Major Management and Performance Challenges Facing the Department of Homeland Security

November 3, 2023

OIG-24-05

OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

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

November 3, 2023

MEMORANDUM FOR:	The Honorable Alejandro N. Mayorkas Secretary Department of Homeland Security
FROM:	Joseph V. Cuffari, Ph.D. Inspector General
SUBJECT:	*Major Management and Performance Challenges Facing the Department of Homeland Security*

JOSEPH V CUFFARI

Digitally signed by JOSEPH V CUFFARI
Date: 2023.11.03 15:11:18 -07'00'

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. Annually, as required by the *Reports Consolidation Act of 2000*, OIG reports on what it determines to be the top management challenges facing the Department. Identifying these challenges highlights the need for enhanced attention by management, to ensure the effective operation of Department programs and the advancement of its strategic goals.

The four overarching challenges identified - *transparency*, *accountability*, *efficiency*, and *sustainability* - 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.

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 2020-2024*[1] and its updated 12 cross-functional priorities[2]. The Department's six strategic goals are:

- Counter Terrorism and Homeland Security Threats;
- Secure U.S. Borders and Approaches;
- Secure Cyberspace and Critical Infrastructure;
- Preserve and uphold the Nation's Prosperity and Economic Security;
- Strengthen Preparedness and Resilience; and
- Champion the DHS Workforce and Strengthen the Department.

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

Additionally, we describe potential risks associated with each of the four challenges and summarize 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 and have not been validated by the OIG. The challenges outlined in this report are based on our judgment and independent research, including discussions with internal and Department component Senior Leaders. In selecting these challenges, OIG considered not only those conversations but also its prior audit, inspection, and investigative oversight work, its 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. This report will be posted 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

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

November 3, 2023

Major Management and Performance Challenges Facing the Department of Homeland Security

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 the OIG's independent research, assessment of prior work, and professional judgement and are aligned to the Departments six strategic goals 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 six strategic goals and assessed the potential impact to program operations and the Department's ability to meet the goals and objectives established in its strategic plan. The Department's six strategic goals are:

- Counter Terrorism and Homeland Security Threats
- Secure U.S. Borders and Approaches
- Secure Cyberspace and Critical Infrastructure
- Preserve and Uphold the Nation's Prosperity and Economic Security
- Strengthen Preparedness and Resilience
- Champion the DHS Workforce and Strengthen the Department.

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 and have not been validated by the 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

A-File	Alien File
AI	artificial intelligence
APR	Annual Performance Report
CBP	U.S. Customs and Border Protection
CISA	Cybersecurity and Infrastructure Security Agency
CSS	cell-site simulators
CTMS	Cybersecurity Talent Management System
DOJ	Department of Justice
FEMA	Federal Emergency Management Agency
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Modernization Act of 2014
GAGAS	Generally Accepted Government Auditing Standards
GDA	Geospatial Data Act of 2018
HSI	ICE's Homeland Security Investigations
HQ	DHS Headquarters
ICE	U.S. Immigration and Customs Enforcement
IMF	CBP's International Mail Facility
IT	information technology
KPI	key performance indicators
LPOE	land ports of entry
OCIO	Office of the Chief Information Officer
OFAM	CBP's Office of Facilities and Asset Management
PBNDS 2011	Performance-Based National Detention Standards 2011
SIP	Coast Guard's Streamlined Inspection Program
SOR	system(s) of record
TBML	trade-based money laundering
TEDS	National Standards on Transport, Escort, Detention, and Search
TSA	Transportation Security Administration
USCIS	U.S. 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 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.

The Department relies on strategic guidance that outlines specifics, such as roles, responsibilities, policies, procedures, 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 mission.

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

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 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 - **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. 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 six strategic goals and 12 cross-functional priorities. Additionally, we describe potential risks associated with each of the four challenges and summarize actions the Department has taken, is taking, or needs to take to further address the foundational challenges. The Department's six strategic goals are:

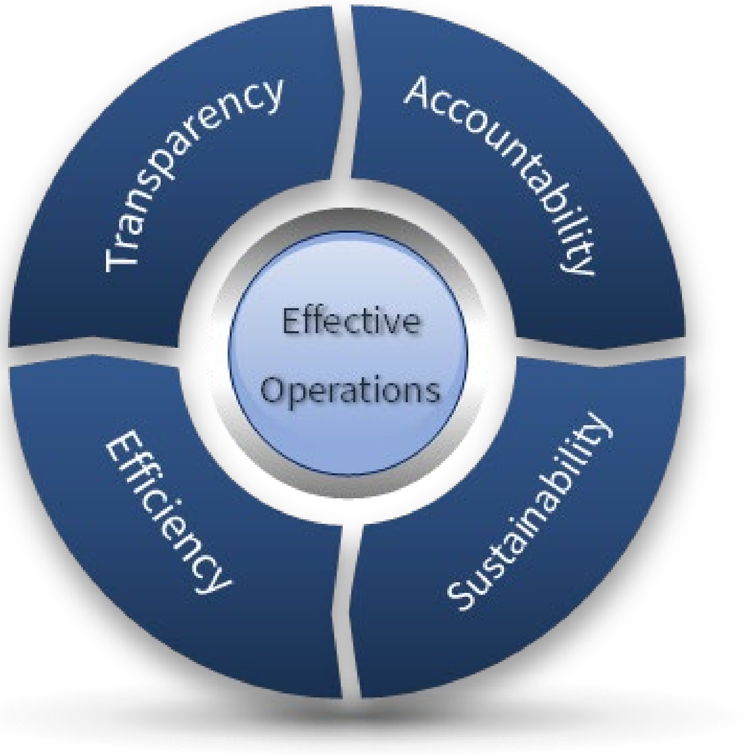
- Counter Terrorism and Homeland Security Threats
- Secure U.S. Borders and Approaches
- Secure Cyberspace and Critical Infrastructure
- Preserve and Uphold the Nation's Prosperity and Economic Security
- Strengthen Preparedness and Resilience
- Champion the DHS Workforce and Strengthen the Department.

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** within the Department's programs and operations can result in a force multiplying effect that advances the Department's mission and secures the Nation from threats.

Transparency is the Department sharing information with citizens and stakeholders. Policy, budget, and programmatic information allows 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 made 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**. Roles and responsibilities should be outlined clearly in strategic guidance (**accountability**).

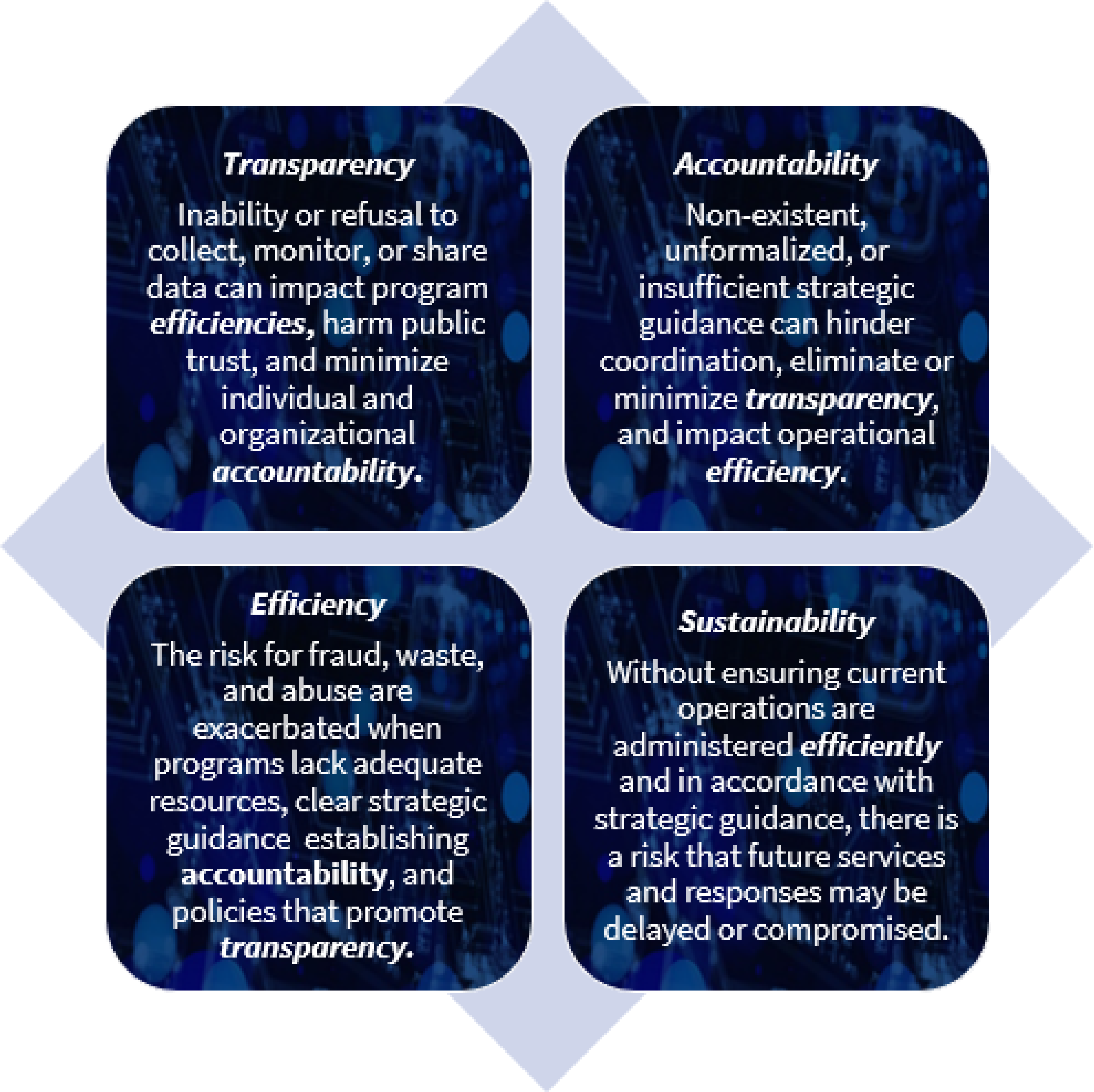
Figure 1: Effective Operations



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 that 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 as necessary to new and emerging threats (**sustainability**).

Sustainability is the Department's ability to support organizational needs and processes, as well as the overarching mission, both now and in the future. **Sustainability** is accomplished 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



Transparency

Inability or refusal to collect, monitor, or share data can impact program ***efficiencies,*** harm public trust, and minimize individual and organizational ***accountability.***

Accountability

Non-existent, unformalized, or insufficient strategic guidance can hinder coordination, eliminate or minimize ***transparency,*** and impact operational ***efficiency.***

Efficiency

The risk for fraud, waste, and abuse are exacerbated when programs lack adequate resources, clear strategic guidance establishing **accountability**, and policies that promote ***transparency.***

Sustainability

Without ensuring current operations are administered ***efficiently*** and in accordance with strategic guidance, there is a risk that future services and responses may be delayed or compromised.

Counter Terrorism and Homeland Security Threats

Components Impacted

All

Related Strategic Priority

7 & 12

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:

- expanding and identifying new operating resources for real-time response and analysis that incorporate multi-modal biometric and analytical tools
- ensuring enhanced technology is available to improve workforce detection capabilities, alarm resolution, and next generation On-Person Screening requirements
- developing automatic vetting engine queries to identify insider threat data
- ensuring information originated from other Intelligence Community agencies needed by our state, local, tribal, territorial, and private sector customers can be provided, and analyzed, on a timely basis at the unclassified level.

DHS Strategic Goal

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.

Recent Office of Inspector General Reports

- DHS Did Not Consistently Comply with National Instant Criminal Background Check System Requirements (OIG-23-05)
- Secret Service and ICE Did Not Always Adhere to Statute and Policies Governing Use of Cell-Site Simulators (REDACTED) (OIG-23-17)
- CBP Released a Migrant on a Terrorist Watchlist, and ICE Faced Information Sharing Challenges Planning and Conducting the Arrest (REDACTED) (OIG-23-31)
- ICE Has Limited Ability to Identify and Combat Trade-Based Money Laundering Schemes (OIG-23-41)

Source: Department

Accountability

Performing essential functions timely is at the core of effective homeland security operations, including sharing actionable intelligence. Countering terrorism and homeland security threats require an aggressive response by the Department and its partners to identify, detect, and prevent attacks on the Nation. To advance this mission, the Department must collect, integrate, analyze, and share actionable intelligence with partners, stakeholders, and senior leaders to inform decisions and operations. Ensuring reliable data is coordinated, timely, and accessible and that modernized technologies are available and used responsibly may improve the Department's ability to counter terrorism and homeland security threats. In instances where organizational responsibilities are not accomplished and result in program **inefficiencies** or minimize **transparency**, Department officials must accept **accountability**. While the Department has taken numerous steps to protect the nation from terrorism and other security threats, enhanced **accountability**, especially in areas where weaknesses were previously identified, could help the Department in meeting its mission goals.

Vulnerabilities Resulting from Accountability Challenges

Department components, along with other Federal agencies, are required to submit complete and accurate certifications detailing the number of records reported to the National Instant Criminal Background Check System, which are then summarized and included in the Department of Justice's (DOJ) required report to Congress. However, OIG found that the Department submitted inaccurate semiannual certifications to DOJ. The Department's submission precipitated an inaccurate semiannual report to Congress and impacted **transparency** between stakeholders.

Prior OIG work further revealed that while **accountable** for collecting and submitting key information to the Federal Bureau of Investigation (FBI), U.S. Customs and Border Protection (CBP) did not always follow established processes. Specifically, CBP is responsible for interdicting migrants suspected of entering the United States without inspection and conducting national security threat screenings. This screening includes collecting and submitting biographical and biometric information to the FBI's Terrorist Screening Center. In one reported instance, CBP used an "Alternative to Detention" technology for tracking and monitoring and released a migrant prior to sharing critical information with the Terrorist Screening Center. Proper reporting would have confirmed a positive terrorist watchlist match before release. In this instance, limited **accountability** of responsibilities bestowed upon the Department impacted program **efficiency**, **sustainability**, and **transparency**, and increased potential risks to national security and public safety.

Further, while some Department components are **accountable** for creating and submitting prohibition records that are essential in conducting background checks on persons purchasing a firearm, work conducted by the OIG revealed that the Department did not submit all required firearms data to DOJ. Specifically, Department components had not consistently ensured that missing disposition information, such as the nature and outcome of criminal proceedings, were updated and did not always respond timely or sufficiently to inquiries. When disposition data, either approving or denying a firearm's sale, is not received within 3 business days, licensed sellers may transfer firearms at their discretion. As such, the lack of **accountability** by the Department led to decreased **transparency** and, in this situation, ultimately increased the risk of a wrongful firearms transfer.

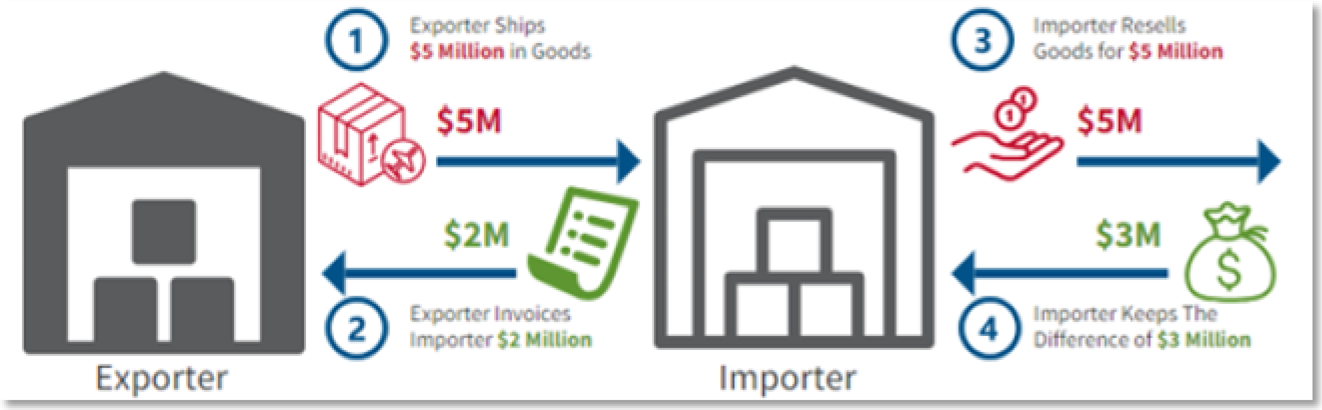
Efficiency

The Department's strategic goal to counter terrorism and homeland security threats focuses on instituting actions that will detect, disrupt, mitigate, and guard against homeland security threats, as well as inform decision makers. To meet these desired outcomes, the Department must ensure **efficiency** within its operations to include deploying its resources, funds, time, and effort.

One aspect of **efficiency** hinges on the Department's development, implementation, and use of technologies that help eliminate administrative burden, improve response time, and aid in criminal investigations, among many other benefits. The Department has a responsibility to the American people to innovate in support of its mission and to do so responsibly and deliberately. However, issues previously reported by OIG highlight **inefficiencies** within the Department as demonstrated by a lack of electronic processes and a less than responsible use of technology.

Vulnerabilities Resulting from Efficiency Challenges

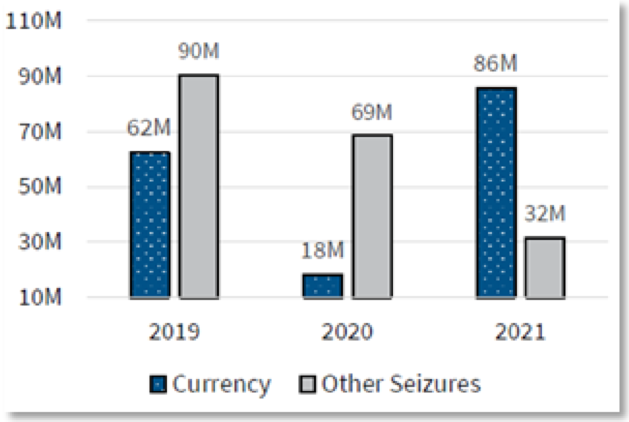
Figure 3: Example of a TBML Scheme


1
Exporter Ships $5 Million in Goods
3
Importer Resells Goods for $5 Million
$5M
$5M
$2M
$3M
2
Exporter Invoices Importer $2 Million
4
Importer Keeps The Difference of $3 Million
Exporter
Importer

Source: OIG depiction of a simple TBML scheme using under-invoicing

ICE's Homeland Security Investigations (HSI) Trade Transparency Unit is responsible for combatting trade-based money laundering (TBML) in the United States. TBML is a scheme that disguises criminal proceeds by using legitimate trade transactions. The Trade Transparency Unit does not have automated technology to identify import commodities at high risk for TBML schemes. Instead, HSI agents identify TBML activities through time-consuming manual searches of import records. Without **efficiencies**, such as resources necessary to analyze and identify suspicious transactions and schemes, TBML-related imports will remain undetected, allowing transnational criminal organizations to continue laundering illicit proceeds to finance activities that threaten national security.

Figure 4: TBML-related Seizures FYs 2019-2021

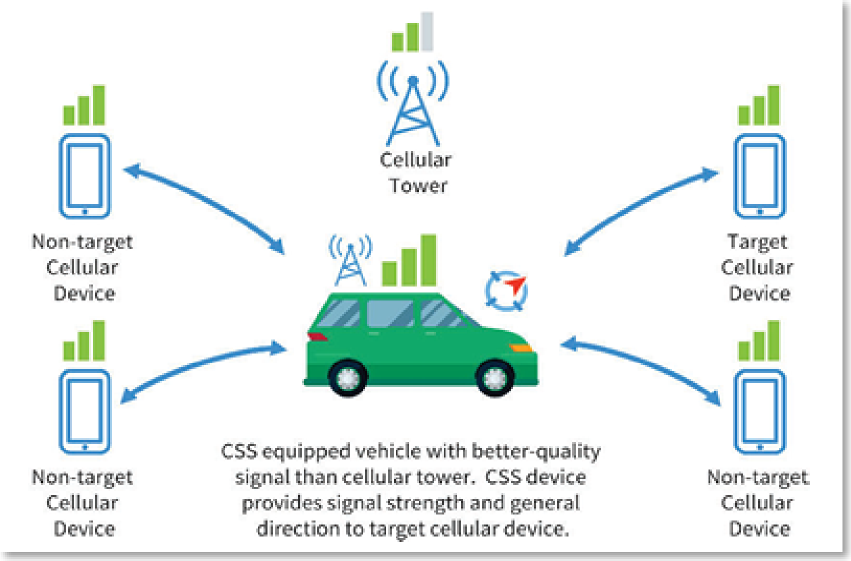


Source: OIG analysis of ICE enforcement statistics

Vulnerabilities Resulting from Efficiency Challenges (continued)

When conducting its work, to include preparation for and ensuing arrests, U.S. Immigration and Customs Enforcement (ICE) officials rely on information contained within migrant Alien Files (A-Files). A-Files contain records of migrants as they move through the immigration process and may include visas, photographs, affidavits, immigration forms, and correspondence. Unfortunately, **inefficiencies** resulting from manual organizational processes exist and in one specific case, this setback resulted in the delayed arrest of a migrant confirmed to be on the Terrorist Watchlist. These **inefficiencies,** reported in prior OIG work, include the untimely receipt of necessary files by ICE personnel and the overabundance of paper A-Files, which can number in the thousands on a weekly basis, all which must be sorted, boxed, and shipped to offices nationwide. Implementing electronic processes could improve program **efficiencies** by ensuring actionable data is readily available to officers in need.

Figure 5: Depiction of CSS


Cellular Tower
Non-target Cellular Device
Target Cellular Device
Non-target Cellular Device
Non-target Cellular Device
CSS equipped vehicle with better-quality signal than cellular tower. CSS device provides signal strength and general direction to target cellular device.

Source: OIG Analysis of CSS Operations

Recent Progress Reported by the Department

The Department reported that it is currently implementing processes to improve program efficiencies, such as transferring migrant documentation electronically and ensuring actionable data is readily available to officers in need.

In contrast, both the United States Secret Service (Secret Service) and ICE HSI implemented advanced technologies to assist in real time location of subjects of criminal investigations and victims. However, the possible exclusion of case evidence, gained through use of these technologies, highlights a need for process **efficiencies** within Secret Service and ICE HSI. Cell-site simulators (CSS) track individuals based on their cellular device location. To ensure compliance with the United States Constitution (i.e., protection from unreasonable searches and seizures by the government), and other applicable statutory authorities, the Department established a policy that incorporates internal controls and **accountability** requirements, such as obtaining warrants and court orders. However, the absence of warrants and court orders in some instances where CSS was used during criminal investigations involving exigent circumstances, highlights **inefficiencies** in the implementation of the Department's policy.

Secure U.S. Borders and Approaches

Components Impacted

CBP, ICE, TSA, USCIS, Coast Guard, HQ/Support

Related Strategic Priority

9 & 10

DHS Strategic Goal

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[3] 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.

Recent OIG Reports

- Intensifying Conditions at the Southwest Border Are Negatively Impacting CBP and ICE Employees' Health and Morale (OIG-23-24)
- Results of an Unannounced Inspection of Northwest ICE Processing Center in Tacoma, Washington (OIG-23-26)
- CBP Facilities in Vermont and New York Generally Met TEDS Standards, but Details to the Southwest Border Affected Morale, Recruitment, and Operations (OIG-23-27)
- Results of Unannounced Inspections of CBP Holding Facilities in the Rio Grande Valley Area (OIG-23-28)
- Results of Unannounced Inspections of CBP Holding Facilities in the Yuma and Tucson Areas (OIG-23-29)
- Results of an Unannounced Inspection of ICE's Stewart Detention Center in Lumpkin, Georgia (OIG-23-38)
- CBP Outbound Inspections Disrupt Transnational Criminal Organization Illicit Operations (REDACTED) (OIG-23-39)
- USCIS Has Generally Met Statutory Requirements to Adjudicate Asylum Applications from Paroled Afghan Evacuees (OIG-23-40)
- CBP Could Do More to Plan for Facilities Along the Southwest Border (OIG-23-45)
- DHS Does Not Have Assurance That All Migrants Can be Located Once Released into the United States (OIG-23-47)
- Results of Unannounced Inspections of CBP Holding Facilities in the El Paso Area (OIG-23-50)

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

- changing job requirements and policy shifts, such as domestic immigration policy
- challenging work locations
- hiring issues due to public perception of law enforcement and burdensome processes to vet and onboard new personnel
- scaling up operations to meet increased program demand.

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

Transparency

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 from terrorism and illegal entry of persons and facilitates the flow of legitimate travelers and trade under immigration, customs, and other laws. The Department may detain people who are inadmissible, deportable, or subject to criminal prosecution in short- and long-term detention facilities, as appropriate. Ultimately, the Department is responsible for repatriating, releasing, or transferring detainees to other agencies. Ensuring internal controls are applied and resources are made available to protect Department staff and detainees, alike, is essential to supporting mission requirements.

Maintenance and availability of accurate records are vital when informing stakeholders, including Congress, on program efforts. Challenges in **transparency** are highlighted by the Department's inability to provide data and information to support decisions and ongoing efforts related to securing the U.S. borders.

Vulnerabilities Resulting from Transparency Challenges

In conducting its mission responsibilities, the Department employs multiple systems of record (SORs), such as the Unified Secondary System utilized to process individuals entering the United States at ports of entry, and the "e3" portal used 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 in the appropriate electronic system(s) of record as soon as practicable." While accurate, complete, and consistent data is critical for CBP to monitor the care of detainees and to ensure compliance with TEDS and other applicable standards, data integrity issues within these SORs have been a recurring theme for CBP. For example, migrants no longer at facilities remained on roll call reports which should list only detainees currently in custody. Additionally, meals and showers were erroneously logged, and health interviews and medical assessments were not properly documented. Unreliable data and inaccurate reporting of detention conditions further highlight the Department's **transparency** challenges.

ICE is required to complete the detainee classification process and initial housing assignments within 12 hours of a detainee's admission to a facility. However, while ICE time stamped admission documentation, it did not time stamp classification forms, making it impossible to calculate the time elapsed between admission and classification. As a result, there is no **transparency** or assurance that ICE adhered to standards put in place to protect detainee's safety and security.

Figure 6: Individuals at the Limit Line Waiting to Enter the United States

Source: OIG photo

Vulnerabilities Resulting from Transparency Challenges (continued)

The Department is responsible for creating and preserving records that document decisions, procedures, and essential transactions for programs such as detainee facility planning. In 2019, because of spikes in migrant encounters, CBP began awarding contracts for temporary soft-sided facilities to supplement its existing permanent facilities. Over a 4-year period, CBP funded more than $1.27 billion in contract task orders for temporary facilities. However, although a significant decline in migrant encounters began in March 2020, CBP did not reassess needs or consider alternatives for temporary facilities and did not consistently document whether cost-benefit analyses were conducted to support informed decision-making regarding the need for facilities, potentially expending more funds than necessary. Further, when requested, the Department was unable to provide sufficient documentation to support decisions it made regarding planning for detention facilities. The advantage of conducting cost benefit analyses to ensure prudent spending of taxpayer dollars was underscored in May 2022, when CBP concluded that temporary facilities are a cost-effective solution if anticipated utilization is under 6 years, at which point CBP could have funded a permanent facility. Unfortunately, these analyses are not a consistent part of CBP's facilities planning process and, in this instance, were only conducted to address a congressional request. As a result, CBP decisions regarding detention facilities may not represent the best interest of taxpayers or be an **efficient** use of taxpayer funding.

Recent Progress Reported by the Department

The Department reported receiving appropriations in fiscal year 2022 to construct two permanent joint processing centers to reduce reliance on temporary facilities.

CBP's Office of Field Operations is responsible for protecting the American people, safeguarding the Nation's borders, and enhancing U.S. economic prosperity at 328 ports of entry at land, air, sea, and preclearance locations. To support its mission, CBP deploys a series of video surveillance cameras, including at land ports of entry (LPOE), which feed into centralized video surveillance systems monitored at command centers and workstations. Per CBP policy, video surveillance systems, including those at LPOEs, are to have an uninterruptible power supply and be designed to operate 24 hours a day, 7 days a week. However, some LPOEs and a command center were not connected to adequate emergency back-up power and experienced multiple power outages, one lasting more than 24 hours. Inadequate emergency power during an outage eliminates **transparency** in sharing potentially critical information and poses real-time, significant security and safety risks for the traveling public, CBP employees, and supporting workforce in impacted LPOE areas. For instance, power outages limit information available to CBP and law enforcement in the event of a significant security, operational, or integrity incident. Additionally, extended power outages impact CBP's ability to **efficiently** process and vet travelers.

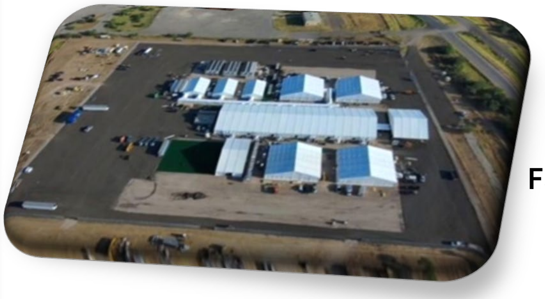


Figure 7: Soft-Sided Facility at Laredo, Texas

Source: CBP website as of February 3, 2023

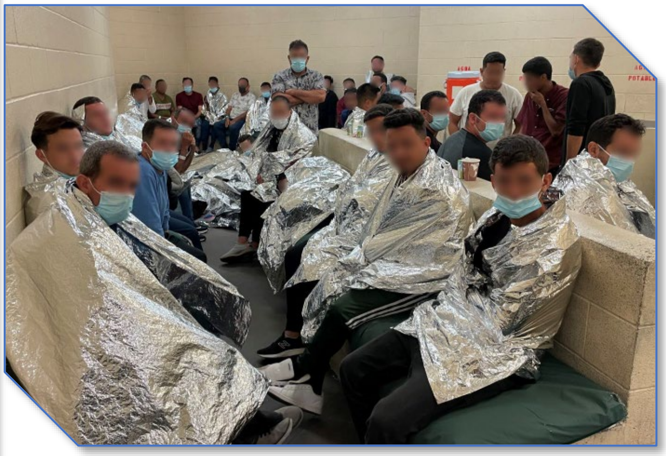
Accountability

Enforcing immigration laws focused on protecting national security is critical, especially as an increasing number of migrants are entering the United States and are subsequently detained or released into the country. The Department issues standards to guide the safety, security, and care for detainees while in custody. In addition, the Department requires critical information to locate migrants after they are released to administer immigration enforcement actions or provide notifications of upcoming immigration proceedings and court hearings.

Vulnerabilities Resulting from Accountability Challenges

When CBP detains people who are inadmissible to the United States or subject to criminal prosecution, it relies on TEDS, which incorporates best practices and reflects 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, the *Performance-Based National Detention Standards 2011*, (PBNDS 2011), revised in 2016, sets expectations for various services ICE is required to provide to detainees, such as medical and mental health services, legal services, communication services for noncitizens with limited English proficiency, a grievance process, and more. Although the Department is **accountable** for complying with these standards, its components do not consistently meet requirements put in place to ensure the safety, security, and care for detainees and facility staff.

Figure 8: Detainees in Overcrowded Cell



Source: OIG photos

Table 1: Detainee Time in Custody for Three CBP Facilities Inspected in FY 2023

Total Detainee Population	Number over 72 Hours	Percentage over 72 Hours
5,535	**2,833**	**51.2%**

Source: Based on analysis of CBP data in OIG Reports (OIG-23-03, OIG-23-28, OIG-23-29)

Table 2: CBP Facilities Over Maximum Capacity

CBP Facility (Month and Year of Inspection)	Detainee Population	Maximum Facility Capacity	Percentage of Facility Capacity
El Centro Border Patrol Station (March 2022)	297	291	102%
Yuma Centralized Processing Center (July 2022)	1,689	875	193%
Tucson Coordination Center (November 2022)	143	100	143%
El Paso Modular Centralized Processing Center (November 2022)	1,903	1,040	183%

Source: Based on analysis of CBP data in OIG Reports (OIG-23-03, OIG-23-29, OIG-23-50)

Based on OIG inspections conducted in fiscal year 2023, four facilities exceeded maximum facility capacity, including some holding cells near or over 200 percent capacity. Additionally, for three of the facilities reviewed, 51 percent (or 2,833) of the total detainees in custody exceeded the 72-hour TEDS standards (see Tables 1 and 2).

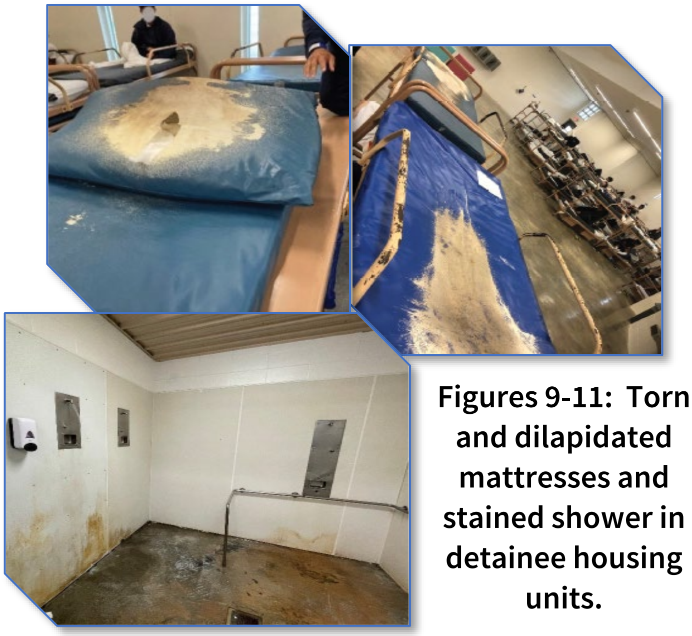
Vulnerabilities Resulting from Accountability Challenges (continued)

ICE Facilities inspected did not comply with PBNDS 2011 requirements, such as with Staff-Detainee Communication and Grievance System requirements. Table 3 provides a sample of non-compliance with detention standards published in OIG's FY 2023 Inspection Reports.

Table 3: PBNDS 2011 Total Requirements Violated by ICE Facility Inspected

Port Isabel Service Center	Richwood Correctional Center	Northwest ICE Processing Center	Stewart Detention Center	Caroline Detention Facility
7	5	4	5	8

Source: Based on analysis of ICE data in OIG Reports (OIG-23-13, OIG-23-18, OIG-23-26, OIG-23-38, OIG-23-51)



Figures 9-11: Torn and dilapidated mattresses and stained shower in detainee housing units.

Source: OIG photos

In accordance with PBNDS 2011, facilities are required to provide medical and support personnel sufficient to perform duties, such as initial health screenings, preventative care, diagnoses, health education, and treatments. ICE is **accountable** for ensuring adequate medical care is provided to detainees. However, some ICE detention facilities do not have medical staff necessary to accommodate the contracted minimum population or its maximum capacity. ICE's inability to provide the appropriate number of medical staff highlights an ongoing challenge in ensuring medical care standards are met at ICE facilities across the country.

Between March 2021 and August 2022, CBP apprehended more than 1.3 million migrants illegally entering the United States across the Southwest border. Under various authorities, certain non-citizens, on a case-by-case basis, can be released into the United States. The Department released more than 1 million migrant individuals and families during that same period, March 2021 to August 2022. Department personnel are **accountable** for obtaining and verifying post-release addresses when processing migrants for release. However, while **accountable** for obtaining this critical information, more than 54,000 address records were left blank for the period reviewed. Additionally, more than 177,000 migrant records contained missing, invalid, or not legitimate residential locations. According to the Department, CBP's ability to obtain address information is contingent on migrants providing a valid address, which is not always possible. As such, valid addresses for migrants were not always received, recorded, or validated prior to their release into the United States. As a result of incomplete or invalid information, ICE may be unable to locate migrants to administer immigration enforcement actions, such as arresting individuals who pose potential threats to national security, issuing final orders of removal, or providing notifications of upcoming immigration proceedings and court hearings. With the number of migrants entering the United States increasing and because CBP must release migrants in cases where the migrant does not have an address or the address is unhabitable, **accountability** related to address validation will likely remain a challenge in the future.

Efficiency

The ability to provide and use resources is key to advancing the Department's mission. However, the Department struggles to properly staff program functions, advance technology, and minimize waste, hampering its efforts to **efficiently** maintain the safety and security of U.S. borders. Shifts in U.S. immigration and border policies, migrant surges, the COVID-19 pandemic, and the overall rising number of migrant encounters along the Southwest border have resulted in a significant increase in CBP and ICE workloads. For instance, the continual surge in encounters at the Southwest border emphasizes the vital need for appropriate levels of law enforcement personnel. However, the Department's mission needs are currently outpacing its ability to timely recruit, hire, and retain personnel with the right skills and expertise, impacting its ability to **efficiently** address mission needs and adapt to the everchanging environment on the Southwest border. Additionally, in the Department's APR, CBP reported that negative public perception of law enforcement, undesirable job locations, and burdensome processes to vet and onboard new personnel hinder the hiring process (**sustainability**).

Vulnerabilities Resulting from Efficiency Challenges

Despite significant increases in CBP and ICE workloads, staffing levels remain stagnant. Solutions employed by the Department impact **efficiency** in conducting mission responsibilities and highlight challenges with **accountability** and **sustainability**. As a result of stagnant staffing levels, detail opportunities and overtime are used to temporarily address border encounters; however, as previously reported in other OIG reports, these techniques negatively impact the health and morale of law enforcement personnel. Specifically, employees reported feeling overworked and unable to perform their primary law enforcement duties (**accountability**). Increased workloads and low morale have the potential to result in higher employee turnover, further exacerbating staffing issues. Overall, the temporary solutions employed by the Department limit CBP and ICE's ability to perform their mission (**efficiency**) and raise questions as to their **sustainability**.

Source: CBP

Recent Progress Reported by the Department

The Department reported in its APR that ICE requested direct-hire authority to address staffing challenges and seeks multi-year dedicated permanent-change-of-station funding to align investigative resources geographically to mission requirements.

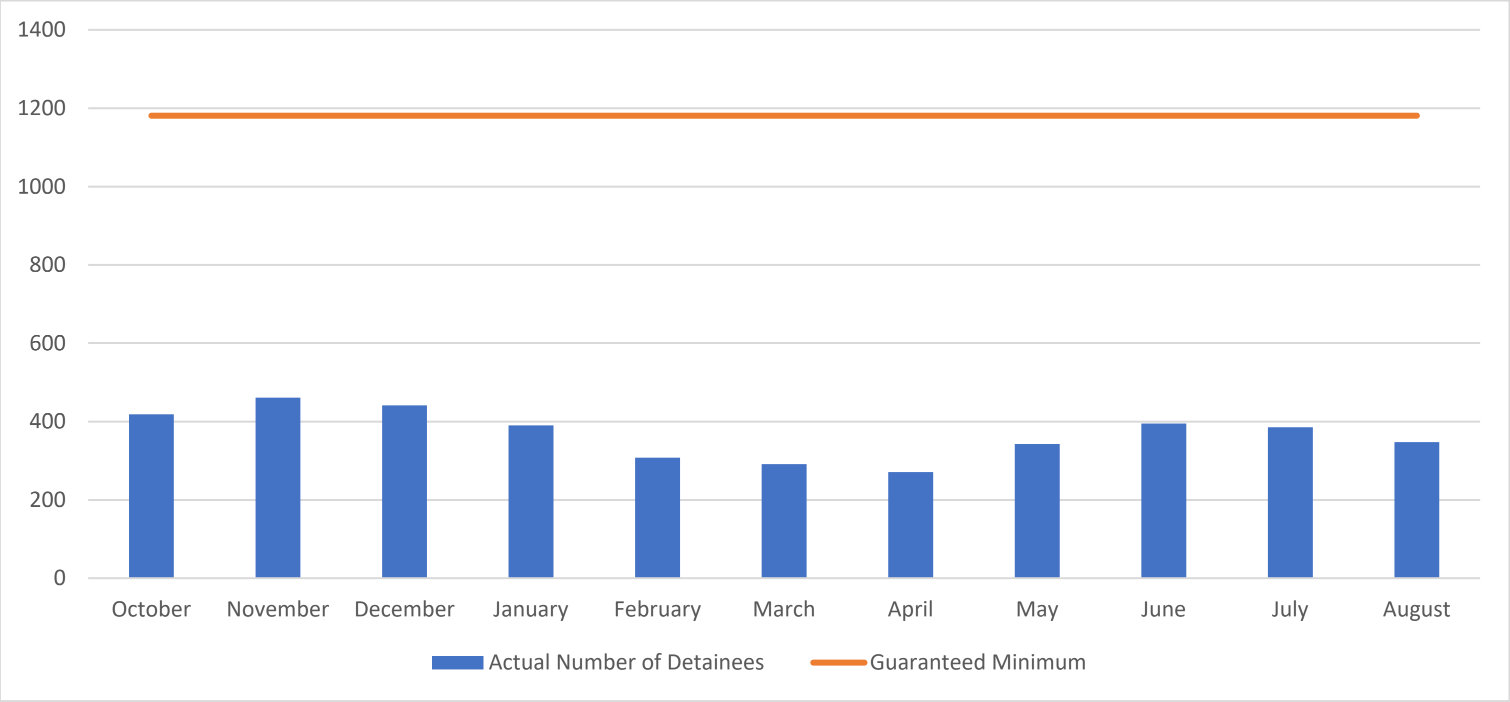
Further, CBP's continued reliance on detailed law enforcement personnel impacted its ability to effectively conduct mission operations. CBP's movement of northern border agents to the Southwest border limited the scheduling of staff for significant enforcement operations, including disrupting cross-border smuggling and assisting with criminal cases (**accountability**). Additionally, an increased reliance on mandatory staff details to the Southwest Border could affect custodial operations, to include CBP's ability to adhere to TEDS timely transfer standards from short-term holding facilities (**efficiency**).

Vulnerabilities Resulting from Efficiency Challenges (continued)

As previously noted, challenges specific to detainee facility planning existed within the Department because of its inability to provide data and information to support critical decisions. However, **efficiency** challenges, exacerbated by limited **transparency**, resulted in some detainee facilities maintaining fewer subjects in custody than capacity limits allowed, while others consistently exceeded their holding capacity. This lack of **efficiency** resulted in the Department potentially spending money on facilities that are not cost effective and in the best interest of taxpayers.

The unnecessary expenditure of more than $61 million in taxpayer funds indicates less than effective management of facilities contracts for detention of migrants. ICE Enforcement and Removal Operations oversee roughly 130 detention facilities which are managed in conjunction with private contractors, state, or local governments. These ICE established facility contracts ensure a fixed daily rate minimum payment to the contractor. As part of unannounced inspections, OIG determined that these funds were dispersed for unused bed space under the guaranteed minimum for a 1-year period. Table 4 illustrates a noticeable and costly gap between the actual number of detainees at Northwest ICE Processing Center compared with the facility's guaranteed minimum. Detention of migrants is critical for ensuring **efficient** border security operations; however, consideration of alternatives or reassessment of facility contracts may be necessary to remediate **inefficiencies** related to facility cost.

Table 4: Average Monthly Detainee Population Compared with the Contracted Guaranteed Minimum at Northwest during fiscal year 2022



Source: OIG analysis of ICE data

Vulnerabilities Resulting from Efficiency Challenges (continued)

Paper-based processes can eliminate organizational resource **efficiencies**, such as those associated with increased staffing, time expended, and costs incurred. In August 2021, the Department was designated to lead and coordinate Operation Allies Welcome, to support Afghans resettling in the United States after the collapse of the Afghan central government. Asylum applications are required to be processed within three business days; however, as a result of paper-based processes and the high application volume, one United States Citizenship and Immigration Services (USCIS) processing center reported a 5-month processing delay and a backlog of 30,000 asylum applications. These delays highlighted the need for implementing **efficiencies** in the asylum application process.

Recent Progress Reported by the Department

In November 2022, online filing for asylum applications became generally available. The process changes USCIS implemented improved the ***efficiency*** *of receiving and entering applications and reduced data entry delays and backlog.*

Sustainability

Adequate program oversight allows the Department to effectively manage programs and make informed decisions to ensure mission operations are **sustainable**. Yet, in many instances, the Department had not formalized comprehensive approaches to carry out program functions. Developing and implementing comprehensive plans can help ensure the Department expends monies in the best interest of taxpayers, is better prepared for future migrant surges, and is better positioned to avoid overcrowding and inhumane conditions. Through enhanced oversight and implementing consistent and **efficient** practices, the Department could recognize greater **sustainability** in critical border operations.

Vulnerabilities Resulting from Sustainability Challenges

Figure 12: Firearms Warning

Source: OIG photo

CBP does not currently have a nationwide program that ensures inspection of outbound personal vehicles and pedestrians at land border crossings are consistent and effective in preventing the illegal exportation of currency, firearms, explosives, ammunitions, and narcotics. However, as previously identified, when applied consistently, outbound inspections are an effective tool to deter criminal activity.

Recent Progress Reported by the Department

CBP reported that it is developing a final comprehensive policy that incorporates planning for temporary and permanent detention facilities along the Southwest border.

Secure Cyberspace and Critical Infrastructure

Related Strategic Priority
8

Components Impacted

CISA, FEMA, ICE, TSA, Coast Guard, Secret Service, HQ/Support

DHS Strategic Goal

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.

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:

- addressing existing and future threats such as degradation of critical infrastructure and evolving technology
- hiring and onboarding staff
- planning for increasingly complex cyber incidents and defending against cybercriminals operating overseas with impunity, enabled by nation-states.

Recent OIG Reports

- CISA Made Progress but Resources, Staffing, and Technology Challenges Hinder Cyber Threat Detection and Mitigation (OIG-23-19)
- Evaluation of DHS' Information Security Program for Fiscal Year 2022 (OIG-23-21)
- Evaluation of DHS' Compliance with Federal Information Security Modernization Act Requirements for Intelligence Systems for Fiscal Year 2022 (OIG-23-30)
- FEMA Did Not Always Secure Information Stored on Mobile Devices to Prevent Unauthorized Access (OIG-23-32)
- ICE Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information (OIG-23-33)
- Cybersecurity System Review of the Transportation Security Administration's Selected High Value Asset (OIG-23-44)
- Homeland Advanced Recognition Technology System Compliance with 28 C.F.R. Part 23 (OIG-23-53)

Accountability

Protecting and enhancing the security and resilience of the Department's cyber systems and critical infrastructure by modernizing efforts, deploying protective capabilities, engaging with stakeholders, prioritizing risk management activities, responding to emerging dangers, and holding criminals accountable is critical in achieving Agency mission goals. Cyberattacks are disruptive and can impair the **sustainability** of mission essential operations. The Department is **accountable** for safeguarding against unauthorized access to systems by ensuring internal controls are implemented and monitored to boost program **efficiencies** and reduce the risk of cyberattacks and sensitive information exposure.

To ensure adequate protection of data held by the government, Congress enacted the *Federal Information Security Modernization Act of 2014* (FISMA). FISMA requires agencies to develop, document, and implement appropriate safeguards to ensure delivery of critical services. Following its fiscal year 2022 evaluation, the Department was rated 2 of 5 in the Data Protection and Privacy domain, indicating policies, procedures, and strategies are formalized and documented, but not consistently implemented. Implementing policies, procedures, and strategies are critical in establishing **accountability** within an organization.

Vulnerabilities Resulting from Accountability Challenges

As previously reported by OIG, the Department had not consistently implemented effective controls to prevent unauthorized access to systems and information. For instance, the Department had not managed and removed access when personnel separated or changed positions, documented and timely sanitized electronic devices, or applied and updated required security settings. Further, the Department had not addressed infrastructure and workstation vulnerabilities, or sufficiently managed service accounts susceptible to password compromise. Encryption of sensitive data can mitigate against the impact of a breach, should one occur. However, the Department has not fully encrypted personally identifiable information and other sensitive data.

Recent Progress Reported by the Department

According to the Department, it reported to Office of Management and Budget in September 2023, that compliance with Executive Order 14028, Improving the Nation's Cybersecurity, was above 95% for multi-factor authentication, encryption of data at rest, and data in transit.

Source: ICE

Efficiency

According to the *National Cybersecurity Strategy*, there are hundreds of thousands of unfilled vacancies in cybersecurity positions nationwide, and this gap continues to grow. In the federal realm, hiring and retaining top cyber professionals that possess the technical skills and specialized experience required is further exacerbated by a highly competitive and well-paid private market. The Department's mission execution depends on a properly staffed organization with the skills, competencies, and performance capabilities necessary to meet cybersecurity challenges. A multiyear strategic workforce plan can ensure the Department hires staff with the relevant knowledge, skills, and abilities to achieve goals and address workforce needs.

Vulnerabilities Resulting from Efficiency Challenges

The *Cybersecurity and Infrastructure Security Agency Act of 2018* designated the Cybersecurity and Infrastructure Security Agency (CISA) as the operational lead for Federal cybersecurity with responsibilities such as heading the national effort to understand, manage, and reduce risks to cyber and physical infrastructure. However, CISA has not hired enough staff to execute its mission, including supporting cyberattack response and mitigation efforts. As of August 2022, CISA was understaffed, with less than half of its authorized, full-time positions filled. Specifically, only 1,201 of its 3,260 allocated positions were staffed. Similarly, its Cybersecurity Division, primarily responsible for defending against cyberattacks and responding to cyber incidents, was 38 percent understaffed. CISA's Office of Chief Human Capital Officer (**accountability**) had not completed a plan (**efficiency**) that would identify workforce gaps and develop strategies and implementation plans (**transparency**), as required; as a result, CISA may not effectively coordinate Federal response efforts (**efficiency** and **sustainability**).

Recent Progress Reported by the Department

In late 2021, the Department officially launched its Cybersecurity Talent Management System (CTMS) to address historical and ongoing challenges recruiting and retaining individuals with skills necessary to execute the Department's dynamic cybersecurity mission. Currently, CISA, the Department's Office of the Chief Information Officer (OCIO), *and the Federal Emergency Management Agency (FEMA) have been granted authority to use CTMS to hire cyber personnel.*

CISA developed a workforce planning strategy that defines workforce goals, objectives, and priorities.

CISA reported a significant increase in hiring since August 2022. According to CISA, as of the end of fiscal year 2023, almost 83% of its full-time positions have been filled.

Sustainability

Part of CISA's cybersecurity mission is to defend and secure cyberspace by leading national efforts to drive and enable effective national cyber defense. To execute its mission, it must fortify cyber defenses against immediate threats and vulnerabilities and build the Nation's long-term capacity to withstand and operate through cyber incidents. CISA's ability to **sustain** its mission depends on ensuring adequate staff, processes, and technology.

Vulnerabilities Resulting from Sustainability Challenges

Recent Progress Reported by the Department

In April 2023, the Department established its first task force dedicated to artificial intelligence (AI) to advance the application of AI to critical homeland security missions in four priority initiatives:

- Enhance the integrity of supply chains and the broader trade environment
- Leverage AI to counter the flow of fentanyl into the United States through better detection methods and disruption of criminal networks
- Apply AI to digital forensic tools to help identify, locate, and rescue victims of online child exploitation and abuse, and to identify and apprehend the perpetrators
- Work with partners in government, industry, and academia, to assess the impact of AI on our ability to secure critical infrastructure.

The SolarWinds breach revealed that CISA was not well-equipped to meet its current and evolving cyber intrusion detection and mitigation responsibilities. Specifically, CISA's SolarWinds response efforts were impacted by not having needed resources, staffing, and plans. For instance, CISA did not have an alternative communication system to use when its main network was compromised, enough staff to achieve its mission, or the secure space necessary to effectively work with available intelligence. In its after-action report, CISA identified gaps in technologies and capabilities needed for cyber incident prevention, detection, and mitigation. Although CISA's capabilities have improved since the SolarWinds breach, any operational or technological gaps may reduce its ability to detect and mitigate threats. Staffing shortages also affect CISA's future development of cyber capabilities. Until CISA's cyber capabilities are fully operational, the Federal Government cannot fully benefit from the cybersecurity protections CISA provides. As a result, the confidentiality, integrity, and availability of Federal data and networks remain at risk at a time when the United States is facing a growing number of increasingly sophisticated cyber threats.

Preserve and Uphold the Nation's Prosperity and Economic Security

Related Strategic Priority

7 & 8

Components Impacted

CBP, ICE, TSA, Coast Guard, Secret Service, HQ/Support

DHS Strategic Goal

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.

Source: Department

Recent OIG Reports

- ❖ The United States Coast Guard Needs to Determine the Impact and Effectiveness of Its Streamlined Inspection Program (OIG-23-46)
- ❖ CBP's Management of International Mail Facilities Puts Officer Safety and Mission Requirements at Risk (OIG-23-48)
- ❖ CBP Did Not Effectively Conduct International Mail Screening or Implement the STOP Act (REDACTED) (OIG-23-56)

The Department's recent APRs include numerous challenges and risks its components face relating to their ability to preserve and uphold the Nation's prosperity and economic security, including but not limited to:

- ❖ defining capability needs associated with cybersecurity for the Electronic Baggage Screening Program
- ❖ ensuring industry continues to develop new technologies that will improve threat detection capabilities
- ❖ rapidly changing climate yields significant weather events with increasing frequency and severity, requiring more forces to surge to events to serve the American people.

Transparency

Key performance indicators (KPI) promote improved federal management and greater **efficiency** and effectiveness by providing a focus for strategic and operational improvement and encouraging data-based decision-making. Federal agencies are required to set goals and report annually on performance regarding program operations. Developing, implementing, and monitoring KPIs can help the Department understand resource needs and ensure program operations are being performed as expected. However, some Federal programs have not established or implemented KPIs.

Vulnerabilities Resulting from Transparency Challenges

Coast Guard offers a Streamlined Inspection Program (SIP) as an optional, alternative inspection program to verify U.S. documented or U.S. registered vessels follow regulations while maintaining a high level of safety. Although required to establish goals and objectives to ensure compliance with relevant regulations, accurate reporting, and effective and **efficient** operations, SIP has not established or implemented KPIs or conducted evaluations on outcomes that would demonstrate it is operating as intended to safeguard U.S. Waterways. Additionally, data reported on SIP enrollment, deficiencies detected, and casualties were not always accurate and reliable.

SIP Goals and Benefits

- Operations in continual compliance with regulations
- Better management of vessel costs
- Increased involvement and responsibility by vessel personnel
- Increased crew professional advancement

Source: Marine Safety: Domestic Inspection programs, COMDTINST 16000.71, September 2021

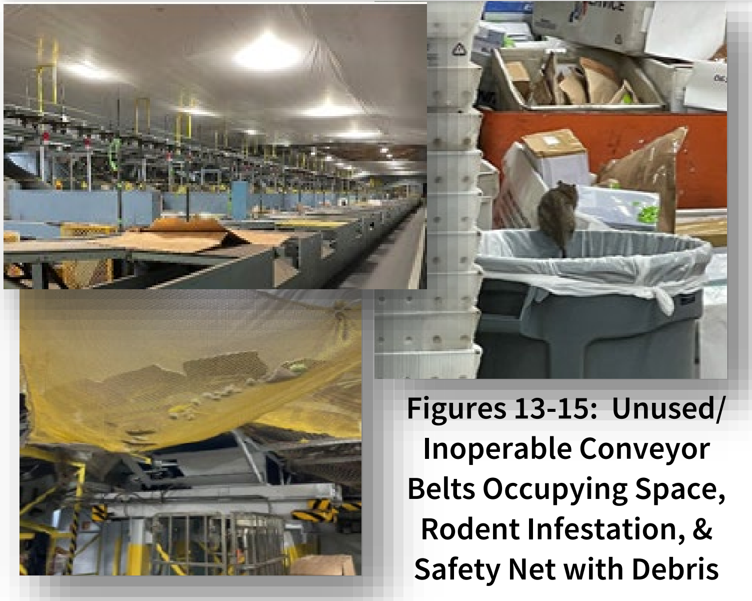
Source: Department

Accountability

CBP plays a critical role in the Nation's efforts to safeguard the American public by interdicting drugs entering the United States, including through international mail inspected at International Mail Facilities (IMFs). Assessing the condition, function, and overall performance of existing facilities can help the Department identify deficiencies, including life safety issues. The Office of Facilities and Asset Management (OFAM) manages CBP's portfolio of owned and leased real property, including IMFs, and is responsible for actively managing facility leases and providing support and review of facility assessments. CBP's regular review of these assessments can help ensure programmatic **efficiencies**, such as facility condition and functionality and optimization of terms and costs.

Vulnerabilities Resulting from Accountability Challenges

CBP hired a contractor to assess eight IMFs and prepare facility assessment reports; subsequently, the contractor notified OFAM of life safety deficiencies and critical maintenance issues at 7 of the 8 IMFs. Although OFAM was aware of deficiencies raised in facility assessment reports and is **accountable** for managing property and ensuring an appropriate level of use, these deficiencies were generally left unresolved and had not been communicated to staff at IMFs. These issues occurred because OFAM did not prioritize monitoring and resolving facility deficiencies and other maintenance issues at IMFs. The lack of communication regarding these deficiencies left staff unaware of potential facility hazards and threatened officer safety. Additionally, OFAM had not taken action to effectively renegotiate space agreements to house its IMFs. Specifically, CBP paid $3.2 million for unusable space at two IMFs and operated without a space agreement at a third IMF. Guidance requires components to **efficiently** use available space and conduct regular reviews to identify property that is underutilized or does not align with mission or intended use. Leasing partial unusable space and operating without a lease agreement are **inefficient** use of Government resources, and in some cases impacted operations, potentially allowing drugs and other illicit items to enter the United States.



Figures 13-15: Unused/ Inoperable Conveyor Belts Occupying Space, Rodent Infestation, & Safety Net with Debris

Source: OIG, General Services Administration, and CBP

Table 5: IMF Assessment Deficiencies

IMF	# of Deficiencies	# of Critical or Life Safety Deficiencies
Chicago	17	3
Honolulu	12	1
JFK	6	1
Los Angeles	9	2
Miami	4	2
Newark	7	1
San Juan	11	0
U.S. Virgin Islands	4	1

Source: OIG analysis of CBP facility assessments and OFAM responses

Strengthen Preparedness and Resilience

Components Impacted

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

Related Strategic Priority

11

Recent OIG Reports

- FEMA Did Not Provide Sufficient Oversight of Project Airbridge (OIG-23-14)
- FEMA Should Increase Oversight to Prevent Misuse of Humanitarian Relief Funds (OIG-23-20)
- FEMA Did Not Effectively Manage the Distribution of COVID-19 Medical Supplies and Equipment (OIG-23-34)
- FEMA Continues to Make Improper Reimbursements through the Presidential Residence Protection Assistance Grant Program (OIG-23-37)
- Ineffective Controls Over COVID-19 Funeral Assistance Leave the Program Susceptible to Waste and Abuse (OIG-23-42)
- FEMA's Technological Hazards Division Assisted State, Local, and Tribal Governments in Preparing to Respond to Radiological and Chemical Incidents (OIG-23-49)

Source: Department

DHS Strategic Goal

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 cyber attacks, 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.

Accountability

Ensuring project requirements have sufficient controls in place to hold contractors or other parties **accountable** is critical when the Department acquires services for program operations. The Department owns the outcomes of project operations and is **accountable** for providing oversight, including training and guidance. However, FEMA experienced challenges overseeing programs related to disaster resilience, hindering its ability to accomplish its mission **efficiently** and effectively.

Vulnerabilities Resulting from Accountability Challenges

FEMA did not provide sufficient oversight of Project Airbridge, a COVID-19 initiative. Project Airbridge was established to mitigate disruptions in global medical supply chains and was intended to be used as a temporary measure to address perceived shortfalls in distributors' personal protective equipment inventories. However, the project actually supplemented the distributors' already large domestic inventory. FEMA, with its limited understanding of commercial supply and demand, did not sufficiently assess whether medical supply distributors needed Project Airbridge to stabilize their supply chains or implement controls to enforce compliance with memorandums of understanding. Further, because it did not have sufficient controls to hold the distributor **accountable**, FEMA expended more than $238 million that may have been better spent on other COVID-19 initiatives. These costs resulted from transporting personal protective equipment not always necessary to meet distributors' needs and delivering to locations not in need of equipment.

FEMA further experienced **accountability** challenges associated with the implementation of effective controls over the COVID-19 Funeral Assistance Program. FEMA acquired the services of a call center contractor to assist with processing the large volume of COVID-19 Funeral Assistance applications. However, it did not always provide its contractor with the guidance and training required to adequately monitor its performance, contributing to FEMA issuing questionable awards for an estimated 41,696 Funeral Assistance applications.

Example of Exceptional Department Accountability

Through the Radiological Emergency Preparedness Program and the Chemical Stockpile Emergency Preparedness Program, FEMA's Technical Hazards Division is **accountable** for and has taken appropriate actions during fiscal years 2018 through 2021 to assist state, local, and tribal governments with preparing to respond to radiological and chemical incidents. These actions are consistent with program requirements, related laws and regulations, and FEMA's responsibilities under two Memorandums of Understanding.

Figures 16 & 17: Radiological and Chemical Emergency Preparedness Exercises

Source: FEMA

Efficiency

Congress holds FEMA **accountable** for administering and overseeing the **efficient** use of funds it appropriates to assist or reimburse eligible entities or individuals or provides for a wide range of preparedness and resilience programs. In turn, FEMA issues application guidance to administer the appropriate use of funding, such as eligibility criteria, documentation requirements, allowable expenses, and maximum award amount, if applicable. Accordingly, government entities and individuals submit applications for assistance or reimbursement to FEMA for review, a determination is made as to applicant eligibility, and funds are issued based on allowable expenses and maximum award, if applicable. However, FEMA did not always manage its disaster and non-disaster assistance funds to ensure financial **accountability** and safeguarding of the funds, hindering its ability to **efficiently** accomplish its mission. For instance, it did not always review expenses in accordance with its policies.

Vulnerabilities Resulting from Efficiency Challenges

Approximately $24.4 million in ineligible expenses were issued as part of FEMA's COVID-19 Funeral Assistance funds. An additional $1.3 million was issued to multiple parties for the same decedent and over $550,000 was awarded for applications that exceeded the $9,000 per decedent maximum. Further, FEMA inconsistently applied documentation review guidance when calculating and issuing awards resulting in an additional almost $600,000 questioned cost. OIG surveyed all FEMA caseworkers assigned to process COVID-19 Funeral Assistance applications; nearly a third of responses ranged from neutral to strong disagreement that FEMA prepared respondents to perform their roles with both program-specific training and guidance on processing applications. In total, OIG identified over $26.9 million in questioned costs related to the COVID-19 Funeral Assistance program, highlighting FEMA's less than **efficient** use of taxpayer funding.

The Office of Management and Budget requires each agency's OIG to review the agency's payment integrity reporting; an agency must meet all 10 Payment Integrity Information Act requirements to be considered compliant. Although the Department complied with 9 of the 10 requirements, it did not ensure that the improper payments risk assessment methodology used adequately concluded whether a program was likely to make improper and unknown payments above or below the statutory threshold.

"…the Department concluded FEMA's Funeral Assistance program was unlikely to make improper or unknown payments."

This was inconsistent with OIG's conclusion, which indicated the program is at high risk for improper payments, fraud, waste, and abuse.

FEMA also administered Presidential Residence Protection grants to local law enforcement agencies, reimbursing $8.9 million for unallowable overtime fringe benefits and $10.2 million for protection activities not directly associated with the President's non-governmental residences.

FEMA awarded $110 million *American Rescue Plan Act of 2021* humanitarian relief funds to provide services to families and individuals in communities most impacted by the humanitarian crisis at the border. After reviewing just $12.9 million from 18 local recipient organizations, OIG questioned $7.4 million, or 58 percent, that lacked the documentation required to support claimed reimbursements.

Champion the DHS Workforce and Strengthen the Department

Components Impacted

All

Related Strategic Priority

All

The Department's recent APRs include numerous challenges and risks its components face relating to their ability to champion the DHS workforce and strengthen the Department, including but not limited to:

- integrating into a common platform across mission areas
- coordinating a joint process of collection, stewardship analysis, and information dissemination
- increasing vacancy rate and human resources challenges.

Recent OIG Reports

- DHS Has Made Progress in Fulfilling Geospatial Data Act Responsibilities, But Additional Work is Needed (OIG-23-07)
- DHS Grants and Contracts Awarded through Other Than Full and Open Competition Fiscal Year 2022 (OIG-23-15)
- DHS Has Refined Its Other than Full and Open Competition Reporting Processes (OIG-23-22)
- The United States Coast Guard Needs to Improve Its Accounting for Non-Capitalized Personal Property Assets (OIG-23-23)
- DHS Components Did Not Always Adhere to Internal Control Policies and Procedures for Ensuring That Bankcard Program Spending Limits are Established Based on Procurement Needs (OIG-23-35)
- United States Coast Guard Instituted Controls for the Offshore Patrol Cutter Extraordinary Relief Request, But Guidance Could Be Improved (OIG-23-36)
- DHS Needs to Update Its Strategy to Better Manage Its Biometric Capability Needs (OIG-23-58)
- ICE Should Improve Controls Over Its Transportation Services Contracts (OIG-23-59)

DHS Strategic Goal

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 four 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.

Transparency

Information and data collection benefit the Department and its many programs. But it is also an asset for ensuring the Department's actions reflect the will of the people. For example, **transparency** and program oversight foster strong partnerships with stakeholders through clear communication of processes, decision-making criteria, and performance, and facilitation of collaborative processes and dialogue. Open lines of communication build trust and enable stakeholders to provide valuable input and feedback, leading to improved practices and increased synergy among stakeholders. Key aspects of the Department's strategic goal 6 include the promotion of **transparency** before the American people and advancement of risk-based decision-making. Alternatively, a lack of **transparent** or comparable data inhibits the public and policymakers' ability to fully understand and address problematic or **inefficient** practices and their consequences.

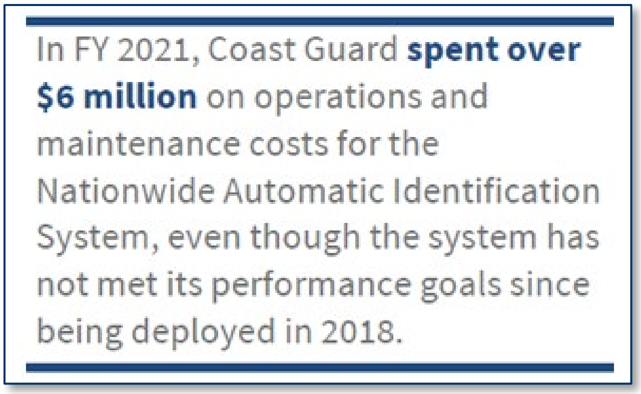
The Department's Data Mission is to "provide transparent access to valid, reliable, and interoperable data that supports the Department's mission and promotes the public good." To meet established requirements and to promote better use and management of data, the Department implemented an Evidence-Based Data Strategy (Data Strategy), with seven goals, to fully address issues that are foundational for strengthening its ability to support evidence building, leverage information sharing, and promote standards that coincide with Department-level strategic planning.

Department Data Strategy Goals

1. **Make Data Visible** – ease of discovery and use of Department data in creating meaningful analyses that have depth and breadth.
2. **Make Data Accessible** – the ease of availability to authorized users in the most relevant and meaningful forms.
3. **Make Data Understandable** – the quantity and quality of sharable insights and visualizations made available to decision makers.
4. **Make Data Linked** – adherence to industry best practices and ensures that connections across disparate sources, relationships, and dependencies can be uncovered, maintained, and leveraged for analytics.
5. **Make Data Trustworthy** – documentable quantitative and qualitative credibility, transferability, dependability, and confirmability of Department information for authorized users and stakeholders.
6. **Make Data Interoperable** – the quality and quantity of machine-to-machine communications across different technology systems and software applications.
7. **Make Data Secure** – the degree to which the guiding principles of risk prioritization, cost effectiveness, innovation, agility, and collaboration are being leveraged to foster resiliency across software, hardware, services, and technologies.

Vulnerabilities Resulting from Transparency Challenges

Although the *Inspector General Act of 1978*, as amended, allows Inspectors General unrestricted access to agency records, OIG's requests have been met with resistance and in many cases denial by the Department. As previously reported in its Semiannual Report to Congress, OIG's requests for data and information system access, critical for conducting oversight responsibilities, have been routinely delayed or denied. Similarly, the Department restricted OIG access to numerous component SharePoint sites containing organizational policies and procedures. This barrier to **transparency** impairs OIG's ability to achieve its mission; specifically, the denial of full and independent access to agency records and information may adversely impact program **sustainability** and **efficiencies** and severely damage its critical oversight function. Additionally, without unfettered oversight, citizens, Congress, and other stakeholders are unable to hold the Department **accountable** for actions and decisions regarding performance, deficiencies, services, and costs.



In FY 2021, Coast Guard **spent over $6 million** on operations and maintenance costs for the Nationwide Automatic Identification System, even though the system has not met its performance goals since being deployed in 2018.

The Department invests billions of dollars to acquire and sustain critical systems to support its many missions. Once a major system is fully deployed, it transitions to the sustainment phase where upon the Office of Management and Budget requires a periodic operational analysis to ensure systems continue to perform as intended. Between fiscal years 2018 and 2021, the Department transitioned 15 major systems to the sustainment phase requiring operational analyses; these systems had operations and maintenance costs totaling about $1.1 billion in fiscal year 2021. Department components completed an operational analysis for 12 of the 15 systems but did not complete all 12 in accordance with Federal and department guidance; additionally, the Transportation Security Administration did not complete an operational analysis for three of its systems. As a result, the Department does not have assurance that its multibillion-dollar systems perform as intended and fully meet mission needs. Without accurate and **transparent** reporting, the Department risks continuing to invest in programs that detract from its mission and create **inefficiencies**, such as significant cost overruns.

Vulnerabilities Resulting from Transparency Challenges (continued)

Geospatial data supports numerous activities such as natural disaster response, law enforcement, and healthcare, and enhances decision-making by organizational leaders. However, prior **inefficiencies** in data collection resulted in duplications of effort and resources. As such, Congress enacted the *Geospatial Data Act of 2018* (GDA) to promote more **efficient** management of geospatial data, technologies, and infrastructure through enhanced coordination among Federal, state, local, and tribal governments, as well as the private sector and academia. The Department published it geospatial data strategy as an addendum to the Data Strategy it published to comply with the *Foundations for Evidence-Based Policymaking Act of 2018* (Evidence Act). The Evidence Act required each agency to develop and maintain a comprehensive data inventory. The Department further included within its Data Strategy that data are to be inventoried in a comprehensive data catalog with relevant information on purpose, ownership, points of contact, security, standards, interfaces, limitations, and restrictions on use (related to Goal 2). However, the Department has not completed its comprehensive inventory of all its geospatial assets. Without a complete inventory, the Department cannot ensure it complies with the GDA for all its geospatial assets.

Recent Progress Reported by the Department

The Department is currently inventorying its data assets and collecting the data's corresponding metadata from its components and responsible offices. It intends to use the metadata to create a one-stop electronic data catalog. The catalog will include what data the Department possesses, which entity within the Department houses the data, and from whom access must be requested to obtain the data.

Accountability

Rooted alongside **transparency**, the Department emphasizes the need for **accountability** in its strategic goal 6; accordingly, policymaking and managing business processes are essential functions for ensuring control activities are implemented throughout the Department. Policies and procedures dictate the responsibilities and actions that drive day-to-day program operations, ensure compliance with laws and regulations, guide decision-making, and streamline processes. However, to achieve its mission, the Department must hold responsible parties **accountable** for enforcing policies and procedures put in place to promote **efficient** programs and prevent fraud, waste, and abuse.

Vulnerabilities Resulting from Accountability Challenges

The OCIO is **accountable** for providing the infrastructure, governance, and oversight necessary to deliver mission capabilities in a secure, **efficient**, and effective manner. As part of its strategy, the OCIO has established its commitment to:

- optimize workplace technologies and introduce innovative solutions
- refine mechanisms to connect with and leverage IT services and solutions
- provide architecture and engineering services to components, programs, and acquisitions for enterprise-wide IT initiatives.

However, as the Department's technology capabilities have expanded, shadow IT organizations have been established within some components, and allowed to operate outside the OCIO's umbrella. As identified recently, these IT organizations have made problematic investments in several software applications without appropriate user engagement, sufficient requirements gathering, or assessment of functionality demonstrated by the loss of data and inoperability. Involvement by subject matter experts is essential to ensuring that invested resources will deliver adequate solutions and customers will be able to perform work **efficiently** and effectively. Establishing the OCIO as the **accountable** party only facilitates successful IT implementation if they are truly responsible and part of the identification and acquisition of technologies. It is vital that as the Department continues to grow and expand its technology capabilities, that OCIO and other relevant parties collaborate to ensure acquisitions onboard capabilities necessary to **efficiently** perform required functions and are capable of **sustaining** Department operations into the future.

Recent Progress Reported by the Department

In January 2023, a memorandum issued by the CISA director, required all CISA divisions and mission enabling offices to transition oversight and management of CISA information technology functions to the OCIO. According to the memorandum, this change in organizational structure allowed a more comprehensive governance of assets and enhanced IT operations and information security.

Vulnerabilities Resulting from Accountability Challenges (continued)

The Department's "Bankcard Program" established a mechanism for the procurement of commercial goods and services in an **efficient** and flexible manner. As a means to ensure effective program operations, internal controls and safeguards were developed to focus on preventing the occurrence of fraud, waste, and abuse. However, although established, the Department did not always adhere to its own policies and procedures. A lack of implementation or adherence to policies and procedures increases the Department's risk for material loss and vulnerability to fraud. The Department may also have limited assurance that the controls in place are effective and support informed decision-making and overarching program management. Ultimately, without the enforcement of established policies and procedures, organizations and individuals are not held **accountable** when loss occurs, and programs fail.

Recent Progress Reported by the Department

ICE HSI drafted and submitted a CSS-related privacy impact assessment for privacy review; it was approved in January 2022.

Additionally, privacy sensitive technology is governed by **accountability** requirements set forth in the *E-Government Act of 2002*, the *Privacy Act of 1974*, and various Department policies, ensuring sufficient protections for privacy of personal information. Specifically, agencies are required to conduct a privacy impact assessment before developing or procuring information technology that collects, maintains, or disseminates information in an identifiable form. However, the Department did not always adhere to the Federal statutes or its own policies that require an approved privacy impact assessment that describes what information an agency is collecting and why the information is collected; how the information will be used, stored, and shared; how the information may be accessed; how the information will be protected from unauthorized use or disclosure; and how long will be retained. For example, ICE HSI did not adhere to the Department's privacy policy and the E-Government Act of 2002 that require CSS to have a privacy impact assessment before its use. This barrier to **transparency** may impact public trust and lead to data privacy and sensitivity issues.

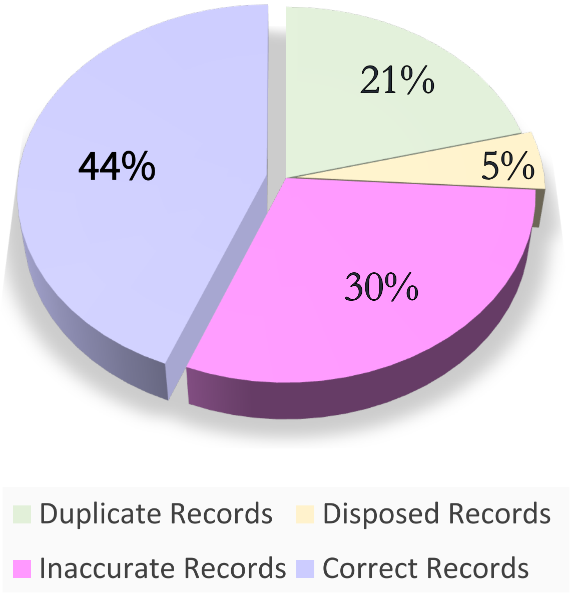
Efficiency

Reporting accurate asset inventory is critical to the Department's ability to accomplish mission goals **efficiently**, such as the prevention of improper disposal, misuse, and theft. Effective controls, such as assessing data quality for accuracy and completeness and conducting physical inventory of assets, should be implemented to help the Department identify duplicate records, invalid or duplicate identifiers, and discrepancies between records and inventory.

Vulnerabilities Resulting from Efficiency Challenges

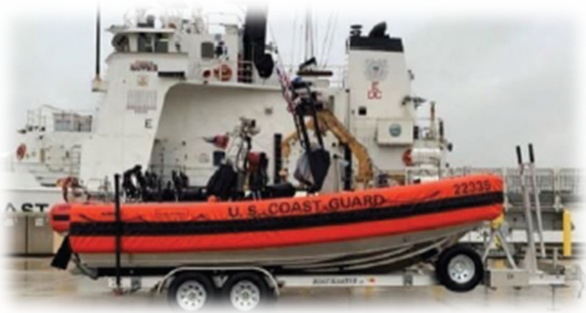
In a recent review, OIG identified that 56 percent of Coast Guard's non-capitalized personal property records sampled were inaccurate or misstated in its SOR. Additionally, Coast Guard has not performed a 100 percent annual inventory of non-capitalized personal property and has not consistently implemented effective controls to maintain accurate, complete, and consistent data records of its physical inventory, as required. As a result, non-capitalized personal property assets valued at approximately $870 million as of September 30, 2022, could be misstated in the SOR and be susceptible to misuse or theft.

Figure 18: Duplicate, Inaccurate, or Disposed of Records in SOR



Source: OIG analysis of Coast Guard-provided

Figure 19: Non-Capitalized Personal Property Asset, Large Cutter Boat



Source: Coast Guard

Sustainability

The Department's Strategic Goal 6 highlights the importance of strengthening departmental governance and management, developing and maintaining a high performing workforce, and optimizing support for mission operations. However, the Department does not establish a clear path for achieving these goals, resulting in the potential inability of program **sustainability**. As noted throughout this year's Management Challenge and Performance report, the Department has struggled to adequately manage and oversee programs and operations and report **transparently** to Congress and other stakeholders regarding the program **efficiencies** for which it is **accountable**. Further, the Department's attempts to recruit, hire, and retain staff to perform operational responsibilities and its lack of adequate internal controls have negatively impacted program **efficiencies** with a potential lasting impact to the Department's overall **sustainability**.

Appendix A - Department of Homeland Security's Six Strategic Goals

Goal 1: Counter Terrorism and Homeland Security Threats

Objective 1.1: Collect, Analyze, and Share Actionable Intelligence

Objective 1.2: Detect and Disrupt Threats

Objective 1.3: Protect Designated Leadership, Events, and Soft Targets

Objective 1.4: Counter Weapons of Mass Destruction and Emerging Threats

Goal 2: Secure U.S. Borders and Approaches

Objective 2.1: Secure and Manage Air, Land, and Maritime Borders

Objective 2.2: Extend the Reach of U.S. Border Security

Objective 2.3: Enforce U.S. Immigration Laws

Objective 2.4: Administer Immigration Benefits to Advance the Security and Prosperity of the Nation

Goal 3: Secure Cyberspace and Critical Infrastructure

Objective 3.1: Secure Federal Civilian Networks

Objective 3.2: Strengthen the Security and Resilience of Critical Infrastructure

Objective 3.3: Assess and Counter Evolving Cybersecurity Risks

Objective 3.4: Combat Cybercrime

Goal 4: Preserve and Uphold the Nation's Prosperity and Economic Security

Objective 4.1: Enforce U.S. Trade Laws and Facilitate Lawful International Trade and Travel

Objective 4.2: Safeguard the U.S. Transportation System

Objective 4.3: Maintain U.S. Waterways and Maritime Resources

Objective 4.4: Safeguard U.S. Financial Systems

Goal 5: Strengthen Preparedness and Resilience

Objective 5.1: Build a National Culture of Preparedness

Objective 5.2: Respond During Incidents

Objective 5.3: Support Outcome-Drive Community Recovery

Objective 5.4: Train and Exercise First Responders

Goal 6: Champion the DHS Workforce and Strengthen the Department

Objective 6.1: Strengthen Departmental Governance and Management

Objective 6.2: Develop and Maintain a High Performing Workforce

Objective 6.3: Optimize Support to Mission Operations

Appendix B - Department of Homeland Security's Updated 12 Cross-Functional Priorities

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

Organization Advancement

1. **Support and champion** the workforce and advance a culture of excellence
2. **Recruit, 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. **Innovate and transform** the delivery of services to advance mission execution, improve the customer experience, and increase access to services
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 the workforce's and the public's need

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 our borders** and modernize 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** human trafficking, labor exploitation, and child exploitation.

Appendix C – Office of Inspector General Audits, Inspections, and Evaluations Published in Fiscal Year 2023

Report Number	Report Title and Issue Date	Standards/ Authority	Related Strategic Goal	Recommendation Status
OIG-23-01	Major Management and Performance Challenges Facing the Department of Homeland Security (October 2022)	Not Applicable	All	No recommendations issued.
OIG-23-02	Independent Auditors' Report on the Department of Homeland Security's Consolidated Financial Statements for FYs 2022 and 2021 and Internal Control over Financial Reporting (November 2022)	GAGAS	3, 5, & 6	19 Recommendations (3 open, 16 closed)
OIG-23-03	El Centro and San Diego Facilities Generally Met CBP's TEDS Standards but Struggled with Prolonged Detention and Data Integrity (December 2022)	Quality Standards for Inspection and Evaluation	2	2 Recommendations (1 open, 1 closed)
OIG-23-04	DHS Did Not Always Promptly Revoke PIV Card Access and Withdraw Security Clearances for Separated Individuals (December 2022)	GAGAS	3	6 Recommendations (6 open, 0 closed)
OIG-23-05	DHS Did Not Consistently Comply with National Instant Criminal Background Check System Requirements (December 2022)	GAGAS	1	4 Recommendations (4 open, 0 closed)
OIG-23-06	Management Alert – CBP Needs to Provide Adequate Emergency Surveillance Systems at the Blaine Area Ports to Ensure Secure and Safe Operations (REDACTED) (January 2023)	GAGAS	2	3 Recommendations (3 open, 0 closed)
OIG-23-07	DHS Has Made Progress in Fulfilling Geospatial Data Act Responsibilities, But Additional Work is Needed (January 2023)	GAGAS	6	4 Recommendations (4 open, 0 closed)

Report Number	Report Title and Issue Date	Standards/ Authority	Related Strategic Goal	Recommendation Status
OIG-23-08	Review of U.S. Coast Guard's Fiscal Year 2022 Detailed Accounting Report for Drug Control Funds (January 2023)	GAGAS	All	No recommendations issued.
OIG-23-09	Review of U.S. Coast Guard's Fiscal Year 2022 Drug Control Budget Formulation Compliance Report (January 2023)	GAGAS	All	No recommendations issued.
OIG-23-10	Review of U.S. Customs and Border Protection's Fiscal Year 2022 Detailed Accounting Report for Drug Control Funds (January 2023)	GAGAS	1, 2, 4, 5, & 6	No recommendations issued.
OIG-23-11	Review of U.S. Customs and Border Protection's Fiscal Year 2022 Drug Control Budget Formulation Compliance Report (January 2023)	GAGAS	1, 2, 4, 5, & 6	No recommendations issued.
OIG-23-12	ICE and CBP Deaths in Custody during FY 2021 (February 2023)	Quality Standards for Inspection and Evaluation	2	No recommendations issued.
OIG-23-13	Violations of Detention Standards at ICE's Port Isabel Service Processing Center (February 2023)	Quality Standards for Inspection and Evaluation	2	9 Recommendations (0 open, 9 closed)
OIG-23-14	FEMA Did Not Provide Sufficient Oversight of Project Airbridge (February 2023)	GAGAS	5	2 Recommendations (2 open, 0 closed)
OIG-23-15	DHS Grants and Contracts Awarded through Other Than Full and Open Competition Fiscal Year 2022 (February 2023)	GAGAS	6	No recommendations issued.
OIG-23-16	FEMA Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information (February 2023)	GAGAS	3	10 Recommendations (9 open, 1 closed)
OIG-23-17	Secret Service and ICE Did Not Always Adhere to Statute and Policies Governing Use of Cell-Site Simulators (REDACTED) (February 2023)	GAGAS	1 & 6	6 Recommendations (6 open, 0 closed)

Report Number	Report Title and Issue Date	Standards/ Authority	Related Strategic Goal	Recommendation Status
OIG-23-18	Violations of ICE Detention Standards at Richwood Correctional Center in Monroe, Louisiana (February 2023)	Quality Standards for Inspection and Evaluation	2	8 Recommendations (7 open, 1 closed)
OIG-23-19	CISA Made Progress but Resources, Staffing, and Technology Challenges Hinder Cyber Threat Detection and Mitigation (March 2023)	Quality Standards for Inspection and Evaluation	3	4 Recommendations (3 open, 1 closed)
OIG-23-20	FEMA Should Increase Oversight to Prevent Misuse of Humanitarian Relief Funds (March 2023)	GAGAS	5	2 Recommendations (1 open, 1 closed)
OIG-23-21	Evaluation of DHS' Information Security Program for Fiscal Year 2022 (April 2023)	Quality Standards for Inspection and Evaluation	3	1 Recommendation (1 open, 0 closed)
OIG-23-22	DHS Has Refined Its Other than Full and Open Competition Reporting Processes (April 2023)	GAGAS	6	No recommendations issued.
OIG-23-23	The United States Coast Guard Needs to Improve Its Accounting for Non-Capitalized Personal Property Assets (April 2023)	GAGAS	6	3 Recommendations (3 open, 0 closed)
OIG-23-24	Intensifying Conditions at the Southwest Border Are Negatively Impacting CBP and ICE Employees' Health and Morale (May 2023)	Modified GAGAS	2	3 Recommendations (2 open, 1 closed)
OIG-23-25	DHS' Fiscal Year 2022 Compliance with the Payment Integrity Information Act of 2019 (May 2023)	GAGAS	5	3 Recommendations (3 open, 0 closed)
OIG-23-26	Results of an Unannounced Inspection of Northwest ICE Processing Center in Tacoma, Washington (May 2023)	Quality Standards for Inspection and Evaluation	2	8 Recommendations (1 open, 7 closed)
OIG-23-27	CBP Facilities in Vermont and New York Generally Met TEDS Standards, but Details to the Southwest Border Affected Morale, Recruitment, and Operations (May 2023)	Quality Standards for Inspection and Evaluation	2	No recommendations issued.

Report Number	Report Title and Issue Date	Standards/ Authority	Related Strategic Goal	Recommendation Status
OIG-23-28	Results of Unannounced Inspections of CBP Holding Facilities in the Rio Grande Valley Area (May 2023)	Quality Standards for Inspection and Evaluation	2	3 Recommendations (3 open, 0 closed)
OIG-23-29	Results of Unannounced Inspections of CBP Holding Facilities in the Yuma and Tucson Areas (June 2023)	Quality Standards for Inspection and Evaluation	2	4 Recommendations (4 open, 0 closed)
OIG-23-30	Evaluation of DHS' Compliance with Federal Information Security Modernization Act Requirements for Intelligence Systems for Fiscal Year 2022 (June 2023)	Quality Standards for Inspection and Evaluation	3	2 Recommendations (2 open, 0 closed)
OIG-23-31	CBP Released a Migrant on a Terrorist Watchlist, and ICE Faced Information Sharing Challenges Planning and Conducting the Arrest (June 2023)	Quality Standards for Inspection and Evaluation	1	3 Recommendations (3 open, 0 closed)
OIG-23-32	FEMA Did Not Always Secure Information Stored on Mobile Devices to Prevent Unauthorized Access (July 2023)	GAGAS	3	4 Recommendations (4 open, 0 closed)
OIG-23-33	ICE Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information (July 2023)	GAGAS	3	7 Recommendations (7 open, 0 closed)
OIG-23-34	FEMA Did Not Effectively Manage the Distribution of COVID-19 Medical Supplies and Equipment (July 2023)	GAGAS	5	3 Recommendations (3 open, 0 closed)
OIG-23-35	DHS Components Did Not Always Adhere to Internal Control Policies and Procedures for Ensuring That Bankcard Program Spending Limits are Established Based on Procurement Needs (July 2023)	GAGAS	6	3 Recommendations (3 open, 0 closed)

Report Number	Report Title and Issue Date	Standards/ Authority	Related Strategic Goal	Recommendation Status
OIG-23-36	United States Coast Guard Instituted Controls for the Offshore Patrol Cutter Extraordinary Relief Request, But Guidance Could Be Improved (July 2023)	GAGAS	6	1 Recommendation (1 open, 0 closed)
OIG-23-37	FEMA Continues to Make Improper Reimbursements through the Presidential Residence Protection Assistance Grant Program (July 2023)	GAGAS	5	3 Recommendations (3 open, 0 closed)
OIG-23-38	Results of an Unannounced Inspection of ICE's Stewart Detention Center in Lumpkin, Georgia (July 2023)	Quality Standards for Inspection and Evaluation	2	9 Recommendations (9 open, 0 closed)
OIG-23-39	CBP Outbound Inspections Disrupt Transnational Criminal Organization Illicit Operations (REDACTED) (August 2023)	GAGAS	2	3 Recommendations (3 open, 0 closed)
OIG-23-40	USCIS Has Generally Met Statutory Requirements to Adjudicate Asylum Applications from Paroled Afghan Evacuees (August 2023)	Quality Standards for Inspection and Evaluation	2	1 Recommendation (1 open, 0 closed)
OIG-23-41	ICE Has Limited Ability to Identify and Combat Trade-Based Money Laundering Schemes (August 2023)	GAGAS	1	2 Recommendations (2 open, 0 closed)
OIG-23-42	Ineffective Controls Over COVID-19 Funeral Assistance Leave the Program Susceptible to Waste and Abuse (August 2023)	GAGAS	5	5 Recommendations (3 open, 2 closed)
OIG-23-43	CBP Implemented Effective Technical Controls to Secure a Selected Tier 1 High Value Asset System (August 2023)	Quality Standards for Inspection and Evaluation	3	No recommendations issued.
OIG-23-44	Cybersecurity System Review of the Transportation Security Administration's Selected High Value Asset (August 2023)	Quality Standards for Inspection and Evaluation	3	12 Recommendations (12 open, 0 closed)
OIG-23-45	CBP Could Do More to Plan for Facilities Along the Southwest Border (August 2023)	GAGAS	2	2 Recommendations (2 open, 0 closed)

Report Number	Report Title and Issue Date	Standards/ Authority	Related Strategic Goal	Recommendation Status
OIG-23-46	The United States Coast Guard Needs to Determine the Impact and Effectiveness of Its Streamlined Inspection Program (August 2023)	GAGAS	4	3 Recommendations (3 open, 0 closed)
OIG-23-47	DHS Does Not Have Assurance That All Migrants Can be Located Once Released into the United States (REDACTED) (September 2023)	GAGAS	2	4 Recommendations (4 open, 0 closed)
OIG-23-48	CBP's Management of International Mail Facilities Puts Officer Safety and Mission Requirements at Risk (August 2023)	GAGAS	4	3 Recommendations (3 open, 0 closed)
OIG-23-49	FEMA's Technological Hazards Division Assisted State, Local, and Tribal Governments in Preparing to Respond to Radiological and Chemical Incidents (September 2023)	GAGAS	5	No recommendations issued.
OIG-23-50	Results of Unannounced Inspections of CBP Holding Facilities in the El Paso Area (September 2023)	Quality Standards for Inspection and Evaluation	2	5 Recommendations (5 open, 0 closed)
OIG-23-51	Results of an Unannounced Inspection of ICE's Caroline Detention Facility in Bowling Green, Virginia (September 2023)	Quality Standards for Inspection and Evaluation	2	8 Recommendations (8 open, 0 closed)
OIG-23-52	ICE Did Not Accurately Measure and Report Its Progress in Disrupting or Dismantling Transnational Criminal Organizations (September 2023)	GAGAS	1, 2, & 3	3 Recommendations (3 open, 0 closed)
OIG-23-53	Homeland Advanced Recognition Technology System Compliance with 28 C.F.R. Part 23 (September 2023)	GAGAS	3	3 Recommendations (3 open, 0 closed)
OIG-23-54	CBP Needs to Improve Its Video and Audio Coverage at Land Ports of Entry (September 2023)	GAGAS	2	7 Recommendations (7 open, 0 closed)

Report Number	Report Title and Issue Date	Standards/ Authority	Related Strategic Goal	Recommendation Status
OIG-23-55	DHS Needs to Improve Annual Monitoring of Major Acquisition Programs to Ensure They Continue to Meet Department Needs (September 2023)	GAGAS	All	3 Recommendations (3 open, 0 closed)
OIG-23-56	CBP Did Not Effectively Conduct International Mail Screening or Implement the STOP Act (REDACTED) (September 2023)	GAGAS	4	5 Recommendations (5 open, 0 closed)
OIG-23-57	Better TSA Tracking and Follow-up for the 2021 Security Directives Implementation Should Strengthen Pipeline Cybersecurity (REDACTED) (September 2023)	GAGAS	3	3 Recommendations (3 open, 0 closed)
OIG-23-58	DHS Needs to Update Its Strategy to Better Manage Its Biometric Capability Needs (September 2023)	GAGAS	6	4 Recommendations (4 open, 0 closed)
OIG-23-59	ICE Should Improve Controls Over Its Transportation Services Contracts (September 2023)	GAGAS	6	7 Recommendations (7 open, 0 closed)
OIG-23-60	CBP Accounted for Its Firearms but Did Not Always Account for Ammunition or Monitor Storage Facilities (September 2023)	GAGAS	1, 2, & 4	7 Recommendations (7 open, 0 closed)
OIG-23-61	CBP, ICE, and Secret Service Did Not Adhere to Privacy Policies or Develop Sufficient Policies Before Procuring and Using Commercial Telemetry Data (Redacted) (September 2023)	GAGAS	6	8 Recommendations (6 open, 2 closed)
OIG-23-62	Results of Unannounced Inspection of CBP Holding Facilities in the Laredo Area (September 2023)	Quality Standards for Inspection and Evaluation	2	3 Recommendations (3 open, 0 closed)

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