The Other Information section contains information on Tax Burden / Tax Gap, Climate Related Financial Risk, Summary of Financial Statement Audit and Management Assurances, Payment Integrity, Grants Programs, Civil Monetary Penalty Adjustment for Inflation, and Other Key Regulatory Requirements. Also included in this section are the OIG's Summary of Major Management and Performance Challenges Facing the Department of Homeland Security and Management's Response (unaudited).

Revenue Gap

The Entry Summary of Trade Compliance Measurement (TCM) program collects objective statistical data to determine the compliance level of commercial imports with U.S. trade laws, regulations, and agreements, and is used to produce a dollar amount for Estimated Net Under-Collections (also called estimated revenue gap), and a percent of Revenue Gap. The Revenue Gap is a calculated estimate that measures potential loss of revenue owing to noncompliance with trade laws, regulations, and trade agreements using a statistically valid sample of the revenue losses and overpayments detected during TCM entry summary reviews conducted throughout the year.

Table 6: Entry Summary of Trade Compliance Measurement

($ in millions)

	FY 2023 (Preliminary)	FY 2022 (Final)
Estimated Revenue Gap	$559	$400
Estimated Revenue Gap of all collectable revenue for year (%)	0.56%	0.36%
Estimated Over-Collection	$175	$172
Estimated Under-Collection	$734	$572
Estimated Overall Trade Compliance Rate (%)	99.35%	99.39%

The preliminary overall compliance rate for Fiscal Year (FY) 2023 is 99.35%. The final overall trade compliance rate and estimated revenue gap for FY 2023 will be issued in April 2024.

Summary of Financial Statement Audit and Management Assurances

The tables below provide a summary of the financial statement audit results and management assurances for FY 2023.

In FY 2023, the external financial statement auditor continued to identify the four previously reported areas of material weakness. In addition, in FY 2023, a new area of material weakness related to Custodial Activity: Seized and Forfeited Property was reported as part of the Integrated Financial Statement audit.

Table 7: Summary of Financial Statement Audit

Audit Opinion	Unmodified				
Restatement	No				
Areas of Material Weakness(es)	Beginning Balance	New	Resolved	Consolidated	Ending Balance
IT Controls and Information Systems	1	0	0	0	1
Financial Reporting	1	0	0	0	1
Insurance Liabilities	1	0	0	0	1
Receipt of Goods and Services[15]	1	0	0	0	1
Seized and Forfeited Property	0	1	0	0	1
Total Areas of Material Weakness(es)	*4*	*1*	*0*	*0*	*5*

Management has performed its evaluation, and the assurance is provided based upon the cumulative assessment work performed in the following areas across the Department:

- Entity Level Controls,
- Financial Reporting,
- Budgetary Resource Management,
- Fund Balance with Treasury,
- Grants Management,
- Human Resources and Payroll Management,
- Information Technology General Controls,
- Insurance Management,
- Payment Management,
- Property Plant and Equipment, and

---

[15] Previously titled New System Obligations.

- Revenue and Receivables.

While DHS has remediation efforts continuing in FY 2024; no additional areas of material weakness were newly identified by DHS as a result of the assessment work performed in FY 2023. The following table indicates the areas of material weakness(es) that have been identified by management and where DHS will continue focused remediation efforts in FY 2024.

Table 8: Summary of Management Assurances

Effectiveness of Internal Control Over Financial Reporting (FMFIA § 2)						
Statement of Assurance	Modified					
Areas of Material Weakness(es)	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
IT Controls and Information Systems	1	0	0	0	0	1
Financial Reporting	1	0	0	0	0	1
Insurance Management[16]	1	0	0	0	0	1
Receipt of Goods and Services[17]	1	0	0	0	0	1
Total Areas of Material Weakness(es)	*4*	*0*	*0*	*0*	*0*	*4*
Effectiveness of Internal Control Over Operations (FMFIA § 2)						
Statement of Assurance	Unmodified					
Areas of Material Weakness(es)	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
None Noted	0	0	0	0	0	0
Total Areas of Material Weakness(es)	*0*	*0*	*0*	*0*	*0*	*0*

---

[16] Previously titled Insurance Liabilities.
[17] Previously titled Budgetary Accounting.

Unaudited

Table 8 (continued): Summary of Management Assurances

| Effectiveness of Internal Control Over Operations (FMFIA § 4)						
Statement of Assurance	Federal Systems do not conform to financial management system requirements					
Areas of Material Weakness(es)	Beginning Balance	New	Resolved	Consolidated	Reassessed	Ending Balance
Federal Financial Management Systems Requirements: Financial System Security & Integration of Financial Management Systems	1	0	0	0	0	1
Federal Accounting Standards	1	0	0	0	0	1
U.S. Government Standard General Ledger (USSGL): Transactional Level Reporting	1	0	0	0	0	1
Total Non-Conformance(s)	*3*	*0*	*0*	*0*	*0*	*3*
COMPLIANCE WITH SECTION 803(a) OF THE FEDERAL FINANCIAL MANAGEMENT IMPROVEMENT ACT (FFMIA)						
		DHS		Auditor		
1. Federal Financial Management System Requirements		Lack of compliance noted		Lack of compliance noted		
2. Applicable Federal Accounting Standards		Lack of compliance noted		Lack of compliance noted		
3. USSGL at Transaction Level		Lack of compliance noted		Lack of compliance noted		

Unaudited

Payment Integrity

The Payment Integrity Information Act of 2019 (PIIA)[18], requires agencies to review and assess all programs and activities they administer and identify those determined to be susceptible to significant improper payments[19], estimate the annual amount of improper payments, and submit those estimates to Congress. In accordance with the Office of Management and Budget (OMB) Circular No. A-123, Appendix C[20], *Requirements for Payment Integrity Improvement,* Federal agencies are required to assess improper payments and report[21] annually on their efforts.

We remain strongly committed to ensuring our agency's transparency and accountability to the American taxpayer and achieving the most cost-effective strategy on the reduction of improper payments.

Payment Type Categories

In accordance with OMB Circular No. A-123, Appendix C, DHS uses sampling and statistical methods to estimate proper payments, improper payments, and unknown payments among its programs. See Figure 1 for an illustration of the payment categories as well as improper payment types and Figure 2 for payment type definitions.

Figure 1: Payment Type Categories

---
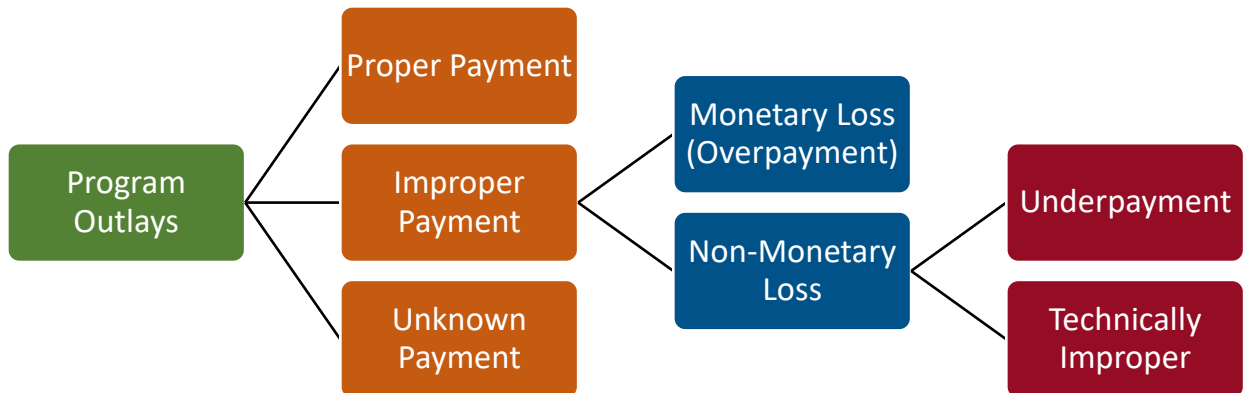
[18] Unless otherwise indicated, the term "PIIA" is used to reflect the current legislative language regarding improper payments as it formal revoked the Improper Payments Information Act of 2002 (IPIA), the Improper Payments Elimination and Recovery Act of 2010 (IPERA), and the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA).

[19] A program with significant improper payments has both a 1.5 percent improper payment rate of program outlays and at least $10 million in improper payments of all program or activity payments made during the year or exceeds $100 million dollars in improper payments regardless of the improper payment rate percentage of total program outlays.

[20] On March 5, 2021, OMB released an updated Circular No. A-123, Appendix C (M-21-19) to formalize implantation expectations under PIIA effective beginning with FY 2021 implementation.

[21] Due to rounding throughout all following figures and tables, amounts and percentages may reflect the exact total respective at the summary amounts and percentages reported. For precise data at the reportable program level, please refer to PaymentAccuracy.gov.

Figure 2: Payment Type Definitions

Payment Type	Definition
Proper Payment	A payment made to the right recipient for the right amount that has met all program specific legally applicable requirements for the payment.
Improper Payment	A payment that was made in an incorrect amount under statutory, contractual, administrative, or other legally applicable requirements. The term improper payment includes any payment to an ineligible recipient; any payment for an ineligible good or service; any duplicate payment; any payment for a good or service not received, except for those payments where authorized by law; and any payment that does not authorized by law; and any payment that does not account for credit for applicable discounts.
Unknown Payment	Instances in which a program cannot determine whether a payment is proper or improper due to insufficient payment documentation. Further, payments should be categorized as unknown if the agency is still conducting research or reviews to determine the appropriateness of the payment at the time the agency must finalize and report its estimates.
Monetary Loss (Overpayment)	Payments to the wrong recipient, or to the correct recipient in a higher amount than what should have been disbursed, are monetary losses to the government.
Non-Monetary Loss	Payments to the correct recipient in a lesser amount than what should have been disbursed are non-monetary losses to the government.
Underpayment	Payments to the correct recipient in a lesser amount than what should have been disbursed.
Technically Improper	A payment was made to the right recipient for the right amount, but the payment process failed to follow all applicable statute and regulation there is no amount that needs to be recovered, however, because the payment failed to adhere to all applicable statutes and regulations during the payment process the payment itself is considered a technically improper payment.

Phases of Assessment

Under Appendix C of OMB Circular No. A-123, all programs with annual outlays greater than $10 million fall into either Phase I (subject to periodic risk assessments but not required to report) or Phase II (subject to statistical testing and reporting requirements). Based on improper payment risk assessments, programs that are likely to have an annual amount of improper and unknown payments below the statutory threshold are categorized as Phase I and are required to complete a risk assessment once every three years. Programs likely to
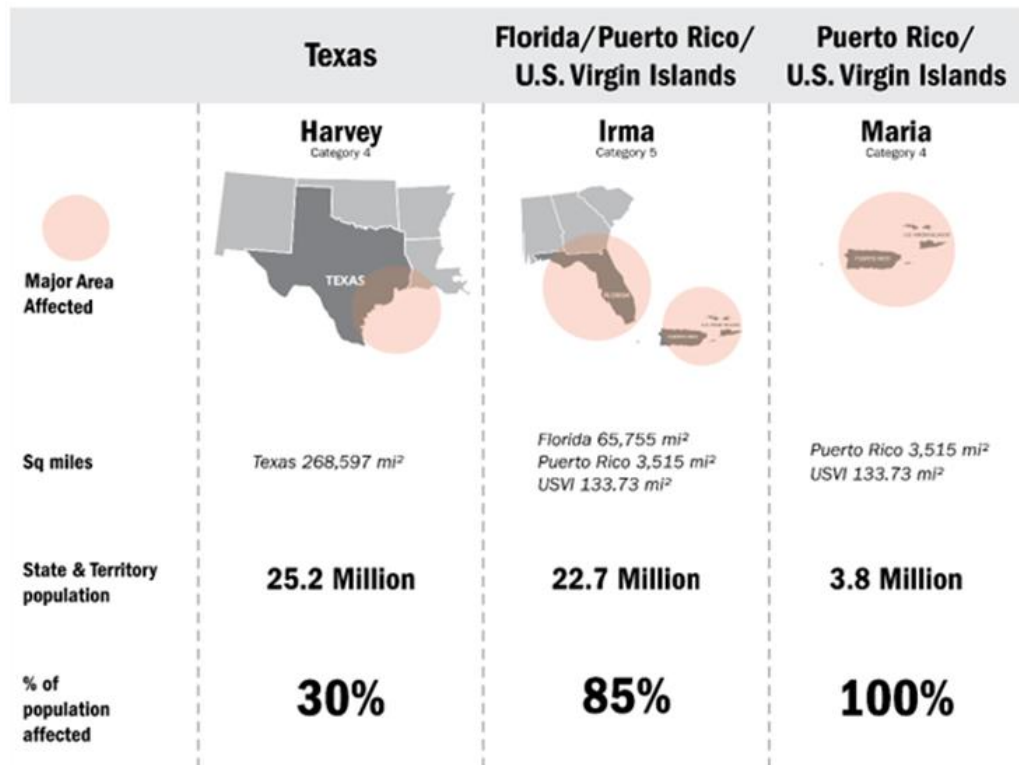
Unaudited

be above the statutory threshold are categorized as Phase II and are required to report an improper payment estimate.

Supplemental Appropriations for Disaster Relief Requirements

In 2017, the nation faced a historic Atlantic hurricane season. The effects from consecutive hurricanes Harvey, Irma and Maria were widespread, causing long-lasting damage across the southern continental U.S. and surrounding islands, as well as Puerto Rico and the U.S. Virgin Islands.

- On August 25, 2017, Hurricane Harvey made landfall in Texas as a Category 4 storm. For several days, the storm hovered near the Houston metropolitan area and set a record for the most rainfall from a U.S. tropical cyclone. Of households impacted by Harvey, 80 percent did not have flood insurance.

- On September 6, 2017, Hurricane Irma became one of the strongest Atlantic hurricanes on record. The storm's center passed just north of the U.S. Virgin Islands and Puerto Rico and destroyed critical infrastructure on St. Thomas and St. John in the U.S. Virgin Island, as well as Puerto Rico and the Florida Keys. As Irma was the first major hurricane to make landfall in Florida since 2005, the public followed evacuation orders as the storm approached Florida, resulting in one of the largest sheltering missions in U.S. history.

- On September 19, 2017, the center of Hurricane Maria passed southeast of St. Croix, U.S. Virgin Islands as a Category 5 storm and made landfall in Puerto Rico as a Category 4 storm the next day. Hurricane Maria severely damaged or destroyed a significant portion of both territories' already fragile critical infrastructure. Maria left Puerto Rico's 3.7 million residents without electricity and the resulting response represents the longest sustained air mission of food and water delivery in FEMA history.

Figure 3: Harvey, Irma, and Maria Locations and Associated Impact

	Texas	Florida/Puerto Rico/ U.S. Virgin Islands	Puerto Rico/ U.S. Virgin Islands
	Harvey Category 4	**Irma** Category 5	**Maria** Category 4
Major Area Affected			
Sq miles	Texas 268,597 mi²	Florida 65,755 mi² Puerto Rico 3,515 mi² USVI 133.73 mi²	Puerto Rico 3,515 mi² USVI 133.73 mi²
State & Territory population	25.2 Million	22.7 Million	3.8 Million
% of population affected	30%	85%	100%

curity

Supplemental appropriations were designated as an emergency requirement in the Supplemental Appropriations for Disaster Relief Requirements, 2017 (P.L. 115-56, the Additional Supplemental Appropriations for Disaster Relief Requirements Act of 201 7 (P.L. 115-72), and the Further Additional Supplemental Appropriations for Disaster Relief Requirements Act, 2018 (P.L. 115-123) were issued to specific agencies to provide the resources needed to recover and rebuild following recent hurricanes and other applicable natural disasters. Within these supplemental appropriations, DHS received a total supplemental appropriation amount of $50.72 billion[22]. The breakout of DHS Components receiving this supplemental funding is documented in the table below.

Table 9: DHS Breakout of Supplemental Appropriation Funding Received

Public Law	Component	Program	Period of Availability (FY)	Appropriated Value ($M)	Transfer-In Value ($M)	Transfer-Out Value ($M)	Value for Program Use ($M)
115-56	Federal Emergency Management Agency	Disaster Relief Fund	No-Year	$7,400.00	$0.00	$0.00	$7,400.00
115-72		Disaster Relief Fund	No-Year	$18,670.00	$0.00	$10.00	$18,660.00
115-123		Operations and Support	18-19	$58.80	$0.00	$0.00	$58.80
		Procurement, Construction, and Improvements	18-20	$1.20	$0.00	$0.00	$1.20
		Disaster Relief Fund	No-Year	$23,500.00	$0.00	$0.00	$23,500.00
115-123	Federal Law Enforcement Training Center	Operations and Support	18-19	$5.37	$0.00	$0.00	$5.37
		Procurement, Construction, and Improvements	18-22	$5.00	$0.00	$0.00	$5.00
115-72	Office of the Inspector General	Operations and Support	No-Year	$0.00	$10.00	$0.00	$10.00
115-123		Operations and Support	18-20	$25.00	$0.00	$0.00	$25.00
115-123	Transportation and Security Administration	Operations and Support	18-19	$10.32	$0.00	$0.00	$10.32
115-123	U.S. Customs and Border Protection	Operations and Support	18-19	$104.49	$0.00	$0.00	$104.49
		Procurement, Construction, and Improvements	18-22	$45.00	$0.00	$0.00	$45.00
115-123	U.S. Immigration and Customs Enforcement	Operations and Support	18-19	$30.91	$0.00	$0.00	$30.91
		Procurement, Construction, and Improvements	18-22	$33.05	$0.00	$0.00	$33.05
115-123	United States Coast Guard	Operating Expenses	18-19	$112.14	$0.00	$0.00	$112.14
		Environmental Compliance and Restoration	18-22	$4.04	$0.00	$0.00	$4.04
		Acquisition, Construction, and Improvements	18-22	$718.92	$0.00	$0.00	$718.92
						TOTAL:	$50,724.24

P.L. 115-123 requires any agency receiving funds under P.L. 115-123 as well as P.L. 115-72 and P.L. 115-56 to consider any programs expending more than $10 million of funds in any one fiscal year highly susceptible to improper payments for the purposes of the PIIA. Once disaster supplemental funded programs met or exceeded the $10 million threshold in payments applicable for PIIA review, the program was deemed susceptible to significant improper payments and thus applicable for statistical sampling and reporting.

---

[22] Due to rounding, amounts may not reflect precise appropriated values.

Payment Reporting

Due to the burden of testing and reporting for the programs related solely to disaster supplemental appropriation disbursements, DHS is reporting statistical testing results two years in arrears. Therefore, FY 2021 disbursement testing and results are reported in the 2023 results noted below for the following programs:

- FEMA Hazard Mitigation Grant Program - Disaster Supplemental Funds
- CBP Procurement, Construction, & Improvement - Disaster Supplemental Funds

Beginning in FY 2020, the FEMA Public Assistance – Validate as You Go (VAYGo) program has expanded coverage beyond the disaster supplemental funding received in response to Hurricanes Harvey, Irma, and Maria. On March 13, 2020, the Presidential declaration of a nationwide COVID emergency increased the level of federal response from FEMA, as well as support to state, local, tribal, and territorial partners across the nation. The agency's response to COVID was unprecedented. When the White House directed FEMA to lead operations, COVID became the first national pandemic response that FEMA has led since it was established in 1979. It was also the first time in U.S. history the President declared a nationwide emergency under Section 501b of the Stafford Act and authorized Major Disaster Declarations for all states and territories for the same incident. FEMA, through its 10 Regions, managed 57 concurrent Presidential Major Disaster Declarations for COVID and

Disaster assistance

Disaster assistance is financial or direct assistance to individuals, families, and businesses whose property has been damaged and whose losses are not covered by insurance. FEMA provides several types of grants following a presidentially declared disaster. Individual Assistance offers help to individuals and families; Public Assistance offers help to state, local, tribal, and territorial governments, and certain nonprofit agencies; and Hazard Mitigation assists state, local, tribal, and territorial governments in reducing long-term risk.

Unaudited

U.S. Department of Homeland Security

worked with 91 tribal nations. Due to the increase in assessment burden, the PIIA Phase II reporting to cover FY 2021 disbursements has been delayed until 2024 for the following program:

- FEMA Public Assistance – VAYGo

The OMB Circular No. A-123, Appendix C provides the definition for an improper payment and serves as applicable guidance to agencies for compliance with PIIA. Following the updated OMB Circular No. A-123, Appendix C guidance, and accounting for the additional requirements within the Supplemental Appropriations for Disaster Relief Requirements, the Department has identified the following programs or activities susceptible to significant improper payments and is able to provide results and reporting this year[23]. Full publication of data and planned corrective actions for Phase II programs can be found on PaymentAccuracy.gov.

Resiliency

DHS works with all levels of government, the private and non-profit sectors, and individual citizens to make our nation more resilient to acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters. The challenges we face are more intense, complex, and frequent than ever before. DHS must be able to leverage its collective expertise and capabilities to manage all types of incidents directly, including those that invoke multiple responsibilities and authorities from across the Department, and to support incident response efforts led by other agencies. As such, the Department readying its entire workforce—not only those already trained in the National Incident Management System—to execute these incident management capabilities as well as regularly exercise and develop them alongside federal, state, local, territorial, tribal, and nongovernmental partners.

---

[23] Due to the burden of testing and reporting for the twelve programs related solely to disaster supplemental appropriation disbursements, DHS is reporting statistical testing results two years in arrears for these programs. For additional information, please refer to the additional detail around the Supplemental Appropriations for Disaster Relief Requirements supplied later in this section.

Disbaster Supplemental[24] DHS Programs for Reporting

FEMA Hazard Mitigation Grant Program (HMGP) – Disaster Supplemental Funds Program
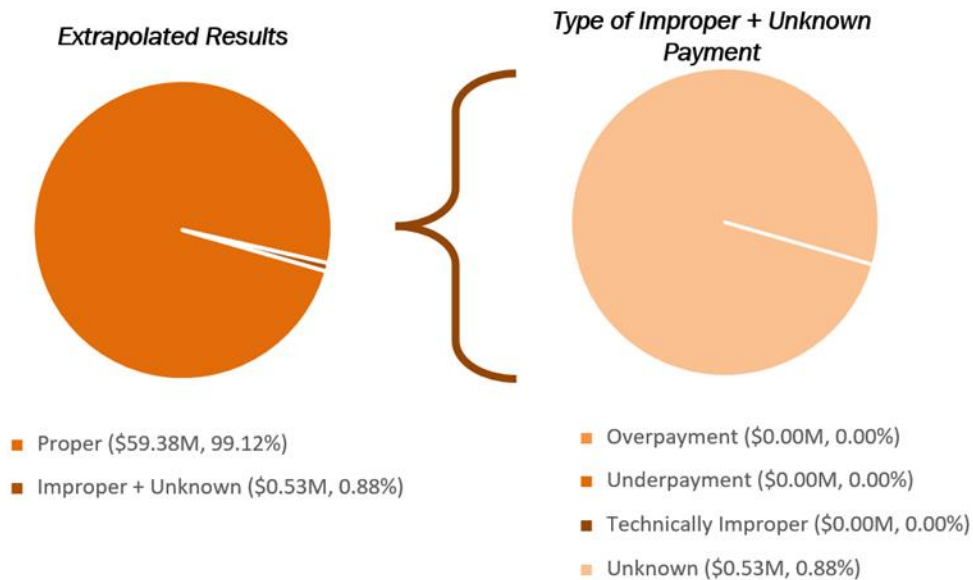
FEMA's Hazard Mitigation Grant Program provides funding to state, local, tribal and territorial governments so they can develop hazard mitigation plans and rebuild in a way that reduces, or mitigates, future disaster losses in their communities. When requested by an authorized representative, this grant funding is available after a presidentially declared disaster.

DID YOU KNOW?

The 2017 storms have provided the U.S. Virgin Islands an opportunity to prioritize projects to reduce the loss of life and property from future disasters and focus on development of a territorial hazard mitigation plan. As of August 31, 2023, over $178M in Hazard Mitigation Grants Program funding has been obligated to support the efforts of the Virgin Islands Territorial Emergency Management Agency.

For the testing conducted in 2023, FEMA's assessment was focused on the associated FY 2021 disaster supplemental funding disbursements of over $59.9 million applicable for review under PIIA. The FEMA HMGP – Disaster Supplemental Funds program reported a 0.88 percent estimated payment error rate in 2023. Please refer to the figure below for additional detail regarding the breakouts and associated error categorization.

Figure 4: FEMA HMGP – Disaster Supplemental Funds Reported Results

Extrapolated Results

- Proper ($59.38M, 99.12%)
- Improper + Unknown ($0.53M, 0.88%)

Type of Improper + Unknown Payment

- Overpayment ($0.00M, 0.00%)
- Underpayment ($0.00M, 0.00%)
- Technically Improper ($0.00M, 0.00%)
- Unknown ($0.53M, 0.88%)

---

[24] Program funding consisting of funding received through the Supplemental Appropriations for Disaster Relief Requirements, 2017 (P.L. 115-56, the Additional Supplemental Appropriations for Disaster Relief Requirements Act of 201 7 (P.L. 115-72), and the Further Additional Supplemental Appropriations for Disaster Relief Requirements Act, 2018 (P.L. 115-123)

During FY 2023, FEMA concluded that $0.46 million in HMGP – Disaster Supplemental Funds disbursements that had been designated as unknown payments in prior years could be adequately supported and classified as proper payments. FEMA will continue to work on determining if previously identified unknown payments are in fact proper or improper. If determined to be improper with a monetary loss associated, FEMA will continue work to recoup those payments as applicable.

<u>CBP Procurement, Construction, & Improvement (PC&I)– Disaster Supplemental Funds Program</u>

The CBP PC&I program builds facilities for CBP Officers and Border Patrol Agents, including buildings and other structures at Border Patrol sector headquarters, stations, checkpoints, and remote forward operating bases. The program received additional funds for necessary expenses related to the consequences of hurricanes Harvey, Irma, and Maria, including for the reconstruction of affected facilities. Funds were provided to carry out these CBP construction activities in Puerto Rico and the U.S. Virgin Islands.

For the testing conducted in 2023, CBP's assessment was focused on the associated FY 2021 disaster supplemental funding disbursements of over $10.8 million applicable for review under PIIA. The CBP PC&I – Disaster Supplemental Funds program had no improper or unknown payments identified in 2023.

Historic facility preservation

The San Juan Customs House, built in 1924, is a Spanish Colonial Revival style building listed on the National Register of Historic Places. Architecturally, it is one of the nation's most distinguished custom houses. CBP's Office of Facilities and Asset Management oversees maintenance, repair, leasing, and construction of all CBP facilities as well as the agency's Historic Preservation Program. The Historic Preservation program provides the guidance and framework necessary to respect historically significant spaces like the Puerto Rican custom houses.
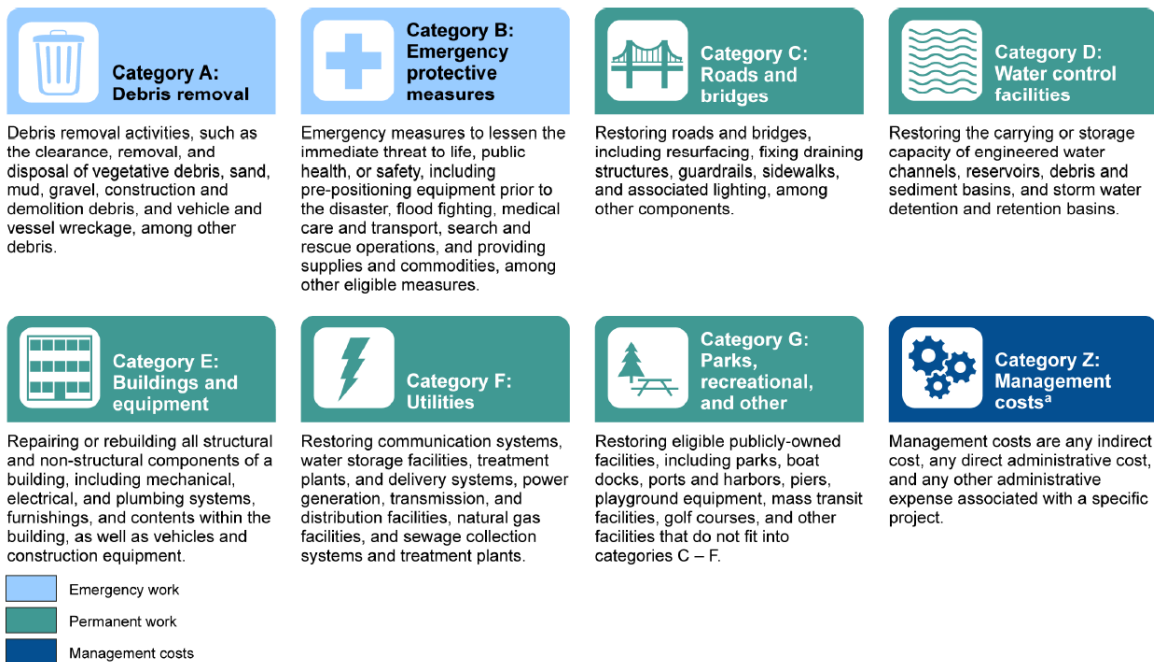
Other DHS Programs for Reporting

FEMA Public Assistance – Validate as You Go (VAYGo) Program

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, as Amended (Stafford Act), Title 42 of the United States Code (U.S.C.) § 5121 et seq., authorizes the President to provide federal assistance when the magnitude of an incident or threatened incident exceeds the affected State, Territorial, Indian Tribal, and local government capabilities to respond or recover.

The purpose of the Public Assistance Grant Program is to support communities' recovery from major disasters by providing them with grant assistance for debris removal, life-saving emergency protective measures, and restoring public infrastructure. Local governments, states, tribes, territories, and certain private nonprofit organizations are eligible to apply.

Figure 5: FEMA Public Assistance Program Categories of Work[25]

Category A: Debris removal
Debris removal activities, such as the clearance, removal, and disposal of vegetative debris, sand, mud, gravel, construction and demolition debris, and vehicle and vessel wreckage, among other debris.

Category B: Emergency protective measures
Emergency measures to lessen the immediate threat to life, public health, or safety, including pre-positioning equipment prior to the disaster, flood fighting, medical care and transport, search and rescue operations, and providing supplies and commodities, among other eligible measures.

Category C: Roads and bridges
Restoring roads and bridges, including resurfacing, fixing draining structures, guardrails, sidewalks, and associated lighting, among other components.

Category D: Water control facilities
Restoring the carrying or storage capacity of engineered water channels, reservoirs, debris and sediment basins, and storm water detention and retention basins.

Category E: Buildings and equipment
Repairing or rebuilding all structural and non-structural components of a building, including mechanical, electrical, and plumbing systems, furnishings, and contents within the building, as well as vehicles and construction equipment.

Category F: Utilities
Restoring communication systems, water storage facilities, treatment plants, and delivery systems, power generation, transmission, and distribution facilities, natural gas facilities, and sewage collection systems and treatment plants.

Category G: Parks, recreational, and other
Restoring eligible publicly-owned facilities, including parks, boat docks, ports and harbors, piers, playground equipment, mass transit facilities, golf courses, and other facilities that do not fit into categories C – F.

Category Z: Management costs[a]
Management costs are any indirect cost, any direct administrative cost, and any other administrative expense associated with a specific project.

Emergency work
Permanent work
Management costs

The FEMA Public Assistance Grant Program relies on Regional Offices to manage, operate, and maintain program activities and operations. For the breakout of FEMA Regions, please refer to the figure on the next page.

---

[25] Source: Federal Emergency Management Agency. | GAO-20-221

Unaudited

U.S. Department of Homeland Security

Figure 6: FEMA Regions and Regional Offices

Public Assistance is FEMA's largest grant program and provides emergency assistance to save lives and protect property and assists communities with repairing public infrastructure affected by federally declared incidents.

FEMA implemented the VAYGo pilot program to test Public Assistance and certain other disaster grant expenditure, originally scoped to Hurricanes Harvey, Irma, and Maria. Since these disasters, the VAYGo program has expanded to include coverage over additional disaster declarations, such as COVID response and disasters declared during or after FY 2020. As part of VAYGo, FEMA reviews project documentation for a sample of funds as they are drawn down by recipients and conducts testing to verify whether the project funding was appropriately expended by the subrecipient. One goal of VAYGo is to identify potential problems earlier, allowing FEMA and recipients—including Public Assistance recipients—to correct or mitigate issues earlier in the process instead of waiting until grant closeout. According to FEMA officials that conduct the testing, VAYGo's goal is to improve grants management internal control processes by consistently assessing payment error rates to identify potential payment integrity issues. VAYGo payment integrity testing results allows recipients to remediate questioned costs and take appropriate actions to strengthen internal controls in grant lifecycle processes. This will prevent or reduce the likelihood of future improper payments.

In a memorandum dated April 18, 2022, FEMA's Office of the Chief Financial Officer (OCFO)memorialized the Administrator's intent to pause and evaluate opportunities to streamline and reduce the complexity of VAYGo processes. FEMA's OCFO conducted thirteen listening sessions early in FY 2023 with FEMA Regions and Recipients to better understand the Public Assistance program and to identify common VAYGo issues and recommendations for improvements for VAYGo. As a result of those listening sessions, FEMA published the VAYGo Guide and distributed to Regions and Recipients. This guide provides implementation

Unaudited

and delivery guidance for the FEMA VAYGo grant payment review process and includes details on documentation requirements to support recipient drawdowns and financial disbursements. The guidance is designed to enhance the customer experience for all stakeholders involved in VAYGo processes while also establishing a framework for implementing measures to reduce the administrative burden of grants management when improper payment rates meet or fall below the minimum threshold established by Appendix C of OMB Circular No. A-123. On Aug. 9, 2023, FEMA reinstated VAYGo, which now includes the new implementation guide and a new closeout benefit for qualifying recipients.

However, the strategic pause impacted FEMA's ability to coordinate the receipt of adequate documentation to fully determine the appropriateness of all selected FY 2021 disbursement sample transactions selected for 2023 review and reporting. DHS, in accordance with instruction received from OMB, has delayed PIIA Phase II reporting based on FY 2021 disbursement activity until 2024.

FEMA developed a Corrective Action Plan in FY 2023 for FEMA Public Assistance – VAYGo to remediate improper and unknown payments as a result of 2022 reporting. The corrective actions focused on FEMA's development of strong relationships among its regions and recipients to help facilitate more efficient and effective improper payment testing and funds management. Additionally, FEMA developed a VAYGo Guide to improve processes and strengthen internal controls. This guide was issued to regions and recipients in August 2023. In addition, FEMA developed a VAYGo Module within the FEMA Grants Manager / Grants Portal platform. The module has workflows to support VAYGo testing, process requests for information, and enable FEMA Recipients to upload documentation for their respective VAYGo tested samples. FEMA continues to collaborate with Public Assistance Business Architecture to enhance the VAYGo Module with the goal of improving the VAYGo customer service experience for internal and external VAYGo stakeholders.
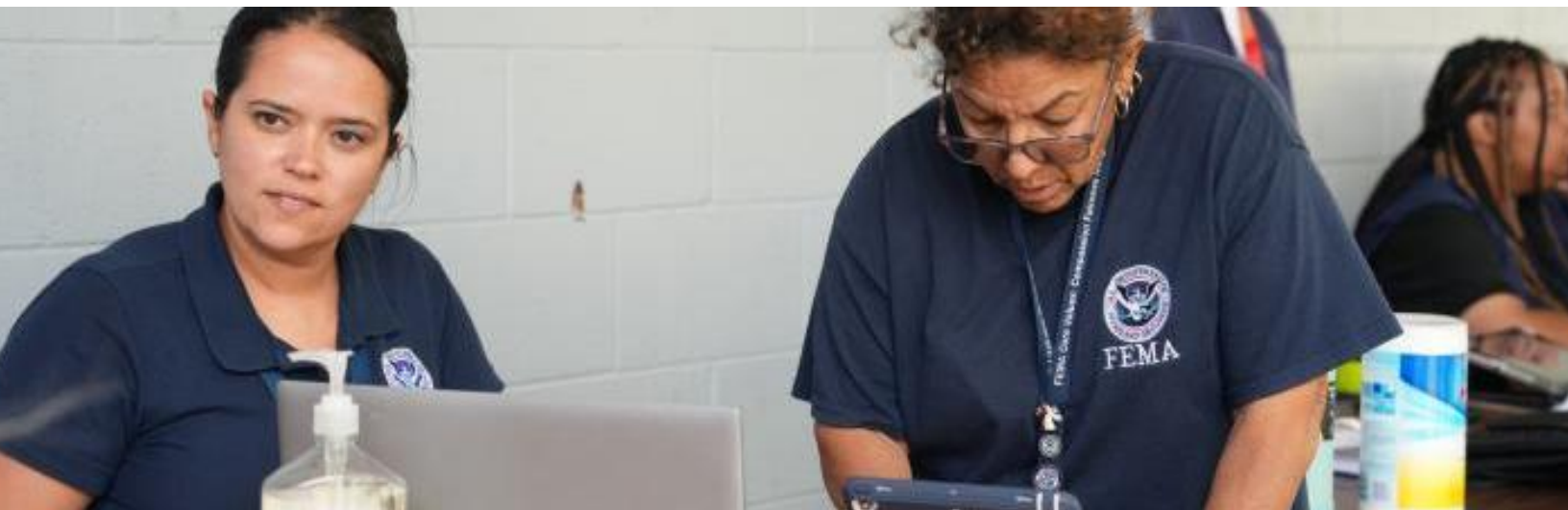
Training and mitigation

Trainings are available and are designed to help FEMA regional partners and state, local, tribal, and territorial governments create effective hazard mitigation plans that meet FEMA's requirements and reduce risk in their communities. The Emergency Management Institute serves as the national focal point for the development and delivery of emergency management training to enhance the capabilities of federal, state, local, tribal, and territorial government officials, volunteer organizations, and the public and private sectors to minimize the impact of disasters.

During FY 2023, FEMA concluded that $1.2 billion in Public Assistance disbursements that had been designated as unknown payments in prior years could be adequately supported and classified as proper payments. FEMA will continue to work on determining if previously identified unknown payments are in fact proper or improper. If determined to be improper with a monetary loss associated, FEMA will work to recoup those payments as applicable.

Disaster Supplemental DHS Programs Not Required to Report[26]

For programs baselined and determined to be below the thresholds to be deemed susceptible to significant improper payments, OMB Circular No. A-123, Appendix C guidance instructs the programs be reverted from Phase II (required to publish reporting) to Phase I (not required to publish reporting). Following FY 2022 reporting, DHS reverted the following programs to Phase I:

- FEMA Disaster Case Management – Disaster Supplemental Funds
- FEMA Payroll – Disaster Supplemental Funds
- FEMA Vendor Pay – Disaster Supplemental Funds
- USCG Aviation Logistics Command – Disaster Supplemental Funds
- USCG PC&I – Disaster Supplemental Funds

As these programs are currently in Phase I, they are not applicable for OMB reporting and publication on PaymentAccuracy.gov.

However, for the FEMA Payroll – Disaster Supplemental Funds and the FEMA Vendor Pay – Disaster Supplemental Funds programs, in order to ensure that the program remained not susceptible to significant improper payments, DHS proactively selected to continue to perform internal statistical testing for the program in FY 2023, over FY 2021 disbursements.

FEMA Payroll – Disaster Supplemental Funds Program

The federal disaster workforce is designed to scale up or down depending on the timing and magnitude of disasters, and primarily includes the following categories of employees:

- **Title 5** – Employees that make up FEMA's day-to-day workforce and are responsible for administering the agency's ongoing program activities. During disasters, these employees can be deployed as needed.

- **Stafford Act** – Stafford Act employees provide support for disaster-related activities and augment FEMA's disaster workforce. Stafford Act employees include on call and recovery staff who are temporary employees and can be deployed to fulfill any role specifically related to the incident for which they are hired and qualified. In addition, reservists can be utilized. These reservists work on an intermittent basis and are deployed as needed to fulfill incident management roles.

- **Surge Capacity Force** – The Surge Capacity Force supplements FEMA's disaster workforce in a major disaster and consists of volunteers who are employees of DHS components, such as the Transportation Security Administration and U.S. Secret

---

[26] OMB Circular No. A-123, Appendix C (M-21-19) states "If a program is in Phase II, has established a baseline, and reports an IP and UP estimate that is below the statutory threshold it will automatically move back into Phase I the following FY". However, the Component can still choose to test these programs to show continued compliance.

Service, as well as employees of other federal agencies, as authorized by the Post-Katrina Emergency Reform Act of 2006.[27]

- **FEMA Corps** – FEMA Corps is a team-based national service program operated by AmeriCorps in partnership with FEMA. Members are not FEMA employees but are deployed to augment FEMA's workforce for disaster readiness, preparedness, response, and recovery work under the supervision of FEMA staff.

For the testing conducted in 2023, FEMA's assessment was focused on the associated FY 2021 disaster supplemental funding disbursements of over $180 million applicable for review under PIIA. The FEMA Payroll – Disaster Supplemental Funds program internally reported a 3.76 percent estimated payment error rate equating to approximately $6.81 million in consolidated improper and unknown payments in 2023. As indicated by the internal review results, the program continues to report below the OMB Circular No. A-123, Appendix C guidance thresholds to be considered susceptible to significant improper payments.

Surge Capacity Force

If an incident exceeds the capacity of the FEMA disaster workforce, the DHS Secretary is authorized to activate the DHS Surge Capacity Force to change the federal response to a catastrophic disaster. FEMA manages this program that relies on federal employees from DHS Components and other federal agencies to support its mission of helping people before, during, and after disasters. Volunteers have the chance to work in a variety of recovery responsibilities, including logistics; public assistance, debris monitoring; individual assistance, such as aid to survivors; disaster survivor assistance, to notify the public about available assistance programs; information technology; human resources; external affairs, acquisitions; and planning.

---

[27] 6 U.S.C. 711(b)

FEMA Vendor Payments – Disaster Supplemental Funds Program

FEMA strives to disburse prompt payments for goods and services that are covered by the Prompt Payment Act. Most of the payments falling under the Vendor Payments – Disaster Supplemental Funds program are contractual, to include rental and lease agreements, purchase orders, delivery orders, blanket purchase agreements, etc., invoice payments based on the receipt of satisfactory performance of contract terms in support of disaster response as a result of Hurricanes Harvey, Irma, and Maria.

For the testing conducted in 2023, FEMA's assessment was focused on the associated FY 2021 disaster supplemental funding disbursements of just under $200 million applicable for review under PIIA. The FEMA Vendor Payments – Disaster Supplemental Funds program internally reported a 0.25 percent estimated payment error rate equating to approximately $0.49 million in consolidated improper and unknown payments in 2023. As indicated by the internal review results, the program continues to report below the OMB Circular No. A-123, Appendix C guidance thresholds to be considered susceptible to significant improper payments.

Payment Integrity Reporting

The table below summarizes improper payment amounts for all DHS programs deemed to be susceptible to significant improper payments. It provides a breakdown of estimated proper as well as consolidated improper and unknown payments and the associated rates for each applicable DHS program or activity. In comparison to prior year reporting, DHS has:

- Removed five programs from PIIA Phase II reporting, effective for the 2023 reporting period as they dropped below the $10 million outlay threshold based on FY 2021 disbursement activity and/ or have adequately baselined the program under PIIA requirements and have been determined to not be susceptible to significant improper payments and thus reverted to PIIA Phase I.
    - FEMA Disaster Case Management – Disaster Supplemental Funds
    - FEMA Payroll – Disaster Supplemental Funds
    - FEMA Vendor Payments - Disaster Supplemental Funds
    - USCG Aviation Logistics Command – Disaster Supplemental Funds
    - USCG PC&I – Disaster Supplemental Funds
- Continued PIIA Phase II reporting for one program, based on FY 2021 disbursement activity, effective for the 2023 reporting period.
    - FEMA HMGP – Disaster Supplemental Funds
- Delayed PIIA Phase II reporting, in accordance with instruction received from OMB, for one program, based on FY 2021 disbursement activity[28].
    - FEMA Public Assistance - VAYGo
- Added one program into PIIA Phase II reporting, based on FY 2021 disbursement activity, effective for the 2023 reporting period.
    - CBP PC&I – Disaster Supplemental Funds

For additional information related to the Department's improper payment efforts, details on the annual results to include error reasoning, corrective actions, as well as other areas of interest, please refer to the government-wide reporting archive available on PaymentAccuracy.gov.

---

[28] Due to the increase in assessment burden, the PIIA Phase II reporting to cover FY 2021 disbursements has been delayed until 2024.

Table 10: DHS Improper Payment Results and Reduction Outlook

DHS Program Name	Testing Conducted in FY 2022			Testing Conducted in FY 2023					Testing Planned for FY 2024
	Outlays ($M)	IP + UP ($M)	IP + UP (%)	Outlays ($M)	Proper ($M)	Proper (%)	IP + UP ($M)	IP + UP (%)	Reduction Target (%)
DHS Programs in Phase II and Reporting on Disbursements from Two Fiscal Years Prior									
CBP PC&I – Disaster Supplemental Funds	*N/A -Program identified to begin reporting in 2023*			$10.89	$10.89	100.00%	$0.00	0.00%	*N/A[29]*
FEMA HMGP – Disaster Supplemental Funds	$32.04	$2.24	6.99%	$59.91	$59.38	99.12%	$0.53	0.88%	1.50%
FEMA Public Assistance – VAYGo[30]	$4,767.94	$242.88	5.09%	N/A	N/A	N/A	N/A	N/A	N/A
Stratum: Disaster Supplemental Funds	*$2,231.69*	*$84.16*	*3.77%*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Stratum: All Other	*$2,536.26*	*$158.73*	*6.26%*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
DHS Programs Moved out of Phase II (Statistical Testing and Reporting) in 2023									
FEMA Disaster Case Management – Disaster Supplemental Funds	$66.21	$1.11	1.68%	*N/A - Program did not exceed $10M of FY 2021 disbursements from Disaster Supplemental Funding. As such, the FEMA Disaster Case Management – Disaster Supplemental Funds program has been reverted to Phase I.*					
FEMA Payroll – Disaster Supplemental Funds[31]	$252.16	$7.27	2.88%	*N/A – As program was below the thresholds to be deemed susceptible to significant improper payments, the FEMA Payroll – Disaster Supplemental Funds program has been reverted to Phase I.*					
FEMA Vendor Payments – Disaster Supplemental Funds[32]	$495.26	$3.47	0.70%	*N/A – As program was below the thresholds to be deemed susceptible to significant improper payments, the FEMA Vendor Pay – Disaster Supplemental Funds program has been reverted to Phase I.*					
USCG Aviation Logistics Command – Disaster Supplemental Funds	$25.11	$0.00	0.00%	*N/A – As program was below the thresholds to be deemed susceptible to significant improper payments, the USCG Aviation Logistics Command – Disaster Supplemental Funds program has been reverted to Phase I.*					
USCG PC&I – Disaster Supplemental Funds	$52.40	$0.30	0.58%	*N/A – As program was below the thresholds to be deemed susceptible to significant improper payments, the USCG PC&I – Disaster Supplemental Funds program has been reverted to Phase I.*					
TOTAL	$5,691.12	$257.28	4.52%[33]	$70.80	$70.27	99.25%	$0.53	0.75%[34]	N/A

---

[29] As the FY 2023 reporting was the first year of PIIA reporting for the CBP PC&I – Disaster Supplemental Funds program, DHS is not considering the program fully baselined and thus has not published a reduction target for this program.

[30] Due to the increase in assessment burden, the PIIA Phase II reporting to cover FY 2021 disbursements has been delayed until 2024..

[31] As program was below the thresholds to be deemed susceptible to significant improper payments, the FEMA Payroll – Disaster Supplemental Funds program has been reverted to Phase I. However, to ensure that the program is truly not susceptible to significant improper payments, DHS selected to continue to perform internal statistical testing for the program in FY 2023, over FY 2021 disbursements. Please refer to the "Disaster Supplemental DHS Programs Not Required to Report" subsection for the results of this effort.

[32] As program was below the thresholds to be deemed susceptible to significant improper payments, the FEMA Vendor Pay – Disaster Supplemental Funds program has been reverted to Phase I. However, to ensure that the program is truly not susceptible to significant improper payments, DHS selected to continue to perform internal statistical testing for the program in FY 2023, over FY 2021 disbursements. Please refer to the "Disaster Supplemental DHS Programs Not Required to Report" subsection for the results of this effort.

[33] The total does not represent a true statistical improper payment estimate for the Department.

[34] The total does not represent a true statistical improper payment estimate for the Department.

Actions Taken to Address Auditor Recovery Recommendations

During FY 2023, the Department did not have any recapture audit activities conducted. As such, DHS did not have any auditor recovery recommendations to be addressed and reported in 2023.

For additional information related to the Department's recovery audit efforts, please refer to PaymentAccuracy.gov.

The DHS continues its efforts in closing out grants and cooperative agreements awards. The summary table below shows the number of awards and balances for which closeouts has not yet occurred, but for which period of performance had elapse by two years or more prior to September 30, 2023 (i.e., on or before September 30, 2021).

Table 11: Grants/Cooperative Agreements Summary Status

Category	Years FY 2021	3-5 Years FYs 2018 - 20	> 5 Years FY 2017 and prior
Number of Grants/Cooperative Agreements with Zero Dollar Balances	30	47	4
Number of Grants/Cooperative Agreements with Undistributed Balances	36	22	9
Total Amount of Undistributed Balances	$17,078,494	$6,688,633	$7,706,670

The above table comprises only FEMA's data and efforts in closing out its grants and cooperative agreements. During FY 2023, FEMA continued to make a concerted effort to reduce the backlog of open grant awards through improved tracking, oversight, and coordination with responsible offices. Due to FEMA's efforts, the FY 2023 reportable population is 7% less than the grant population that the agency reported in FY 2022 and an 91% reduction since the agency reported in FY 2020. FEMA also significantly reduced the Total Amount of Undistributed Balances from $44.39M in FY22 to $31.47M in FY 2023, a 29% reduction.

FEMA has deployed electronic closeout capabilities within FEMA GO, which will ensure a consistent closeout process across grants. This capability will positively support the timely closure of grant awards. Actions to be taken to closeout reported awards include, but are not limited to, continued tracking, oversight, and coordination with responsible officers, and systematic closeout functionality development.

Additionally, FEMA is monitoring and reporting on the timely closure of disaster and non-disaster grant awards on an annual basis via the Government Performance and Results Act (GPRA) Closeout Performance Measure. Since implementing this monitoring activity, FEMA has met and exceeded the established target goals for FY21 (70%), FY22 (72%), and FY23 (75%). The target goal for FY24 will be to close 80% of the monitored grant population within 365 calendar days from POP expiration.

In FY 2023, DHS awarded $36.5 billion in grants and cooperative agreements through seven DHS financial assistance awarding offices. The awarding offices include the Federal Emergency Management Agency, U.S. Coast Guard, U.S. Citizenship and Immigration Services, Cybersecurity and Infrastructure Security Agency, U.S. Immigration and Customs Enforcement, Science and Technology Directorate, and Countering Weapons of Mass Destruction Office. FEMA awarded 99% of DHS grants and cooperative agreements in FY 2023.

The DHS continues its efforts in closing out grants and cooperative agreements awards. The summary table below shows the number of awards and balances for which closeouts has not yet occurred, but for which period of performance had elapse by two years or more prior to September 30, 2023 (i.e., on or before September 30, 2021)

Unaudited

Civil Monetary Penalty Adjustment for Inflation

The Federal Civil Penalties Inflation Adjustment Act of 1990, as amended, requires agencies to make regular and consistent inflationary adjustments of civil monetary penalties to maintain their deterrent effect.

The following represents the Department's civil monetary penalties, all of which were last updated via regulation in 2023. Additional information about these penalties and the latest adjustment is available in the Federal Register Volume 88, No. 2175.

Table 12: Civil Monetary Penalties

Penalty	Authority	Year Enacted	Adjusted New Penalty
CBP			
Non-compliance with arrival and departure manifest requirements for passengers, crew members, or occupants transported on commercial vessels or aircraft arriving to or departing from the United States	8 USC 1221(g); INA Section 231(g); 8 CFR 280.53(b)(1)	2002	$1,643
Non-compliance with landing requirements at designated ports of entry for aircraft transporting aliens	8 USC 1224; INA Section 234; 8 CFR 280.53(b)(2)	1990	$4,465
Violations of removal orders relating to aliens transported on vessels or aircraft under section 241(d) of the INA, or for costs associated with removal under section 241(e) of the INA	8 USC 1253(c)(1)(A); INA Section 243(c)(1)(A); 8 CFR 280.53(b)(4)	1996	$3,765
Failure to remove alien stowaways under section 241(d)(2) of the INA	8 USC 1253(c)(1)(B); INA Section 243(c)(1)(B); 8 CFR 280.53(b)(5)	1996	$9,413
Failure to report an illegal landing or desertion of alien crewmen, and for each alien not reported on arrival or departure manifest or lists required in accordance with section 251 of the INA (for each alien)	8 USC 1281(d); INA Section 251(d); 8 CFR 280.53(b)(6)	1990	$446
Use of alien crewmen for longshore work in violation of section 251(d) of the INA	8 USC 1281(d); INA Section 251(d); 8 CFR 280.53(b)(6)	1990	$11,162
Failure to control, detain, or remove alien crewmen	8 USC 1284(a); INA Section 254(a); 8 CFR 280.53(b)(7)	1990	Minimum $1,116 Maximum $6,696
Employment on passenger vessels of aliens afflicted with certain disabilities	8 USC 1285; INA Section 255; 8 CFR 280.53(b)(8)	1990	$2,232
Discharge of alien crewmen	8 USC 1286; INA Section 256; 8 CFR 280.53(b)(9)	1990	Minimum $3,348 Maximum $6,696
Bringing into the United States alien crewmen with intent to evade immigration laws	8 USC 1287; INA Section 257; 8 CFR 280.53(b)(10)	1990	$22,324

Unaudited

Penalty	Authority	Year Enacted	Adjusted New Penalty
Failure to prevent the unauthorized landing of aliens	8 USC § 1321(a); INA Section 271(a); 8 CFR 280.53(b)(11)	1990	$6,696
Bringing to the United States aliens subject to denial of admission on a health-related ground	8 USC § 1322(a); INA Section 272(a); 8 CFR 280.53(b)(12)	1990	$6,696
Bringing to the United States aliens without required documentation	8 USC § 1323(b); INA Section 273(b); 8 CFR 280.53(b)(13)	1990	$6,696
Improper entry	8 USC § 1325(b) INA Section 275(b); 8 CFR 280.53(b)(15)	1996	Minimum $94 Maximum $472
Dealing in or using empty stamped imported liquor containers	19 USC 469	1879	$625
Transporting passengers between coastwise points in the United States by a non-coastwise qualified vessel	46 USC 55103(b); 19 CFR 4.80(b)(2)	1898	$941
Towing a vessel between coastwise points in the United States by a non-coastwise qualified vessel	46 USC 55111(c); 19 CFR 4.92	1940	Minimum $1,096 Maximum $3,446 plus $187 per ton
Failure to depart voluntarily	8 USC 1229(c)(d); INA Section 243(c)(1)(A); 8 CFR 280.53(b)(3)	1952	Minimum $1,881; Maximum $9,413
Failure to depart	8 USC 1324d; INA Section 274D; 8 CFR 280.53(b)(14)	1952	$942
Employing a vessel in a trade without a required Certificate of Documentation	19 USC 1706(a); 19 CFR 4.80(i)	1980	$1,566
Transporting passengers coastwise for hire by certain vessels (knows as Bowaters vessels) that do not meet specified conditions	46 USC 12118(f)(3)	1958	$625
CISA			
Non-compliance with CFATS regulations	6 USC 624(b)(1); 6 CFR 27.300(b)(3)	2002	$41,093
ICE			
Violation of Immigration and Naturalization Act (INA) sections 274C(a)(1)–(a)(4) (First offense)	8 CFR 270.3(b)(1)(ii)(A)	1990	Minimum $ 557 Maximum $4,465
Violation of Immigration and Naturalization Act (INA) sections 274C(a)(5)–(a)(6) (First offense)	8 CFR 270.3(b)(1)(ii)(B)	1996	Minimum $472 Maximum $3,765

Unaudited

Penalty	Authority	Year Enacted	Adjusted New Penalty
Violation of Immigration and Naturalization Act (INA) sections 274C(a)(1)–(a)(4) (Subsequent offenses)	8 CFR 270.3(b)(1)(ii)(C)	1990	Minimum $4,465 Maximum $11,162
Violation of Immigration and Naturalization Act (INA) sections 274C(a)(5)–(a)(6) (Subsequent offenses)	8 CFR 270.3(b)(1)(ii)(D)	1996	Minimum $3,765 Maximum $9,413
Violation/prohibition of indemnity bonds	8 CFR 274a.8(b)	1986	$2,701
Knowingly hiring, recruiting, referral, or retention of unauthorized aliens (per unauthorized alien) (First offense)	8 CFR 274a.10(b)(1)(ii)(A)	1986	Minimum $676 Maximum $5,404
Knowingly hiring, recruiting, referral, or retention of unauthorized aliens (per unauthorized alien) (Second offense)	8 CFR 274a.10(b)(1)(ii)(B)	1986	Minimum $5,404 Maximum $13,508
Knowingly hiring, recruiting, referral, or retention of unauthorized aliens (per unauthorized alien) (Subsequent offenses)	8 CFR 274a.10(b)(1)(ii)(C)	1986	Minimum $8,106 Maximum $27,018
I–9 paperwork violations	8 CFR 274a.10(b)(2)	1986	Minimum $272 Maximum $2,701
Failure to depart voluntarily	8 USC 1229c(d); INA Section 240B(d); 8 CFR 280.53(b)(3)	1996	Minimum $1,881 Maximum $9,413
Failure to depart	8 USC 1324(d); INA Section 274D; 8 CFR 280.53(b)(14)	1996	$942
TSA			
Certain aviation related violations by an individual or small business concern (49 CFR Ch. XII § 1503.401(c)(1))	49 USC 46301(a)(1), (4), (5); 49 USC 46301(d)(8)	2003	$16,108 (up to a total of $80,544,total for small business, $644,343 for others)
Certain aviation related violations by any other person not operating an aircraft for the transportation of passengers or property for compensation (49 CFR Ch. XII § 1503.401(c)(2))	49 USC 46301(a)(1), (4), (5); 49 USC 46301(d)(8)	2003	$16,108 (up to a total of $80,544,total for small business, $644,343 for others)
Certain aviation related violations by a person operating an aircraft for the transportation of passengers or property for compensation (49 CFR Ch. XII § 1503.401(c)(3))	49 USC 46301(a)(1), (4), (5), (6); 49 USC 46301(d)(2), (8)	2003	$40,272 (up to a total of $644,343 per civil penalty action)

Unaudited

Penalty	Authority	Year Enacted	Adjusted New Penalty
Violation of any other provision of title 49 USC or of 46 USC Ch. 701, a regulation prescribed, or order issued under thereunder (49 CFR Ch. XII § 1503.401(b))	49 USC 114(u)	2009	$13,785 (up to a total of $68,928 for individuals and small businesses, $551,417 for others)
USCG			
Saving Life and Property	14 USC 521(c)	2014	$12,551
Saving Life and Property (Intentional Interference with Broadcast)	14 USC 521(e)	2012	$1,288
Confidentiality of Medical Quality Assurance Records (first offense)	14 USC 645(i); 33 CFR 27.3	1992	$6,304
Confidentiality of Medical Quality Assurance Records (subsequent offenses)	14 USC 645(i); 33 CFR 27.3	1992	$42,032
Aquatic Nuisance Species in Waters of the United States	16 USC 4711(g)(1); 33 CFR 27.3	1996	$47,061
Obstruction of Revenue Officers by Masters of Vessels	19 USC 70; 33 CFR 27.3	1935	$9,399
Obstruction of Revenue Officers by Masters of Vessels—Minimum Penalty	19 USC 70; 33 CFR 27.3	1935	$2,193
Failure to Stop Vessel When Directed; Master, Owner, Operator or Person in Charge	19 USC 1581(d)	1930	$5,891
Failure to Stop Vessel When Directed; Master, Owner, Operator or Person in Charge - Minimum Penalty	19 USC 1581(d)	1930	$1,179
Anchorage Ground/Harbor Regulations General	33 USC 471; 33 CFR 27.3	2010	$13,627
Anchorage Ground/Harbor Regulations St. Mary's River	33 USC 474; 33 CFR 27.3	1946	$941
Bridges/Failure to Comply with Regulations	33 USC 495(b); 33 CFR 27.3	2008	$34,401
Bridges/Drawbridges	33 USC 499(c); 33 CFR 27.3	2008	$34,401
Bridges/Failure to Alter Bridge Obstructing Navigation	33 USC 502(c); 33 CFR 27.3	2008	$34,401
Bridges/Maintenance and Operation	33 USC 533(b); 33 CFR 27.3	2008	$34,401
Bridge to Bridge Communication; Master, Person in Charge or Pilot	33 USC 1208(a); 33 CFR 27.3	1971	$2,506
Bridge to Bridge Communication; Vessel	33 USC 1208(b); 33 CFR 27.3	1971	$2,506
PWSA Regulations	33 USC 1232(a)	1978	$111,031

Unaudited

Penalty	Authority	Year Enacted	Adjusted New Penalty
Vessel Navigation: Regattas or Marine Parades; Unlicensed Person in Charge	46 USC 70041(d)(1)(B); 33 CFR 27.3	1990	$11,162
Vessel Navigation: Regattas or Marine Parades; Owner Onboard Vessel	46 USC 70041(d)(1)(C); 33 CFR 27.3	1990	$11,162
Vessel Navigation: Regattas or Marine Parades; Other Persons	46 USC 70041(d)(1)(D); 33 CFR 27.3	1990	$5,580
Oil/Hazardous Substances: Discharges (Class I per violation)	33 USC 1321(b)(6)(B)(i); 33 CFR 27.3	1990	$22,324
Oil/Hazardous Substances: Discharges (Class I total under paragraph)	33 USC 1321(b)(6)(B)(i); 33 CFR 27.3	1990	$55,808
Oil/Hazardous Substances: Discharges (Class II per day of violation)	33 USC 1321(b)(6)(B)(ii); 33 CFR 27.3	1990	$22,324
Oil/Hazardous Substances: Discharges (Class II total under paragraph)	33 USC 1321(b)(6)(B)(ii); 33 CFR 27.3	1990	$279,036
Oil/Hazardous Substances: Discharges (per day of violation) Judicial Assessment	33 USC 1321(b)(7)(A); 33 CFR 27.3	1990	$55,808
Oil/Hazardous Substances: Discharges (per barrel of oil or unit discharged) Judicial Assessment	33 USC 1321(b)(7)(A); 33 CFR 27.3	1990	$2,232
Oil/Hazardous Substances: Failure to Carry Out Removal/Comply With Order (Judicial Assessment)	33 USC 1321(b)(7)(B); 33 CFR 27.3	1990	$55,808
Oil/Hazardous Substances: Failure to Comply with Regulation Issued Under 1321(j) (Judicial Assessment)	33 USC 1321(b)(7)(C); 33 CFR 27.3	1990	$55,808
Oil/Hazardous Substances: Discharges, Gross Negligence (per barrel of oil or unit discharged) Judicial Assessment	33 USC 1321(b)(7)(D); 33 CFR 27.3	1990	$6,696
Oil/Hazardous Substances: Discharges, Gross Negligence—Minimum Penalty (Judicial Assessment)	33 USC 1321(b)(7)(D); 33 CFR 27.3	1990	$223,229
Marine Sanitation Devices; Operating	33 USC 1322(j); 33 CFR 27.3	1972	$9,399
Marine Sanitation Devices; Sale or Manufacture	33 USC 1322(j); 33 CFR 27.3	1972	$25,059
International Navigation Rules; Operator	33 USC 1608(a); 33 CFR 27.3	1980	$17,570
International Navigation Rules; Vessel	33 USC 1608(b); 33 CFR 27.3	1980	$17,570
Pollution from Ships; General	33 USC 1908(b)(1); 33 CFR 27.3	1980	$87,855
Pollution from Ships; False Statement	33 USC 1908(b)(2); 33 CFR 27.3	1980	$17,570
Inland Navigation Rules; Operator	33 USC 2072(a); 33 CFR 27.3	1980	$17,570

Unaudited

Penalty	Authority	Year Enacted	Adjusted New Penalty
Inland Navigation Rules; Vessel	33 USC 2072(b); 33 CFR 27.3	1980	$17,570
Shore Protection; General	33 USC 2609(a); 33 CFR 27.3	1988	$61,982
Shore Protection; Operating Without Permit	33 USC 2609(b); 33 CFR 27.3	1988	$24,793
Oil Pollution Liability and Compensation	33 USC 2716a(a); 33 CFR 27.3	1990	$55,808
Clean Hulls; Civil Enforcement	33 USC 3852(a)(1)(A); 33 CFR 27.3	2010	$51,097
Clean Hulls; False statements	33 USC 3852(a)(1)(A); 33 CFR 27.3	2010	$68,129
Clean Hulls; Recreational Vessel	33 USC 3852(c); 33 CFR 27.3	2010	$6,813
Hazardous Substances, Releases Liability, Compensation (Class I)	42 USC 9609(a); 33 CFR 27.3	1986	$67,544
Hazardous Substances, Releases Liability, Compensation (Class II)	42 USC 9609(b); 33 CFR 27.3	1986	$67,544
Hazardous Substances, Releases Liability, Compensation (Class II subsequent offense)	42 USC 9609(b); 33 CFR 27.3	1986	$202,635
Hazardous Substances, Releases, Liability, Compensation (Judicial Assessment)	42 USC 9609(c); 33 CFR 27.3	1986	$67,544
Hazardous Substances, Releases, Liability, Compensation (Judicial Assessment subsequent offense)	42 USC 9609(c); 33 CFR 27.3	1986	$202,635
Safe Containers for International Cargo	46 USC 80509; 33 CFR 27.3	2006	$7,383
Suspension of Passenger Service	46 USC 70305; 33 CFR 27.3	2006	$73,837
Vessel Inspection or Examination Fees	46 USC 2110(e); 33 CFR 27.3	1990	$11,162
Alcohol and Dangerous Drug Testing	46 USC 2115; 33 CFR 27.3	1998	$9,086
Negligent Operations: Recreational Vessels	46 USC 2302(a); 33 CFR 27.3	2002	$8,219
Negligent Operations: Other Vessels	46 USC 2302(a); 33 CFR 27.3	2002	$41,093
Operating a Vessel While Under the Influence of Alcohol or a Dangerous Drug	46 USC 2302(c)(1); 33 CFR 27.3	1998	$9,086
Vessel Reporting Requirements: Owner, Charterer, Managing Operator, or Agent	46 USC 2306(a)(4); 33 CFR 27.3	1984	$14,149
Vessel Reporting Requirements: Master	46 USC 2306(b)(2); 33 CFR 27.3	1984	$2,830
Immersion Suits	46 USC 3102(c)(1); 33 CFR 27.3	1984	$14,149
Inspection Permit	46 USC 3302(i)(5); 33 CFR 27.3	1983	$2,951
Vessel Inspection; General	46 USC 3318(a); 33 CFR 27.3	1984	$14,149
Vessel Inspection; Nautical School Vessel	46 USC 3318(g); 33 CFR 27.3	1984	$14,149

Unaudited

U.S. Department of Homeland Security

Penalty	Authority	Year Enacted	Adjusted New Penalty
Vessel Inspection; Failure to Give Notice IAW 3304(b)	46 USC 3318(h); 33 CFR 27.3	1984	$2,830
Vessel Inspection; Failure to Give Notice IAW 3309 (c)	46 USC 3318(i); 33 CFR 27.3	1984	$2,830
Vessel Inspection; Vessel ≥ 1600 Gross Tons	46 USC 3318(j)(1); 33 CFR 27.3	1984	$28,304
Vessel Inspection; Vessel <1600 Gross Tons	46 USC 3318(j)(1); 33 CFR 27.3	1984	$5,661
Vessel Inspection; Failure to Comply with 3311(b)	46 USC 3318(k); 33 CFR 27.3	1984	$28,304
Vessel Inspection; Violation of 3318(b)-3318(f)	46 USC 3318(l); 33 CFR 27.3	1984	$14,149
List/count of Passengers	46 USC 3502(e); 33 CFR 27.3	1983	$294
Notification to Passengers	46 USC 3504(c); 33 CFR 27.3	1983	$29,505
Notification to Passengers; Sale of Tickets	46 USC 3504(c); 33 CFR 27.3	1983	$1,474
Copies of Laws on Passenger Vessels; Master	46 USC 3506; 33 CFR 27.3	1983	$590
Liquid Bulk/Dangerous Cargo	46 USC 3718(a)(1); 33 CFR 27.3	1983	$73,764
Uninspected Vessels	46 USC 4106; 33 CFR 27.3	1988	$12,397
Recreational Vessels (maximum for related series of violations)	46 USC 4311(b)(1); 33 CFR 27.3	2004	$390,271
Recreational Vessels; Violation of 4307(a)	46 USC 4311(b)(1); 33 CFR 27.3	2004	$7,805
Recreational Vessels	46 USC 4311(c); 33 CFR 27.3	1983	$2,951
Uninspected Commercial Fishing Industry Vessels	46 USC 4507; 33 CFR 27.3	1988	$12,397
Abandonment of Barges	46 USC 4703; 33 CFR 27.3	1992	$2,100
Load Lines	46 USC 5116(a); 33 CFR 27.3	1986	$13,508
Load Lines; Violation of 5112(a)	46 USC 5116(b); 33 CFR 27.3	1986	$27,018
Load Lines; Violation of 5112(b)	46 USC 5116(c); 33 CFR 27.3	1986	$13,508
Reporting Marine Casualties	46 USC 6103(a); 33 CFR 27.3	1996	$47,061
Reporting Marine Casualties; Violation of 6104	46 USC 6103(b); 33 CFR 27.3	1988	$12,397
Manning of Inspected Vessels; Failure to Report Deficiency in Vessel Complement	46 USC 8101(e); 33 CFR 27.3	1990	$2,232
Manning of Inspected Vessels	46 USC 8101(f); 33 CFR 27.3	1990	$22,324

Unaudited

Penalty	Authority	Year Enacted	Adjusted New Penalty
Manning of Inspected Vessels; Employing or Serving in Capacity not Licensed by USCG	46 USC 8101(g); 33 CFR 27.3	1990	$22,324
Manning of Inspected Vessels; Freight Vessel <100 GT, Small Passenger Vessel, or Sailing School Vessel	46 USC 8101(h); 33 CFR 27.3	1983	$2,951
Watchmen on Passenger Vessels	46 USC 8102(a)	1983	$2,951
Citizenship Requirements	46 USC 8103(f)	1983	$1,474
Watches on Vessels; Violation of 8104(a) or (b)	46 USC 8104(i)	1990	$22,324
Watches on Vessels; Violation of 8104(c), (d), (e), or (h)	46 USC 8104(j)	1990	$22,324
Staff Department on Vessels	46 USC 8302(e)	1983	$294
Officer's Competency Certificates	46 USC 8304(d)	1983	$294
Coastwise Pilotage; Owner, Charterer, Managing Operator, Agent, Master or Individual in Charge	46 USC 8502(e)	1990	$22,324
Coastwise Pilotage; Individual	46 USC 8502(f)	1990	$22,324
Federal Pilots	46 USC 8503	1984	$70,752
Merchant Mariners Documents	46 USC 8701(d)	1983	$1,474
Crew Requirements	46 USC 8702(e)	1990	$22,324
Small Vessel Manning	46 USC 8906	1996	$47,061
Pilotage: Great Lakes; Owner, Charterer, Managing Operator, Agent, Master or Individual in Charge	46 USC 9308(a)	1990	$22,324
Pilotage: Great Lakes; Individual	46 USC 9308(b)	1990	$22,324
Pilotage: Great Lakes; Violation of 9303	46 USC 9308(c)	1990	$22,324
Failure to Report Sexual Offense	46 USC 10104(b)	1989	$11,864
Pay Advances to Seamen	46 USC 10314(a)(2)	1983	$1,474
Pay Advances to Seamen; Remuneration for Employment	46 USC 10314(b)	1983	$1,474
Allotment to Seamen	46 USC 10315(c)	1983	$1,474
Seamen Protection; General	46 USC 10321	1993	$10,226
Coastwise Voyages: Advances	46 USC 10505(a)(2)	1993	$10,226

Unaudited

U.S. Department of Homeland Security

Penalty	Authority	Year Enacted	Adjusted New Penalty
Coastwise Voyages: Advances; Remuneration for Employment	46 USC 10505(b)	1993	$10,226
Coastwise Voyages: Seamen Protection; General	46 USC 10508(b)	1993	$10,226
Effects of Deceased Seamen	46 USC 10711	1983	$590
Complaints of Unfitness	46 USC 10902(a)(2)	1983	$1,474
Proceedings on Examination of Vessel	46 USC 10903(d)	1983	$294
Permission to Make Complaint	46 USC 10907(b)	1983	$1,474
Accommodations for Seamen	46 USC 11101(f)	1983	$1,474
Medicine Chests on Vessels	46 USC 11102(b)	1983	$1,474
Destitute Seamen	46 USC 11104(b)	1983	$294
Wages on Discharge	46 USC 11105(c)	1983	$1,474
Log Books; Master Failing to Maintain	46 USC 11303(a)	1983	$590
Log Books; Master Failing to Make Entry	46 USC 11303(b)	1983	$590
Log Books; Late Entry	46 USC 11303(c)	1983	$443
Carrying of Sheath Knives	46 USC 11506	1983	$148
Documentation of Vessels	46 USC 12151(a)(1)	2012	$19,324
Documentation of Vessels; Activities involving mobile offshore drilling units	46 USC 12151(a)(2)	2012	$32,208
Engaging in Fishing After Falsifying Eligibility (fine per day)	46 USC 12151(c)	2006	$147,675
Numbering of Undocumented Vessel; Willful violation	46 USC 12309(a)	1983	$14,754
Numbering of Undocumented Vessels	46 USC 12309(b)	1983	$2,951
Vessel Identification System	46 USC 12507(b)	1988	$24,793
Measurement of Vessels	46 USC 14701	1986	$54,038
Measurement; False Statements	46 USC 14702	1986	$54,038
Commercial Instruments and Maritime Liens	46 USC 31309	1988	$24,793
Commercial Instruments and Maritime Liens; Mortgagor	46 USC 31330(a)(2)	1988	$24,793
Commercial Instruments and Maritime Liens; Violation of 31329	46 USC 31330(b)(2)	1988	$61,982

Unaudited

Penalty	Authority	Year Enacted	Adjusted New Penalty
Port Security	46 USC 70119(a)	2002	$41,093
Port Security; Continuing Violations	46 USC 70119(b)	2006	$73,837
Maritime Drug Law Enforcement	46 USC 70506(c)	2010	$6,813
Hazardous Materials: Related to Vessels	49 USC 5123(a)(1)	2012	$96,624
Hazardous Materials: Related to Vessels; Penalty from Fatalities, Serious Injuries/ Illness or substantial Damage to Property	49 USC 5123(a)(2)	2012	$225,455
Hazardous Materials: Related to Vessels; Training	49 USC 5123(a)(3)	2012	$582

Unaudited

U.S. Department of Homeland Security

Other Key Regulatory Requirements

Prompt Payment Act

The Prompt Payment Act requires federal agencies to make timely payments (within 30 days of receipt of invoice) to vendors for supplies and services, to pay interest penalties when payments are made after the due date, and to take cash discounts only when they are economically justified. The Department's Components submit Prompt Payment data for the OMB CFO Council's Metric Tracking System. Metric statistics are reported with at least a six-week lag. DHS Components conduct periodic reviews to identify potential problems. On time-payments for FY 2023 were 89% versus the goal of 98%. Total interest paid in FY 2023 was $2,932,604.64 or $113.95 per million invoiced. During FY 2022 the total interest paid was $2,446,172.28 or $110.93 per million invoiced. The increase in interest paid from FY 2022 to 2023 is due to a combination of a financial system transition at the U.S. Coast Guard and the ability to timely pay invoices during the transition and stabilization period in the early months of FY 2023 as well as a significant increase in interest rates used to calculate the interest penalties.

Debt Collection Improvement Act

The Debt Collection Improvement Act (DCIA) of 1996 passed as part of the Omnibus Consolidated Rescissions and Appropriations Act of 1996 (P.L. 100-134) tasked Treasury with certain governmentwide debt collection responsibilities. Among other things, the law provides that delinquent non-tax debts generally must be turned over to the Treasury for appropriate action to collect the debt. Certain types of debts are exempt from this requirement. In compliance with DCIA, the Department manages its debt collection activities under the DHS DCIA regulation. The regulation is implemented under the Department's comprehensive debt collection policies that provide guidance to the Components on the administrative collection of debt; referring non-taxable debt; writing off non-taxable debt; reporting debt to consumer reporting agencies; assessing interest, penalties, and administrative costs; and reporting receivables to the Treasury. The Digital Accountability and Transparency Act of 2014 was passed on May 2014 and updated DCIA requirements for referring non-taxable debt.

Unaudited

Office of Inspector General's Report on Major Management and Performance Challenges Facing the Department of Homeland Security

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

November 3, 2023

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

Major Management and Performance Challenges Facing the Department of Homeland Security

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.

OIG-24-05

Unaudited

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

Table of Contents

Unaudited

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

1

OIG-24-05

Unaudited

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

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.

2

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

Summary of Major Management Challenges

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

The challenges outlined in this report are a culmination of our judgment, independent research, including discussions with internal and Department component Senior Leaders, and review of our own audits, inspections, and evaluations, as well as relevant U.S. Government Accountability Office 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.

3

Unaudited

2024 Major Management and Performance Challenges

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**.

4

Unaudited

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.

5

Counter Terrorism and Homeland Security Threats

Components Impacted	Related Strategic Priority
All	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

6

Unaudited

U.S. Department of Homeland Security

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.

OIG-24-05

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

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
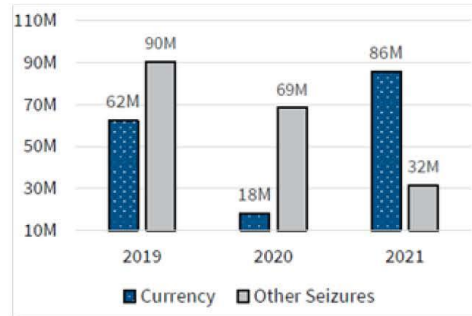
Source: OIG analysis of ICE enforcement statistics

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.

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.

Figure 5: Depiction of CSS

Source: OIG Analysis of CSS Operations

9

Unaudited

Secure U.S. Borders and Approaches

Components Impacted	Related Strategic Priority
CBP, ICE, TSA, USCIS, Coast Guard, HQ/Support	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."

10

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

11

Unaudited

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

12

OIG-24-05

Unaudited

U.S. Department of Homeland Security

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).

13

www.oig.dhs.gov

OIG-24-05

Unaudited

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**).

15

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

Actual Number of Detainees / Guaranteed Minimum
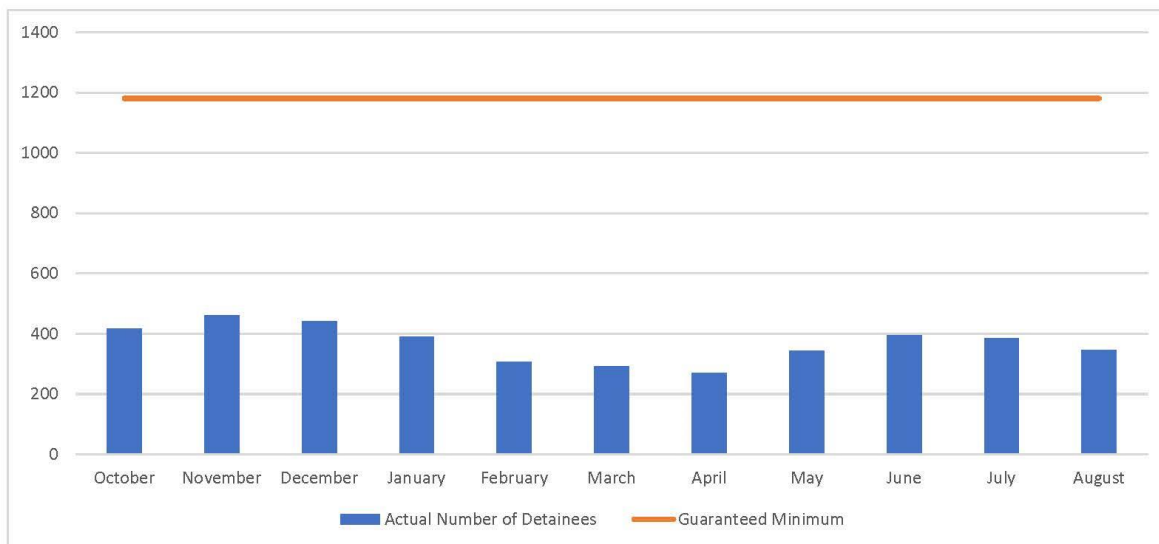
Source: OIG analysis of ICE data

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.*

17

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.

18

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)

19

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

Unaudited

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

Recent Progress Reported by the Department

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**).

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.

21

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.

Unaudited

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.

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.

Source: Department

23

OIG-24-05

Unaudited

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

24

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

25

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.

26

OIG-24-05

Unaudited

U.S. Department of Homeland Security

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

27

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 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.

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.

28

Champion the DHS Workforce and Strengthen the Department

Components Impacted	Related Strategic Priority
All	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.

29

www.oig.dhs.gov

OIG-24-05

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.

31

Unaudited

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.

32

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.

33

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.

34

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

- Duplicate Records
- Disposed Records
- Inaccurate Records
- Correct Records
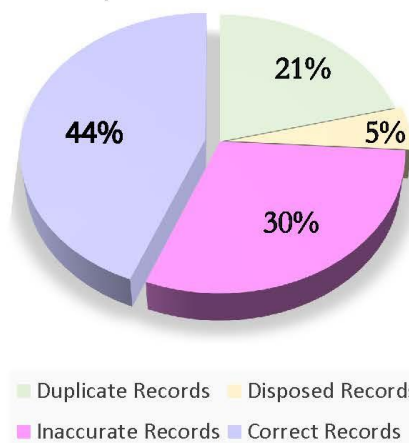
Source: OIG analysis of Coast Guard-provided

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

Source: Coast Guard

Unaudited

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

37

Unaudited

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.

Unaudited

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)

39

OIG-24-05

Unaudited

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)

Unaudited

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.

41

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)

42

Unaudited

U.S. Department of Homeland Security

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)

OIG-24-05

Unaudited

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)

44

Unaudited

U.S. Department of Homeland Security

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)

45

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

Homeland Security

November 7, 2023

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

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

JIM H CRUMPACKER Digitally signed by JIM H
CRUMPACKER
Date: 2023.11.07
08:39:45 -05'00'

SUBJECT: Management Response to Draft Report: "Major Management
                             and Performance Challenges Facing the Department of
                             Homeland Security" (Project No. 24-003-NONE-DHS)

Thank you for the opportunity to comment on this draft report. Senior U.S. Department
of Homeland Security (DHS or the Department) leadership recognizes the Office of
Inspector General's (OIG's) work in planning and conducting its review and issuing this
report. This included OIG's independent research, assessment of prior work, and
professional judgment to identify what the OIG considers as the most serious
management and performance challenges facing the Department, and DHS's progress in
addressing these challenges.

Senior DHS leadership, Component-level program officials, subject matter experts, and
others throughout the Department will give appropriate consideration to the OIG
perspectives offered in this major management and performance challenges (MMPC)
report as part of continuing efforts to improve the effectiveness and efficiency with which
the Department carries out its mission of safeguarding the American people, our
homeland, and our values. In particular, DHS appreciates OIG's redesign of this year's
report to highlight overarching challenges—transparency, accountability, efficiency, and
sustainability—as opposed to identifying challenges focusing more narrowly on
programs and operations, as the "Performing Fully and Effectively during COVID-19"
challenge reported last year.

However, leadership believes the overall usefulness of the report can be improved,
including by providing additional context for statements that appear to overstate some of
the findings in OIG's prior work without providing sufficient background or accounting
for concerns and other information raised in Departmental management responses to that
work. Furthermore, leadership disagrees with OIG's assertion that the Department has

In a departure from well-established practice, the Office of Inspector General (OIG) published its Major Management and Performance Challenges report without the Department's management response letter, which was provided in accordance with OMB Circular No. A-136. Despite many efforts to engage with the Office of Inspector General leadership, the OIG did not respond to our inquiries relating to the shortened timeline for review and reasons why our management response letter was not included. Accordingly, the Department's recourse to acknowledge the challenges and ensure that our concerns with accuracy and lack of proper context in the report are taken into consideration is to include our management response letter in the Department's Agency Financial Report, as part of the section which includes the OIG report in its entirety.

inappropriately "delayed" or "denied" OIG access to Information Technology (IT) systems and data. Finally, the process and timeline OIG used when developing and socializing this year's MMPC report with DHS officials deviated significantly from past practice and provided inadequate time for management to respond. Each of these issues is described in greater detail below.

Overall Usefulness of the Report

DHS leadership believes the revised construct for this year's MMPC report represents an improvement over prior reports in that the report highlights four broad themes as challenges to fully achieving the Department's strategic goals compared to being more narrowly focused on programs and operations. However, leadership generally observed that the draft report seems to primarily be a compendium of OIG reports issued during the past year, the majority of which focused on Component-specific activities without (1) clearly tying these activities to Department-wide strategic challenges, or (2) sufficiently addressing DHS efforts as discussed in the management response letters and other follow-up activities. DHS and its Components also expressed numerous accuracy and context concerns with the MMPC and separately highlighted those in technical comments for OIG's consideration. Some of these comments noted that the MMPC report did not accurately portray the information in the underlying reports it referenced.

For example, the MMPC report cites several recent OIG reports to address the DHS strategic goal of securing the borders but does not recognize the extent of initiatives DHS has implemented, as discussed throughout this response. Furthermore, the MMPC report cites the Department's latest Annual Performance Report (APR) as noting that "policy shifts, such as domestic immigration policy," have created challenges and risks in meeting this goal. The underlying reporting states that "Border Patrol agents continue to face demands including implementing COVID-19 procedures, challenging work locations, changing job requirements, and policy shifts," but does not make reference to shifts in "domestic immigration policy" specifically. While DHS appreciates that the OIG considered the APR when preparing the MMPC, the Department believes that proper context is critical for "cold readers" of the report, particularly when making wide-reaching claims without providing a factual foundation for the claims.

Similarly, the Department believes that additional background would be helpful for readers of the MMPC to understand the context related to the "vulnerabilities resulting from efficiency challenges" it cites, including the staffing issues raised. While the MMPC addresses recent progress made by the Department through the direct-hire authority request by U.S. Immigration and Customs Enforcement (ICE), it does not recognize the extent of initiatives DHS has implemented to support its personnel. For example, the MMPC does not mention the new Border Patrol Processing Coordinator positions established by U.S. Customs and Border Protection (CBP) and outlined in Departmental materials provided to the OIG, including in the management response letter

2

to OIG's report on "Intensifying Conditions at the Southwest Border are Negatively Impacting CBP and ICE Employees' Health and Morale" (OIG-23-24, dated May 3, 2023). These new positions support U.S. Border Patrol agents in performing administrative tasks and allow agents to return to the frontline and focus on their border security mission. Rather, the MMPC falsely gives the impression that the Department is relying on "temporary solutions" by not more fully considering the numerous policies and efforts taken, ongoing, or planned to address such challenges. Further, to the extent that some of these conclusions arise from workforce challenge survey results, DHS reiterates its concerns that such survey results are not necessarily representative of the workforce issues that frontline law enforcement personnel may be experiencing, especially given the very low survey response rate of 18 percent. OIG's report did not identify any steps it took to mitigate the potential for nonresponse bias since opinions of those individuals who chose to respond may be meaningfully different from those who chose not to respond.[1]

In addition, ICE leadership noted that the draft report could be misleading to some readers because of inaccurate, contextually incomplete, and confusing statements about its efforts to carry out Department and Component missions. Specifically, ICE expressed concern that the report does not acknowledge completed and ongoing actions taken to address OIG recommendations associated with the "Counter Terrorism and Homeland Security Threats" and "Secure U.S. Borders and Approaches" strategic goals. This includes recommendations from OIG reports OIG-23-17, OIG-23-31, OIG-23-41, OIG-23-24, OIG-23-26, and OIG 23-38 (see Appendix C of the MMPC report for specific report titles and dates issued). Furthermore, while OIG highlights compliance shortfalls with the 2011 Performance-Based National Detention Standards at five ICE facilities, no mention is made in the MMPC of ICE's substantial disagreement with some of OIG's recommendations in the underlying reports or ICE's overarching concerns about the accuracy of some reports and whether they met "Quality Standards for Inspection and Evaluation" requirements issued by the Council of Inspectors General on Integrity and Efficiency (i.e., the "Blue Book," dated December 2020).[2]

Similarly, the MMPC report cites CBP apprehension numbers between March 2021 and August 2022 as well as tracking of migrant addresses of these individuals without providing sufficient background on the issue and the Departmental responses. This summary does not contextualize the longstanding challenges associated with collecting noncitizens' addresses at the time of initial border processing, nor does it address the significant improvements DHS has made in how it processes noncitizens encountered along our borders and technology improvements to facilitate better information-sharing to

---

[1] https://www.oig.dhs.gov/reports/2023/intensifying-conditions-southwest-border-are-negatively-impacting-cbp-and-ice-employees-health-and-morale/oig-23-24-may23
[2] https://www.ignet.gov/sites/default/files/files/QualityStandardsforInspectionandEvaluation-2020.pdf

3

support accurate and timely processing and tracking of migrants among various Components and agencies. Such efforts are outlined in the Department's management response letter to the underlying report[3] and provide important context that does not appear to have been fully considered by the OIG in developing the MMPC. Without proper context for these ongoing efforts, the MMPC is incomplete and potentially misleading to its readers.

Multiple components also remarked that the MMPC would be significantly more useful if it contained a holistic analysis of its recommendations as they relate to the Department's priorities. For example, Cybersecurity and Infrastructure Security Agency leadership advised that the MMPC report would be more useful if it provided an overall assessment of recommendations from its body of audit-related work associated with the Department's strategic goals and specifically identified actions OIG believes are needed to improve DHS's performance against its goals, so that DHS officials have something to act towards and measure progress against. This could include a breakdown of actionable open and unimplemented recommendations relating to each strategic goal that OIG believes are the most critical ones for DHS for focus on implementing, similar to the annual letter the Comptroller General of the United States sends the Secretary of Homeland Security identifying "Priority" recommendations that the U.S. Government Accountability Office (GAO) believes warrant the Secretary's personal attention.[4] Both Federal Emergency Management Agency and DHS Office of Homeland Security Situational Awareness (OSA) leadership also commented that future MMPC reports would be more of a value-add if they include an overall assessment or set of recommendations on what the Department and/or its Components could do to improve in the overarching challenges OIG highlights.

OSA leadership also noted that they did not see any mention in the MMPC report about how cross-departmental boards and bodies are functioning, especially with regard to information-sharing and collaboration. For example, the Countering Weapons of Mass Destruction Office in partnership with the DHS Counterterrorism Coordinator chartered a new executive group to conduct strategic coordination for NSPM-36, "Guidelines for United States Government Interagency Response to Terrorist Threats or Incidents in the United States and Overseas," promulgated in January 2021, and OSA created a Senior Leader Situational Awareness Forum to promote situational awareness and information-sharing across the Department.

Lastly, DHS believes the MMPC report could be more useful if, rather than simply mentioning that the OIG reviewed relevant GAO reports, it also provided insights about which reports were reviewed and how those reports and the Departmental management responses to them helped inform the OIG's perspective on the most serious management

---

[3] https://www.oig.dhs.gov/sites/default/files/assets/2023-09/OIG-23-47-Sep23-Redacted.pdf
[4] https://www.gao.gov/products/gao-23-106483

4

and performance challenges facing the Department, and DHS's progress in addressing these challenges. The Department also notes that like the OIG's 2022 MMPC report, its 2023 draft report does not include an "Objective, Scope, and Methodology" section similar to the one included in all OIG audit and inspection reports. DHS continues to believe that including such a section in OIG's annual MMPC report would provide readers of the report important insights about the independent research conducted, assessment of prior work and Departmental communications relating to any recommendations, and professional judgment used to identify what the OIG considers as the most serious management and performance challenges facing the Department, and DHS's progress in addressing these challenges.

IT System and Data Access Requests

DHS leadership adamantly disagrees with OIG's assertion that the Department has inappropriately "delayed" or "denied" OIG access to IT systems and data. OIG has made similar allegations in the past and each time the Department has specifically refuted them, most recently via the Secretary of Homeland Security's transmittal letter to Congress on the OIG's semiannual report to Congress (for the period ending March 31, 2023), dated July 14, 2023. DHS notes that OIG's allegations frequently raise more questions than answers, do not acknowledge Departmental efforts to resolve the OIG concerns, and often lack meaningful specifics.

The Department is fully committed to cooperating with OIG requests for information and is not aware of any record requested by the OIG that has been withheld. For example, the MMPC notes that OIG does not have access to numerous Component SharePoint sites containing organizational policies and procedures and alleges this impairs OIG's ability to achieve its mission. On the contrary, while DHS is not always able to provide wholesale access to Departmental or Component IT databases in the exact manner the OIG requests, DHS offices and Components have never restricted OIG access to organizational policies and procedures. The Department and Components evaluate OIG requests for direct access to IT databases, including SharePoint, on a case-by-case, basis while also carrying out due diligence related to requirements for safeguarding sensitive information and systems. For example, SharePoint may be used differently by Components and offices, and in some instances, SharePoint is used as a collaboration tool for real-time deliberations. Because the wholesale access OIG seeks could result in chilling effect on real-time, ongoing deliberations, program officials have sometimes used alternative means to provide the OIG-requested information, but the information has always been provided.

DHS leadership supports providing the OIG timely access to relevant information, including requests for data related to programs, operations, and activities that are within the scope and objectives of an identified audit, evaluation, inspection, or review (OIG criminal investigations are handled differently). As the steward of its data, DHS is

5

responsible for engaging with the OIG on the relevance of a data request to the scope and objectives of the OIG's work, especially in light of the types of sensitive data held by DHS, including sensitive security information, personally identifiable information of vulnerable populations and others, as well as proprietary, classified, and investigative law enforcement sensitive information. In some instances, DHS IT systems hold data from other partner federal departments and agencies which requires further coordination with these partners for access. Although the Department has sometimes justifiably questioned the breadth of some the OIG requests for IT systems access, it has nonetheless attempted to work closely with the OIG in every instance to ensure that information is made available, as appropriate. This includes offers to provide the OIG with executive-level access, assistance from program officials and subject-matter experts familiar with the databases by running unlimited searches of the databases, using queries provided by the OIG and pulling the requested data based on those queries, and allowing for real-time viewing of such searches to ensure the OIG receives all information it believes is needed for its engagements. The OIG has not always been receptive to these offers in part because of stated concerns about whether working with the Department in this manner might compromise OIG independence, which DHS does not believe would be adversely impacted by this narrow collaboration on provision of data.

Further, DHS is concerned that the examples cited in the MMPC were not sufficiently discussed or raised to Departmental leadership to allow for an opportunity to arrive at an agreed-upon resolution before sharing these disagreements with Congress and the public. The Department values having the OIG's independent and unique perspective on DHS's many programs, operations, and activities. The OIG's independence, however, is not impinged by discussing access concerns with the Department's leadership in a good-faith attempt to reach resolution.

Process and Timeline Concerns

DHS leadership is concerned that OIG's process and timeline for developing and publishing this annual MMPC report was not reasonable nor sufficiently inclusive of management officials across the Department. For this 2023 draft report, OIG:

- Did not, to our knowledge, issue an announcement letter identifying point(s) of contact (POC) or hold an Entrance or Exit Conference, nor any in-progress (i.e., fieldwork) meetings with DHS officials either at the Headquarters or Component levels to discuss its work as is its normal practice for other audit and inspection-related work. In addition, once DHS identified a POC for this work, multiple OIG officials at the Senior Executive Service level were not responsive to Departmental requests seeking to discuss the process and timeline of this work.

6

- Requested DHS-wide (i.e., all Components and the Headquarters offices) technical comment feedback[5] "as soon as possible" and no later one calendar week (i.e., 7 days) after receipt of the draft, which was an unreasonable request that DHS could not meet, especially since DHS was just learning about the redesigned report for the first time. By contrast, for the 2022 and 2021 reports, OIG asked for the Department's feedback within 21 days. For context, OIG generally asks for feedback on most of its reports within 30 calendar days. There is no basis for the drastically different timeline for the 2023 MMPC with no previous notification to the Department of a change to the well-established process.

- Did not provide the Department a copy of its OIG's draft report until October 11, 2023, just over a month before the final report must—by law—be available for inclusion in the DHS 2023 Agency Financial Report, which is published no later than November 15th each year. Collecting, consolidating, and providing DHS-wide feedback (from 14 Components and 15 other offices) on a draft report as significant as the MMPC takes considerable time to obtain an informed response. DHS would prefer a schedule where the draft MMPC report is released for management review and comment in late August or early September (OIG's 2022 draft report was released on September 16, 2022) for a 30-day comment period.

Again, thank you for the opportunity to review and comment on this draft report. DHS also submitted technical comments addressing several accuracy, contextual and other concerns under a separate cover for OIG's consideration. We look forward to more closely working with OIG in a mutually open and transparent manner during development of the 2024 MMPC report.

---

[5] Agency comments focus on accuracy, sensitivity context, and editorial issues. As a part of the sensitivity review, components identify any information that, either on its own or in connection with other information, is inappropriate for public disclosure. This includes classified information, Sensitive but Unclassified Information, Law Enforcement Sensitive information, information subject to Executive Privilege, and information that is subject to statutory or regulatory confidentiality requirements. The comments are not intended to substantively alter any of OIG's overall findings, conclusions, or recommendations, but rather to strengthen final work products.

7

Appendices

Appendix A: Acronym List

A

ADA – Americans with Disabilities Act

AFR – Agency Financial Report

AGA -- Association of Government Accountants

AI – Artificial Intelligence

AITF – Artificial Intelligence Task Force

AMO – Air and Marine Operations

APB – Acquisition Program Baseline

APG – Agency Priority Goal

API – Application Programming Interface

APP – Annual Performance Plan

APR – Annual Performance Report

ARPA – American Rescue Plan Act, 2021

ATON – Aids to Navigation

B

BCA – Benefit-Cost-Analysis

BFCT – Biometric Facial Comparison Technology

BOD – Binding Operational Directive

BRIC – Building Resilient Infrastructure and Communities

BRS – Blended Retirement System

C

CAA – Consolidated Appropriations Act

CARES – Coronavirus Aid, Relief, and Economic Security Act, 2020

CBP – U.S. Customs and Border Protection

CBRN – Chemical, Biological, Radiological and Nuclear

CBRNE – Chemical, Biological, Radiological, Nuclear, and Explosive

CDL – Community Disaster Loans

CDP – Center for Domestic Preparedness

CEAR – Certificate of Excellence in Accountability Reporting

CEIU – Child Exploitation Investigations Unit

CFIUS – Committee on Foreign Investment in the United States

CFO – Chief Financial Officer

CFTF – Cyber Fraud Task Force

CIO – Chief Information Officer

CIP – Construction in Progress

CIO – Chief Information Officer

CISA – Cybersecurity and Infrastructure Security Agency

COBRA – Chemical, Ordinance, Biological, and Radiological

COBRA – Consolidated Omnibus Budget Reconciliation Act, 1985

COLA – Cost of Living Allowance

COP – Common Operating Picture

COTS – Commercial Off–the–Shelf

CPI – Consumer Price Index

CPSS – Checkpoint Property Screening System

CSEA – Child Sexual Exploitation and Abuse

CSRB – Cyber Safety Review Board

CTMS – Cybersecurity Talent Management System

C-UAS – Counter Unmanned Aircraft Systems

CWMD -- Countering Weapons of Mass Destruction Office

CX – Customer Experience

D

DADLP – Disaster Assistance Direct Loan Program

DCIA – Debt Collection Improvement Act, 1996

DEF – Disaster Emergency Fund

DEIA – Diversity, Equity, Inclusion, and Accessibility

DHS – Department of Homeland Security

DOD – Department of Defense

DOJ – Department of Justice

DOL – Department of Labor

DRF – Disaster Relief Fund

DVE – Domestic Violent Extremism

E

E2C2 – Export Enforcement Coordination Center

ECTF – European Electronic Crime Task Force

EDS – Explosive Detection System

EOIR – Executive Office for Immigration Review

ERM – Enterprise Risk Management

ERO – Enforcement and Removal Operations

EV – Electric Vehicle

F

FAA – Federal Aviation Administration

FAA – DHS Financial Accountability Act

FAST – Fentanyl Abatement and Suppression Team

FBwT – Fund Balance with Treasury

FCC – Federal Communications Commission

FCEB – Federal Civilian Executive Branch

FCU – Financial Crimes Unit

FECA – Federal Employees Compensation Act, 1916

FEMA – Federal Emergency Management Agency

FERS – Federal Employees Retirement System

FEVB – Federal Employee and Veterans' Benefits

FFMIA – Federal Financial Management Improvement Act, 1996

FFRD – Future of Flood Risk Data

FIFO – First In-First Out

FIMA – Flood Insurance Mitigation Administration

FISMA – Federal Information Security Management Act

FLETC – Federal Law Enforcement Training Centers

FMA – Flood Mitigation Assistance

FMFIA – Federal Managers' Financial Integrity Act

FPS – Federal Protective Service

FSMS – Financial Systems Modernization Solution

FY – Fiscal Year

G

GAAP – Generally Accepted Accounting Principles

GAO – U.S. Government Accountability Office

GE – Global Entry

GPRA – Government Performance and Results Act, 1993

GPRAMA – GPRA Modernization Act, 2010

GS – General Service

GSA – General Services Administration

GTAS – Government-wide Treasury Account Symbol Adjusted Trial Balance System

H

HART – Humanitarian, Adjustment, Removing Conditions and Travel

HMA – Hazard Mitigation Assistance

HMGP – Hazard Mitigation Grant Program

HSI – Homeland Security Investigations

HVE – Homegrown Violent Extremists

I

I&A – Office of Intelligence and Analysis

ICE – U.S. Immigration and Customs Enforcement

ICMM – Internal Control Maturity Model

ICOFR – Internal Control Over Financial Reporting

IEFA – Immigration Examination Fee Account

IHP – Individuals and Households Program

IHSC – ICE Health Service Corps

IIJA – Infrastructure Investment and Jobs Act, 2022

INA – Immigration and Nationality Act

IPE – Information Produced by Entity

IPERA – Improper Payments Elimination and Recovery Act, 2010

IPERIA – Improper Payments Elimination and Recovery Improvement Act, 2012

IPIA – Improper Payments Information Act, 2002

IT – Information Technology

ITGC – Information Technology General Controls

IUC – Information Used in Controls

IUUF – Illegal, Unreported, and Unregulated Fishing

J

JCDC – Joint Cyber Defense Collaborative

JPMO – Joint Program Management Office

K

KEVS – Known Exploited Vulnerabilities

L

LECC – Law Enforcement Coordination Council

LOI – Letter of Intent

M

MERHCF – Medicare–Eligible Retiree Health Care Fund

MGMT – Management Directorate

MHS – Military Health System

MMPC – Major Management and Performance Challenges

M-UAS – Medium UAS

N

NAGC – National Association of Government Communications

NATO – North Atlantic Treaty Organization

NCATC – National Criminal Analysis and Targeting Center

NCFI – National Computer Forensics Institute

NCP – Normal Cost Percentage

NCR – National Capital Region

NDAA – National Defense Authorization Act

NDD – Non-Detained Docket

NFIP – National Flood Insurance Program

NGO – Nongovernmental Organization

NICE – National Initiative for Cybersecurity Education

NICS – Next Generation Incident Command System

NII – Non-Intrusive Inspection

NIMS – National Incident Management System

NISAC – National Infrastructure Simulation and Analysis Center

NOC – National Operations Center

NPFC – National Pollution Funds Center

NRCC – National Response Coordination Center

NRMC – National Risk Management Center

NSC – National Security Cutter

NSSE – National Special Security Event

NTAC – National Threat Assessment Center

O

OCFO – Office of the Chief Financial Officer

OCIO – Office of the Chief Information Officer

OIG – Office of Inspector General

OM&S – Operating Materials and Supplies

OMB – Office of Management and Budget

OPEB – Other Post Retirement Benefits

OPLA – Office of the Principal Legal Advisor

OPM – Office of Personnel Management

ORB – Other Retirement Benefits

OSA – Office of Homeland Security Situational Awareness

OSLTF – Oil Spill Liability Trust Fund

OTA – Other Transaction Agreement

P

PA – Public Assistance

PA&E – Program Analysis and Evaluation

PC&I – Procurement, Construction, and Improvement

PIIA – Payment Integrity Information Act, 2019

PM – Performance Management

PMDF – Performance Measure Definition Form

POA&M – Plan of Action and Milestones

PP&E – Property, Plant, and Equipment

PPA – Programs, Projects, and Activities

Q

QHSR – Quadrennial Homeland Security Review

R

RPA – Robotic Process Automation

RSI – Required Supplementary Information

S

S&T – Science and Technology Directorate

SBR – Statement of Budgetary Resources

SEACATS – Seized Assets and Case Tracking System

SES – Senior Executive Service

SFFAS – Statement of Federal Financial Accounting Standards

SFRBTF – Sport Fish Restoration Boating Trust Fund

SLTT – State, Local, Tribal, and Territorial

SMD – Strategic Management Division

SOC – Service Organization Control

SPM – Service Provider Monitoring

S-UAS – Small UAS

SWB – Southwest Border

T

TAK – Team Awareness Kit

TBI – Treasury Breakeven Inflation

TIER - Treasury Information Executive Repository

TSA – Transportation Security Administration

TSO – Transportation Security Officer

TSP – Thrift Saving Plan

TTP – Trusted Traveler Program

TVS – Travel Verification System

U

UAS – Unmanned Aircraft System

UCMM – Unified Cybersecurity Maturity Model

UFLPA – Uyghur Forced Labor Prevention Act, 2022

UN – United Nations

UPR – Unearned Premium Reserve

USBP – U.S. Border Patrol

USCG – U.S. Coast Guard

USCIS – U. S. Citizenship and Immigration Services

USFA – U.S. Fire Administration

USM – Under Secretary for Management

USPS – U.S. Postal Service

USSGL – U.S. Standard General Ledger

USSS – U.S. Secret Service

V

VAP – Victim Assistance Program

VAV – Virtual Attorney Visitation

VAYGo – Validate as You Go

W

WFFR – Wildland Firefighter Respirator

WYO – Write Your Own

Appendix B: Acknowledgements

This AFR was produced with the tireless energies and talents of Department of Homeland Security Headquarters and Component employees and contract partners.

Within the Office of the Chief Financial Officer, the division of Financial Management is responsible for financial management policy, preparing annual financial statements and related notes and schedules, and coordinating the external audit of the Department's financial statements.

The division of Risk Management and Assurance provides direction in the areas of internal control to support the Secretary's assurance statement, risk management, and improper payments.

The division of Program Analysis and Evaluation conducts analysis for the Department on resource allocation issues and the measurement, reporting, and improvement of DHS performance, and coordinates the Performance Overview section of the AFR.

The division of GAO-OIG Audit Liaison facilitates Department relationships with audit organizations and coordinates with OIG on the Management Challenges report.

We offer our sincerest thanks to all the offices involved in the Department's FY 2023 Agency Financial Report for their hard work and contributions.

U.S. CUSTOMS AND BORDER PROTECTION

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

FEDERAL EMERGENCY MANAGEMENT AGENCY

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

TRANSPORTATION SECURITY ADMINISTRATION

U.S. COAST GUARD

U.S. CITIZENSHIP AND IMMIGRATION SERVICES

U.S. SECRET SERVICE

COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE

FEDERAL LAW ENFORCEMENT TRAINING CENTERS

OFFICE OF HOMELAND SECURITY SITUATIONAL AWARENESS

OFFICE OF INTELLIGENCE AND ANALYSIS

OFFICE OF INSPECTOR GENERAL

MANAGEMENT DIRECTORATE

SCIENCE AND TECHNOLOGY DIRECTORATE

WE ARE DHS.