WITH HONOR AND INTEGRITY, WE WILL SAFEGUARD THE AMERICAN PEOPLE, OUR HOMELAND, AND OUR VALUES.

FY 2025

U.S. DEPARTMENT OF HOMELAND SECURITY

AGENCY FINANCIAL REPORT

WELCOME TO THE U.S. DEPARTMENT OF HOMELAND SECURITY'S FISCAL YEAR 2025 AGENCY FINANCIAL REPORT.

The U.S. Department of Homeland Security (DHS) is committed to safeguarding the American people, our homeland, and our values. The Agency Financial Report (AFR) for fiscal year (FY) 2025 provides a detailed overview of how DHS manages the resources entrusted to us, highlighting our priorities, achievements, and challenges in delivering on our mission.

At the heart of DHS operations are eight Operational Components that directly execute the Department's core missions:

U.S. Customs and Border Protection (CBP): Controls, secures, and defends America's borders at and between official ports of entry while facilitating lawful trade and travel. See more at cbp.gov.

U.S. Coast Guard (USCG): Controls, secures, and defends America's borders while facilitating the flow of commerce and responding to crises and contingencies. See more at uscg.mil.

U.S. Citizenship and Immigration Services (USCIS): Administers the Nation's lawful immigration system, processing applications and ensuring system integrity. See more at uscis.gov.

Cybersecurity and Infrastructure Security Agency (CISA): Leads efforts to strengthen the security and resilience of the Nation's cyber and physical infrastructure. See more at cisa.gov.

Federal Emergency Management Agency (FEMA): Coordinates federal disaster response and recovery efforts, helping communities before, during, and after emergencies. See more at fema.gov.

U.S. Immigration and Customs Enforcement (ICE): Enforces immigration laws and investigates Transnational Criminal Organizations to protect national security and public safety. See more at ice.gov.

U.S. Secret Service (USSS): Safeguards national leaders, events, and the U.S. financial system through protection and criminal investigations. See more at usss.gov.

Transportation Security Administration (TSA): Ensures the security of the Nation's transportation systems, screening millions of passengers and goods annually. See more at tsa.gov.

Supporting these Operational Components are the Department's Support Components, which provide essential services to enable mission success and include:

- Countering Weapons of Mass Destruction Office (CWMD)
- Federal Law Enforcement Training Centers (FLETC)
- Office of Intelligence and Analysis (I&A)
- Office of Homeland Security Situational Awareness (OSA)
- Science and Technology Directorate (S&T)

The FY 2025 AFR highlights the financial stewardship and operational performance of the Department's Operational Components, which lead the Department's core missions, while also addressing the critical contributions of Support Components that enable mission success. To learn more about DHS and our missions, visit us at dhs.gov.

TABLE OF CONTENTS

This report is available online at:
dhs.gov/performance-financial-reports

MESSAGE FROM THE SECRETARY

January 22, 2026

I am honored to present the Department of Homeland Security's (DHS) Agency Financial Report for Fiscal Year (FY) 2025. This report provides a detailed account of our financial and operational performance, underscoring our steadfast commitment to protecting the American people, ensuring responsible stewardship of taxpayers' money, securing our homeland, and upholding our Nation's values.

Under President Trump's leadership, DHS has achieved significant milestones in securing the southern border, removing dangerous illegal aliens, and empowering our law enforcement and front-line personnel. By leveraging the Department's unique authorities, we have strengthened efforts to combat Foreign Terrorist Organizations, Transnational Criminal Organizations, and other threats to our national security. These achievements reflect our dedication to protecting our homeland – including delivering justice for victims of illegal immigration, modernizing disaster relief, strengthening cybersecurity, and ushering in a new era of excellence in American air travel.

The *One Big Beautiful Bill Act* represents a landmark commitment to border security, immigration enforcement, and other national security priorities. This legislation will enable DHS to complete the Southwest Border wall, invest in new ships and aircraft for the United States Coast Guard, procure advanced security technologies, and modernize the specialized roles of our Component agencies.

DHS continues to strengthen its management functions and operational capabilities. For the thirteenth consecutive year, we have achieved a clean annual audit opinion for all five financial statements, demonstrating our dedication to accountability and sound financial stewardship. Through the implementation of the Integrated Strategy for High-Risk Management, we are addressing high-risk areas and building on our progress to ensure the Department's long-term success.

Our Integrated Strategy is available on our public website at dhs.gov/publication/dhs-integrated-strategy. Additionally, our annual financial and performance reports can be accessed at dhs.gov/performance-financial-reports, reflecting our commitment to transparency and continuous improvement.

As we move into FY 2026, DHS remains resolute in its mission to safeguard the homeland and advance national security. With the support of Congress, and through the exceptional dedication of the DHS workforce, we will continue to build a safer, stronger future for all Americans.

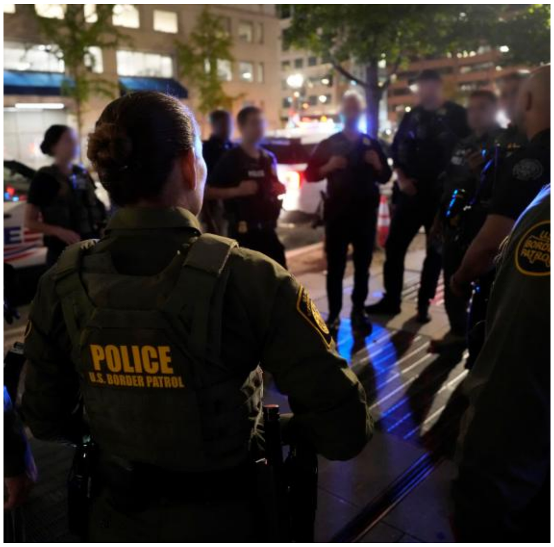
Sincerely,

Kristi Noem

Secretary of Homeland Security

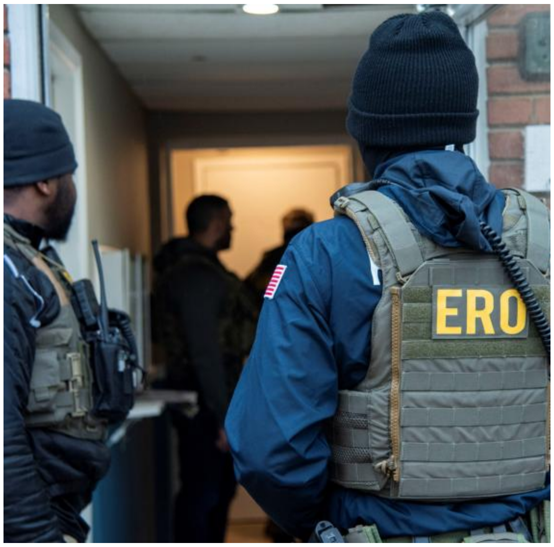
MANAGEMENT'S DISCUSSION AND ANALYSIS

SECTION CONTENTS

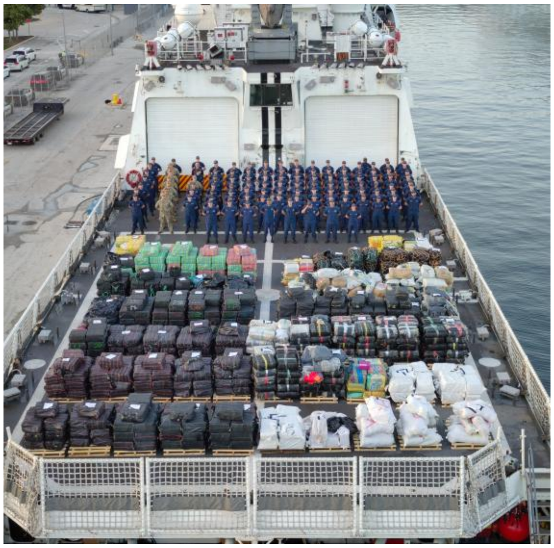


The Management's Discussion and Analysis (MD&A) provides an overview of the Department's financial and operational performance for FY 2025.

It begins with a summary of the Department's history, organizational structure, and annual net cost of operations, followed by key financial outcomes, critical initiatives, and notable risk management efforts across the Department's eight Operational Components. The MD&A also reviews the Department's financial statements, internal controls, and legal compliance, ensuring transparency and accountability to the public.



About the Section Cover Photo: CBP and ICE coordinating with the Department of Defense (DoD) to deport illegal aliens at Biggs Army Airfield, Fort Bliss, Texas, February 7, 2025.
About the Top Photo on This Page: CBP agents with U.S. Border Patrol assisting the Washington, D.C. Metropolitan Police Department, under the direction of the U.S. Marshals Service, to enhance public safety in Washington, D.C., August 14, 2025.
About the Middle Photo on This Page: ICE officers conduct enhanced enforcement operations in Chicago, Illinois, January 26, 2025.
About the Bottom Photo on This Page: Following counterdrug operations aided by partner agencies during FY 2025, USCG Cutter Hamilton offloads 76,140 lbs. of cocaine at Port Everglades, Florida, August 25, 2025—the largest offload in USCG history.



INTRODUCTION

DHS was established in the aftermath of the September 11, 2001, terrorist attacks, reshaping the Nation's approach to homeland security. Guided by its mission to protect the United States from evolving threats, DHS remains focused on securing borders, enforcing immigration laws, safeguarding cyberspace and critical infrastructure, protecting national leaders, deterring terrorism, combating Transnational Criminal Organizations, responding to disasters, and ensuring public safety.

The FY 2025 AFR MD&A provides an overview of the Department's financial and operational performance, highlighting contributions from its eight Operational Components—CBP, USCG, USCIS, CISA, FEMA, ICE, USSS, and TSA. For details on the Department's organizational structure, visit dhs.gov/organization.

The Department's financial and performance reporting is anchored in two key documents: the AFR, which focuses on financial results and high-level performance summaries, and the Annual Performance Report and Plan (APR/APP), which provides detailed performance measures and targets, end-of-year results, and planned corrective actions. Together, these reports ensure transparency and accountability to the American taxpayer, offering a comprehensive view of how DHS uses resources to achieve strategic objectives. Access both reports at dhs.gov/performance-financial-reports.

In FY 2025, the Department's net cost of operations totaled $123.6 billion. During FY 2025, DHS made historic progress in securing the southwest border and removing criminal illegal aliens from U.S. communities, reflecting its commitment to protecting the Nation's security, upholding immigration laws, and ensuring public safety. Further efforts supported the Department's personnel, upgraded operational technology across Components, expanded cybersecurity protections, enhanced disaster response capabilities, and modernized immigration systems. These efforts align with the Department's strategic priorities to improve operational capacity, increase resilience, and ensure efficient use of resources.

Looking ahead, DHS will continue to refine financial operations, strengthen performance measures and risk management, and prioritize investments that deliver measurable outcomes for the American people.

DHS Net Cost of Operations, FY 2025

$123.6 billion

U.S. CUSTOMS AND BORDER PROTECTION

Component Overview

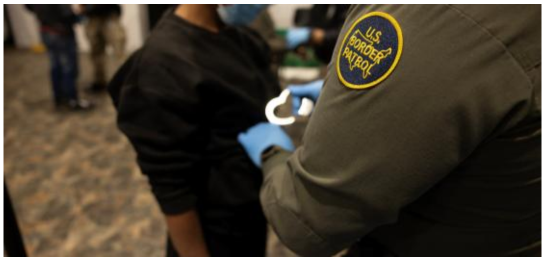
In FY 2025, CBP's net cost of operations totaled $23.0 billion. During FY 2025, CBP prioritized efforts to achieve complete operational control of the U.S. border, modernize fleet operations, strengthen trade policies, and disrupt Transnational Criminal Organizations.

CBP Net Cost of Operations, FY 2025

$23.0 billion

The following highlights showcase significant achievements and innovative approaches that advanced CBP's objectives. The following also highlights CBP's efforts to mitigate risks and seize opportunities to strengthen border security, improve operational efficiency, and protect U.S. communities.

Significant Initiatives and Success Stories



Achieving Unprecedented Progress in Border Security: In FY 2025, CBP achieved a historic reduction in illegal border crossings, leveraging enhanced enforcement measures and operational control to strengthen national security and uphold immigration laws. For example, by May 2025, illegal crossings had decreased by 93% compared to May 2024, with zero releases into the U.S. These results highlight CBP's strategic leadership in securing the border, protecting U.S. communities, and ensuring the integrity of the immigration system.

CBP Secures Super Bowl LIX: CBP played a critical role in securing Super Bowl LIX in New Orleans, Louisiana. CBP ensured aerial and waterfront security, while CBP officers screened inbound materials for threats like weapons, explosives, and counterfeit goods. These efforts protected public safety, safeguarded intellectual property, and demonstrated CBP's ability to secure major events.

San Diego Border Patrol Disrupts Drug Smuggling Tunnel: CBP Border Patrol agents in San Diego uncovered a sophisticated drug smuggling tunnel connecting Tijuana to the U.S. The 2,900-foot tunnel featured advanced systems like lighting and ventilation. Working with Homeland Security Investigations and

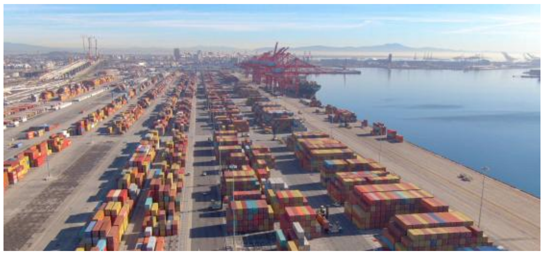
Mexican authorities, CBP dismantled the tunnel, disrupting a major criminal network and enhancing community safety.

CBP Supports Security for 60th Presidential Inauguration: CBP contributed to securing the 60th Presidential Inauguration in Washington, D.C., by deploying over 700 personnel for inspections, perimeter security, and emergency operations. Despite freezing temperatures and heightened security concerns, CBP ensured public safety and further demonstrated its ability to protect high-profile national events.

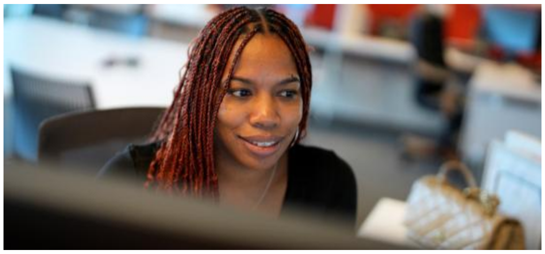
Efficient Use of Resources: CBP closed six temporary processing facilities along the southwest border following a drop in illegal border crossings, saving approximately $84 million per month. This initiative reflects CBP's commitment to resource efficiency while maintaining border security.

Managing Risks and Opportunities

Modernizing Border Crossing Infrastructure: Aging land ports of entry can create bottlenecks for trade and travel while increasing vulnerabilities to security threats. CBP is addressing this challenge through a major infrastructure modernization program, upgrading 34 ports of entry along the Northern and Southern borders. These improvements enhance security, facilitate economic growth, and meet growing trade and travel demands.



Record Tariff Collections Reflect Transformative Trade Policy: Unfair trade practices and illegal supply chains can harm the U.S. economy. In FY 2025, executive orders introduced higher tariffs and consumption duties, guiding CBP's efforts to address these risks. These measures have resulted in record tariff collections, helping protect the U.S. economy, promote fair trade, and significantly boost federal revenue.



Enhancing Workforce Efficiency Through Technology: Inefficient manual processes and outdated human resources systems can delay operations and reduce productivity. CBP addressed these challenges by implementing robotic process automation and launching a centralized human resources portal. Together, these innovations have saved over 13,000 staff hours annually, improved accuracy, and reduced task completion time by 69%. By streamlining access to personnel data and automating repetitive tasks, CBP has enhanced service delivery, boosted workforce productivity, and improved operational efficiency.

U.S. COAST GUARD

Component Overview

In FY 2025, USCG's net cost of operations was $14.8 billion. During FY 2025, USCG implemented transformative change through Force Design 2028 to maximize operational capabilities to control, secure, and defend the U.S. border and maritime approaches, facilitate commerce vital to U.S. economic prosperity, and respond to crises and contingencies.

USCG Net Cost of Operations, FY 2025

$14.8 billion

The following highlights showcase significant achievements and innovative approaches that advanced USCG's objectives. The following also highlights USCG's efforts to mitigate risks and seize opportunities to safeguard against opioid overdoses, ensure value for the American taxpayer, and rapidly turn reconciliation funding into operational capabilities.

Significant Initiatives and Success Stories

Record-Setting Year in Counterdrug Operations: In FY 2025, USCG seized approximately 510,000 pounds of cocaine valued at $3.8 billion and equivalent to 183 million lethal doses, achieving a historic milestone in counterdrug operations. This included the largest offload in USCG history—76,140 pounds of cocaine—by Cutter Hamilton at Port Everglades, Florida, on August 25, 2025. These operations, conducted with partner agencies, disrupted Transnational Criminal Organizations, prevented dangerous substances from entering the U.S., and reinforced USCG's vital role in combating illicit trafficking and safeguarding national security.

HITRON's 1000th Interdiction: USCG's Helicopter Interdiction Tactical Squadron (HITRON) exemplifies USCG's unique authorities and specialized capabilities to secure and defend U.S. borders. HITRON's precision airborne use of force, unmatched by other agencies, has enabled the maritime interdiction of $33 billion in illicit narcotics since its establishment in 1999, significantly disrupting Transnational Criminal Organizations. On August 25, 2025, HITRON completed its 1,000th interdiction of suspected narco-trafficking vessels, underscoring its critical role in the fight against maritime drug smuggling.

Controlling the U.S. Border and Maritime Approaches: In March 2025, USCG launched and led Operation Border Trident, an interagency approach to detection, monitoring, interdiction, and apprehension operations to combat Transnational Criminal Organizations and illegal alien activity in the California Coastal Region. USCG surged assets, including Fast Response Cutters, National Security Cutters, and aircraft, to the area around San Diego, to curb the flow of illegal maritime migration, increasing interdictions in the region by 44% over the prior year.

Commissioning the First Arctic Icebreaker in 25 Years: On August 10, 2025, USCG officially commissioned the Storis in Juneau, Alaska. The commissioning of this polar icebreaker marks a crucial step in the Administration's directive to rebuild USCG, which will include historic investments through the *One Big Beautiful Bill Act* (OB3) (Public Law (P.L.) 119-21), enacted in 2025. This vessel is USCG's first polar icebreaker acquired in over 25 years. As a medium polar icebreaker, Storis will enhance the Nation's maritime capabilities in the Arctic, continuing USCG's modernization through Force Design 2028, an initiative introduced in FY 2025 to transform USCG into a more agile, capable, and responsive fighting force.

Managing Risks and Opportunities

Distributing Narcan to Address the Opioid Crisis: The growing threat of opioid overdoses poses risks to public safety and USCG personnel who may be exposed during operations. To address this, USCG distributed over 6,000 doses of Narcan nasal spray to more than 400 units. Narcan reverses opioid overdoses, ensuring responders are equipped to save lives and maintain operational readiness in the face of the opioid crisis.

Ensuring Value for the American Taxpayer: Demonstrating unwavering commitment to the American people and stewardship of resources, USCG reviewed contracts across the enterprise that were failing to meet delivery agreements. USCG took decisive action to terminate major contracts related to vessel acquisitions, information technology (IT), and other services, resulting in a significant cost avoidance of taxpayer funds. These actions mitigated risks associated with potential resource inefficiencies and ensured USCG could better allocate funding to critical operations and mission objectives.

Rapidly Turning Reconciliation Funding into Operational Capabilities: USCG capitalized on $2 billion in OB3 funding to strengthen operational readiness and expand mission capabilities. This included contracting for 10 Fast Response Cutters and immediate depot maintenance needs, as well as obligating $150 million for advanced Counter-Unmanned Aerial Systems. These investments position USCG and DHS to provide critical protection and security during high-profile events such as the 2026 FIFA World Cup and Sail250 celebrations, ensuring the safety of the public and key infrastructure across the Nation.

U.S. CITIZENSHIP AND IMMIGRATION SERVICES

Component Overview

In FY 2025, USCIS's operating surplus (i.e., the excess of revenues over expenses) was $(780) million, with fee collections exceeding operational expenses. During FY 2025, USCIS prioritized enhancements to screening and vetting, continued to consistently adjudicate in accordance with law and policy, and advanced modernization of its benefits-processing IT systems.

USCIS Operating Surplus
(Excess of revenues over expenses), FY 2025

$(780) million

The following highlights showcase significant achievements and innovative approaches that advanced USCIS's mission objectives. The following also highlights USCIS's efforts to mitigate risks and seize opportunities to strengthen the integrity of the immigration system, improve operational efficiency, and foster public trust.

Significant Initiatives and Success Stories

Strengthening Immigration System Integrity and Public Safety: USCIS implemented the Alien Registration Requirement under Executive Order 14159, enabling the federal government to track the presence of aliens, review criminal records, and monitor activities. Since January 2025, USCIS has deployed over 500 volunteers to 85 ICE facilities and partnered with ICE to conduct more than 695 facilitated arrests at USCIS field offices. These efforts enhance public safety and restore trust in the immigration system.

Ending Abuse of Humanitarian Parole Authority: USCIS terminated categorical parole programs, including those for Cuban, Haitian, Nicaraguan, and Venezuelan nationals, to address widespread abuse of humanitarian parole authority. Parole requests are now considered on a case-by-case basis, aligning with the Administration's commitment to restoring integrity and fairness to the immigration system.

Restoring Robust Screening and Vetting Policies: In support of Executive Order 14161, USCIS reinstated stronger screening and vetting measures to protect the Nation from foreign terrorists and individuals posing security risks. Aliens who use false information to obtain immigration benefits now face severe consequences, including prison, fines, and removal from the U.S.

These measures uphold the integrity of the immigration system and safeguard national security.

Protecting Election Integrity: USCIS upgraded the Systematic Alien Verification for Entitlements (SAVE) system under Executive Order 14248 to prevent aliens from illegally voting or exploiting taxpayer benefits. Enhancements include fee elimination for state and local governments, bulk upload capabilities, and queries using social security numbers. These updates ensure accurate voter rolls, protect taxpayer resources, and restore public confidence in the electoral process.

Managing Risks and Opportunities

Securing Access to Critical Vetting Resources: USCIS's designation as a "non-criminal" justice agency limits its access to full criminal history information in the National Crime Information Center's index, creating risks of inadvertently approving filings for ineligible or dangerous individuals. To address this, USCIS is collaborating with DHS, federal agencies, and lawmakers to secure access through agreements, policy changes, or legislative solutions. Improved access to vetting resources enhances USCIS's ability to protect public safety and ensure the integrity of the immigration system.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Component Overview

In FY 2025, CISA's net cost of operations was $2.7 billion. During FY 2025, CISA prioritized efforts to expand cybersecurity protections, enhance critical infrastructure resilience, and modernize emergency communication systems.

CISA Net Cost of Operations, FY 2025

$2.7 billion

The following highlights showcase significant achievements and innovative approaches that advanced CISA's mission objectives. The following also highlights CISA's efforts to mitigate risks and seize opportunities to strengthen cybersecurity, improve operational efficiency, and protect critical infrastructure.

Significant Initiatives and Success Stories

Addressing Ransomware Threats with Proactive Notifications: CISA's Ransomware Vulnerability Warning Pilot (RVWP) and Pre-Ransomware Notification Initiative (PRNI) help organizations address a spectrum of ransomware risks and threats. RVWP identifies vulnerabilities and PRNI alerts affected entities to intrusions that may indicate early-stage ransomware attacks. Since January 20, 2025, RVWP sent notifications to over 920 vulnerable systems across 14 critical infrastructure sectors, with 52% of systems apparently mitigated. PRNI sent more than 800 notifications regarding early-stage intrusions over the same time period, saving an estimated $1.4 billion in potential ransomware recovery costs.

Preparedness through Cyber Resilient 911: CISA's Cyber Resilient 911 initiative improves the cybersecurity of U.S. Emergency Communications Centers by engaging with managers, conducting briefings, and developing protective solutions. Partnerships with academic institutions have also advanced proofs of concept for the 911 Cyber Defense Lab. These efforts enhance the resilience of critical emergency communications infrastructure, ensuring reliable services during cyber incidents.

Supporting Disaster Response During Southern California Wildfires: During the January 2025 Southern California Wildfires, CISA Region 9 coordinated with FEMA, emergency responders, and local authorities to safeguard lives and critical infrastructure. Through daily coordination calls, global information systems mapping, and unified communication strategies, CISA minimized disruptions and strengthened community safety. These actions demonstrate the importance of cross-sector collaboration in disaster response.

Preparing for FIFA World Cup 2026 with Full-Scale Exercise: CISA partnered with the Philadelphia Eagles, FIFA, and government agencies to conduct the Lincoln Financial Field Full-Scale Exercise, simulating responses to multiple threats in preparation for the FIFA World Cup 2026. More than 730 participants from over 40 organizations refined security, communications, and incident response plans, enhancing preparedness for the tournament and ensuring public safety.

Mitigating Cyber Risks with Vulnerability Response: Since January 2025, CISA has taken major steps to help government and private sector partners tackle cybersecurity risks. The agency added 183 vulnerabilities to its Known Exploited Vulnerabilities Catalog, helping organizations focus on the most critical threats. CISA also assessed over 34,000 vulnerabilities using the Stakeholder Specific Vulnerability Categorization method. This approach simplifies complex data by evaluating factors like exploitability, technical impact, and automation potential. These efforts guide partner IT teams in prioritizing and addressing vulnerabilities based on real-world risks.

Managing Risks and Opportunities

Streamlining Operations to Increase Efficiency: Redundant processes and unclear guidance can hinder agency effectiveness and divert resources from critical priorities. To mitigate these risks, CISA conducted mission and operational deep dives to identify inefficiencies, reduce redundancies, and align operations with statutory requirements. These efforts have improved agency performance, ensuring resources are allocated to areas of greatest impact and enabling CISA to better fulfill its core mission.

Modernizing Technology to Strengthen Mission Capabilities: Outdated IT systems and manual workflows can limit CISA's ability to adapt to evolving challenges and manage risks effectively. To address these issues, CISA established CISANet, a secure, cloud-first IT environment that enhances scalability, security, and operational efficiency. Additionally, the agency adopted automation technologies to streamline workflows, consolidate data sets, and improve risk analysis capabilities. Together, these innovations ensure timely responses to emerging threats, strengthen CISA's ability to protect critical infrastructure, and enable the agency to meet changing mission requirements.

FEDERAL EMERGENCY MANAGEMENT AGENCY

Component Overview

In FY 2025, FEMA's net cost of operations was $56.1 billion. During FY 2025, FEMA prioritized efforts to enhance disaster response capabilities; build state, local, tribal, and territorial response and recovery capabilities; and modernize grant management.

FEMA Net Cost of Operations, FY 2025

$56.1 billion

The following highlights showcase significant achievements and innovative approaches that advanced FEMA's mission objectives. The following also highlights FEMA's efforts to mitigate risks and seize opportunities to strengthen disaster preparedness, improve operational efficiency, and build community resilience.

Significant Initiatives and Success Stories

Driving Cost Efficiency and Accountability in Grants Programs: FEMA has taken actions related to financial assistance either to terminate awards or to cancel programs that do not meet current Administration priorities. In FY 2025, FEMA also awarded $3.5 billion across more than 20 programs, helping communities hire firefighters, improve cybersecurity, protect infrastructure, enhance security, upgrade warning systems, and bolster safety initiatives. These investments empower local leaders to prepare for fires, floods, cyber incidents, and terrorist threats. Enhanced oversight safeguards taxpayer dollars and drives cost efficiency and accountability in projects that improve resilience nationwide.

Enhancing Emergency Power Resources: FEMA ensures rapid deployment of emergency power during disasters by maintaining a fleet of generators. In FY 2025, FEMA replaced 15 outdated generators with high-efficiency models, increasing capacity and reducing operational costs. These upgrades supported power restoration in 12 disaster-affected communities, ensuring continuity of critical services and infrastructure. By proactively addressing emergency power needs, FEMA mitigates risks to public safety and accelerates recovery efforts.

Strengthening Supply Chain Resilience: FEMA's supply chain analysis network assessed private sector supply chains for food, fuel, power, and transportation during three major disaster responses. These analyses enabled faster restoration of essential services and minimized disruptions to affected communities. Collaboration with industry partners strengthened nationwide supply chain resilience, ensuring critical goods and services reach those in need during emergencies.

Strengthening Field Leadership for Disaster Response: FEMA enhanced disaster response capabilities by recruiting 120 new field leaders, providing advanced training to 350 personnel, and implementing mentorship programs. These initiatives increased Federal Coordinating Officer deployment readiness by 25% and bolstered incident workforce capacity, ensuring FEMA can respond effectively to complex disasters and support impacted communities. By investing in leadership development, FEMA builds a workforce capable of meeting evolving challenges.

Expanding Emergency Response Data Capabilities: FEMA is integrating data to improve nationwide situational awareness during emergency response. This effort supports state, local, tribal, and territorial partners in making data-driven decisions. In FY 2025, FEMA's National Emergency Response Information System expanded access to advanced data analytics for fire departments. A total of 91 departments logged more than 15,000 incidents, reducing response times by 20%. These improvements were made possible through real-time decision-making powered by Geographic Information System technology. These enhanced capabilities strengthen emergency operations and save lives.

Managing Risks and Opportunities

Strengthening Hurricane Response and Supporting Community Recovery: FEMA is enhancing disaster response and recovery efforts to address the challenges posed by increasingly complex hurricane seasons. In FY 2025, through three week-long symposiums at the Incident Workforce Academy in Alabama, 450 field leaders received advanced training using real-world hurricane scenarios, improving operational readiness for hurricane season. FEMA is also prioritizing locally-led recovery across the Southeast by partnering with states, tribes, and communities to rebuild stronger after devastating storms. By cutting red tape and accelerating recovery funding, FEMA empowers communities to clear debris and advance critical infrastructure projects, ensuring resilience and preparedness for future disasters.

Expanding Wildfire Evacuation Planning: Wildfires threaten communities across the United States, especially in areas where population growth has increased exposure to fire hazards. FEMA's U.S. Fire Administration expanded its wildfire evacuation tabletop exercise series, delivered in three communities during initial rollout, to six additional counties during FY 2025. These exercises strengthen evacuation planning, improve community resilience, and enhance collaboration with public and private partners. By proactively addressing wildfire risks, FEMA reduces the potential for loss of life and property while building capacity for future emergencies.

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

Component Overview

In FY 2025, ICE's net cost of operations was $11.5 billion. During FY 2025, ICE prioritized efforts to enhance interior enforcement operations, expand detention capacity, and combat human trafficking and illicit narcotics networks.

ICE Net Cost of Operations, FY 2025

$11.5 billion

The following highlights showcase significant achievements and innovative approaches that advanced ICE's mission objectives. The following also highlights ICE's efforts to mitigate risks and seize opportunities to strengthen immigration enforcement, improve operational efficiency, and protect U.S. communities.

Significant Initiatives and Success Stories

Record-High Arrests by Enforcement and Removal Operations: ICE's Enforcement and Removal Operations achieved its highest daily administrative arrest total on June 3, 2025, with arrests increasing by 103.2% compared to the same period in 2024. Arrests of individuals convicted of or charged with crimes rose by 110%, including violent criminals, gang members, and suspected terrorists. These results highlight ICE's commitment to enforcing immigration laws and protecting communities from dangerous individuals.

Project Athens Targets Violent Criminal Gangs: Project Athens, a Homeland Security Investigations-led initiative targeting violent gangs, resulted in 34 federal indictments, 674 criminal arrests, and 2,278 administrative arrests between January and June 2025. The operation disrupted activities of Tren de Aragua, a Venezuelan gang designated as a Foreign Terrorist Organization, mitigating threats to public safety and curbing the spread of violent actors in the U.S.

U.S.-Guatemala Security Alliance Strengthens Cooperation: On June 11, 2025, ICE signed a Memorandum of Cooperation with Guatemala to formalize a fugitive information-sharing program. Since 2015, this program has facilitated the removal of 1,588 Guatemalan fugitives residing illegally in the U.S. ICE is working to establish similar agreements with El Salvador, Honduras, and Mexico, enhancing transnational cooperation to address crime and improve public safety.

Special High-Risk Charter Removals: ICE conducted a multinational removal mission to Egypt and Kenya on June 12, 2025, targeting high-risk individuals subject to Interpol Red Notices or prior removal orders. By coordinating with foreign authorities, ICE overcame logistical challenges to enforce immigration laws globally. This mission demonstrates ICE's innovative approach to complex removal operations.

Protecting Unaccompanied Alien Children from Exploitation: In February 2025, and in collaboration with the DHS Center for Countering Human Trafficking, ICE launched an urgent initiative to locate unaccounted-for unaccompanied alien children. By June 30, 2025, ICE had located over 10,300 children, ensuring their safety and confirming they were not victims of human trafficking or exploitation. This effort underscores ICE's dedication to protecting vulnerable populations and combating trafficking risks.

Managing Risks and Opportunities

Preventing Online Child Exploitation: Online child sexual exploitation is a growing global threat. DHS's Know2Protect campaign raises awareness and provides tools to prevent online exploitation and abuse. In FY 2025, through Know2Protect's in-person training initiative—Project iGuardian—Homeland Security Investigations special agents and other experts delivered nearly 1,300 presentations worldwide, reaching approximately 2.4 million people. These efforts led to 87 victim disclosures and generated 27 investigative leads. These efforts empower communities to recognize and prevent exploitation, enhancing child safety.

Combating Human Trafficking Through Public Engagement: Human trafficking remains a pervasive threat to vulnerable populations. ICE support for the Blue Campaign educates the public, law enforcement, and industry on recognizing and responding to trafficking. In FY 2025, the campaign partnered with 24 new organizations and hosted 94 events for nearly 14,000 participants. These efforts strengthen public engagement and collaboration, enhancing the government's ability to prevent trafficking and protect victims.

Expanding State and Local Partnerships to Enhance Public Safety: State and local law enforcement agencies are critical partners in immigration enforcement. ICE's 287(g) program expanded significantly in FY 2025, with 839 agreements and 7,640 trained immigration officers—an over 900% increase since January 2025. These partnerships act as a force multiplier, enabling local officers to assist in identifying and detaining foreign-born individuals involved in criminal activity. This collaboration enhances public safety and supports ICE's mission to enforce immigration laws.

U.S. SECRET SERVICE

Component Overview

In FY 2025, USSS's net cost of operations was $3.5 billion. During FY 2025, USSS prioritized efforts to enhance protective operations for national leaders, combat financial crimes, and modernize cybersecurity measures.

USSS Net Cost of Operations, FY 2025

$3.5 billion

The following highlights showcase significant achievements and innovative approaches that advanced USSS's mission objectives. The following also highlights USSS's efforts to mitigate risks and seize opportunities to strengthen protective operations, improve operational efficiency, and address emerging threats.

Significant Initiatives and Success Stories

Securing the Army 250th Birthday Parade: On June 14, 2025, USSS led security planning for the Army 250th Birthday Parade National Special Security Event in Washington, D.C. Coordinating with over 2,000 interagency partners, USSS ensured the safety of 7,000 participants and 100,000 attendees, including the President. Security measures included civil disturbance units, medical response teams, and an 18-mile perimeter of fencing. This operation demonstrates USSS's expertise in securing large-scale, high-profile events and protecting national leaders.

Innovative Use of K9s to Combat Financial Crime: USSS-trained electronic storage detection K9s are addressing the rise in electronic crime. On May 17, 2025, K9 Perl, deployed in Placer County, California, alerted investigators to hidden cryptocurrency wallets and a cellphone containing theft records. These items facilitated the recovery of over $28 million in stolen cryptocurrency and led to the suspect's confession. This success highlights the innovative use of K9s in recovering stolen assets and combating financial crimes.

Combating EBT/SNAP Fraud: USSS is actively fighting fraud targeting the Electronic Benefit Transfer (EBT) and Supplemental Nutrition Assistance Program (SNAP), which suffered nearly $18 billion in theft during 2024. In FY 2025, USSS partnered with public and private organizations to inspect approximately 30,000 Point-of-Sale devices in eight major cities. These efforts uncovered 210 illegal skimming devices, led to 20 federal arrests, and prevented an estimated $218 million in fraud losses. By disrupting Transnational Criminal Organizations, USSS safeguarded critical benefit programs that support millions of Americans in need.

Managing Risks and Opportunities

Enhancing Protective Operations with Autonomous Systems: Evolving threats require advanced security measures to safeguard protectees and sensitive environments. USSS deployed quadruped robotic platforms equipped with chemical and radiological sensors through its Autonomous System and Technical Robotic Operations Pilot Program. These systems were successfully used at two National Special Security Events and included the first permanent fixed-site unit providing autonomous perimeter security. These innovations enhance USSS's ability to adapt to emerging threats and ensure the safety of protectees and sensitive locations.

Expanding Counter-Unmanned Aircraft Systems Capabilities: Unauthorized drones pose increasing risks to protective operations and sensitive locations. USSS expanded its Counter-Unmanned Aircraft Systems Program, acquiring advanced technologies to detect, track, and mitigate drones near protective sites. These systems integrate multiple detection technologies into a single operational package, enabling efficient responses to potential threats. This expansion strengthens USSS's ability to safeguard protectees, secure high-risk environments, and address the challenges posed by unauthorized drones.

Modernizing Recruitment Strategies to Meet Workforce Demands: Growing operational demands require innovative recruitment approaches. USSS enhanced its recruitment strategy by leveraging artificial intelligence, programmatic job boards, Google analytics, and targeted social media outreach to individuals aged 20 to 37. These efforts increased application volume and improved hiring outcomes, with special agent hires rising significantly. By focusing on populations with a history of success, such as military personnel and athletes, USSS is ensuring it can meet future challenges and maintain operational excellence.

TRANSPORTATION SECURITY ADMINISTRATION

Component Overview

In FY 2025, TSA's net cost of operations was $7.1 billion. During FY 2025, TSA prioritized efforts to deploy advanced screening technologies, enhance workforce training programs, and strengthen cybersecurity measures to protect transportation systems.

TSA Net Cost of Operations, FY 2025

$7.1 billion

The following highlights showcase significant achievements and innovative approaches that advanced TSA's mission objectives. The following also highlights TSA's efforts to mitigate risks and seize opportunities to enhance transportation security, improve operational efficiency, and safeguard the traveling public.

Significant Initiatives and Success Stories

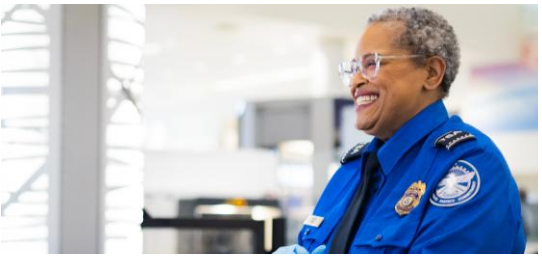
Managing Record-Breaking Passenger Volumes: In the past year, TSA screened over 900 million passengers and more than 2 billion carry-on items across more than 430 domestic airports and 250 overseas last points of departure. TSA also experienced its ten highest passenger volume days in history—all occurring since July 2024—while exceeding PreCheck® and Standard wait time standards. These achievements demonstrate TSA's ability to manage unprecedented passenger volumes efficiently while enhancing the customer experience.

Seamless REAL ID Enforcement: On May 7, 2025, TSA began full enforcement of the REAL ID Act (P.L. 109-13), requiring domestic travelers to present a REAL ID-compliant driver's license or another acceptable form of identification. Through strong partnerships with stakeholders, TSA implemented REAL ID enforcement seamlessly, achieving 93% compliance nationwide, and ensuring more secure passenger identify verification.

Deploying Next-Generation Screening Technologies: TSA is deploying advanced screening technologies to enhance security and streamline the passenger experience. These innovations include improved identity verification, enhanced equipment connectivity, and less-intrusive security policies. By integrating these technologies, TSA is expediting precise threat detection while ensuring a seamless travel experience, demonstrating its commitment to innovation and security during the Golden Age of Travel.

Securing All Modes of Transportation: TSA safeguards the Nation's transportation systems, to include aviation (commercial and general), surface transportation (mass transit, freight and passenger rail, highways, and pipelines), and maritime (ports and intermodal connections). TSA oversees security for 3 million tons of domestic air cargo, 3.3 million miles of pipelines, 7 billion public transportation passengers, 25 million students, 140,000 miles of freight rail track, and 360 ports. By partnering with stakeholders across all modes of transportation, TSA ensures the security of passengers and goods transported around the Nation.

Managing Risks and Opportunities



Preparing for Mega-Events: Major events—like the 2026 FIFA World Cup, the 2028 Summer Olympics, and America's 250th anniversary—will drive record travel and heightened security demands. TSA is preparing early with coordinated planning, surge staffing and scheduling, tested playbooks with airports and airlines, and upgrades to screening technology and queuing. These steps help manage higher passenger volumes, protect transportation systems, and maintain a safe, efficient trip for the public experience.

Adapting Screening Operations to Demand and Complexity: Passenger surges and complex screening requirements can strain checkpoints, increase wait times, and affect screening operations. TSA mitigates these risks by optimizing staffing and shift plans, applying risk-based security measures, deploying advanced screening solutions, and strengthening coordination among Transportation Security Officers, the Federal Air Marshals, and law enforcement partners. These actions help TSA sustain throughput and security performance during routine operations and peak periods.

Strengthening Cybersecurity Across Transportation Systems: More connected transportation systems and increasingly sophisticated cyber-attacks can disrupt operations and threaten the safety of passengers and goods. TSA reduces this risk by securing its own networks and working with transportation owners and operators to improve cyber readiness through clear requirements, security awareness, information sharing, assessments and exercises, and modern monitoring and response tools. These efforts increase resilience across aviation and surface transportation and support safe, reliable travel.

FINANCIAL OVERVIEW

Introduction

This section is presented as an analysis of the Department's principal financial statements. Included in this analysis is a summary of key financial balances, nature of significant changes, and highlights of key financial events to assist readers in establishing the relevance of the financial statements to the operations of DHS.

The Department's principal financial statements—Balance Sheet, Statement of Net Cost, Statement of Changes in Net Position, Statement of Budgetary Resources, Statement of Custodial Activity, and notes to the principal financial statements—are prepared to report the financial position, financial condition, and results of operations of the Department, consistent with the requirements of 31 United States Code (U.S.C.) §3515(b).

The statements are prepared from records of Federal entities in accordance with Federal generally accepted accounting principles (GAAP) and the formats prescribed by the U.S. Office of Management and Budget (OMB). Reports used to monitor and control budgetary resources are prepared from the same records. Users of the statements are advised that the statements are for a component of the U.S. Government.

Financial Position

The Balance Sheet presents the resources owned or managed by the Department that have future economic benefits (assets) and the amounts owed by DHS that will require future payments (liabilities). The difference between the Department's assets and liabilities is the residual amount retained by DHS (net position) that is available for future programs and capital investments. The Department's condensed FY 2025 Balance Sheet and Statement of Net Cost are presented below as Financial Position and Results of Operations, respectively.

Financial Position ($ in millions)		FY 2025
Fund Balance with Treasury	$	359,102
Property, Plant, and Equipment, Net		33,995
Taxes Receivable, Net		25,230
Other Assets		21,644
Total Assets	**$**	**439,971**
Liability to the General Fund of the U.S. Government	$	25,254
Debt		22,533
Federal Employee Salary, Leave, and Benefits Payable		3,665
Pension, Post-Employment, and Veterans Benefits Payable		17,689
Accounts Payable		6,497
Insurance Liabilities		3,510
Other Liabilities		17,965
Total Liabilities	**$**	**97,113**
Total Net Position		**342,858**
Total Liabilities and Net Position	**$**	**439,971**

(table continued on next page)

(table continued from prior page)

Results of Operations ($ in millions)		FY 2025
Gross Cost	$	143,518
Less: Earned Revenue		(20,329)
Net Cost Before Gains and Losses on Assumption Changes	**$**	**123,189**
Loss on Assumption Changes		459
Total Net Cost	**$**	**123,648**

Assets – What We Own and Manage

Assets represent resources owned or managed by the Department that can be used to accomplish its mission. The Department's largest asset is **Fund Balance with Treasury**, which consists primarily of appropriated, revolving, trust, deposit, receipt, and special funds remaining at the end of the fiscal year.

Property, Plant, and Equipment (PP&E), Net is the second largest asset, and includes buildings and facilities, vessels, aircraft, construction in progress, and other equipment. In acquiring these assets, the Department either spent resources or incurred a liability to make payment at a future date; however, because these assets should provide future benefits to help accomplish the DHS mission, the Department reports these items as assets rather than expenses.

Taxes Receivable, Net includes excise taxes and customs duties, and trade receivables.

Other Assets includes items such as investments; accounts receivable; cash and other monetary assets; and inventory and related property.

Liabilities – What We Owe

Liabilities are the amounts owed to the public or other federal agencies for goods and services provided but not yet paid for; to DHS employees for wages and future benefits; and for other liabilities.

Liability to the General Fund of the U.S. Government is the Department's largest liability and consists of duties, taxes, and fees collected by CBP to be remitted to various general fund accounts maintained by Treasury. The increase in custodial liability is attributed to the rise in taxes receivable due to unpaid entry releases and cash collections for imported duties.

Debt is the Department's second largest liability and results from Treasury loans to fund FEMA's National Flood Insurance Program (NFIP) and Disaster Assistance Direct Loan Program (DADLP). Given the current premium rate structure, FEMA will not be able to generate sufficient resources from premiums to fully pay its debt. This is discussed further in Note 14, Debt in the Financial Information section.

Federal Employee Salary, Leave, and Benefits Payable and **Pension, Post-Employment, and Veterans Benefits Payable** include amounts owed to current and separated personnel for pension and other post-employment benefits, as well as the liability for medical costs for approved workers' compensation cases. For more information, see Note 15, Federal Employee and Veteran Benefits Payable in the Financial Information section. These liabilities are not covered by current budgetary resources, and the Department will use future appropriations to cover these liabilities (see Note 13, Liabilities Not Covered by Budgetary Resources in the Financial Information section).

Accounts Payable consists primarily of amounts owed for goods, services, or capitalized assets received, progress on contract performance by others, and other expenses due to other entities.

Insurance Liabilities are primarily the result of the Department's sale or continuation-in-force of flood insurance policies within the NFIP, which is managed by FEMA.

Other Liabilities include amounts owed to other federal agencies and the public for goods and services received by the Department, amounts received by the Department for goods or services that have not been fully rendered, unpaid benefit contributions payable for current and separated DHS employees, environmental liabilities, refunds and drawbacks, and other liabilities.

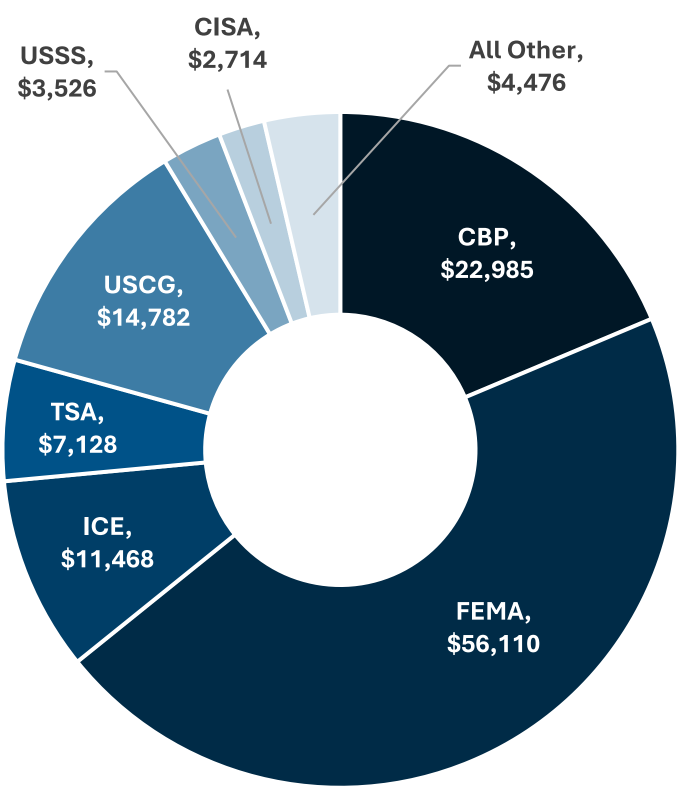
Net Position – Where We Stand

Net position represents the accumulation of revenue, expenses, budgetary, and other financing sources since inception, as represented by an agency's balances in unexpended appropriations, $330.1 billion, and cumulative results of operations, $12.8 billion, on the Statement of Changes in Net Position.

Financing sources increase net position and include, but are not limited to, appropriations, user fees, and excise taxes. The net costs, as well as transfers to other agencies, decrease net position.

Net Cost of Operations

Net costs are presented by Operational Components which carry out the Department's major mission activities, with the remaining Support Components representing "All Other" (see adjacent figure). Net cost of operations, before gains and losses, represents the difference between the costs incurred and revenue earned by DHS programs.



$ in millions

During FY 2025, FEMA had an increase in gross costs from the prior year due to an increase in support for continuing disaster recovery efforts, including losses related to Hurricanes Helene and Milton.

During FY 2025, the Department earned approximately $20 billion in exchange revenue. Exchange revenue arises from transactions in which the Department provides goods and/or services that are directly related to its operations to the other receiving party.

The Department also collects non-exchange duties, taxes, and fee revenue on behalf of the Federal Government. This non-exchange revenue is presented in the Statement of Custodial Activity or Statement of Changes in Net Position, rather than the Statement of Net Cost.

Budgetary Resources

The Statement of Budgetary Resources provides information about how budgetary resources were made available as well as their status at the end of the period. Budgetary accounting rules require recording the obligation of funds based on legal requirements, which often occurs before the actual transaction under the accrual accounting method. The recognition of budgetary accounting transactions is essential for compliance with legal constraints and controls over the use of federal funds.

The budget represents our plan for efficiently and effectively achieving the strategic objectives to carry out our mission and to ensure that the Department manages its operations within the appropriated amounts using budgetary controls.

Sources of Funds ($ in millions)		FY 2025
Unobligated Balance from Prior Year Budget Authority, Net	$	48,701
Appropriations		332,715
Spending Authority from Offsetting Collections		14,390
Borrowing Authority		2,502
Total Budgetary Resources	**$**	**398,308**

In FY 2025, the Department's total budgetary resources increased from the prior year mainly due to the $191 billion in appropriations DHS received from OB3. This Act significantly increased the funding DHS received to improve border security, increase immigration enforcement, and recapitalize USCG fleets along with support for state and local entities supporting the Department's mission. OB3 includes funding for physical barriers, advanced surveillance systems, immigrant detention requirements, USCG fleet and equipment modernization, CBP and ICE personnel, State Homeland Security Grant Programs support, and a new State Border Security Reinforcement Fund.

Custodial Activities

Custodial activity involves the Department collecting revenue, such as duties, taxes, and fees, for others and distributing it to the appropriate recipients. This non-exchange revenue is either used by the Department to support its mission or sent to the Treasury's general fund and other federal agencies.

Cash Collections ($ in millions)		FY 2025
Duties	$	201,007
Excise Taxes		5,213
Other		2,823
Total Cash Collections	**$**	**209,043**

Duties collected on imports increased significantly from the prior year primarily due to higher tariffs and consumption duties. This change is driven by several executive orders issued in FY 2025. These orders resulted in higher accruals for duties on imports, including antidumping, countervailing, informal entries, and consumption duties. The overall growth in duties reflects the impact of these executive orders and modifications, which targeted trade practices, border security, and illicit supply chains.

In FY 2025, custom duties collected by CBP accounted for 96% of total cash collections. The remaining 4% is comprised of excise taxes, user fees, and various other fees.

Other Key Regulatory Requirements

For a discussion on the Department's compliance with the *Prompt Payment Act of 1982* (P.L. 97-177) and the *Debt Collection Improvement Act of 1996* (P.L. 104-134), see the Other Information section.

ANALYSIS OF SYSTEMS, CONTROLS, AND LEGAL COMPLIANCE

Federal Managers' Financial Integrity Act

The *Federal Managers' Financial Integrity Act of 1982* (FMFIA) (P.L. 97-255) requires agencies to conduct an annual evaluation of their internal control and financial management systems and report the results to the President and the Congress. Each agency then prepares an annual Statement of Assurance to report on the effectiveness of its internal control and financial management systems' compliance based on the assessment related to:

- Effectiveness and efficiency of operations,
- Compliance with applicable laws and regulations, and
- Reliability of reporting for internal and external use.

FMFIA also requires the Statement of Assurance to include assurance on whether the agency's financial management systems substantially comply with government-wide requirements in accordance with Section 803(a) of the *Federal Financial Management Improvement Act of 1996* (FFMIA) (P.L. 104-208).

DHS is also upheld to financial accountability and stewardship requirements as outlined in the *Department of Homeland Security Financial Accountability Act of 2004* (P.L. 108-330). As noted within that legislation:

> *"The Department of Homeland Security was created by consolidation of 22 separate Federal agencies, each with its own accounting and financial management system. None of these systems was developed with a view to executing the mission of the Department of Homeland Security to prevent terrorist attacks within the United States, reduce the Nation's vulnerability to terrorism, and minimize the damage and assist in the recovery from terrorist attacks. For these reasons, a strong Chief Financial Officer is needed within the Department both to consolidate financial management operations, and to insure that management control systems are comprehensively designed to achieve the mission and execute the strategy of the Department."*

To strengthen performance in executing a homeland security strategy, the *Department of Homeland Security Financial Accountability Act* highlighted the responsibilities of the Chief Financial Officer (CFO) of DHS while also imposing a DHS-specific mandate for the Secretary of Homeland Security to obtain an audit opinion of Department's internal control over financial reporting. Since the *Department of Homeland Security Financial Accountability Act* became law in 2004, DHS remains the only agency subject to the *Chief Financial Officers Act of 1990* (CFO Act) (P.L. 101-576) that must produce an internal control over financial reporting annual audit opinion.

DHS management is responsible for establishing, maintaining, and assessing internal controls to provide reasonable assurance that the objectives of the FMFIA, FFMIA, and the *Department of Homeland Security Financial Accountability Act* are achieved.

Assessing Internal Control Effectiveness

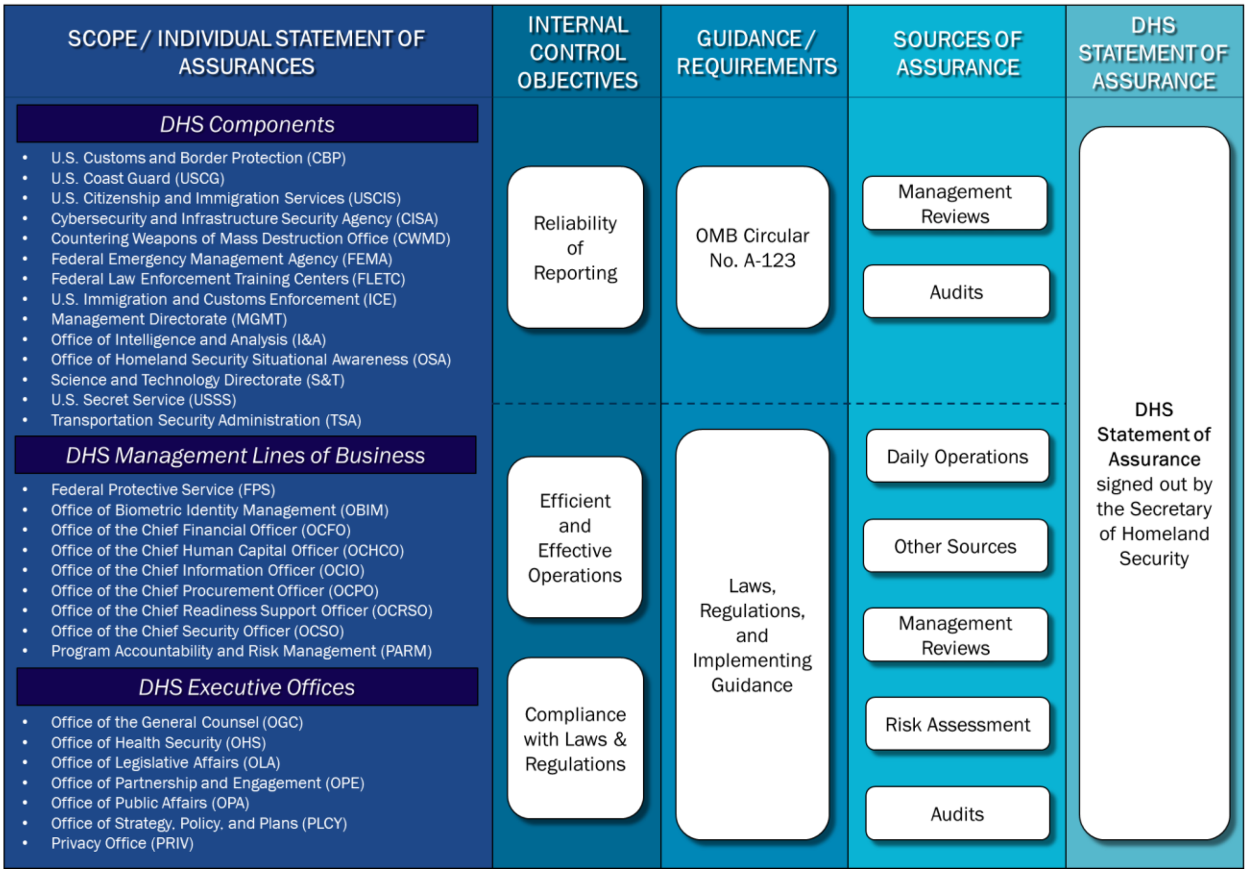
The U.S. Government Accountability Office (GAO) prescribes *Standards for Internal Control in the Federal Government*, more commonly known as the Green Book. These standards provide the internal control framework and criteria federal managers must use in designing, implementing, and operating an effective system of internal control. The Green Book defines internal control as a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity are achieved.

OMB, in consultation with GAO, establishes guidelines for agencies to evaluate their systems of internal control to determine FMFIA Section 2 and Section 4 compliance.

- OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, provides implementation guidance to federal managers on improving the accountability and effectiveness of federal programs and operations by identifying and managing risks and establishing requirements to assess, correct, and report on the effectiveness of internal controls.
- OMB Circular No. A-123, Appendix D, *Management of Financial Management Systems – Risk and Compliance*, provides guidance in determining compliance with FFMIA for agencies subject to the CFO Act of 1990 and encourage agency management of financial management systems integrity risk.

In accordance with OMB Circular No. A-123 guidance, the Department performs assessments over the effectiveness of its internal controls. The results of these assessments provide management with an understanding of the effectiveness and efficiency of operations, reliability of reporting, and compliance with laws and regulations.

DHS Statement of Assurance Process



Per OMB Circular No. A-123, management gathered information from various sources, including management-initiated internal control assessments, program reviews, and evaluations. Management also considered results of reviews, audits, inspections, and investigations performed by the Department's Office of Inspector General (OIG) and GAO. Using available information, each Component performs an analysis on the pervasiveness and materiality over any identified deficiencies to determine their impact and uses the result as the basis for the respective Component assurance statement signed by the Component Head. The Secretary provides assurances over the Department's internal controls in the annual assurance statement considering the state of internal controls at each Component.

SECRETARY'S ASSURANCE STATEMENT

January 22, 2026

The Department of Homeland Security is responsible for meeting the objectives of Sections 2 and 4 of the *Federal Managers' Financial Integrity Act of 1982* (FMFIA) to establish and maintain effective internal controls, inclusive of financial management systems, that protect the integrity of federal programs. Management satisfies these objectives by managing risks and maintaining effective internal controls in three areas: 1) effectiveness and efficiency of operations; 2) reliability of reporting; and 3) compliance with applicable laws and regulations. The Department conducted its assessment of risk and internal controls in accordance with the Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. Based on the results of the assessment, the Department can provide reasonable assurance that internal control over operations, reporting, and compliance were operating effectively as of September 30, 2025, except for the disclosures noted in the subsequent sections.

Pursuant to the *Department of Homeland Security Financial Accountability Act*, the Department is required to obtain an opinion on its internal control over financial reporting. The Department conducted its assessment of the effectiveness of internal controls over financial reporting in accordance with OMB Circular No. A-123 and based on the criteria established by the Government Accountability Office (GAO), *Standards for Internal Control in the Federal Government*. Based on the results of this assessment, the Department can provide reasonable assurance that its internal control over financial reporting was designed and operating effectively as of September 30, 2025, except for aspects of Information Technology Controls and Information Systems, Financial Reporting, Insurance Management, Budgetary Accounting, and Revenue and Receivables Reporting where material weakness areas were identified, and remediation is in process.

The *Federal Financial Management Improvement Act of 1996* (FFMIA) requires agencies to implement and maintain financial management systems that substantially comply with Federal financial management system requirements, Federal accounting standards, and United States Standard General Ledger reporting at the transaction level. The material weakness area specifically related to Information Technology Controls and Information Systems affects the Department's ability to substantially comply with financial management system requirements. In addition, as a result of numerous Component agencies' financial management system limitations, the Department does not fully comply with certain government-wide accounting and reporting requirements. Therefore, the Department is reporting non-compliance with FFMIA and Section 4 of FMFIA. To address this non-compliance, the Department has undertaken a multi-year financial systems consolidation program, in alignment with Executive Order 14249, *Protecting America's Bank Account Against Fraud, Waste, and Abuse.*

As a result of the assessments conducted, the Department continues to enhance its internal controls and financial management program. For noted areas of weakness, the Department is continuing previously initiated remediation efforts and incorporating additional improvements going forward, as highlighted in the Management Assurances section of the Agency Financial Report.

Sincerely,

Kristi Noem

Secretary of Homeland Security

MANAGEMENT'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING

January 22, 2026

Mr. Joseph V. Cuffari
Inspector General
Department of Homeland Security
Washington, DC

Dear Inspector General Cuffari:

The United States Department of Homeland Security (DHS) internal control over financial reporting constitutes a process effected by those charged with governance, management, and other personnel, designed to provide reasonable assurance regarding the preparation of reliable financial statements in accordance with the United States' generally accepted accounting principles. An organization's internal control over financial reporting includes those policies and procedures that:

- Pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the entity;
- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with the United States' generally accepted accounting principles, and that receipts and expenditures of the organization are being made only in accordance with authorizations of management and those charged with governance; and
- Provide reasonable assurance regarding prevention, or timely detection and correction, of unauthorized acquisition, use, or disposition of the organization's assets that could have a material effect on the financial statements.

DHS is responsible for designing, implementing, and maintaining effective internal control over financial reporting. Management assessed the effectiveness of DHS's internal control over financial reporting as of September 30, 2025, based on criteria established in the Standards for Internal Controls in the Federal Government (GAO-14-704G) issued by the Comptroller General of the United States. Based on that assessment, Management concluded that, as of September 30, 2025, DHS's system of internal control over financial reporting is effective except for areas of material weaknesses in Information Technology Controls and Information Systems, Financial Reporting, Insurance Management, Budgetary Accounting, and Revenue and Receivables Reporting. Specifically:

1. Information Technology Controls and Information Systems: Control deficiencies identified related to financial management systems, including those performed by service organizations; and information derived from systems.
2. Financial Reporting: Control deficiencies identified related to monitoring of reports used in financial reporting controls; service provider monitoring; and other conditions to include application controls, construction in progress, journal entries, and suspense account balances.
3. Insurance Management: Control deficiencies identified related to financial data, review of the valuation approach of the flood insurance liability, and monitoring of applicable service providers.
4. Budgetary Accounting: Control deficiencies identified related to the monitoring of budgetary resources to include undelivered orders and the financial reporting of apportionments allocated for future periods.

5. Revenue and Receivables Reporting: Control deficiencies identified related to the monitoring of immigration fee revenue and entry/taxes receivables activity to ensure complete and accurate reporting.

Internal control over financial reporting has inherent limitations as it involves human diligence and compliance and is subject to lapses in judgment and breakdowns resulting from human failures. Internal control over financial reporting can also be circumvented by collusion or improper management override. Because of these inherent limitations, internal control over financial reporting may not prevent, or detect and correct, misstatements. Also, projections of any assessment of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

The Seized and Forfeited Property Other than Monetary Instruments area of material weakness disclosed by the auditor during previous engagements has been reduced in severity during fiscal year 2025. The United States Coast Guard continues to implement compensating manual controls as necessary and to correct legacy data, but system functionality has been significantly enhanced and the modernized core accounting systems has achieved full operating capability in fiscal year 2025. In addition, the Federal Emergency Management Agency has maintained its focus on disaster response and directly supported these efforts financially through grants, disaster loans, and flood insurance payments. However, areas for improvement continue to be noted. While keeping the mission in the forefront, DHS continues to make progress in improving its internal controls and financial management program and management commits to implementing corrective actions to resolve the remaining areas of material weakness that had been communicated during previous engagement as well as any newly identified areas of deficiency.

Sincerely,

Kristi Noem

Secretary of Homeland Security

Holly C. Mehringer

Senior Official Performing the Duties of the Chief Financial Officer

Areas of Material Weaknesses and Corrective Action Plans

In FY 2025, management is reporting five areas of material weaknesses: 1) IT Controls and System Functionality, 2) Financial Reporting, 3) Insurance Management, 4) Budgetary Accounting, and 5) Revenue and Receivables Reporting. Despite the noted deficiencies, DHS has determined that compensating controls have been sufficiently implemented to mitigate the risk to financial statements as highlighted by the Department's receipt of its 13th consecutive unmodified financial statement audit opinion. While these challenges have not resulted in a material misstatement for the Department, resolution of identified control deficiencies will be critical for an efficient and effective internal control over financial reporting and sustained effective system of internal control for the Department.

Area of Material Weakness		
IT Controls and Information Systems		
DHS Component(s)	**Year Identified**	**Target Correction Date**
All	FY 2003	FY 2028

Multiple deficiency areas exist that are attributed to the IT Controls and Information Systems area of material weakness, which include the following:

Financial System Requirements (Contributing Component(s): All)

Deficiency Details

Insufficient design and implementation of controls in accordance with the DHS Information System Security program, Sensitive Systems policy, and federal information security requirements.

Corrective Actions Taken in FY 2025

- The Department continued to utilize a risk-based approach for the IT Internal Control Program to help with scoping for systems as well as controls to prioritize remediation and internal assessments.
- Management developed and executed Plans of Action and Milestones to facilitate the remediation of the Information Technology General Controls (ITGC) deficiencies.
- DHS Components prioritized remediation efforts related to Access Control, Audit Logging, and Segregation of Duties deficiencies for high impact financial related systems.

Additional Corrective Actions Planned

Multi-year corrective actions are expected to continue, to include:

- Execution of a find, fix, test, and assert strategy that allows for risk-based prioritization and adjustments;
- Utilization of IT Commitment Letters, signed by both the respective CFO and the Chief Information Officer leadership;
- Leadership support, oversight, and accountability over the design and implementation of internal controls in accordance with DHS IT policy requirements; and
- Continued consolidation efforts for legacy financial systems and applications.

(table continued on next page)

(table continued from prior page)

Area of Material Weakness		
IT Controls and Information Systems *(continued)*		
DHS Component(s)	**Year Identified**	**Target Correction Date**
All	FY 2003	FY 2028
Service Provider Monitoring (Contributing Component(s): All) <u>Deficiency Details</u> Ineffective internal control related to service organizations, including the monitoring of ITGC for external systems to ensure adequate reliance. • Ineffective internal control related to service organizations, including the monitoring of ITGC for external systems to ensure adequate reliance. • Insufficient evaluation and documentation of service organizations roles, performing effective reviews of Service Organization Controls (SOC) reports, and addressing service provider risk in absence of SOC reports. <u>Corrective Actions Taken in FY 2025</u> • The Department updated its Enterprise-wide Service Provider Population to capture applicable organizations which impact the DHS internal control over financial reporting environment; • The Office of the Chief Financial Officer (OCFO) continued to provide optional work guidance documentation provided for walkthrough questionnaires, as well as templates to support the documentation of population, risk assessments, and roles and responsibilities. • OCFO provided related training through the DHS quarterly internal controls and risk management training events. <u>Additional Corrective Actions Planned</u> DHS will continue to execute improvements and corrective actions as cost beneficial. Annual updates and/or multi-year actions to be completed include: • Identifying and updating the population of service providers; • Conducting risk assessments; • Executing appropriate service provider risk response, management, and oversight; and • Ensuring agreements with and utilization of service providers enable adequate assurance related to service provider performed activities and controls. ***System Functionality / Information Derived from Systems*** (Contributing Component(s): All) <u>Deficiency Details</u> Ineffective IT security control and inadequate application / functionality controls impact the ability for management to fully rely on system generated data and reports. <u>Corrective Actions Taken in FY 2025</u> • OCFO continued efforts to update and enhance guidance related to alternative testing procedures for Business Process Application Controls. • Components continued efforts to identify and assess their Information Used in Controls (IUC) for key control activities through annual A-123 assessments.		

(table continued on next page)

(table continued from prior page)

Area of Material Weakness		
IT Controls and Information Systems *(continued)*		
DHS Component(s)	**Year Identified**	**Target Correction Date**
All	FY 2003	FY 2028
• OCFO provided related training through DHS quarterly internal controls and risk management training events. Additional Corrective Actions Planned Multi-year actions to be completed, as cost beneficial, include: • Identifying automated controls within business processes, assessing the design and effectiveness of automated controls that address business process risks and objectives, and validating the effectiveness of automated controls; and • Identifying the population of IUC relied upon for internal controls over financial reporting, performing a risk assessment over those IUCs to determine the highest risk items, and implementing procedures to obtain assurance related to the quality and reliability of IUC.		

Area of Material Weakness		
Financial Reporting		
DHS Component(s)	**Year Identified**	**Target Correction Date**
All	FY 2003	FY 2027
Multiple deficiency areas exist that are attributed to the Financial Accounting area of material weakness, which include the following: ***Information Used in Controls*** (Contributing Component(s): All) Deficiency Details Ineffective monitoring over information utilized in DHS internal control over financial reporting processes and control activities. Corrective Actions Taken in FY 2025 • Components continued efforts to identify and assess their IUC for key control activities through annual A-123 assessments and walkthroughs; • Components substantially performed testing over identified high-risk IUCs in alignment with the Department's IUC Guidance; and • OCFO provided training through DHS quarterly internal controls and risk management training. Additional Corrective Actions Planned DHS continues to implement its multi-year, risk-based approach as documented in the Department's IUC Guidance with actions to include: • Identifying the population of IUC relied upon for internal control over financial reporting; • Performing a risk assessment over those IUCs to determine the highest risk items; and • Implementing procedures to obtain assurance related to the quality and reliability of IUCs.		

(table continued on next page)

(table continued from prior page)

Area of Material Weakness		
Financial Reporting *(continued)*		
DHS Component(s)	**Year Identified**	**Target Correction Date**
All	FY 2003	FY 2027

Service Provider Monitoring (Contributing Component(s): All)

Deficiency Details

Process deficiencies related to monitoring of external service providers, to include 1) adequately assessing and responding to service provider introduced risks, and 2) obtaining and reviewing SOC reports related to financial services.

Corrective Actions Taken in FY 2025

- The Department updated its Enterprise-wide Service Provider Population to capture applicable organizations which impact the DHS internal control over financial reporting environment.
- Components providing financial servicing to other DHS entities continued the use of DHS templates and implementation of DHS guidance to enhance controls and reliance.
- OCFO provided training through the DHS quarterly internal controls and risk management training events.

Additional Corrective Actions Planned

DHS will continue to execute improvements and corrective actions as cost beneficial. Multi-year actions to be completed include:

- Identifying and updating the population of service providers;
- Conducting risk assessments;
- Executing appropriate service provider risk response, management, and oversight; and
- Ensuring that agreements with and utilization of new service providers enable adequate assurance related to service provider performed activities and controls.

Other (Contributing Component(s): All)

Deficiency Details

Deficiencies aggregated to substantiate inclusion into this area of material weakness, include:

- Application Controls, to include posting logic (All Components)
- Construction in Progress (CIP) reporting (USCG Specific)
- Journal entries (CBP and USCG Specific)
- Suspense account balances (USCG Specific)

Corrective Actions Taken in FY 2025

For efforts associated with application controls, refer to the IT Controls and Information Systems area of material weakness and corrective actions for more detail.

- USCG resolved a significant portion of its CIP transaction backlog and is working through processing of capitalized assets packages and manual processing of depreciation calculations and accrual postings.

(table continued on next page)

(table continued from prior page)

Area of Material Weakness		
Financial Reporting *(continued)*		
DHS Component(s)	**Year Identified**	**Target Correction Date**
All	FY 2003	FY 2027

- OCFO's Joint Program Management Office implemented a system solution to expense CIP transactions and allocate purchases across multiple projects and tasks.
- Components continued to enhance process implementation against policies and processes to include providing detailed support and ensuring appropriate reviews and approvals are captured.
- USCG continued efforts to reduce its suspense backlog and has substantially decreased its suspense balances from prior year amounts.

Additional Corrective Actions Planned

- For efforts associated with application controls, refer to the IT Controls and Information Systems area of material weakness and corrective actions for more detail.
- USCG will continue to implement manual workarounds for CIP processing while designing and implementing data clean up and system automation enhancements.
- Additional process improvements for journal entries will be developed, implemented, and assessed in accordance with remediation plans at CBP and USCG. While USCG volume for journal entries continues to remain high due to initial system challenges and manual workarounds related to CIP and suspense, it is expected that total journal entry activity will significantly reduce in volume and amount as system and legacy data issues are resolved.
- DHS is continuing its implementation efforts related to G-invoicing which will reduce the risk of system limitations associated with federal trading partners and help reduce USCG suspense intragovernmental balances going forward.

Area of Material Weakness		
Insurance Management		
DHS Component(s)	**Year Identified**	**Target Correction Date**
FEMA	FY 2022	FY 2026

Insurance Data and Process Assurances (Contributing Component(s): FEMA)

Deficiency Details

FEMA oversight and execution of the NFIP continues to note deficiencies in the following areas:

- Lack of control over the NFIP financial data and ineffective controls over the Statistical and Financial Variance Reporting process.
- Lack of adequate monitoring of the NFIP Service Provider and Write Your Own (WYO) Companies to ensure compliance with FEMA policies and procedures.
- Lack of evidence of the formal review and approval over the rating methodology to confirm that rates comply with the applicable statutory and regulatory provisions.

(table continued on next page)

(table continued from prior page)

Area of Material Weakness		
Insurance Management *(continued)*		
DHS Component(s)	**Year Identified**	**Target Correction Date**
FEMA	FY 2022	FY 2026

Corrective Actions Taken in FY 2025

- Designed and implemented new controls to mature NFIP's financial reporting process and control environment and developed Management improvement plans to ensure that actions are compliant with laws and regulations.
- Improved the NFIP financial posture through reinsurance; phase out of select program subsidies, updated rating system; updated electronic document management system; standard flood insurance policy amendment; and ongoing flood mapping program initiatives.

Additional Corrective Actions Planned

FEMA corrective actions are expected to continue into FY 2026, to include:

- Enhance reporting capabilities to support oversight over the validity, accuracy, and completeness of the WYO Companies financial data.
- Utilize the NFIP PIVOT system, and ensure quality source information, to help facilitate and consolidate NFIP core business processes and improve data quality.
- Utilization of the Statistical Variance Report to support the monitoring of variances identified from the financial exhibit and reconciliation reviews.

Area of Material Weakness		
Budgetary Accounting		
DHS Component(s)	**Year Identified**	**Target Correction Date**
CISA, FEMA, MGMT, USCG, USSS	FY 2022	FY 2026

Budgetary Resource Management and Monitoring (Contributing Component(s): CISA, FEMA, the DHS Management Directorate (MGMT), USCG, and USSS)

Deficiency Details

- CISA, MGMT, USCG, and USSS have noted deficiencies related to the review and analysis of open obligation to ensure accuracy, validity, and completeness around undelivered orders.
- FEMA executed insufficient funds control related to grants termination processing to ensure that obligations are maintained within the financial system at an adequate amount to cover liabilities until the completion of the closeout process.

Corrective Actions Taken in FY 2025

- CISA, MGMT, USCG, and USSS continued corrective actions as planned in prior year remediation plans. Of note:
    - CISA transitioned the obligation analysis functions to a new team.
    - USCG implemented its Open Obligation Management Tool in late FY 2024 and has continue operations and enhancements to the review and analysis throughout FY 2025.

(table continued on next page)

(table continued from prior page)

Area of Material Weakness		
Budgetary Accounting *(continued)*		
DHS Component(s)	**Year Identified**	**Target Correction Date**
CISA, FEMA, MGMT, USCG, USSS	FY 2022	FY 2026

- FEMA implemented a manual workaround in FY 2025 to obligated and post an accrued liability for financial statement reporting.

<u>Additional Corrective Actions Planned</u>

- CISA, MGMT, USCG, and USSS will continue to improve open undelivered order classifications and verifications over the accuracy of the information utilized for analysis. In addition, CISA plans to implement remediated quarterly obligation analysis procedures in early FY 2026.
- FEMA is working to process official grant closeout actions for grant awards terminated in FY 2025. As closeout actions are completed, open obligations can be reduced and closed out based on finalized liability calculations.

Area of Material Weakness		
Revenue and Receivables Reporting		
DHS Component(s)	**Year Identified**	**Target Correction Date**
CBP and USCIS	FY 2025	FY 2026

Entry Receivable Reporting (Contributing Component(s): CBP)

<u>Deficiency Details</u>

- A discrepancy in the Entry Receivable balance was noted due to a failure in report configurations and subsequent monitoring.

<u>Corrective Actions Taken in FY 2025</u>

- CBP has updated the applicable report to ensure that collections activity is appropriately aligned with open receivable entries. In addition, a monitoring process has been implemented to review and compare collections report(s) against report(s) used to post the entry receivable.

<u>Additional Corrective Actions Planned</u>

- Additional evaluation of the process and reports will be conducted during FY 2026 to ensure root cause remediation and implement any control enhancements.

Revenue Monitoring and Reporting (Contributing Component(s): USCIS)

<u>Deficiency Details</u>

- USCIS does not have an effective control process in place to reconcile complete and accurate immigration services form fee data to revenue recorded.

(table continued on next page)

(table continued from prior page)

Area of Material Weakness		
Revenue and Receivables Reporting *(continued)*		
DHS Component(s)	**Year Identified**	**Target Correction Date**
CBP and USCIS	FY 2025	FY 2026
Corrective Actions Planned • USCIS is conducting root cause analysis to work through form fee data complexities and reporting challenges to ensure that complete and accurate data sets are available for use in a reconciliation / monitoring control activity. • USCIS will review the current deferred revenue reporting process and make enhancements as needed to ensure that both deferred revenue and earned revenue balances can be reconciled and monitored on an ongoing basis.		

Federal Financial Management Improvement Act

FFMIA requires federal agencies to implement and maintain financial management systems that substantially comply with federal financial management systems requirements, applicable federal accounting standards, and the U.S. Standard General Ledger (USSGL) at the transaction level. A financial management system includes an agency's overall financial operation, reflecting the people, processes, and technology to capture, classify, summarize, and report data in a meaningful manner to support business decisions.

Financial Management Systems

Annually, the Department updates the CFO Designated Systems List to formally document the information systems and applications that are key to the flow of financial data or have an impact on financial processing and financial reporting. In FY 2025, DHS leadership designated 64 CFO Designated Systems spanning from property, human capital, and payment processing support systems to core accounting systems utilized by the Department.

DHS assesses financial management systems annually for compliance with the requirements of Appendix D to OMB Circular No. A-123 and other federal financial system requirements. In addition, available information from audit reports and other relevant and appropriate sources, such as *Federal Information Security Modernization Act of 2014* (FISMA) (P.L. 113-283) compliance activities, is reviewed to determine whether DHS financial management systems substantially comply with FFMIA. Improvements and ongoing efforts to strengthen financial management systems are considered as well as the impact of instances of non-compliance on overall financial management system performance.

Based on the results of the overall assessment, the IT Controls and Information Systems area of material weaknesses continues to affect the Department's ability to fully comply with financial management system requirements. Therefore, the Department is reporting a non-compliance with FFMIA. The Department is actively engaged to correct the area of material weakness through significant compensating controls while undergoing system improvement and consolidation efforts. The outcome of these multi-year efforts will efficiently enable the Department to comply with government-wide requirements and thus reduce the need for manual compensating controls.

<table>
<tr><th colspan="3">Area of Non-Compliance</th></tr>
<tr><td colspan="3">FFMIA</td></tr>
<tr><th>DHS Component(s)</th><th>Year Identified</th><th>Target Correction Date</th></tr>
<tr><td>All</td><td>FY 2003</td><td>FY 2028</td></tr>
<tr><td colspan="3">
Multiple deficiency areas exist that are attributed to the FFMIA area of non-compliance, which include the following:

Financial System Requirements (Contributing Component(s): All)

<u>Non-Compliance Details</u>
• DHS does not substantially comply with FFMIA primarily due to lack of compliance with financial system requirements as disclosed in the IT Controls and System Functionality area of material weakness.

<u>Corrective Actions Taken in FY 2025 and Additional Corrective Actions Planned</u>
• Refer to the corrective actions taken for the IT Controls and System Functionality area of material weakness.

Federal Accounting Standards (Contributing Component(s): MGMT as a Core Financial System Owner)

<u>Non-Compliance Details</u>
• Although there are no known cases of misappropriation or financial reporting that has not manually accounted for and corrected variances, occurrences of non-conformance with accounting standards to include instances of invalid posting logic have been identified.

<u>Corrective Actions Taken in FY 2025 and Additional Corrective Actions Planned</u>
• Annually, the system's accounting treatment manual undergoes an update process to ensure review and approval by applicable parties. Accounting extracts from the system are validated to proactively identify system accounting issues.
• As accounting issues are identified, system management reviews areas of concern to identify if accounting treatment updates are needed. If confirmed, accounting incidents are raised for resolution through formal tickets to enable tracking and reporting.

U.S. Standard General Ledger Requirements (Contributing Component(s): FEMA and ICE)

<u>Non-Compliance Details</u>
• FEMA and ICE noted that certain key systems are unable to produce transaction level activity that reconciles at the USSGL-level.

<u>Corrective Actions Taken in FY 2025 and Additional Corrective Actions Planned</u>
• FEMA has continued to enhance its transactional Disaster Emergency Fund Code reporting with aggregate cumulative gross outlays reported per DHS instructions for FY 2024 and FY 2025. Efforts are ongoing to update prior year files.
• As part of the financial system consolidation initiative, ICE has begun documenting enhanced system requirements to assist in resolving interface and reconciliation issues to the property management systems.
</td></tr>
</table>

Financial Management Systems Improvement Strategy

The DHS CFO, as mandated by the CFO of 1990, oversees the development and maintenance of agency accounting and financial management systems to ensure compliance with applicable standards and internal controls. The Financial Systems Modernization program is central to this effort, focusing on standardization, modernization, and consolidation across DHS Components.

Key Objectives of Financial Systems Modernization:

- **Business Process Standardization:** Define and implement common financial management processes across Components to enhance efficiency and consistency.
- **Data Standardization:** Adopt standardized financial data structures, such as the DHS Accounting Classification and Common Appropriation Structures, to improve reporting and reduce manual processes.
- **Modernization Projects:** Migrate Components to modern common platforms with integrated asset and procurement management systems, leveraging cloud-based solutions and existing infrastructure to strengthen internal controls and reduce manual efforts.
- **Operational Consolidation:** Consolidate financial systems across DHS operations and transaction processing centers, where cost-effective.

Initial projects transitioned CWMD, USCG, and TSA (the Trio) to the DHS Financial Systems Modernization Solution. After overcoming several initial challenges, this system achieved Final Operational Capability in 2025. Follow-on efforts to develop a common financial system for CBP, USCIS, CISA, FEMA, and ICE started in 2023 with the intent to begin transitioning in 2026.

Modernized financial systems will enhance efficiency, strengthen cybersecurity, address material weaknesses in financial reporting and IT controls, and support DHS's goal of achieving a clean audit opinion on Internal Control over Financial Reporting.

This modernization and consolidation effort reflects DHS's commitment to improving financial management and operational effectiveness across the Department.

Efforts to Maintain Compliance with Other Applicable Laws

Antideficiency Act

The *Antideficiency Act of 1982* (ADA) (P.L. 97-258) prohibits federal agencies from obligating or expending federal funds in advance or in excess of an appropriation, and from accepting voluntary services. Specifically, the ADA prohibits federal employees from:

- Making or authorizing an expenditure from, or creating or authorizing an obligation under, any appropriation or fund in excess of the amount available in the appropriation or fund unless authorized by law;
- Involving the government in any obligation to pay money before funds have been appropriated for that purpose, unless otherwise allowed by law;
- Accepting voluntary services for the United States, or employing personal services not authorized by law, except in cases of emergency involving the safety of human life or the protection of property; or
- Making obligations or expenditures in excess of an apportionment or reapportionment, or in excess of the amount permitted by agency regulations.

The Department has well established policy and procedural guidance in place as it relates to funds control administration and DHS is not aware of any violations of the ADA in FY 2025.

Digital Accountability and Transparency Act

The *Digital Accountability and Transparency Act of 2014* (DATA Act) (P.L. 113-101) makes information on Federal spending more easily accessible and transparent to the public. The DATA Act requires agencies to report spending data quarterly to USAspending.gov in accordance with government-wide financial data standards established by the Department of the Treasury and OMB.

Pursuant to OMB Circular No. A-123, Appendix A, *Management of Reporting and Data Integrity Risk*, the Department issued its latest DATA Act Data Quality Plan in July 2025. The plan describes the organizational structure, operating environment, internal controls processes, and systems used to generate, validate, and evaluate the data published to USAspending.gov. The plan includes DHS's processes for compiling, reviewing, and monitoring the quality of data provided to USAspending.gov. In addition, the plan describes the processes to assess the level of data quality, methods for increasing the data quality, and the data risk management strategy. The outcomes of this plan align with the Administration's goal for greater transparency, ultimately benefiting citizens and holding the Government accountable for its stewardship over its assets.

DHS Components assess the design and operating effectiveness of their respective DATA Act reporting processes and controls over consolidation as well as variance resolution of data submitted to DHS Headquarters. DHS also utilizes a risk assessment process to identify high risk data elements and tests the accuracy, completeness, and timeliness of the recorded transactions against source documents. This two-pronged approach ensures that the Department can provide reasonable assurance that reports over DATA Act are reliable both at reporting and transaction-levels, further supporting the fidelity of reported transactions to Treasury.

In FY 2025, FEMA and USCG continued to report material inadequacies associated with DATA Act reporting. The FEMA inadequacy has been substantially compensated due to DHS validation pre-check processes as well as regular oversight and metrics reporting. Alternately, USCG continues to face challenges generating a complete and accurate financial data report following its core accounting system transition. Despite the FEMA and USCG noted exceptions, DHS has successfully matched over 98.6% of financial data (File C) and award data (File D) dollars that correspond to approximately $75 billion as of September 30, 2025.

Federal Civil Penalties Inflation Adjustment Act Improvements Act

The *Federal Civil Penalties Inflation Adjustment Act of 1990* (P.L. 101-410), amended by the *Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015* (P.L. 114-74), requires agencies to adjust penalty amounts periodically for inflation. Specific details about the civil penalties, the authority for the penalty, adjustment dates, and current penalty amount can be found in the Other Information section of this report.

Federal Information Security Modernization Act

FISMA requires Federal agencies to identify and provide security protection commensurate with the risk and magnitude of potential harm resulting from the loss, misuse of, unauthorized access to, disclosure of, disruption to, or modification of information collected to be maintained by or on behalf of an agency. FISMA also requires that each agency report annually on the adequacy and effectiveness of information security policies, procedures, and practices and on

FISMA compliance and have an independent evaluation performed over their information security programs and practices.

The agency Chief Information Officer, Inspector General, and Senior Agency Official for Privacy metrics together provide insight into an agency's information security and privacy performance. DHS conducted a joint annual assessment as required by OMB Memorandum 25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements.*

- The Department submitted to OMB required quarterly Chief Information Officer metrics in January, April, and August 2025.
- The DHS Chief Information Officer and Senior Agency Official for Privacy submitted annual metrics and the agency report for FY 2025 on October 31, 2025.
- On June 30, 2025, the DHS OIG published its final report, *Evaluation of DHS' Information Security Program for Fiscal Year 2024*. The DHS OIG, using an independent contractor for assessment fieldwork, rated the Department's information security program as "effective" for FY 2024.

Federal Information Technology Acquisition Reform Act

The *Federal Information Technology Acquisition Reform Act* (P.L. 113-291), passed in December 2014, strengthened the role of agency Chief Information Officers and provided greater accountability for the delivery of IT capabilities across the Federal Government. Federal agencies are required by OMB to participate in several reporting activities for the planning, programming, management, and execution of IT.

DHS, as required by OMB Memorandum M-15-14, *Management and Oversight of Federal Information Technology*, completed annual reporting in FY 2025, to include Capital Planning and Investment Control process reporting requirements.

Government Charge Card Abuse Prevention Act

The *Government Charge Card Abuse Prevention Act of 2012* (P.L. 112-194) requires agencies to establish and maintain safeguards and internal controls for purchase cards, travel cards, integrated cards, and centrally billed accounts. As part of the Department's oversight of the government charge cards, DHS has developed detailed guidance and implemented internal controls to mitigate the risk of fraud, waste, and abuse. These controls are documented in the program oversight documentation as well as charge card policies and procedures.

This Act requires the Inspector General to periodically conduct a risk assessment on the agency's charge card programs. The DHS OIG last published an audit report in July 2023, titled *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*. The report identified that "Although the Department of Homeland Security and its components implemented internal controls to ensure Bankcard Program spending limits are established based on procurement needs, components did not always adhere to internal control policies and procedures." DHS has successfully closed two of the recommendations and is pending a final closure determination by the DHS Inspector General for the last remaining open and resolved recommendation.

Freedom of Information Act

The *Freedom of Information Act of 1966* (FOIA) (P.L. 89-487), as amended, provides the public the right to request access to records from any federal agency. Federal agencies are required to disclose any information requested under the

FOIA unless it falls under one of nine exemptions which protect interests such as personal privacy, national security, and law enforcement.

Due to the Department's significant increase in FOIA requests and litigation cases received over the past three fiscal years, DHS is processing responses in a timely manner but has noted non-compliances with the mandate for each FOIA request to be completed within twenty business days of receipt by the agency. Notably, in FY 2024, the DHS backlog was only 15% of the total requests received, despite a more than 30% increase.

The DHS Privacy Office continues to invest, develop, and implement upgrades in FOIA technology. Current efforts are ongoing to launch additional automation tools to improve efficiency and reduce administrative burden related to FOIA processing.

Payment Integrity Information Act

The *Payment Integrity Information Act of 2019* (PIIA) (P.L. 116-117) was signed into law in March 2020 and repealed and replaced the *Improper Payments Information Act of 2002*, the *Improper Payments Information Act of 2002*, the *Improper Payments Elimination and Recovery Act of 2010*, the *Improper Payments Elimination and Recovery Improvement Act of 2012*, and the *Fraud Reduction and Data Analytics Act of 2015*. OMB Circular No. A-123, Appendix C, has been revised to mirror the updates set forth in the PIIA.

In addition, on June 18, 2010, the Office of the President issued an Executive Memorandum directing agencies to check a series of data sources prior to issuing a payment or award. Additionally, the memo called for the creation of a single point of entry to access these databases. The U.S. Department of the Treasury was directed by OMB to take the lead in developing the single point of entry, or Do Not Pay. The PIIA is the current legislation that governs Do Not Pay.

In FY 2024, DHS has reported payment integrity error estimation results for the FEMA Public Assistance – Validate as You Go (VAYGo) program, based on consolidated results from FY 2021 and FY 2022 disbursement activity, that exceeded the OMB Circular No. A-123, Appendix C, *Requirements for Payment Integrity Improvement*, thresholds to be designated as a High-Priority program. As such, DHS completed High-Priority program reporting for this program throughout FY 2025. For additional information, please refer to the Department's payment integrity information reported in the in the Other Information section as well as PaymentAccuracy.gov.

As reported in the Department's compliance plan submission in response to Executive Order 14249, *Protecting America's Bank Account Against Fraud, Waste, and Abuse*, the Department is not fully compliant with Do Not Pay usage requirements. Modifications and enhancements are underway as DHS continues its partnership with the Department of Treasury to onboard and modify programs for Do Not Pay review and analysis.