of the application to exploitation. (OIG-24-48)

Secure High Value Asset Systems

During our annual *Federal Information Security Modernization Act of 2014* (FISMA) review, we determined the Department's information security rating was effective. However, we identified component systems that were operating without proper authority. Without an Authority to Operate, the Department cannot be assured effective controls are in place to protect sensitive information stored and processed by these systems. These systems included some of the Department's most critical technology, referred to as High Value Asset systems. Components are *accountable* for developing and testing the backup and disaster recovery procedures outlined in the information system contingency plans periodically. As of May 2023, six components had not tested contingency plans for 16 unclassified systems. If a component's contingency plan has not been tested, the plan may fail during a crisis, delaying a return to a fully operational system, and potentially damaging the Department's ability to protect the Nation. The Department plans to achieve 100 percent compliance for "systems operating with an authority to operate" and "updated contingency plans" metrics by September 30, 2024, for High Value Assets and Sensitive but Unclassified Systems and by September 30, 2025, for National Security Systems. (OIG-24-26)

[13] Per DHS Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems* (DHS 4300A)

Adopting a risk-based approach to management can help programs assess and address threats and vulnerabilities to better prioritize resources. However, components did not always use a risk-based approach, impacting its ability to *efficiently* execute operations related to securing critical infrastructure and U.S. borders.

As of September 18, 2024, we made 7 recommendations to the Department and its components in FY2024 regarding *efficiency* challenges it faces when securing cyberspace and critical infrastructure. Of the 7 recommendations, OIG considers 6 open and resolved and 1 closed. Although each Component has a unique mission, conducting periodic risk assessments to identify and rank threats, assess vulnerabilities, and establish a structured process to set risk-based priorities can help better manage resources and tools to execute Department missions *efficiently*.

Vulnerabilities Resulting from Efficiency Challenges

Modernize and Improve Land Ports of Entry

The Infrastructure Investment and Jobs Act (IIJA) appropriated $3.85 billion to modernize and improve land ports of entry (LPOEs) where CBP officers perform immigration and customs functions at the U.S. border with Mexico and Canada. CBP spent $60 million of IIJA procurement, construction, and improvement funding on six contracts in FY 2022 and FY 2023 to modernize and improve CBP-owned LPOEs, but its processes for identifying, validating, prioritizing, and resolving priority, critical, and life safety repairs (critical repairs) did not consistently ensure prompt resolution of these repairs.[14] Although the Department requires components to complete Facility Condition Assessments (FCAs) every 5 years, CBP had not conducted FCAs for over 8 years at 5 of the 40 CBP-owned LPOEs resulting in delays on spending decisions.

The FCAs listed CBP as the entity *accountable* for 102 critical repairs with planned action dates to complete them "as soon as possible" or within 1 year. However, because CBP did not have reliable processes for validating repairs identified as critical in FCAs, it inaccurately categorized 38 of the 102 (37 percent) as critical when they were not critical repairs. Additionally, CBP did not prioritize 25 critical repairs. Instead, contract work included lower priority repairs, such as painting and upgrading light fixtures. Unresolved maintenance and life safety issues can threaten the safety of CBP officers and those entering the Nation from Mexico or Canada through LPOEs. In its spending plan submitted to Congress, CBP allocated $36 million in IIJA procurement, construction, and improvement funding for FY 2024 enhancements at CBP-owned LPOEs. Based on preliminary priorities shared with OIG, CBP identified $28 million in potential investments in FY 2024, including health and life safety repairs, such as heating, ventilation, and air conditioning upgrades as well as water system and public water connection upgrades, to increase its *efficiency* in the process of identifying, validating, prioritizing, and resolving critical repairs at CBP-owned LPOEs. (OIG-24-32)

[14] Throughout OIG-24-32, OIG uses critical repairs to refer to 'critical and life safety' repairs. CBP's Office of Facilities and Assets Management, *Centralized Facility and Personnel Impact Reporting Policy*, August 2023, defines life safety issues as, "Facility disruption impacts which limit occupants a reasonable level of safety during fire and other emergencies."

Vulnerabilities Resulting from Efficiency Challenges

Apply Appropriate Internal Controls to Critical Infrastructure Research and Development Projects

The Science and Technology Directorate (S&T) administers the Department's research, development, testing, and evaluation (R&D) activities, including determining, coordinating, and integrating the long-term R&D needs, capabilities, and activities for all Department components. Under the IIJA, S&T received $157.5 million for critical infrastructure R&D projects. However, S&T did not use a risk-based holistic approach to prioritize department-wide R&D programs and projects nor did it follow established project management principles or its own project management policies and procedures. Additionally, S&T relied on inaccurate and incomplete information to manage its critical infrastructure R&D projects. Without adequate controls in place to plan, manage, and execute its R&D activities consistently, S&T may not be able to *efficiently* support the Department's critical infrastructure R&D needs. The issues we identified also raise concerns as to S&T's ability to *efficiently* plan, manage, and spend the $157.5 million in IIJA funding. (OIG-24-47)

Figure 26: CBP One™ mobile application
Source: DHS Video by Mary Roh/Kyle Fordrung

Streamline the Port of Entry Experience

As noted earlier (Mission 4, Accountability), the CBP One™ application offers an Appointment scheduling feature to allow undocumented noncitizens seeking admission into the United States to submit advance information and schedule appointments at one of eight POEs along the Southwest border. In the previous section, the need for *accountability* on issues with the functionality of the application was highlighted, and in this section, the missed opportunities for *efficiency* with information gathered by the application are highlighted. The Appointment feature streamlines the application process by providing CBP with advance biographic and biometric information intended to reduce the administrative burden of manually entering information into systems of record to conduct pre-arrival noncitizen vetting. CBP may be missing an important opportunity to create *efficiencies* because it does not leverage its CBP One™ application information to identify suspicious trends across the eight Southwest border POEs. Historically, CBP has not received advanced information about noncitizens prior to their arrivals at land POEs. The introduction of CBP One™ changes could improve *efficiencies* by potentially enabling CBP to conduct and supply POE officers with trend analyses to enhance their ability to identify and disrupt national security threats, such as human trafficking. (OIG-24-48)

Mission 5: Build a Resilient Nation and Respond to Incidents

Figure 27: FEMA staff observing damage
Source: 2022-2026 FEMA Strategic Plan

Mission 5 Overview:

The Department is working to create a set of tools and reforms to promote national resilience and adaptation, bolster innovation and partnerships, and look internally at its own roles and responsibilities to decrease the risks posed to our nation by climate change.

Related Strategic Goal: 5

Related Strategic Priority: 11

Components Impacted: CBP, CISA, FEMA, ICE, TSA, Coast Guard, Secret Service, HQ/Support

Recent Mission-Related OIG Reports:

- FEMA Region IV Has a Process to Identify Single Sites Damaged by Multiple Events (OIG-24-34)
- FEMA's Emergency Non-Congregate Sheltering Interim Policy Provided Greater Flexibility for Emergency Sheltering During the COVID-19 Pandemic (OIG-24-38)
- FEMA Did Not Fully Implement the State-Administered Direct Housing Grant Program - (REDACTED) (OIG-24-41)
- FEMA's Inadequate Oversight Led to Delays in Closing Out Declared Disasters (OIG-24-45)

APR Challenges

The Department's recent APRs include numerous challenges and risks its components face relating to their ability to build a resilient nation and respond to incidents, including but not limited to:

- Increasing demand for FEMA to support non-*Robert T. Stafford Disaster Relief and Emergency Assistance Act* Incidents
- Growing severity of disasters and the increasing time it takes for communities to recover — a process that can be further complicated by repeat events in areas already struggling to bounce back
- Lacking authority to direct other partner agencies to streamline processes and programs they own

Figure 28: FEMA staff observes house damaged by tornado
Source: FEMA/Jocelyn Augustino

Recent Progress as Reported in the APR

- FEMA's National Flood Insurance Program responded to more than 48,000 policy holders across Florida, Georgia, South Carolina, North Carolina, and Virginia following Hurricane Ian in September 2022. As of July 2023, the Program paid more than $4.3 billion in claims, and the average payment on closed claims for Hurricane Ian is over $111,000. Across the nation this program insures more than 4.7 million Americans and $1.3 trillion in assets against the financial devastation created by flooding.
- In May 2023, FEMA supported 17 exercises across 10 locations in the United States and Virgin Islands. The exercises included more than 300 participants and provided federal and territorial partners an opportunity to evaluate disaster response plans, address gaps in evacuation and sheltering operations, and discuss long-term recovery considerations. These exercises also enhanced coordination efforts and strengthened stakeholders' understanding of all phases of disaster management.

Communicating timely information to Congress helps ensure Congress is fully aware of program implementation efforts, including related challenges that may impact the Department's ability to fully execute a statutorily mandated program. Although Congress often requires the Department to submit reports and provide briefings on program execution, the Department does not always communicate information to Congress in a timely manner, creating a barrier to *transparency* and impairing Congress' ability to make informed oversight, policy, and funding decisions.

We made one recommendation to FEMA regarding *transparency* challenges it faces when helping to build a more resilient Nation. As of September 18, 2024, OIG considers this recommendation open and resolved.

Vulnerabilities Resulting from Transparency Challenges

Communicate Timely Information to Congress

Section 1211(a) of the *Disaster Recovery Reform Act of 2018* (DRRA)[15] authorizes FEMA to issue grants to state, territorial, and tribal (STT) governments to administer direct housing assistance on FEMA's behalf. DRRA required FEMA to submit a report to Congress on a potential incentive structure for awards to encourage STT participation in the program by October 2019. Additionally, the House Committee on Appropriations directed FEMA to provide quarterly briefings to Congress on its DRRA implementation efforts. However, FEMA did not submit the required report to Congress until 3 years after the mandated date and has not provided required quarterly briefings to the Appropriations Committees. As a result of this barrier to *transparency*, Congress is not fully aware of FEMA's efforts to implement the State-Administered Direct Housing Grant Program, including challenges and actions taken, ongoing, or planned to address those challenges, impairing its ability to make informed oversight, policy, and funding decisions. (OIG-24-41)

Figure 29: Wildfires destroyed a neighborhood in California
Source: FEMA Multimedia

Figure 30: FEMA opened a disaster recovery center for survivors affected by the Maui Wildfires
Source: DHS, Photo by Dominick Del Vecchio

[15] *Disaster Recovery Reform Act of 2018*, Division D of Pub. L. No. 115–254.

FEMA is *accountable* for ensuring proper payment is made to the right recipient for the right amount. Between 2019 and 2022, we issued four OIG audit reports that, collectively, identified more than $7 billion in improper payments and, potentially, fraudulent payments. We attributed this to FEMA's refusal to institute sufficient controls to mitigate the risk of relying on self-certification of applicant eligibility. We remain at an impasse with FEMA on nine recommendations requesting FEMA address vulnerabilities and internal control deficiencies to reduce the risk of potentially fraudulent payments. In August 2024, the Inspector General referred the nine recommendations to the Department's Deputy Under Secretary for Management, who serves as the Department's Audit Follow-up and Resolution Official, for a final resolution decision. While we do agree a vast majority of disaster assistance applicants have a legitimate need for the assistance they seek, there are also individuals who falsely claim benefits for their own personal gain. It is FEMA's fiduciary responsibility to implement adequate controls to help deter attempts to improperly acquire government funds through fraudulent activity. Recognizing the importance of expediency in FEMA's mission, we do not recommend verification of all applicant information. Rather, we are recommending FEMA, as the *accountable* agency, implement preventative controls to reduce the significant risk of improper payments and potential fraud clearly demonstrated through these four audits.

GAO projects the frequency and intensity of natural disasters to increase in the future. These events, along with biological and manmade incidents highlight challenges the Department will continue to face in responding to disasters. GAO's *A Framework for Managing Fraud Risks in Federal Programs* (GAO-15-593SP) identifies leading practices for managing fraud risks and organizing them into a Fraud Risk Management Framework. The Department can use this framework to aid in combatting fraud and preserving program integrity.

GAO also published *A Framework for Managing Improper Payments in Emergency Assistance Programs* (GAO-23-105876) to combat substantial shortcomings it identified in agencies' internal controls and fraud risk management practices. In this framework, GAO notes that some significant improper payments are the result of fraud and provides five principles to help federal program managers mitigate improper payments in emergency assistance programs.

Figure 31: Tornado Damage in Mississippi
Source: DHS, Photo by Tara Molle

Holding Bad Actors Accountable

Combating Natural Disaster-Related Fraud

FEMA is authorized to provide Public Assistance funds to assist communities responding to and recovering from major disasters or emergencies declared by the President. STT entities can hire contractors to assist with disaster recovery efforts. However, in some cases, contractors submit fraudulent requests on behalf of the STT or misrepresent funding eligibility. For example, in FY 2024, an architecture and engineering firm based in Dallas agreed to pay $11.8 million to resolve allegations that it violated the *False Claims Act* by knowingly submitting false claims to FEMA for the replacement of certain educational facilities in Louisiana damaged by Hurricane Katrina. In another case, an individual was ordered to pay almost $600,000 in restitution to a local government for misrepresenting the amount of Public Assistance grant funds the town was eligible for.

Similarly, FEMA provides Individual Assistance to help disaster survivors recover. In FY 2024, a woman was charged with defrauding FEMA of over $1.5 million in disaster benefits. The indictment alleges the woman advertised over social media that she could assist others in applying for FEMA benefits. She then submitted fraudulent documents on behalf of dozens of her social media recruits in exchange for collecting half of the payout for herself. If convicted, she faces a maximum possible sentence of 960 years of imprisonment.[16]

Fighting COVID-19 Relief Fraud

In response to widespread fraud involving many COVID-19 relief programs, DOJ established the COVID-19 Fraud Enforcement Task Force. Key interagency partners include the Department's components and OIG. Over the last 3 years, the task force has charged more than 3,500 defendants, seized or forfeited over $1.4 billion in stolen COVID-19 relief funds, and filed more than 400 civil lawsuits resulting in court judgments and settlements. During FY 2024, several individuals were indicted or pled guilty to fraud in connection with COVID-19 relief funding, collectively obtaining over $2.3 million through false and fraudulent loan applications.[17]

---

[16] AECOM to Pay $11.8 Million to Resolve False Claims Act Allegations in Connection with Hurricane Disaster Relief
East Feliciana Man Sentenced for Wire Fraud
Montgomery County Woman Charged for Defrauding FEMA of Over $1.5 Million of Hurricane Ida Disaster Benefits

[17] U.S. Attorney's Eastern Washington COVID-19 Strike Force Announces Indictment of Spokane Valley Couple in Connection with Fraudulent COVID Relief Loan
Two Men Plead Guilty to Defrauding COVID-19 Pandemic Relief Programs
Houstonian charged with filing over $500,000 in fraudulent disaster relief loans/ Houstonian admits to filing over $500,000 in fraudulent disaster relief loans
Houston Woman Pleads Guilty to Covid Fraud Scheme
COVID-19 Fraud Enforcement Task Force Releases 2024 Report
Richland Man Indicted for Stealing More than $339,000 in COVID-19 Unemployment Insurance Fraud Scheme
Mead Man Pleads Guilty to Bank Fraud for Defrauding COVID-19 Relief Programs
United States Attorney's Eastern Washington COVID-19 Strike Force Announces Additional Indictments, Arrests

Public health emergencies and natural disasters often coincide with implementation of new federal programs or swift expansion of existing programs and can stress FEMA's ability to provide *efficient* and effective program oversight and fund management, such as ensuring funds are spent timely and in accordance with applicable laws and guidance. *Efficient* grant implementation and closeout processes ensure *accountability* for grant dollars awarded, *transparency* in decision making, and compliance with Federal requirements.

We made five recommendations to FEMA regarding *efficiency* challenges it faces when implementing and supporting disaster relief efforts. As of September 18, 2024, OIG considers one recommendation open and resolved, three recommendations open and unresolved, and one recommendation closed.

Vulnerabilities Resulting from Efficiency Challenges

Empower State, Territorial, and Tribal Governments

As noted earlier in this report (Mission 5, Transparency), Section 1211(a) of the DRRA authorized FEMA to provide grants to STT governments to administer direct housing assistance on FEMA's behalf. However, FEMA did not implement the State-Administered Direct Housing Grant Program fully, impacting its ability to provide grants *efficiently.* Although the DRRA required the program's final regulations to be issued by October 2020, as of March 2024, FEMA had not yet included these regulations in the Office of Management and Budget's (OMB) *Unified Agenda of Federal Regulatory and Deregulatory Actions*. Additionally, during the program's 2-year pilot period, FEMA issued one narrowly focused grant award that did not authorize the recipient state to administer direct housing on FEMA's behalf. Due to FEMA's *inefficient* implementation of the State-Administered Direct Housing Grant Program, STT governments missed opportunities to play a greater role in identifying and implementing innovative, cost-effective, and locally tailored disaster housing solutions.

While FEMA concurred with the four recommendations made to improve its implementation of the State-Administered Direct Housing Grant Program, two recommendations remain open and unresolved. FEMA submitted planned corrective actions that are responsive to the recommendations without an estimated completion date. (OIG-24-41)

Closeout Grants Timely

We recently reviewed 79 disaster declarations and identified 26 programs with nearly $9.4 million in unliquidated funds that remained open beyond their approved periods of performance. Additionally, FEMA extended 41 program periods of performance or closeout liquidation periods without required detailed document justifications. The programs represent more than $7 billion in unliquidated funds. The extensions delayed project closures by up to 16 years. Due to *inefficient* oversight and weak policies, billions of dollars of unliquidated funds remain obligated to state, territorial, tribal, or local governments and unavailable for use in providing relief in connection with current disasters.

We made two recommendations to improve FEMA's closeout of declared disasters; one recommendation remains open and unresolved, as its corrective action plan does not fully address the recommendation. Per Title 44 of the Code of Federal Regulations § 13.50(a), FEMA should include all expired and open programs in its planned review and take appropriate closeout and deobligation actions. (OIG-24-45)

Mission 6: Combat Crimes of Exploitation and Protect Victims

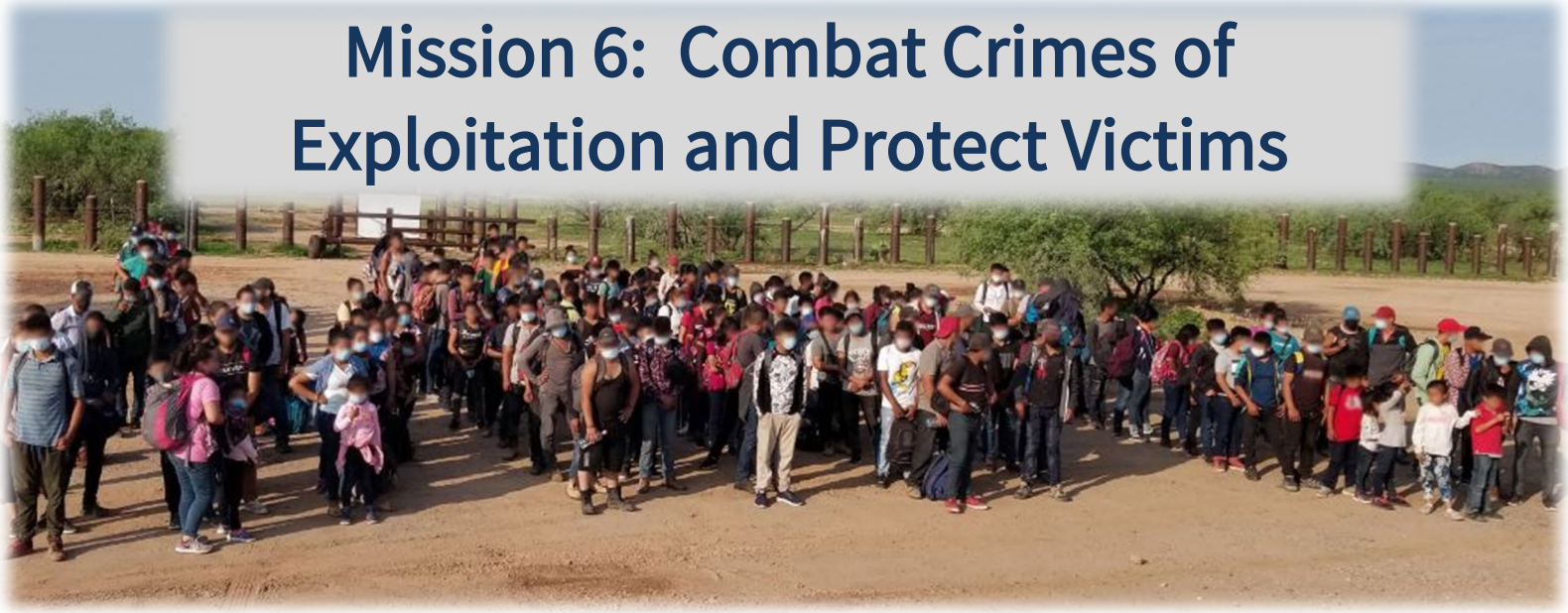


Figure 32: Unaccompanied migrant children encountered by U.S. Border Patrol near San Miguel, Arizona
Source: CBP Photo Library

Mission 6 Overview:

The Department is enhancing its efforts to combat crimes of exploitation — child sexual exploitation and abuse (CSEA), human trafficking, and labor exploitation—and protect victims.

Related Strategic Goal: 1

Related Strategic Priority: 12

Components Impacted:
CBP, ICE, Secret Service, HQ/Support

Recent Mission-Related OIG Reports

Management Alert - ICE Cannot Monitor All Unaccompanied Migrant Children Released from DHS and U.S. Department of Health and Human Services' Custody (OIG-24-46)

APR Challenges

The Department's recent APRs include challenges and risks its components face relating to their ability to combat crimes of exploitation and protect victims, including but not limited to:

- Lack of public awareness creating opportunity for the crimes to flourish
- Workers afraid to report violations of law by exploitative employers or to cooperate in employment and labor standards investigations fearing removal or other immigration-related retaliation from an abusive employer

Recent Progress as Reported in the APR

- In FY 2023, HSI rescued or assisted 2,926 victims as a result of investigations, including 731 human trafficking victims and 2,195 victims of child exploitation. This is up 53.7 percent from FY 2022 when HSI reported they rescued or assisted 1,904 victims. HSI achieved these results by integrating a victim-centered approach to place equal value on victim identification and stabilization and target deterrence, investigation, and prosecution.
- The Department announced process enhancements to support labor and employment agency investigations by streamlining the handling of workers' requests for deferred action.

The Department added "combat crimes of exploitation and protect victims" as a new Homeland Security Mission in the FY 2023–2025 APR, reflecting the importance of investigating, apprehending, and prosecuting offenders and identifying, protecting, and supporting victims of trafficking and other crimes of exploitation. The Department relies on strong partnerships with stakeholders, including robust coordination and information sharing, adequate oversight, and sufficient resources to *sustain* its mission to detect, apprehend, and disrupt perpetrators and to protect individuals at higher risk for trafficking, exploitation, and forced labor.

In FY 2024, we made two recommendations to ICE regarding *sustainability* challenges it faces when executing operations to protect individuals from trafficking, exploitation, and forced labor. As of September 18, 2024, OIG considers one recommendation open and resolved and one recommendation open and unresolved.

Vulnerabilities Resulting from Sustainability Challenges

Protect Individuals from Trafficking, Exploitation, and Forced Labor

ICE ERO protects the homeland by arresting and removing individuals who undermine the safety of our communities and the integrity of our immigration laws. ICE ERO is responsible for managing and monitoring the cases of unaccompanied migrant children (UC) in immigration proceedings.[18] When the Department apprehends UCs, ICE generally transfers them to the U.S. Department of Health and Human Services' (HHS) for care and custody while awaiting immigration proceedings.

ICE retains responsibility for managing its immigration cases, including serving UCs an NTA for immigration court. Between FYs 2019 and 2023, ICE transferred more than 448,000 UCs to HHS. However, more than 32,000 UCs failed to appear for their immigration hearings. ICE did not always inform HHS when UCs failed to appear in immigration court after release from HHS' custody. Further, ICE did not serve an NTA on all UCs, after release from HHS custody, who warranted placement in removal proceedings under 8 U.S. Code Section 1229(a). As of May 2024, ICE has not served NTAs on more than 291,000 UCs who do not yet have an immigration court date.

Based on our audit work and according to ICE officials, UCs who did not appear in immigration court are considered more at risk for trafficking, exploitation, or forced labor. By not issuing NTAs to all UCs, ICE limits its chances of having contact with UCs when HHS releases them from custody, which reduces the Department's ability to *sustain* its mission to protect these individuals.

ICE provided a corrective action plan to evaluate options to automate internal data sharing between ICE's Office of Principal Legal Advisor, ERO systems, and other stakeholders. However, until ICE confirms when it will implement an automated process for sharing information, the recommendation will remain open and unresolved. (OIG-24-46)

[18] A UC is a child who has no lawful immigration status in the United States, has not attained 18 years of age, and has no parent or legal guardian in the United States to provide care and physical custody.

Countering Child Exploitation

Educate and Raise Public Awareness

In 2023, the National Center for Missing and Exploited Children received over 36 million cyber-tips reporting online CSEA. In April 2024, the Department launched *Know2Protect,* the U.S. Government's first national public awareness campaign to educate and empower children, teens, trusted adults, and policymakers to prevent and combat online CSEA; explain how to report online enticement and victimization; and offer response and support resources for victims and survivors The Department has partnered with professional sports leagues and organizations, including the National Football League, the National Hockey League, and Major League Baseball; technology and gaming companies, such as Roblox, Google, and Meta; civil organizations; law enforcement organizations; and many more. Additionally, the Department is working with other partners around the globe. *Know2Protect* demonstrates a commitment to *sustain* combatting crimes of exploitation and protecting victims. The following link provides more information about the campaign, resources available for download, and how to take action: www.know2protect.gov.

know2protect™
Together We Can Stop Online Child Exploitation

Detect, Apprehend, and Disrupt Perpetrators

In May 2024, a former law enforcement officer was found guilty of attempted online enticement of a minor. Evidence established that in July 2022, a 49-year-old ICE officer replied to a Craigslist ad as part of an undercover law enforcement operation meant to identify individuals interested in and willing to meet with minors for sex. Over the next three days, the officer texted with 13-year-old "Rebecca," regarding her age, the rates she charges for sex acts, and the man's employment as a "cop" and arranged to meet at a hotel for sex.

On July 26, 2022, the officer arrived at the hotel in Othello, Washington to meet "Rebecca," but instead was contacted by law enforcement and arrested. Following a search, officers located the man's ICE badge and over $4,000 cash.

The Federal Bureau of Investigation, DHS OIG, and the Othello Police Department investigated the case. The case was brought as part of DOJ's Project Safe Childhood program, launched in May 2006, as a nationwide initiative to combat the growing epidemic of CSEA. Project Safe Childhood marshals federal, state, and local resources to better locate, apprehend, and prosecute individuals who exploit children via the Internet, as well as to identify and rescue victims.[19] This law enforcement partnership, coordination, and information sharing contributes to increased *sustainability* to protect children from exploitation. The following link provides more information about Project Safe Childhood: www.projectsafechildhood.gov.

[19] Former Law Enforcement Officer Found Guilty of Attempted Online Enticement of a Minor

Mission "E": Enable Mission Success by Strengthening the Enterprise

Mission "E" Overview:

DHS will continue to build its capacity to conduct its critical missions and anticipate the challenges to come. Essential to this is better understanding and protecting against threats from emerging technologies, as well as developing our most important assets: people, physical assets, data, and technology.

Related Strategic Goal: 6

Related Strategic Priority: All

Components Impacted: All

Recent Mission-Related OIG Reports:

- CBP Did Not Fully Implement the Requirements of the Synthetic Opioid Exposure Prevention and Training Act (OIG-24-01)
- Major Management and Performance Challenges Facing the Department of Homeland Security (MMPC) (OIG-24-05)
- Independent Auditors' Report on the Department of Homeland Security's Consolidated Financial Statements for FYs 2023 and 2022 and Internal Control over Financial Reporting (OIG-24-06)
- Coast Guard National Maritime Center's Oversight of Merchant Mariner Training and Examinations (OIG-24-08)
- Review of U.S. Immigration and Customs Enforcement's Fiscal Year 2023 Detailed Accounting Report for Drug Control Funds (OIG-24-12)
- Review of Federal Law Enforcement Training Centers' Fiscal Year 2023 Detailed Accounting Report for Drug Control Funds (OIG-24-13)
- Review of U.S. Customs and Border Protection's Fiscal Year 2023 Drug Control Budget Formulation Compliance Report (OIG-24-14)
- Review of U.S. Immigration and Customs Enforcement's Fiscal Year 2023 Drug Control Budget Formulation Compliance Report (OIG-24-15)
- Review of Federal Law Enforcement Training Centers' Fiscal Year 2023 Drug Control Budget Formulation Compliance Report (OIG-24-17)
- Review of U.S. Customs and Border Protection's Fiscal Year 2023 Detailed Accounting Report for Drug Control Funds (OIG-24-18)
- DHS Grants and Contracts Awarded by Any Means Other Than Full and Open Competition During Fiscal Year 2023 (OIG-24-19)
- DHS' Fiscal Year 2023 Compliance with the Payment Integrity Information Act of 2019 (OIG-24-25)
- DHS Has Made Progress in Implementing an Enhanced Personnel Vetting Program (OIG-24-43)
- CBP's Office of Field Operations Used Overtime in Accordance with Policies and Procedures (OIG-24-54)
- Audit of Office of Intelligence and Analysis Contract and Funding Management Processes (OIG-24-57)
- CBP Needs to Improve Its Management of the Facility Condition Assessment Program (OIG-24-58)

APR Challenges

As identified by GAO, the Department's recent APRs include numerous government-wide challenges and risks its components face relating to their ability to champion the DHS workforce and strengthen the Department, including but not limited to:

- Addressing national challenges requires a high-performing federal workforce able to safeguard the homeland against national threats and emergencies. However, current budget and long-term fiscal pressures, declining levels of federal employee satisfaction, the changing nature of federal work, and a potential increase of employee retirements could produce gaps in leadership and institutional knowledge. Mission-critical skills gaps impede federal agencies from cost-effectively serving the public and achieving results
- Managing Federal real property, including excess and underutilized property, data reliability, and facility security
- Managing Information Technology (IT) acquisitions and operations due to overly broad scopes, delivery of functionality several years after initiation, and ineffective executive-level IT governance and oversight in general
- Processing personnel security clearances timely and measuring investigation quality

Recent Progress as Reported in the APR

S&T installed, tested, and fixed multi-energy drive-through systems to enable CBP to non-intrusively inspect cargo at some POEs. The systems use low energies to safely scan an occupied cab and have higher penetrating x-rays to scan cargo. This is the first pre-primary cargo inspection system for CBP, and it has increased the daily average of cargo scanned from 24 percent to over 80 percent.

Figure 33: Multi-energy portal demonstration
Source: Department of Homeland Security Annual Performance Report for Fiscal Years 2023-2025

Inspectors General (IG) conduct independent oversight to prevent and detect fraud, waste, and abuse in government programs and operations. Recommendations in IG audits, evaluations, and inspections have resulted in program *efficiencies*, including improved delivery of government services to citizens. Likewise, IG investigations of individuals who defy laws at the expense of taxpayers, contractors who misrepresent goods and services for financial gain, and others who defraud the government have led to the return of billions of taxpayer dollars.

OIG leverages data analytics to support and guide audits, inspections, evaluations, and investigations. The Inspector General Act of 1978 (IG Act), as amended, grants OIG authority to receive full access to all records and materials available to the Department, with some exceptions. Allowing OIG access to systems and information necessary to achieve its oversight mission facilitates *transparency,* aligns with the Department's Data Mission, and contributes to OIG's ability to perform effective oversight and report on program operations and challenges to stakeholders, such as Congress. A key component of data *transparency* in the context of OIG oversight is direct access to component systems and data.

Vulnerabilities Resulting from Transparency Challenges

System Access

The Foundations for *Evidence-Based Policymaking Act of 2018*, also referred to as the Evidence Act of 2018 (PL 115-435), assigns the Department responsibility to promote better use and management of data and evidence consistent with the GPRA Modernization Act of 2010 and OMB Circular A-11, Part 6. The Evidence Act of 2018 mandates that agency Chief Data Officers implement policies that ensure stakeholders participate in an "integrated and direct connection to data and evidence needs."

To meet requirements of the Evidence Act of 2018 and to promote better use and management of data, the Department implemented an Evidence-Based Data Strategy (EDS). The Department's Data Mission within the EDS is to "provide *transparent* access to valid, reliable, and interoperable data that supports the Department's mission and promotes the public good." Key aspects of enabling mission success by strengthening the enterprise include the promotion of *transparency* before the American people and advancement of risk-based decision making. A lack of *transparent* data inhibits OIG's (and thus the public's) ability to fully understand and address problematic or *inefficient* practices.

In FY 2024, the Department fully cooperated with requests for access to its systems that were the subject of OIG assessments of the Department's cybersecurity posture. As a result of this cooperation, OIG conducted cybersecurity testing of 11 FISMA systems across 6 components, identifying weaknesses in the areas of patching and configuration management, flaw remediation, and access controls, and the Department has addressed critical security issues of which it was previously unaware.

However, the Department has not fully cooperated with the OIG's efforts to collect information to perform comprehensive risk assessments to protect the department against fraud, waste, and abuse. To ensure OIG's ability to conduct timely, thorough analytic reviews based on transactional and authoritative data, it is OIG's policy to request direct, read-only access to Department data systems for all engagements. Although the IG Act allows Inspectors General unrestricted access to

records, OIG's requests for access have been met with resistance, and in the majority of cases, denials by the Department. In FY 2024, OIG submitted 17 system access requests to the Department or its components. The Department approved only four of the 17 system access requests; the remaining 13 (76.5 percent) requests were denied. In lieu of access, the Department generally provided simple extracts of the narrowest set of data possible, based on its own interpretation of the scope of the ongoing engagement.

The Department often justifies access denials on the grounds of data sensitivity and the inability to partition specific data relevant to OIG engagements from the rest of the data in the system. OIG recognizes the sensitivity of the data it requests, stores, and analyzes, and adheres to established Department privacy, records management, and cybersecurity policies. OIG employs additional controls to safeguard the information, going beyond the Department mandated controls.

Direct, read-only system access enhances OIG's ability to make data-driven decisions concerning the most impactful oversight work it should be conducting. The use of advanced data analytics,[20] such as data mining, descriptive statistics, and predictive modeling, on comprehensive Department data would enable OIG to identify issues more effectively, such as potential fraud or improper payments, evaluate weaknesses in underlying system controls or processes, and make recommendations to protect the Department against future fraud, waste, and abuse. Direct system access would also ensure the OIG is reviewing and working with original data and not data altered through an extraction and transfer process. This would contribute to data reliability and ensure the OIG is using independently verified data for findings and conclusions in audit, inspection, and evaluation reports.

Through detailed analyses in recent projects, OIG data analysts determined that the Component provided incomplete sets of data that did not meet the requirements of OIG's requests. The Component provided new sets of data when requested, but this resulted in delays to project timelines and ultimately prevented the OIG from conducting comprehensive data analytics to assess and evaluate risk.

Additionally, receiving direct system access reduces resources the Department needs to expend on data requests and contributes to a more *efficient* process overall. System access allows OIG to analyze relevant data directly in the system and only extract the information needed for a given engagement. This reduces the burden on Components to provide complete and reliable large-scale data extracts and refreshes. Direct systems access contributes to the OIG's independence and assurance to the public and Congress of OIG's independence and objectivity.

This *transparency* barrier impairs OIG's ability to achieve its mission. The denial of full and independent access to agency records and information may adversely impact Department program *sustainability* and *efficiency*, and severely damage OIG's critical oversight function. Without unfettered oversight, citizens, Congress, and other stakeholders are unable to hold the Department *accountable* for actions and decisions regarding performance, deficiencies, services, and cost.

[20] Advanced data analytics is the process of analyzing raw data to identify patterns, trends, anomalies, and correlations to draw conclusions about the information.

One of the Department's fundamental responsibilities is to act as an effective steward of taxpayer funds. The Department is *accountable* for adhering to relevant laws and regulations and promoting *efficient* operations.

As of September 18, 2024, we made 36 recommendations to the Department and its components in FY 2024 regarding *accountability* and *efficiency* challenges that impact its ability to support operations and complete missions at an enterprise-level. Of the 36 recommendations, OIG considers 21 open and resolved and 15 closed. The Department can ensure smoother and more *efficient* operations by enforcing *accountability* and designing internal control systems to safeguard its programs and finances from potential issues such as fraud, waste, and abuse, and unauthorized access to sensitive data, and to protect staff from physical harm.

Vulnerabilities Resulting from Accountability and Efficiency Challenges

Protect the Workforce

In FY 2022, CBP seized more than 16,000 pounds of fentanyl. In 2020, the *Synthetic Opioid Exposure Prevention and Training Act* was enacted and aimed to reduce the risk of injury and death to CBP personnel and canines from accidental exposure to synthetic opioids, such as fentanyl. The Act included several requirements for CBP to protect its workforce. However, CBP did not fully implement the requirements. Specifically, CBP did not issue component-wide policy to handle potential synthetic opioids safely, make the opioid inhibitor naloxone available and readily accessible to all personnel at risk of opioid exposures, or require initial and recurrent training for all personnel at risk of opioid exposure. CBP relies on individual subcomponents to implement and manage their own opioid handling and naloxone programs without central oversight leading to less *efficient* operations. Enhanced oversight and a formalized, consistent, and *efficient* component-wide policy could recognize greater *sustainability* to protect its workforce. (OIG-24-01)

Figure 34: Lethal Dose of Fentanyl
Source: CBP Graphic

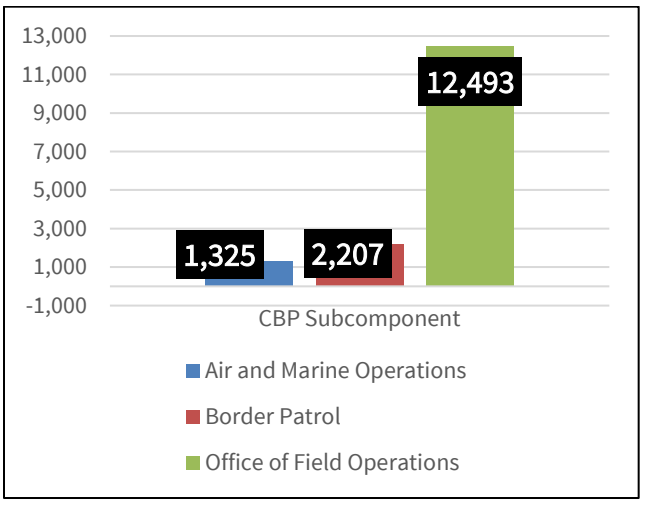


Figure 35: CBP's FY 2022 Fentanyl Seizure in Pounds
Source: OIG-24-01

Vulnerabilities Resulting from Accountability and Efficiency Challenges (continued)

Improve Internal Controls Over Financial Reporting

KPMG LLP, an independent public accounting firm, issued an adverse opinion on the Department's internal controls over financial reporting as of September 30, 2023. The report identifies six significant deficiencies in internal controls, five of which KPMG LLP considers material weaknesses:

- *Information Technology Controls and Information Systems* - increased risk of unauthorized access to information systems or data and inappropriate disclosures of sensitive data.
- *Financial Reporting* - possibility the Department will not prevent, detect, or correct material misstatements on a timely basis.
- *Insurance Liabilities* - possibility the Department will not prevent, detect, or correct material misstatements in the flood insurance liabilities and future funded costs on a timely basis.
- *Receipt of Goods and Services* - possibility the Department will not prevent, detect, or correct material misstatements of gross costs and new obligations and upward adjustments on a timely basis.
- *Seized and Forfeited Property Other than Monetary Instruments* - possibility the Department will not prevent, detect, or correct material misstatements in the seized and forfeited property note on a timely basis.
- *Grants Management* - possibility of inaccurate or unauthorized expense reporting by grant recipients and ineffective monitoring of open and closed grants.

Correcting these deficiencies leads to the increased *accountability* to promote *efficient* operations. (OIG-24-06)

Mitigate Fraud, Waste, and Abuse

The *Payment Integrity Information Act of 2019* (PIIA) requires agencies to identify and review all programs and activities that may be susceptible to significant improper payments. The Department must meet all 10 PIIA requirements to be compliant. Although it adhered to nine of the 10 requirements, the Department did not publish improper and unknown payment estimates for FEMA's Public Assistance Validate As You Go program. Noncompliance hinders the Department's *accountability* requirement to properly test programs highly susceptible to fraud, waste, and abuse. Improper and unknown payments are more likely to go undetected, impacting programmatic *efficiencies*. Additionally, if the Department remains noncompliant with the PIIA, it will be subject to additional OMB reporting requirements, which will hamper *efficiency* further. (OIG-24-25)

Protect Civil Liberties

During FY 2024, several CBP officers were held *accountable* when they were convicted in federal courts of deprivation of the right to be free from an unreasonable use of force against individuals coming into the United States from Mexico[21]. As a result of unlawful use of force, the victims suffered bodily injury. Two of the three offending CBP officers falsely reported occurrences following these incidents; they face up to 10 years in prison for deprivation of rights and up to 20 years in prison for falsifying records. The third CBP officer faces a maximum of 1 year in prison and a $100,000 fine. "Federal law enforcement officers are expected to treat the public with courtesy and respect," says DHS Inspector General Joseph V. Cuffari. "Those who fail to adhere to this standard will be held accountable."

[21] Customs and Border Protection Officer Admits Using Unreasonable Force and Agrees to Resign from Law Enforcement
Federal Jury Convicts U.S. Customs and Border Protection Officer of Depriving a U.S. Citizen of Rights
Federal Judge Finds CBP Officer Guilty of Using Excessive Force

Appendix A – Crosswalk between the Department's Strategic Goals & Objectives and Its Missions & Objectives

DHS Strategic Goals and Objectives[22]	DHS Missions and Objective[23]
Goal 1: Counter Terrorism and Homeland Security Threats	**Mission 1: Counter Terrorism and Prevent Threats**
Objective 1.1: Collect, Analyze, and Share Actionable Intelligence	Objective 1.1: Collect, Analyze, and Share Actionable Intelligence and Information
Objective 1.2: Detect and Disrupt Threats	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
Objective 1.3: Protect Designated Leadership, Events, and Soft Targets	Objective 1.3: Protect Leaders and Designated Individuals, Facilities, and Events
Objective 1.4: Counter Weapons of Mass Destruction and Emerging Threats	Objective 1.4: Identify and Counter Emerging and Chemical, Biological, Radiological, and Nuclear Threats
Goal 2: Secure U.S. Borders and Approaches	**Mission 2: Secure and Manage Our Borders**
Objective 2.1: Secure and Manage Air, Land, and Maritime Borders	Objective 2.1: Secure and Manage Air, Land, and Maritime Borders
Objective 2.2: Extend the Reach of U.S. Border Security	Objective 2.2: Expedite Lawful Trade and Travel
The Department split **Goal 2** between **Missions 2 & 3**	Objective 2.3: Counter Transnational Criminal Organizations and Other Illicit Actions
	Mission 3: Administer the Nation's Immigration System
Objective 2.3: Enforce U.S. Immigration Laws	Objective 3.1: Administer the Immigration System
Objective 2.4: Administer Immigration Benefits to Advance the Security and Prosperity of the Nation	Objective 3.2: Enforce U.S. Immigration Laws

[22] *The DHS Strategic Plan, Fiscal Years 2020-2024*
[23] *Department of Homeland Security Annual Performance Report for Fiscal Years 2023-2025*

DHS Strategic Goals and Objectives[22]	DHS Missions and Objective[23]
Goal 3: Secure Cyberspace and Critical Infrastructure	**Mission 4: Secure Cyberspace and Critical Infrastructure**
Objective 3.1: Secure Federal Civilian Networks	Objective 4.1: Support the Cybersecurity of Federal Civilian Networks
Objective 3.2: Strengthen the Security and Resilience of Critical Infrastructure	Objective 4.2: Strengthen the Security and Resilience of Critical Infrastructure
Objective 3.3: Assess and Counter Evolving Cybersecurity Risks	Objective 4.3: Assess and Counter Evolving Cyber and Emerging Technology Risks
Objective 3.4: Combat Cybercrime	Objective 4.4: Combat Cybercrime
Goal 4: Preserve and Uphold the Nation's Prosperity and Economic Security	The Department absorbed **Goal 4** into other Mission areas.
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	**Mission 5: Build a Resilient Nation and Respond to Incidents**
Objective 5.1: Build a National Culture of Preparedness	Objective 5.1: Coordinate Federal Response to Incidents
Objective 5.2: Respond During Incidents	Objective 5.2: Strengthen National Resilience
Objective 5.3: Support Outcome-Drive Community Recovery	Objective 5.3: Support Equitable Community Recovery
Objective 5.4: Train and Exercise First Responders	Objective 5.4: Enhance Training and Readiness of First Responders
The Department expanded **Objective 1.2** into **Mission 6**.	**Mission 6: Combat Crimes of Exploitation and Protect Victims**
	Objective 6.1: Enhance Prevention through Public Education and Training
	Objective 6.2: Identify, Protect, and Support Victims
	Objective 6.3: Detect, Apprehend, and Disrupt Perpetrators

DHS Strategic Goals and Objectives[22]	DHS Missions and Objective[23]
Goal 6: Champion the DHS Workforce and Strengthen the Department	**Enable Mission Success by Strengthening the Enterprise**
Objective 6.1: Strengthen Departmental Governance and Management	Objective E.1: Mature Organization Governance
Objective 6.2: Develop and Maintain a High Performing Workforce	Objective E.2: Champion the Workforce
Objective 6.3: Optimize Support to Mission Operations	Objective E.3: Harness Data and Technology to Advance Mission Delivery

Appendix B – The Department's Strategic Goals[24]

Goal 1: Counter Terrorism and Homeland Security Threats	One of the Department's top priorities is to resolutely protect Americans from terrorism and other homeland security threats by preventing nation-states and their proxies, transnational criminal organizations, and groups or individuals from engaging in terrorist or criminal acts that threaten the Homeland. In recent years, terrorists and criminals have increasingly adopted new techniques and advanced tactics in an effort to circumvent homeland security and threaten the safety, security, and prosperity of the American public and our allies. The rapidly evolving threat environment demands a proactive response by DHS and its partners to identify, detect, and prevent attacks against the United States.
Goal 2: Secure U.S. Borders and Approaches	Secure borders are essential to our national sovereignty. Managing the flow of people and goods into the United States is critical to maintaining our national security. Illegal aliens[25] compromised the security of our Nation by illegally entering the United States or overstaying their authorized period of admission. Illegal aliens who enter the United States and those who overstay their visas disregard our national sovereignty, threaten our national security, compromise our public safety, exploit our social welfare programs, and ignore lawful immigration processes. As a result, DHS is implementing a comprehensive border security approach to secure and maintain our borders, prevent, and intercept foreign threats so they do not reach U.S. soil, enforce immigration laws throughout the United States, and properly administer immigration benefits.

[24] *The DHS Strategic Plan, Fiscal Years 2020-2024*

[25] The Department's 2020-2024 Strategic Plan uses the term "illegal alien; however, the current preferred term is "undocumented citizens."

Goal 3: Secure Cyberspace and Critical Infrastructure	Increased connectivity of people and devices to the Internet and to each other has created an ever-expanding attack surface that extends throughout the world and into almost every American home. As a result, cyberspace has become the most active threat domain in the world and the most dynamic threat to the Homeland. Nation-states and their proxies, transnational criminal organizations, and cyber criminals use sophisticated and malicious tactics to undermine critical infrastructure, steal intellectual property and innovation, engage in espionage, and threaten our democratic institutions. By 2021, cybercrime damages are likely to exceed $6 trillion per year. Moreover, the interconnectivity of critical infrastructure systems raises the possibility of cyber attacks that cause devastating kinetic and non-kinetic effects. As innovation, hyper-connectivity, and digital dependencies all outpace cybersecurity defenses, the warning signs are all present for a potential "cyber 9/11" on the horizon. Critical infrastructure provides the services that are the backbone of our national and economic security and the health and well-being of all Americans. Cybersecurity threats to critical infrastructure are one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. In particular, nation-states are targeting critical infrastructure to collect information and gain access to industrial control systems in the energy, nuclear, water, aviation, and critical manufacturing sectors. Additionally, sophisticated nation-state attacks against government and private-sector organizations, critical infrastructure providers, and Internet service providers support espionage, extract intellectual property, maintain persistent access on networks, and potentially lay a foundation for future offensive operations. Meanwhile, the heightened threat from physical terrorism and violent crime remains, increasingly local and often aimed at places like malls and theaters, stadiums, and schools. Moreover, the advent of hybrid attacks, where adversaries use both physical and electronic means to inflict and compound harm, renders the threat landscape more challenging than ever. DHS works to protect critical infrastructure against these and other threats of today, while also focusing on tomorrow's emerging risks. As the national lead for protecting and enhancing the security and resilience of the Nation's civilian cyber systems and critical infrastructure, DHS is adopting a risk management approach that reduces systemic vulnerabilities across the Nation to collectively increase our defensive posture against malicious cyber activity. Simultaneously, DHS law enforcement investigations are focused on prosecuting cyber criminals, disrupting and dismantling criminal organizations, and deterring future malicious activity. These complementary initiatives address both threats and vulnerabilities across the threat spectrum.

Goal 4: Preserve and Uphold the Nation's Prosperity and Economic Security	America's prosperity and economic security are integral to DHS's homeland security operations, which affect international trade, national transportation systems, maritime activities and resources, and financial systems. In many ways, these pre-DHS legacy functions are just as much a part of DHS's culture as its counterterrorism, border security, immigration, cybersecurity, and emergency management responsibilities. Similarly, many DHS activities that advance this important element of homeland security affect the American public just as much as DHS's core security functions. Accordingly, DHS continues to advance these critical operations while exploring new opportunities to better serve the American public.

Goal 5: Strengthen Preparedness and Resilience	The United States will never be completely impervious to present and emerging threats and hazards across the homeland security mission space. Preparedness is a shared responsibility across federal, state, local, tribal, and territorial governments; the private sector; non-governmental organizations; and the American people. Some incidents will surpass the capabilities of communities, so the Federal Government must remain capable of responding to natural disasters, physical and cyberattacks, weapons of mass destruction attacks, critical infrastructure disruptions, and search and rescue distress signals. Following disasters, the Federal Government must be prepared to support local communities with long-term recovery assistance. The United States can effectively manage emergencies and mitigate the harm to American communities by thoroughly preparing local communities, rapidly responding during crises, and supporting recovery.

Goal 6: Champion the DHS Workforce and Strengthen the Department	Since the Department's formation, each Secretary has recognized the importance of strengthening the integrated relationships between and among Headquarters Offices and Operational Components to optimize the Department's efficiency and effectiveness. Despite the considerable progress during the last 15 years to establish and strengthen DHS management functions, the Department has much to improve. Over the next 4 years, DHS will continue to mature as an institution by increasing integration, clarifying roles and responsibilities, championing its workforce, advancing risk-based decision-making, and promoting transparency and accountability before the American people. In an important step forward, DHS is beginning to consolidate Support Components and the Office of the Secretary on the St. Elizabeths Campus, which will further promote integration.

Appendix C – The Department's Updated 12 Functional Priorities

Prior to the Department's 20th anniversary, Secretary Alejandro Mayorkas updated the following cross-functional priorities, first issued in 2022. The priorities were intended to guide the Department's focus through better preparation, enhanced prevention, and enhanced response to threats and challenges.

Organizational Advancement

1. Support and champion our workforce and advance a culture of excellence.
2. Hire and retain a world-class, diverse workforce to create an inclusive, representative, and trusted Department.
3. Advance cohesion across the Department to improve mission execution and drive greater efficiency.
4. Responsibly harness artificial intelligence to advance mission execution, as well as transform our delivery of services to improve the customer experience.
5. Enhance openness and transparency to build greater trust with the American people and ensure the protection of the privacy, civil rights, civil liberties, and human rights of the communities we serve.
6. Transform the Department's infrastructure to ensure it is a more productive and flexible workplace responsive to our workforce's and the public's needs.

Mission-Specific Advancement

7. Combat all forms of terrorism and targeted violence.
8. Increase cybersecurity of our nation's networks and critical infrastructure, including election infrastructure.
9. Secure and modernize our borders and ports of entry.
10. Build a fair, orderly, and humane immigration system.
11. Ready the nation to respond to and recover from disasters and combat the climate crisis.
12. Combat crimes of exploitation and protect victims.

Appendix D – OIG Audits, Inspections, and Evaluations Published in FY 2024

Report Number	Report Title and Issue Date	Standards or Authority	Related Strategic Mission	Recommendation Status as of September 18, 2024
OIG-24-01	CBP Did Not Fully Implement the Requirements of the Synthetic Opioid Exposure Prevention and Training Act (October 2023)	GAGAS	E	1 Recommendation (1 open, 0 closed)
OIG-24-02	Management Alert - ICE Management and Oversight of Mobile Applications - (REDACTED) (October 2023)	GAGAS	4	6 Recommendations (6 open, 0 closed)
OIG-24-03	Limited-Scope Unannounced Inspection of Mesa Verde ICE Processing Center in Bakersfield, California (November 2023)	Quality Standards for Inspection and Evaluation	2	3 Recommendations (0 open, 3 closed)
OIG-24-04	Results of Unannounced Inspections of CBP Holding Facilities in the Miami Area (November 2023)	Quality Standards for Inspection and Evaluation	2	2 Recommendations (0 open, 2 closed)
OIG-24-05	Major Management and Performance Challenges Facing the Department of Homeland Security (MMPC) (November 2023)	Not Applicable	All	No recommendations issued.
OIG-24-06	Independent Auditors' Report on the Department of Homeland Security's Consolidated Financial Statements for FYs 2023 and 2022 and Internal Control over Financial Reporting (November 2023)	GAGAS	E	24 Recommendations (9 open, 15 closed)
OIG-24-07	Results of Unannounced Inspections of CBP Holding Facilities in the San Diego Area (November 2023)	GAGAS	2	2 Recommendations (0 open, 2 closed)

Report Number	Report Title and Issue Date	Standards or Authority	Related Strategic Mission	Recommendation Status as of September 18, 2024
OIG-24-08	Coast Guard National Maritime Center's Oversight of Merchant Mariner Training and Examinations (December 2023)	Quality Standards for Inspection and Evaluation	E	7 Recommendations (7 open, 0 closed)
OIG-24-09	CISA Needs to Improve Collaboration to Enhance Cyber Resiliency in the Water and Wastewater Sector (January 2024)	GAGAS	4	3 Recommendations (3 open, 0 closed)
OIG-24-10	Summary of Previously Issued Recommendations and Other Insights to Improve Operational Conditions at the Southwest Border (January 2024)	Quality Standards for Inspection and Evaluation	2	No recommendations issued.
OIG-24-11	Summary of Selected DHS Components that Did Not Consistently Restrict Access to Systems and Information (January 2024)	GAGAS	4	No recommendations issued.
OIG-24-12	Review of U.S. Immigration and Customs Enforcement's Fiscal Year 2023 Detailed Accounting Report for Drug Control Funds (January 2024)	GAGAS	E	No recommendations issued.
OIG-24-13	Review of Federal Law Enforcement Training Centers' Fiscal Year 2023 Detailed Accounting Report for Drug Control Funds (January 2024)	GAGAS	E	No recommendations issued.
OIG-24-14	Review of U.S. Customs and Border Protection's Fiscal Year 2023 Drug Control Budget Formulation Compliance Report (January 2024)	GAGAS	E	No recommendations issued.
OIG-24-15	Review of U.S. Immigration and Customs Enforcement's Fiscal Year 2023 Drug Control Budget Formulation Compliance Report (January 2024)	GAGAS	E	No recommendations issued.

Report Number	Report Title and Issue Date	Standards or Authority	Related Strategic Mission	Recommendation Status as of September 18, 2024
OIG-24-16	ICE Major Surgeries Were Not Always Properly Reviewed and Approved for Medical Necessity (January 2024)	GAGAS	2	1 Recommendation (1 open, 0 closed)
OIG-24-17	Review of Federal Law Enforcement Training Centers' Fiscal Year 2023 Drug Control Budget Formulation Compliance Report (January 2024)	GAGAS	E	No recommendations issued.
OIG-24-18	Review of U.S. Customs and Border Protections Fiscal Year 2023 Detailed Accounting Report for Drug Control Funds (January 2024)	GAGAS	E	No recommendations issued.
OIG-24-19	DHS Grants and Contracts Awarded by Any Means Other Than Full and Open Competition During Fiscal Year 2023 (February 2024)	GAGAS	E	No recommendations issued.
OIG-24-20	Results of July 2023 Unannounced Inspections of CBP Holding Facilities in the Rio Grande Valley Area (March 2024)	Quality Standards for Inspection and Evaluation	2	4 Recommendations (2 open, 2 closed)
OIG-24-21	Results of an Unannounced Inspection of ICE's Krome North Service Processing Center in Miami, Florida (April 2024)	Quality Standards for Inspection and Evaluation	2	8 Recommendations (5 open, 3 closed)
OIG-24-22	CISA's Use of Infrastructure Investment and Job Act Funds (April 2024)	Quality Standards for Inspection and Evaluation	4	No recommendations issued.
OIG-24-23	Results of an Unannounced Inspection of ICE's Golden State Annex in McFarland, California (April 2024)	Quality Standards for Inspection and Evaluation	2	7 Recommendations (5 open, 2 closed)
OIG-24-24	DHS Has a Fragmented Process for Identifying and Resolving Derogatory Information for Operation Allies Welcome Parolees (May 2024)	Quality Standards for Inspection and Evaluation	3	5 Recommendations (5 open, 0 closed)

Report Number	Report Title and Issue Date	Standards or Authority	Related Strategic Mission	Recommendation Status as of September 18, 2024
OIG-24-25	DHS' Fiscal Year 2023 Compliance with the Payment Integrity Information Act of 2019 (June 2024)	GAGAS	E	2 Recommendations (2 open, 0 closed)
OIG-24-26	Evaluation of DHS' Information Security Program for Fiscal Year 2023 (June 2024)	Quality Standards for Inspection and Evaluation	4	2 Recommendations (2 open, 0 closed)
OIG-24-27	DHS Needs to Improve Its Screening and Vetting of Asylum Seekers and Noncitizens Applying for Admission into the United States - (REDACTED) (June 2024)	GAGAS	2 & 3	5 Recommendations (5 open, 0 closed)
OIG-24-28	(U) Evaluation of DHS' Compliance with Federal Information Security Modernization Act Requirements for Intelligence Systems for Fiscal Year 2023 (June 2024)	Quality Standards for Inspection and Evaluation	4	2 Recommendations (2 open, 0 closed)
OIG-24-29	Results of an Unannounced Inspection of ICE's Denver Contract Detention Facility in Aurora, Colorado (June 2024)	Quality Standards for Inspection and Evaluation	2	14 Recommendations (8 open, 6 closed)
OIG-24-30	CBP and ICE Did Not Have an Effective Process for Detaining and Removing Inadmissible Travelers at an International Airport - (REDACTED) (June 2024)	Quality Standards for Inspection and Evaluation	3	3 Recommendations (3 open, 0 closed)
OIG-24-31	ICE's Risk Classification Assessment Process Was Not Consistently Used to Prevent the Release of High-Risk Individuals (June 2024)	GAGAS	2	2 Recommendations (2 open, 0 closed)
OIG-24-32	Infrastructure Investment and Jobs Act Funding: CBP Must Improve Processes for Addressing Critical Repairs at CBP-owned Land Ports of Entry (June 2024)	Quality Standards for Inspection and Evaluation	4	1 Recommendation (1 open, 0 closed)

Report Number	Report Title and Issue Date	Standards or Authority	Related Strategic Mission	Recommendation Status as of September 18, 2024
OIG-24-33	Management Alert - CBP Has Limited Information to Assess Interview-Waived Nonimmigrant Visa Holders - (REDACTED) (June 2024)	GAGAS	3	2 Recommendations (2 open, 0 closed)
OIG-24-34	FEMA Region IV Has a Process to Identify Single Sites Damaged by Multiple Events (June 2024)	GAGAS	5	No recommendations issued.
OIG-24-35	TSA Could Not Assess Impact of Federal Air Marshal Service Personnel Deployed to Support Southwest Border Security - (REDACTED) (July 2024)	Quality Standards for Inspection and Evaluation	2	1 Recommendation (1 open, 0 closed)
OIG-24-36	USCIS Faces Challenges Meeting Statutory Timelines and Reducing its Backlog of Affirmative Asylum Claims (July 2024)	GAGAS	3	2 Recommendations (2 open, 0 closed)
OIG-24-37	Coast Guard Should Take Additional Steps to Secure the Marine Transportation System Against Cyberattacks (July 2024)	GAGAS	4	4 Recommendations (4 open, 0 closed)
OIG-24-38	FEMA's Emergency Non-Congregate Sheltering Interim Policy Provided Greater Flexibility for Emergency Sheltering During the COVID-19 Pandemic (July 2024)	GAGAS	5	No recommendations issued.
OIG-24-39	Results of October 2023 Unannounced Inspections of CBP Holding Facilities in the El Paso Area (July 2024)	Quality Standards for Inspection and Evaluation	2	3 Recommendations (3 open, 0 closed)
OIG-24-40	Management Alert - CISA and FLETC Did Not Take Action to Protect Personally Identifiable Information and Sensitive Law Enforcement Training Curricula (July 2024)	GAGAS	4	2 Recommendations (2 open, 0 closed)

Report Number	Report Title and Issue Date	Standards or Authority	Related Strategic Mission	Recommendation Status as of September 18, 2024
OIG-24-41	FEMA Did Not Fully Implement the State-Administered Direct Housing Grant Program - (REDACTED) (July 2024)	GAGAS	5	4 Recommendations (3 open, 1 closed)
OIG-24-42	The Secret Service's Preparation for, and Response to, the Events of January 6, 2021 - (REDACTED) (July 2024)	Quality Standards for Inspection and Evaluation	1	6 Recommendations (6 open, 0 closed)
OIG-24-43	DHS Has Made Progress in Implementing an Enhanced Personnel Vetting Program (August 2024)	Quality Standards for Inspection and Evaluation	E	No recommendations issued.
OIG-24-44	Results of January 2024 Unannounced Inspections of CBP Holding Facilities in the Del Rio Area - (REDACTED) (August 2024)	Quality Standards for Inspection and Evaluation	2	3 Recommendations (2 open, 1 closed)
OIG-24-45	FEMA's Inadequate Oversight Led to Delays in Closing Out Declared Disasters (August 2024)	GAGAS	5	2 Recommendations (2 open, 0 closed)
OIG-24-46	Management Alert - ICE Cannot Monitor All Unaccompanied Migrant Children Released from DHS and U.S. Department of Health and Human Services' Custody (August 2024)	GAGAS	6	2 Recommendations (2 open, 0 closed)
OIG-24-47	S&T Inconsistently Managed Critical Infrastructure Security and Resilience Research and Development Activities (August 2024)	GAGAS	4 & 5	4 Recommendations (3 open, 1 closed)
OIG-24-48	CBP Did Not Thoroughly Plan for CBP One™ Risks, and Opportunities to Implement Improvements Exist (August 2024)	Quality Standards for Inspection and Evaluation	2 & 4	3 Recommendations (3 open, 0 closed)
OIG-24-49	CBP Needs to Improve its Oversight and Monitoring of Penalty Cases (September 2024)	GAGAS	E	2 Recommendations (2 open, 0 closed)

Report Number	Report Title and Issue Date	Standards or Authority	Related Strategic Mission	Recommendation Status as of September 18, 2024
OIG-24-50	TSA Made Progress Implementing Requirements of the 9/11 and TSA Modernization Acts but Additional Work Remains (September 2024)	Quality Standards for Inspection and Evaluation	1	3 Recommendations (3 open, 0 closed)
OIG-24-51	CBP Conducts Individualized Assessments but Does Not Comprehensively Assess Land Port of Entry Operations (September 2024)	GAGAS	2	2 Recommendations (2 open, 0 closed)
OIG-24-52	DHS Improved Election Infrastructure Security, but Its Role in Countering Disinformation Has Been Reduced (September 2024)	Quality Standards for Inspection and Evaluation	1, 4, & 5	1 Recommendation (1 open, 0 closed)
OIG-24-53	ICE Did Not Fully Implement Effective Security Controls on Selected High Value Asset Systems (September 2024)	Quality Standards for Inspection and Evaluation	4	6 Recommendations (6 open, 0 closed)
OIG-24-54	CBP's Office of Field Operations Used Overtime in Accordance with Policies and Procedures (September 2024)	GAGAS	E	No recommendations issued.
OIG-24-55	I&A Needs to Improve Its Security Inspection Program to Reduce the Risk of Unauthorized Access to Classified Information (September 2024)	GAGAS	4 & E	2 Recommendations (2 open, 0 closed)
OIG-24-56	Coast Guard Needs to Implement Effective Planning for Infrastructure Investment and Jobs Act Projects (September 2024)	GAGAS	4	4 Recommendations (4 open, 0 closed)
OIG-24-57	Audit of Office of Intelligence and Analysis Contract and Funding Management Processes (September 2024)	GAGAS	E	4 Recommendations (4 open, 0 closed)

Report Number	Report Title and Issue Date	Standards or Authority	Related Strategic Mission	Recommendation Status as of September 18, 2024
OIG-24-58[26]	CBP Needs to Improve Its Management of the Facility Condition Assessment Program (September 2024)	GAGAS	E	3 Recommendations (3 open, 0 closed)
OIG-24-59	Summary of Unannounced Inspections of ICE Facilities Conducted in Fiscal Years 2020-2023 (September 2024)	Quality Standards for Inspection and Evaluation	2	No recommendations issued.
OIG-24-60	CISA Faces Challenges Sharing Cyber Threat Information as Required by the Cybersecurity Act of 2015 (September 2024)	Quality Standards for Inspection and Evaluation	4	2 Recommendations (2 open, 0 closed)
OIG-24-61	ICE Did Not Always Manage and Secure Mobile Devices to Prevent Unauthorized Access to Sensitive Information (September 2024)	GAGAS	4	8 Recommendations (8 open, 0 closed)
OIG-24-62	DHS Partners Did Not Always Use DHS Technology to Obtain Emerging Threat Information (September 2024)	GAGAS	1	4 Recommendations (4 open, 0 closed)
OIG-24-63	Results of an Unannounced Inspection of Baker County Sheriff's Office in Macclenny, Florida (September 2024)	Quality Standards for Inspection and Evaluation	2	5 Recommendations (3 open, 2 closed)
OIG-24-64	Oversight Reports Identify Recurring Challenges with DHS Strategic Planning (September 2024)	Quality Standards for Inspection and Evaluation	1	2 Recommendations (2 open, 0 closed)
OIG-24-65	CBP, ICE, and TSA Did Not Fully Assess Risks Associated with Releasing Noncitizens without Identification into the United States and Allowing Them to Travel on Domestic Flights - (REDACTED) (September 2024)	Quality Standards for Inspection and Evaluation	1	3 Recommendations (3 open, 0 closed)

[26] OIG issued reports ending in 24-58, 24-59, 24-60, 24-61, 24-62, 24-63, 24-64 and 24-65 after September 18, 2024; recommendations pertaining to these reports were not summarized within the Mission Areas.

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

BY ELECTRONIC SUBMISSION

October 30, 2024

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

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

JIM H CRUMPACKER
Digitally signed by JIM H CRUMPACKER
Date: 2024.10.30 15:02:08 -04'00'

SUBJECT: Management Response to Draft Report: "Major Management and Performance Challenges Facing the Department of Homeland Security"

Thank you for the opportunity to comment on this major management and performance challenges (MMPC) report. Senior U.S. Department of Homeland Security (DHS, or the Department) leadership appreciates the Office of Inspector General's (OIG) work in developing and issuing this report. In particular, DHS recognizes changes OIG made to improve this year's report including: (1) aligning the overarching challenges with the Department's seven strategic missions as outlined in the DHS Annual Performance Report (APR); and (2) adding more information about specific recommendations within the challenge area narrative sections. Senior DHS leadership, Component-level program officials, subject matter experts, and others throughout the Department will give due consideration to the perspectives offered in this report as part of our unwavering commitment, with honor and integrity, to safeguard the American people, our homeland, and our values.

However, some of OIG's analysis and conclusions in this report contain inaccurate statements, lack important context, and are potentially misleading about the Department's efforts to successfully carry out its various missions. For example, this report continues to minimize or ignore DHS efforts to accommodate OIG information requests—specifically those related to accessing various information technology (IT) systems—which the OIG then uses as a primary basis for justifying an overarching challenge related to transparency. DHS Leadership believes improvements can be made to: (1) the overall process for developing the MMPC report through increased communication and collaboration (akin to concerns expressed last year); and (2) the usefulness of the report

by more clearly identifying specific outcomes needed to remediate the challenges noted in each of the DHS mission areas.

IT System and Data Access Requests

Leadership is disappointed with OIG's continued mischaracterization of Departmental cooperation when responding to OIG requests to access various IT systems and data, as well as OIG's use of this issue as a primary basis for justifying an overarching challenge related to transparency. In this report, OIG alleges that it made 17 system access requests to the Department or Components during fiscal year (FY) 2024, of which 13 were denied and only four were approved. This claim is inaccurate and misleading as it does not appropriately acknowledge Departmental efforts to resolve OIG's concerns and lacks meaningful specifics, thereby limiting the value of this MMPC report to the Department, Congress, and the public.

As mentioned in numerous prior correspondence from Secretary of Homeland Security Alejandro N. Mayorkas, and reiterated here, DHS respects the OIG's unique role in reviewing DHS's many programs, operations, and activities. Early in his tenure, Secretary Mayorkas issued a memorandum to all Department personnel stating that he expected them to cooperate with the OIG (including its contractors) and facilitate its work, noting that the OIG "plays a critical role in helping the Department prevent and detect fraud, waste, abuse, and mismanagement" and that "it cannot do so alone."[1] This memorandum and the Department's ensuing record belie the OIG's allegation that DHS is restricting the OIG's ability to conduct work and provide information to "citizens, Congress, and other stakeholders."

Perhaps the most significant allegation of purported access challenges alleged by the OIG involved OIG's access to information regarding the January 6, 2021, attack on the U.S. Capitol. This situation serves as an illustrative example of OIG's many allegations of delayed or denied access to IT systems and data, and is therefore highlighted in the attachment to this response. DHS adamantly disagrees with OIG's assertion in this MMPC report that "the Department generally provided simple extracts of the narrowest set of data possible, based on its own interpretation of the scope of the ongoing engagement."

In this MMPC report, OIG also cites the Evidence-Based Policymaking Act of 2018 as a basis for its conclusion that the Department is required to provide the OIG unrestricted access to its IT systems, regardless of the scope and objectives of any specific audit. In support of its position, the OIG references the Act's intent to promote the public good and transparency before the American people and the advancement of evidence-based policymaking. The OIG concludes that the Department's lack of transparent data

[1] "Cooperation with the Office of Inspector General," dated September 30, 2021.

"inhibits OIG's (and thus the public's) ability to fully understand and address problematic or inefficient practices." However, the Department disagrees with the OIG's conclusions regarding the extent to which the Act is either applicable or relevant to the Department's relationship with the OIG.

First, it is important to understand the Act's context. The Act is designed to improve agency transparency concerning improved policymaking based on the best evidence available, but it does not address the dynamics between agencies and their OIGs, nor does it mandate that agencies grant OIGs unrestricted access to agency information or IT systems.

Secondly, the OIG infers that because the Evidence Act promotes transparency with the public with respect to evidence based policymaking, that OIG must have wholesale access to agency information systems to facilitate reporting its findings to the public. This reasoning is flawed. Even if the OIG's inference were correct, it is important to note that the Department believes in full transparency, providing all requested information pertinent to the scope and objectives of the OIG's announced audits, evaluations, inspections, and other reviews. Extracting and providing all relevant information directly from Departmental systems—rather than granting unfettered access to the agency systems regardless of relevance—does not compromise the OIG's ability to assess agency programs and operations or to make those findings available to the public, as appropriate.

Therefore, the OIG's reliance on the Evidence Act to conclude that it must have unlimited access to all information maintained by the Department, regardless of the scope and objectives of an OIG engagement, is misplaced as the Act simply does not authorize that. It's clear that the Act is about evidence building—that is, statistical activities for statistical purpose. Furthermore, use of agency (or statistical agency) data for any non-statistical purpose is not covered under the Act. Office of Management and Budget (OMB) guidance distinguishes evaluation, which is required of agencies under Title 1, as distinct from internal control activities conducted by OIG and the U.S. Government Accountability Office (GAO).[2]

Overall Report Development Process and Usefulness

Leadership also believes improvements can be made to: (1) the overall process for developing the MMPC report through increased communication and collaboration (akin to concerns DHS expressed last year); and (2) the usefulness of the report by more clearly identifying specific outcomes needed to remediate the challenges noted in each of the

[2] OMB M-19-23, "Phase I Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance," dated July 10, 2019, and OMB M-21-37, "Evidence-Based Policymaking: Learning Agendas and Annual Evaluation Plans," dated June 30, 2021.

DHS mission areas similar to the approach used by the GAO in its biennial High-Risk report.[3]

Increased Collaboration and Communication

Beyond relatively short, simple "meet and greet" meetings, the OIG did not materially engage with senior DHS and Component leadership about this report during FY 2024. We are aware of one Headquarters meeting with the Associate Deputy Under Secretary for Management on August 29, 2024, in which the OIG discussed the MMPC; however, we understand that most senior Component leaders did not have any substantive meetings with OIG to discuss specifics and help inform the MMPC report, including leaders from the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Emergency Management Agency, Transportation Security Administration, and the U.S. Citizenship and Immigration Services. To the extent any such meetings occurred, the report does not disclose which senior leaders OIG met with (i.e., by title, not name), which DHS believes would have increased the credibility of the MMPC report.

In addition, the MMPC report highlighted that OIG aligned its four overarching challenges with Departmental operations and activities under its seven strategic missions, as outlined in the APR for FYs 2023-2025.[4] This APR presents a summary of the Department's performance for FY 2023 (i.e., ending September 30, 2023), with performance measure results, explanations, and targets for FY 2024-2025 included. However, by relying so heavily on APR for the "Recent Progress" section of each Mission Area narrative and not being more inclusive of senior leadership input, OIG missed including significant activities occurring during FY 2024 that could have made the report timelier and more relevant.

For example, the MMPC:

- Makes no mention of the Department's unmodified (i.e., clean) financial statement audit opinion achievement, having earned its eleventh consecutive unmodified audit opinion for all five financial statements.

- Addresses "Accountability" within the Mission 4: Security Cyberspace and Critical Infrastructure area, but does not mention Cross-Sector Cybersecurity Performance Goals (CPGs). More specifically, CISA released a cybersecurity framework through CPGs in March 2023, and is now actively promoting this framework. CPGs are high-impact, high-priority practices for critical infrastructure owners that address common adversary tactics, techniques, and

[3] GAO-23-106203, "High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas," dated April 20, 2023; (https://www.gao.gov/products/gao-23-106203).
[4] "U.S. Department of Homeland Security Annual Performance Report FY 2023-2025;" (https://www.dhs.gov/sites/default/files/2024-03/2024_0305_annual_performance_report_for_fiscal_years_2023_2025.pdf).

procedures and manage risks to IT and operational technology (OT). CPGs are intended to enable the critical infrastructure community, across both public and private sectors, to effectively reduce risk and prioritize cybersecurity outcomes across both IT and OT assets. Since these CPGs were released, CISA is encouraging their adoption to reduce the prevalence and impact of cyber intrusions affecting American organizations through tools such as the Ransomware Vulnerability Warning Pilot and the Shields Up campaign.

- Does not mention employee engagement/morale, a significant focus area for the Department. More specifically, the Secretary's priority on employee morale and engagement led to the creation of a new Employee Experience Framework, which includes the following key elements:
    - Focus groups with employees from across the Department;
    - A quarterly pulse survey program that provides opportunities for employees to provide direct feedback, including open-ended questions; and
    - Field tests that explore innovative ways to address key areas of the Employee Experience Framework, by bringing DHS and Component headquarters personnel into the field to better understand and address the basic needs of the frontline workforce.

- Does not mention recent improvements led by the DHS Office of the Chief Information Officer, such as:
    - Awarding funding to DHS Components to advance modernization needs within the Department;
    - Coordinating with DHS Office of Program Accountability and Risk Management on ways to improve the oversight for modernization efforts occurring within existing IT programs;
    - Reinvigorating the Chief Information Officer (CIO) Council to further strengthen effectiveness of DHS and Component CIOs in decision-making;
    - Building on DHS IT workforce efforts to advance the hiring, upskilling, and training to meet emerging Artificial Intelligence (AI) needs; and
    - Collaborating with the DHS Office of the Chief Financial Officer on key Departmental resourcing needs during the FY 2026-2030 budget cycle including AI and Automated Screening and Vetting.

OIG also repeatedly stated in the MMPC's "Recent Progress" sections that Department and Component progress statements taken from the APR **had not been validated by OIG** (emphasis added). DHS believes that OIG' inclusion of a statement of negative assurance in the report is a more appropriate approach, and would provide greater value to end users of the report. OIG advising whether or not it believes the Recent Progress statements to be accurate would create greater confidence in the report, especially given that OIG found no contrary evidence to dispute the statements. Further, this action would

be more aligned with the intent of the Reports Consolidation Act of 2000 requirement for OIG to *assess* DHS progress in addressing the management and performance challenges.

In addition, it is important to highlight that—similar to the 2023 MMPC report—the time OIG allowed DHS to collect, consolidate, and clear technical comments (TCs) feedback[5] and develop a formal management response letter (MRL) for the 2024 MMPC report was not reasonable. Specifically, OIG only allowed 17 calendar days for DHS to perform these actions, which is just over half the time provided in OIG's normal practice of allowing 30 calendar days to staff and coordinate a response to typical draft reports. This is unreasonable considering this MMPC report has DHS-wide equities and requires more staffing and coordination than is needed to respond to a typical draft report, not less. Further, the OIG's Chief of Staff said the Department's TCs would not be considered, nor an MRL included in the final report, if either were received by the OIG after October 31, 2024. The deadline for incorporating the MMPC into the Department's Agency Financial Report (AFR) is November 13, 2024, in order to allow time to publish and deliver the AFR to Congress, OMB, the U.S. Department of Treasury, and GAO by close of business on November 15, 2024, as required by statute. This begs the question of why the OIG, which has traditionally just simply inserted the MRL into its final MMPC report as an Appendix, without writing any analysis or evaluation of the response, would need nearly as much time to do this as it allowed the Department to develop its TCs and MRL.[6]

Further, the OIG report's narrative about the recommendations with which DHS non-concurred is incomplete and should have included a more extensive discussion. For example, in a footnote on the next to last page of the MMPC report, OIG discloses that recommendations from the last eight reports it published during FY 2024 (from September 19-30, 2024) were not summarized within the Department's seven strategic mission areas. Three of these reports accounted for 42 percent (5 of 12) of recommendations with which the Department non-concurred during FY 2024.

More specifically, a recommendation is considered "unresolved" when OIG and the Department do not agree on actions taken, on-going, or planned to address the

[5] Such feedback is not intended to substantially alter any of OIG's overall findings, conclusions, or recommendations; rather; they are to strengthen audit products by improving accuracy, heling to ensure and validate workable solutions, and minimizing the number of non-concurrences. This process also helps foster mutually beneficial and production relationships with the audit agencies, while maintaining and respecting auditor independence.

[6] MRLs for MMPC reports are provided in accordance with OMB Circular No. A-136, "Financial Reporting Requirements," dated May 22, 2023. Of note, the OIG published its 2023 MMPC report without the Department's management response letter, in a departure from a well-established, years-long practice, apparently at least in part because the draft report was released so late in the year for Department comments. As a result, the MRL had to be included in the "Department's FY 2023 AFR," as part of the section that includes the OIG report in its entirety; however, **unfortunately, readers of the OIG's report likely did not know where to find the response and, therefore, assumed the Department did not have one.**

recommendations. Simply noting the number of "resolved" and "unresolved" recommendations from selected reports by Mission Area or otherwise incompletely summarizing the disagreement, leaves it subject to interpretation as to whether OIG did not agree with the Department's corrective action plans or whether DHS/the involved Component(s) disagreed with OIG's recommendation, which is a very important distinction.

For example, while the draft MMPC report stated that the U.S. Secret Service (USSS) did not concur with two of the recommendations in OIG-24-42,[7] OIG did not adequately disclose all pertinent facts related to these issues. More precisely, although OIG acknowledged that USSS stated its primary mission limits its ability to provide emergency support to other law enforcement partners, the OIG insisted that USSS nevertheless take action to develop and implement protocols for providing Civil Disturbance Unit support to law enforcement partners in the event of an emergency. However, this perspective disregards USSS' fundamental disagreement with the intent of the recommendation—that the USSS must always be prepared to dedicate its resources—especially during emergencies—to ensure continuity of executive branch leadership and government operations, and taking the recommended action could result in compromising the agency's foremost responsibility to protect the White House and the President, as well as its other protected sites and persons.

For the second recommendation in this report, OIG recommended that USSS develop and implement training for site agents on directing canine sweeps if a specialized Technical Security Division agent is not assigned to a site. However, USSS had already taken action years ago that effectively addressed the intent of this recommendation by issuing an update to OPO-06, Office of Protective Operation (OPO), "Protective Operations Manual," dated April 7, 2022. With this update, OPO-06 provides direction to agents on how to proceed when specialized personnel are not available to assist, thus ensuring the continuity of operations and the protection of USSS protectees negating the need for site agents to be trained on directing canine sweeps.

In another example, involving OIG-24-57,[8] OIG recommended that DHS' Office of the Chief Procurement Officer (OCPO) develop a process to obtain and retain a Contracting Officer Representative (COR) appointment letter as part of the required documentation for monitoring contracts. However, the MMPC report does not acknowledge the basis for OCPO's disagreement with this recommendation; that it did not need to create such a process because current policies and procedures were sufficient to ensure inclusion of the COR letters in applicable contract files. As an alternative, OCPO agreed to issue an

[7] OIG-24-42, "The Secret Service's Preparation for, and Response to, the Events of January 6, 2021," dated July 31, 2024: (https://www.oig.dhs.gov/sites/default/files/assets/2024-08/OIG-24-42-Aug24-Redacted.pdf).
[8] OIG-24-57, "Audit of Office of Intelligence and Analysis Contract and Funding Management Processes," dated September 19, 2024; (https://www.oig.dhs.gov/reports/2024/audit-office-intelligence-and-analysis-contract-and-funding-management-processes/oig-24-57-sep24).

Acquisition Alert to remind contracting officials of the requirement to issue COR appointment letters, where required, and maintain those in the official contract files. The OIG subsequently agreed with this alternative corrective action.

The Department remains concerned about a June 2021 GAO report which concluded, in part, that the OIG suffered from long-standing management and operational weaknesses.[9] DHS leadership agreed with the many concerns raised by GAO in this report, especially those related to quality assurance and that the OIG: (1) had no overarching system of internal quality assurance for audit, inspection, evaluation, and other work; and (2) cannot know if its internal processes ensure that its work adheres to its policies and meets established standards of performance. GAO's report included 21 recommendations, 11 of which remain open as of October 22, 2024, more than three years later (GAO considers five of these as "Partially Addressed" [i.e., actions that partially satisfy the intent of the recommendations have been taken]). As the Secretary of Homeland Security has previously highlighted in letters to Congress, the public trust relies heavily on an OIG that maintains high standards of professionalism and does work that can be relied upon by others.

More Clearly Identifying Outcomes Needed to Remediate the Challenges

Senior DHS leadership is committed to addressing the MMPCs identified in this report; however, leadership attention by itself is not enough. Unfortunately, OIG's report does not identify any criteria for assessing progress in remediating the MMPCs shown in the report for each of the DHS mission areas. A more structured approach of assessing DHS progress would better guide the Department in achieving these goals.

To help make future MMPC reports more "value added," DHS recommends that the OIG consider developing criteria, similar to the approach used by GAO for assessing progress in addressing the areas on its High-Risk List with its biennial High-Risk report such as: [10]

- Leadership commitment to initiate and sustain progress;
- Capacity (i.e., skilled staff, adequate funding, internal controls, technology, and management and organization infrastructure) to resolve key risks;
- An action plan to define the root causes and solutions and provide an approach for substantially completing corrective measures;
- Monitoring to help agency leaders track and independently validate effectiveness and sustainability of corrective measures; and
- Demonstrated progress in implementing corrective measure that address the root causes of high-risk areas.

[9] GAO-21-316, "DHS Office of Inspector General: Actions Needed to Address Long-Standing Management Weaknesses," dated June 3, 2021; (https://www.gao.gov/products/gao-21-316).
[10] GAO-22-105184, "High-Risk Series: Key Practices to Successfully Address High-Risk Areas and Remove Them from the List," dated March 3, 2022; (https://www.gao.gov/products/GAO-22-105184)

The OIG represents a critical component of DHS' control environment and, as such, it is important that the Department has a constructive and productive working relationship with OIG staff. While the Department and OIG might disagree at times, DHS has the utmost confidence and respect for the men and women of the OIG be they auditors, inspectors, evaluators, investigators, or support staff.

The Department remains committed to working with the OIG to address the MMPC discussed in this report and the related concerns summarized above. In particular, DHS leadership looks forward to development of the 2025 MMPC report being initiated earlier in the year than recent past years and working more closely with OIG leadership counterparts.

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, as appropriate.

Attachment

Attachment: Illustrative Example of DHS Responses to OIG's Years Long Allegations of Delayed or Denied Access to IT Systems and Data Related to the January 6, 2021, Attack on the U.S. Capitol

As the Secretary of Homeland Security wrote on November 29, 2021,[11] when transmitting OIG's semiannual report (SAR) to Congress for the period ending September 30, 2021, DHS strongly disagrees with the suggestion that the Department restricted and significantly delayed the OIG's access to information regarding the January 6, 2021, attack on the U.S. Capitol.

More specifically, as the Department explained, at no time did DHS refuse access to relevant information or impede progress on any of OIG's January 6-related reviews.[12] To the contrary, throughout these reviews, the USSS and other DHS agencies made available countless documents and hundreds of personnel to be interviewed by the OIG, often within days of an initial request. The breadth and scope of the original OIG requests were extensive and often required discussion to ensure proper handling of highly sensitive information, much of which was not relevant to the specific investigation. While OIG stated that for a months-long period "the Department did not cite any legal authority consistent with section 6(a)(1)(B) of the IG Act that would have justified withholding the information," in fact the Department repeatedly cited relevant statutes, including the Privacy Act and the Presidential Records Act, in support of its concerns. Despite its legitimate concerns, the Department did not withhold any information and it accommodated the OIG's sweeping requests.

Similarly, as the Secretary of Homeland Security wrote on June 14, 2022,[13] when responding to the SAR for the period ending March 31, 2022, one of the Department's top priorities is understanding what led to and occurred on January 6, 2021. The Department reiterated that DHS made every effort to coordinate with the OIG on its reviews related to the January 6, 2021, attack on the U.S. Capitol, including by providing timely access to relevant information. The Department worked diligently with the OIG to provide broad access to information, and to minimize any delays in accommodating the OIG's sweeping requests, subject to the Department's legal obligations.

---

[11] Letter from Secretary of Homeland Security Alejandro N. Mayorkas to nearly 30 different members of Congress; dated November 29, 2021.

[12] Reviews include: (1) OIG-22-29, "I&A Identified Threats Prior to January 6, 2021, but Did Not Issue Any Intelligence Products before the U.S. Capitol Breach," dated March 4, 2022 (https://www.oig.dhs.gov/sites/default/files/assets/2022-04/OIG-22-29-Mar22-Redacted.pdf); (2) OIG-24-42, "The Secret Service's Preparation for, and Response to, the Events of January 6, 2021; dated July 31, 2024, (https://www.oig.dhs.gov/sites/default/files/assets/2024-08/OIG-24-42-Aug24-Redacted.pdf) ; and (3) OIG Project Number. 21-025-SRE-DHS(a), "DHS Law Enforcement Preparation for and Response to the January 6, 2021 Events at the U.S. Capitol (II)," announced on February 5, 2021, and still in fieldwork.

[13] Letter from Secretary of Homeland Security Alejandro N. Mayorkas to Senator Maria Cantwell, dated June 14, 2022.

The Secretary of Homeland Security provided a yet more detailed response in a letter dated December 23, 2022,[14] responding to the SAR for the period ending September 30, 2022, and explaining why the OIG's alleged "data access issues" are unfounded. Among other concerns, the Department noted that DHS evaluates OIG requests for direct access to agency databases on a case-by-case basis. Further, as the Department explained, it is not improper for an agency, as the steward of the data, to seek information on the relevance of a data request to the scope and objectives of OIG's work, especially in light of the types of sensitive data held by DHS, including sensitive security information, personally identifiable information (PII) of vulnerable populations and others, as well as proprietary, classified, and investigative information. The Department explained that the vast majority of data in the databases OIG identified in its SAR are unrelated to, or beyond the scope and objectives of, the OIG engagements at issue.

When responding to the SAR for the reporting period ending on March 31, 2023,[15] the Secretary of Homeland Security again emphasized the Department's position that Congress and the public expect that DHS must first understand what information the OIG needs to accomplish its work, and then work with the OIG—respecting the OIG independence at every step—to determine how best to provide that information, while addressing all involved parties' duties and responsibilities related to the information. The time needed to do this, however, should not be viewed as a "delay" or "denial." Reporting these types of instances in the manner chosen by the OIG portrays constructive conversations as adversarial arguments and does a disservice to end users of the OIG's SARs, including Congress and the public. In its transmittal letter responding to the SAR for the reporting period ending on March 31, 2023, the Department walked through several instances where it was not feasible to provide the OIG with wholesale access to sensitive agency systems, whether because the system contained sensitive data well outside the bounds of the investigation or such access was not technologically feasible, and where the Department in good faith provided responsive system extracts to fulfill the OIG's stated objectives.

Finally, when responding to the SAR for the reporting period ending on September 30, 2023,[16] the Secretary of Homeland Security noted the OIG again alleged numerous attempts by DHS to restrict or delay access to information. The Department in turn reiterated its position that the OIG's allegations generally fail to fully acknowledge Departmental efforts to resolve the OIG concerns, and lack meaningful specifics, thereby limiting the SAR's value to end users. For example, the OIG asked multiple times for

[14] Letter from Secretary of Homeland Security Alejandro N. Mayorkas to Senator Charles E. Schumer, dated December 23, 2022.
[15] Letters from Secretary of Homeland Security Alejandro N. Mayorkas to Senator Katie Britt and Congressman Kevin McCarthy, dated July 14, 2023.
[16] Letters from Secretary of Homeland Security Alejandro N. Mayorkas to Senator Mitch McConnell and Congressman Mike Johnson, dated January 26, 2024.

"back-end access" to selected IT systems, but when DHS program office and cybersecurity experts asked for more specifics about what that phrase means, the OIG staff were unable to explain it. Further, the OIG has not been responsive in addressing DHS concerns about protecting large quantities of PII and other information requested as part of apparent overly broad OIG data requests. DHS believes these requests could be satisfied without compromising the OIG's independence using a more targeted and reasonable approach, and without potentially leaving sensitive information vulnerable to misappropriation and loss. The Department also reiterated its position that taking an appropriate amount of time to understand and reach an accommodation on IT systems and data access requests when needed should not be viewed as a "delay" or "denial," and that erroneous OIG allegations and actions in this regard are increasingly disruptive to having a meaningful and productive relationship with the Department that adds value to DHS programs, operations, and activities.

The mission of the Office of Inspector General is to provide independent oversight and promote excellence, integrity, and accountability within DHS.

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 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

For further information or questions, please contact Office of Inspector General Public Affairs at:

DHS-OIG.OfficePublicAffairs@oig.dhs.gov