

# U.S. Department of Homeland Security

## AGENCY FINANCIAL REPORT



**FY 2022**

# Connect with DHS

## Social Media

DHS has multiple social media platforms that allow citizens to keep informed about homeland security issues and activities the Department is taking to make America safe.



<https://www.dhs.gov/facebook>

<https://www.dhs.gov/twitter>

<https://www.dhs.gov/instagram>

<https://www.dhs.gov/linkedin>

<https://www.dhs.gov/flickr>

<https://www.dhs.gov/youtube>

<https://public.govdelivery.com/accounts/USDHS/subscriber/new>

For more information,  
please scan the QR  
code and visit  
DHS.gov



## DHS Components

DHS's Operational Components (shaded in blue) lead the Department's operational activities to protect our Nation. The DHS Support Components (shaded in green) provide mission support and business support activities to ensure the operational organizations have what they need to accomplish the DHS mission. Click on the Component links to find out more about DHS and the Components that execute and support the mission. For the most up to date information on the Department's structure and leadership, visit our website at <http://www.dhs.gov/organization>.

### Operational Components

[CBP – U.S. Customs and Border Protection](#)

[CISA – Cybersecurity and Infrastructure Security Agency](#)

[FEMA – Federal Emergency Management Agency](#)

[ICE – U.S. Immigration and Customs Enforcement](#)

[TSA – Transportation Security Administration](#)

[USCG – U.S. Coast Guard](#)

[USCIS – U.S. Citizenship and Immigration Services](#)

[USSS – U.S. Secret Service](#)

### Support Components

[CWMD – Countering Weapons of Mass Destruction Office](#)

[FLETC – Federal Law Enforcement Training Centers](#)

[I&A – Office of Intelligence and Analysis](#)

[MGMT - Management Directorate](#)

[OIG – Office of Inspector General](#)

[OPS – Office of Operations Coordination](#)

[S&T – Science and Technology Directorate](#)

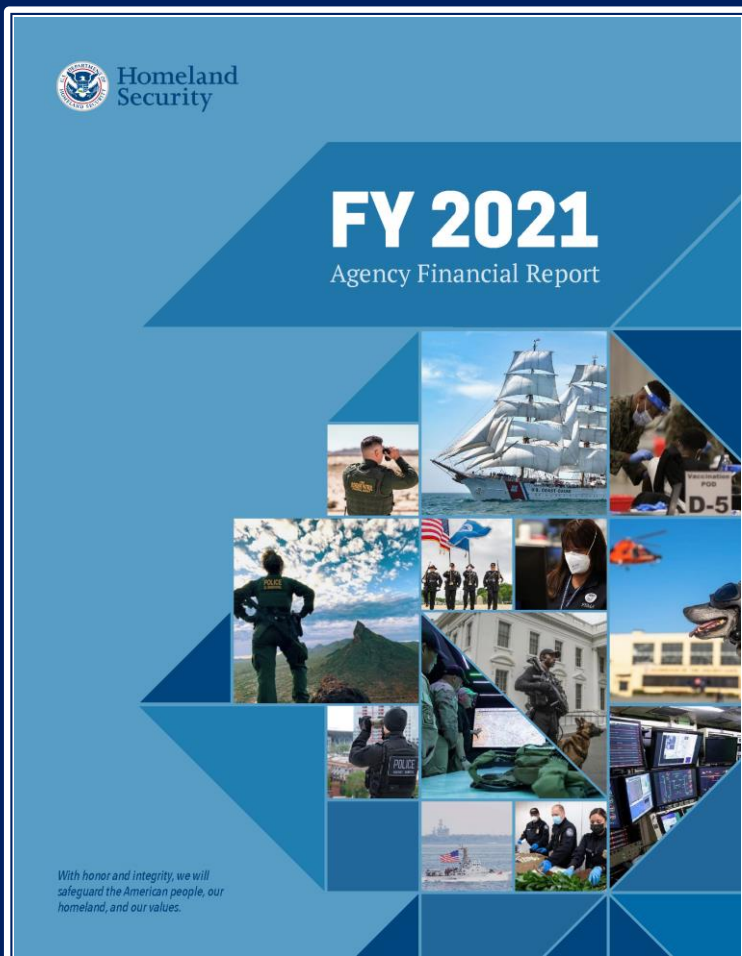


# Certificate of Excellence in Accountability Reporting

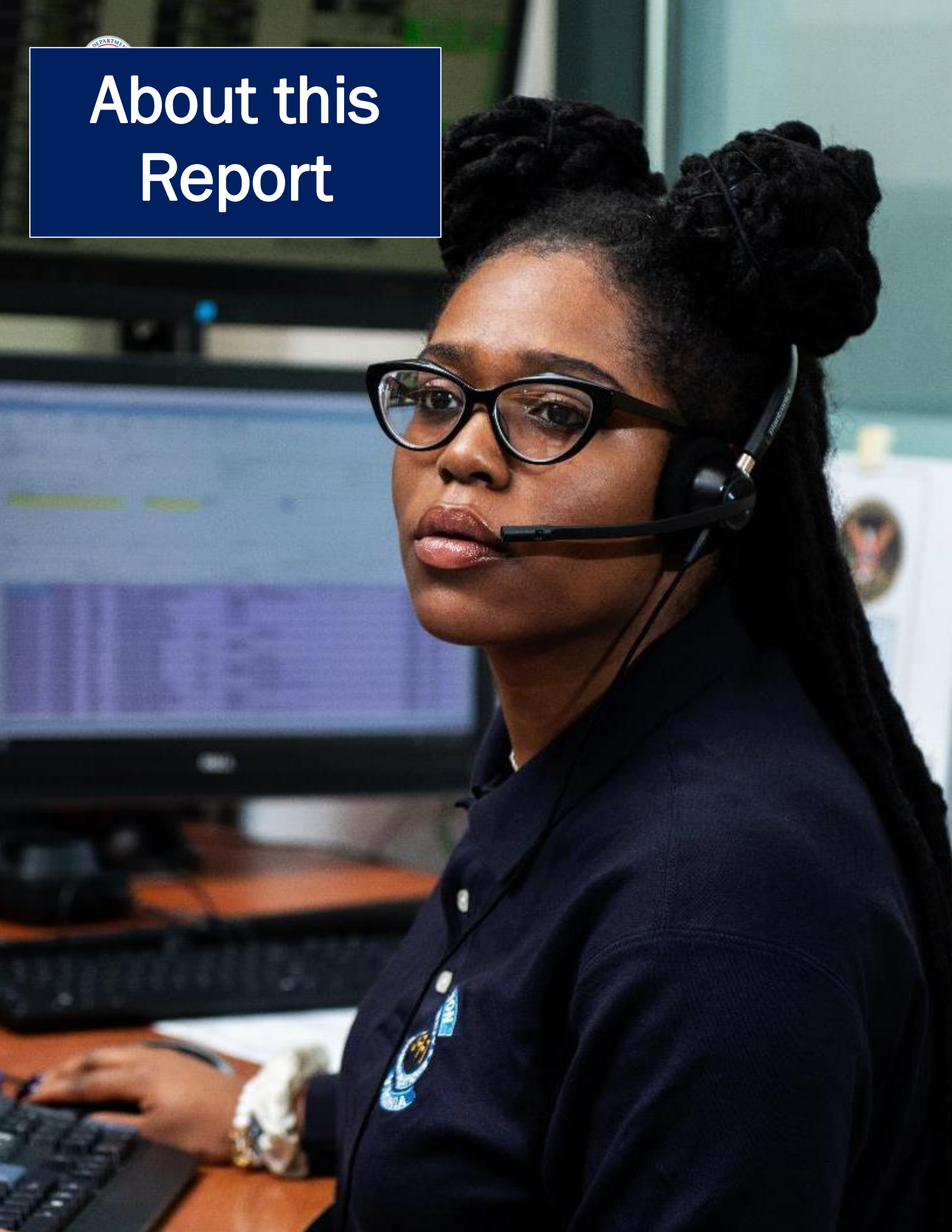
In June 2022, DHS received its ninth consecutive Certificate of Excellence in Accountability Reporting (CEAR) from the Association of Government Accountants (AGA) for its Fiscal Year (FY) 2021 Agency Financial Report. The [CEAR Program](#) was established by the AGA, in conjunction with the Chief Financial Officers Council and the Office of Management and Budget, to further performance and accountability reporting.

In addition to the coveted CEAR award, DHS was presented with a Best-in-Class Award for Informative Payment Integrity Disclosures. This is the first time the AGA has recognized an agency in this category.

[AGA](#) is an association for professionals that work in the areas of financial management, accounting, auditing, IT, budgeting, policy, grants management, performance management, and other business operations areas to help government work more efficiently and effectively.



# About this Report



The U.S. Department of Homeland Security's Agency Financial Report for FY 2022 presents the Department's detailed financial information relative to our mission and the stewardship of those resources entrusted to us. It also highlights the Department's priorities, strengths, and challenges in implementing programs to enhance the safety and security of our Nation.

For FY 2022, the Department's Performance and Accountability Reports consist of the following three reports:

- DHS Agency Financial Report | Publication date: November 15, 2022
- DHS Annual Performance Report | Publication date: April 11, 2023. This report is submitted with the Department's Congressional Budget Justification.
- DHS Report to our Citizens (Summary of Performance and Financial Information) | Publication date: April 11, 2023

When published, all three reports will be located on our public website at: <http://www.dhs.gov/performance-accountability>.

## Contact Information

For more information, contact:

Department of Homeland Security  
Office of the Chief Financial Officer  
Office of Program Analysis and Evaluation  
245 Murray Lane, SW  
Mailstop 200  
Washington, DC 20528



# Table of Contents

<b>Message from the Secretary</b>	<b>iv</b>
<b>Management’s Discussion and Analysis</b>	<b>1</b>
Organization	3
Performance Overview	5
Financial Overview	37
Analysis of Systems, Controls, and Legal Compliance	44
Secretary’s Assurance Statement	44
<b>Financial Information</b>	<b>58</b>
Message from the Senior Official Performing the Duties of the Chief Financial Officer	60
Introduction	62
Financial Statements	63
Notes to the Financial Statements	71
Required Supplementary Information	152
Independent Auditor’s Report	158
<b>Other Information</b>	<b>186</b>
Tax Burden/Tax Gap	188
Climate Related Financial Risk	188
Summary of Financial Statement Audit and Management Assurances	189
Payment Integrity	191
Grants Programs	204
Civil Monetary Penalty Adjustment for Inflation	205
Other Key Regulatory Requirements	219
Office of Inspector General’s Report on Major Management and Performance Challenges Facing the Department of Homeland Security	220
<b>Appendix A: Acronyms</b>	<b>249</b>
<b>Appendix B: Acknowledgements</b>	<b>253</b>

This report is available at: <http://www.dhs.gov/performance-accountability>.



## Message from the Secretary

November 14, 2022



I am pleased to present the Department of Homeland Security's (DHS) Agency Financial Report for Fiscal Year 2022. This report provides a detailed assessment of the Department's financial status and demonstrates how the resources entrusted to us were used to support our homeland security mission.

DHS was created through the combination of more than 20 different federal departments and agencies into a unified homeland security enterprise to achieve a more secure America that is better prepared to confront the range of threats we face. DHS is responsible for counterterrorism, cybersecurity, aviation security, border security, port security, maritime security, administration and enforcement of our immigration laws, protection of our national leaders, protection of critical infrastructure, and detection of and protection against chemical, biological and nuclear threats to the homeland, and response and resilience to disasters.

Today, more than ever, the Department is focused on its mission to ensure we safeguard the American people, our homeland, and our values. As we face a range of diverse threats and challenges, we continue to assure the American people that the resources entrusted to the Department are used effectively and efficiently to support our mission and to respond to our nation's need. The performance and financial data in this report provide a more detailed summary of how we continue to invest on our nation's security.

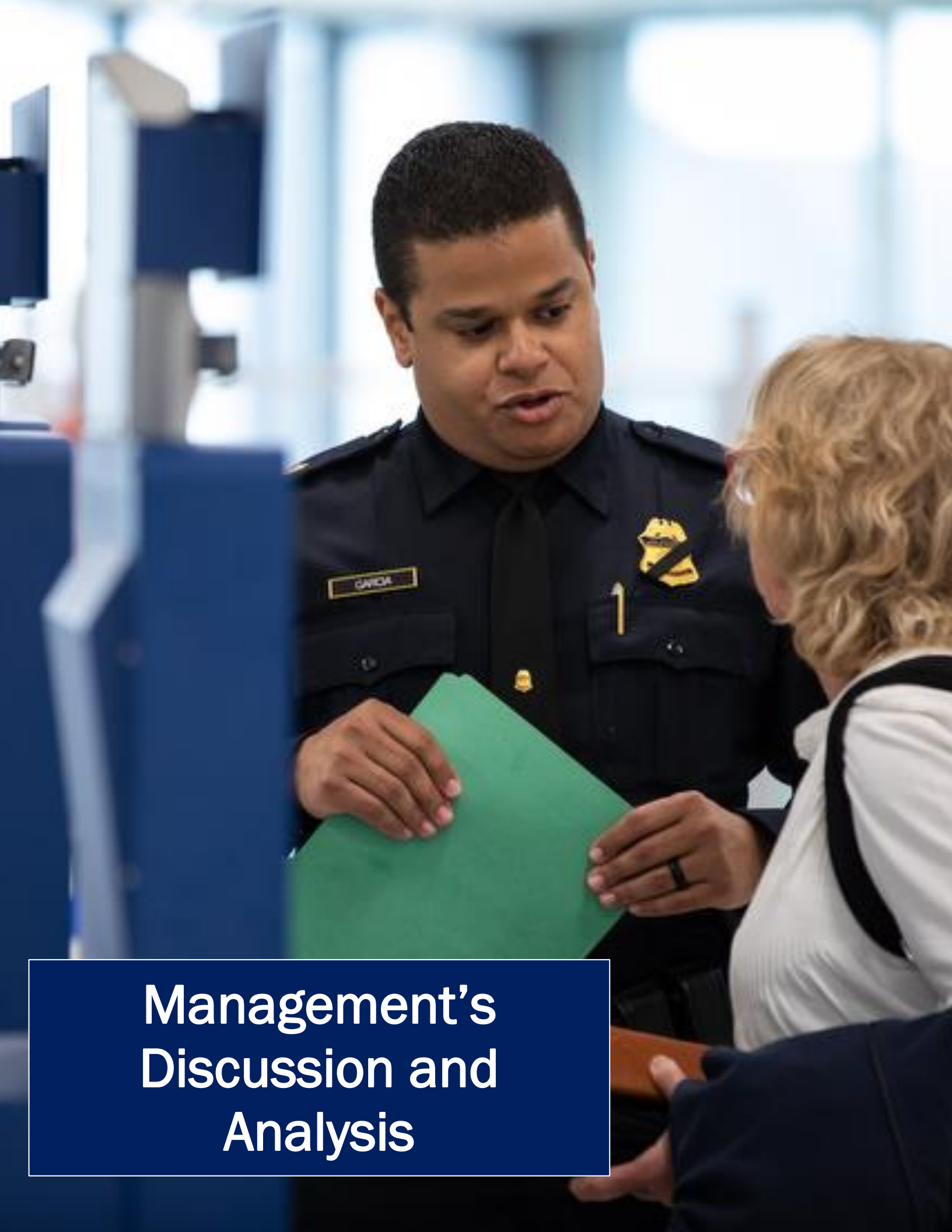
As Secretary, I have seen firsthand how the personnel of DHS steadfastly serve the nation. Our commitment to service and the American public is unwavering. The information in the Department's performance and accountability reports is complete and reliable, except as otherwise reported in our Annual Performance Report. DHS's performance and accountability reports for this and previous years are available on our public website: <https://www.dhs.gov/performance-accountability>.

We have much more to do, and we will succeed because of the immeasurable dedication and talent of the DHS workforce.

I am privileged to support our mission and those who enable it, and I am proud of what we have achieved. I look forward to the Department's accomplishments in years to come.

Sincerely,

Alejandro N. Mayorkas  
Secretary of Homeland Security



## Management's Discussion and Analysis



The Management's Discussion and Analysis is required supplementary information to the financial statements and provides a high level overview of DHS.

The Our Organization section displays the Department's organization with links to the Department's Components.

The Performance Overview section provides a summary of progress for each of our Components, selected accomplishments, key performance measures, and future initiatives to strengthen the Department's efforts in achieving a safer and more secure Nation.

The Financial Overview section provides a summary of DHS's financial data explaining the major sources and uses of funds and provides a quick look at our Balance Sheets, Statements of Net Cost, Statements of Changes in Net Position, Statements of Budgetary Resources, and Statements of Custodial Activity.

The Analysis of Systems, Controls, and Legal Compliance section provides the Secretary's Assurance Statement related to the Federal Managers' Financial Integrity Act, the Federal Financial Management Improvement Act, and the Department of Homeland Security Financial Accountability Act. This section also describes the Department's efforts to address our financial management systems to ensure systems comply with applicable accounting principles, standards, requirements, and with internal control standards.

Management's Discussion and Analysis .....	1
Organization .....	3
Performance Overview .....	5
Financial Overview .....	37
Analysis of Systems, Controls, and Legal Compliance .....	44
Secretary's Assurance Statement .....	44



## Organization

The Department of Homeland Security has a vital mission: to secure the nation from the many threats we face. This requires the dedication of more than 240,000 employees in jobs that range from aviation and border security, administering our lawful immigration system, to emergency preparedness and response, strengthening cybersecurity, and critical infrastructure protection. Our duties are wide-ranging, and our goal is clear - keeping America safe. For the most up to date information on the Department’s structure, visit our web site at <https://www.dhs.gov/organization>. Below is a listing and description of the Components of DHS.

### Operational Components



#### [Customs and Border Protection \(CBP\)](#)

CBP is one of the world's largest law enforcement organizations and is charged with keeping terrorists and their weapons out of the U.S. while facilitating lawful international travel and trade.



#### [Cybersecurity and Infrastructure Security Agency \(CISA\)](#)

CISA leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.



#### [Federal Emergency Management Agency \(FEMA\)](#)

FEMA helps people before, during, and after disasters. FEMA does this by supporting our citizens and first responders to ensure that, as a Nation, we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.



#### [Transportation Security Administration \(TSA\)](#)

TSA protects the Nation’s transportation systems to ensure freedom of movement for people and commerce.



#### [U.S. Citizenship and Immigration Services \(USCIS\)](#)

USCIS administers the Nation’s lawful immigration system, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting Americans, securing the homeland, and honoring our values.



#### [United States Immigration and Customs Enforcement \(ICE\)](#)

ICE promotes homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.



#### [United States Coast Guard \(USCG\)](#)

USCG is one of the six armed forces of the United States and the only military organization within DHS. The USCG protects the maritime economy and the environment, defends our maritime borders, and saves those in peril.



#### [United States Secret Service \(USSS\)](#)

USSS has an integrated mission of protecting national leaders, visiting heads of state and government, designated sites, and National Special Security Events, as well as safeguarding the Nation’s financial infrastructure and payment systems to preserve the integrity of the economy.



## Support Components



### [Countering Weapons of Mass Destruction Office \(CWMD\)](#)

CWMD leads DHS efforts and coordinates with domestic and international partners to safeguard the United States against Chemical, Biological, Radiological, Nuclear, and health security threats.



### [Federal Law Enforcement Training Centers \(FLETC\)](#)

FLETC provides career-long training to law enforcement professionals to help them fulfill their responsibilities safely and proficiently.



### [Management Directorate \(MGMT\)](#)

MGMT is responsible for budget, appropriations, expenditure of funds, accounting and finance; procurement; human resources and personnel; information technology systems; facilities, property, equipment, and other material resources; providing biometric identification services; and identification and tracking of performance measurements relating to the responsibilities of the Department.



### [Office of Intelligence and Analysis \(I&A\)](#)

I&A equips the Homeland Security Enterprise with the timely intelligence and information it needs to keep the homeland safe, secure, and resilient.



### [Office of Inspector General \(OIG\)](#)

OIG was established by the Homeland Security Act of 2002 (P.L. 107-296) by an amendment to the Inspector General Act of 1978 (92 Stat. 1101). OIG has a dual reporting responsibility to the Secretary of DHS and to Congress. OIG serves as an independent and objective audit, inspection, and investigative body to promote economy, effectiveness, and efficiency in DHS programs and operations, and to prevent and detect fraud, waste, and abuse.



### [Office of Operations Coordination \(OPS\)](#)

OPS provides information daily to the Secretary of Homeland Security, senior leaders, and the Homeland Security Enterprise to enable decision-making; oversees the National Operations Center; manages the DHS Special Events Program; and leads the Department's Continuity of Operations and Government Programs to enable continuation of primary mission essential functions in the event of a degraded or crisis operating environment.



### [Science and Technology Directorate \(S&T\)](#)

S&T is the primary research and development arm of the Department. It provides federal, state and local officials with the technology and capabilities to protect the homeland.



## Performance Overview

The Performance Overview provides an overview of our performance management framework, a summary of key performance measures, and selected accomplishments, as well as forward-looking initiatives to strengthen the Department's efforts in achieving a safer and more secure Nation. A complete list of all performance measures and results will be published in the DHS FY 2022-2024 Annual Performance Report with the FY 2023 Congressional Budget Justification and will be available at: <https://www.dhs.gov/performance-accountability>. All previous reports can be found at this link as well.

## Organizational Performance Management Framework

With the enactment of the Government Performance and Results Act (GPRA) of 1993, federal agencies were required for the first time to develop Strategic Plans, annual performance plans, and Annual Performance and Accountability Reports [Agency Financial Report and Annual Performance Report (APR)] to communicate progress made against strategic plan goals and objectives to the public and other stakeholders. Efforts continued to mature the organizational performance management framework, resulting in the passage of the GPRA Modernization Act of 2010 (GPRAMA). GPRAMA sets the statutory foundation for the Federal Performance Framework as we know it today, which is a more integrated and coordinated government-wide performance management approach.

Figure 1: DHS Performance Management Framework





DHS uses a robust organizational performance management framework to implement GPRA and GPRAMA and assess our mission program progress.<sup>1</sup> We leverage data and evidence to help define success for the organization, ensure measure results are reliable, engage leaders, and drive the delivery of value to external stakeholders. The graphic above (Figure 1) shows how this performance management framework incorporates the initiatives that come from both GPRA and GPRAMA.

**Performance Community**

The DHS Performance Community is led by the Chief Operating Officer (a collateral duty of the Deputy Secretary of DHS), the Performance Improvement Officer (PIO) who is also the Director of Program Analysis and Evaluation (PA&E), and the Deputy PIO (DPIO) who is also the Assistant Director for Performance Management in PA&E. These leaders are supported by Performance Analysts in PA&E under the DHS Chief Financial Officer (CFO) in the Management Directorate of DHS. The PIO, DPIO, and PA&E Performance Analysts are the liaisons to our DHS Component performance management leaders and collaborators, along with various external stakeholders interested in performance management (shown in the graphic below).

**Figure 2: DHS Organizational Performance Community**



DHS Component PIOs, Agency Priority Goal (APG) Leads, and Strategic Review Assessment Leads are senior leaders driving performance management efforts in their respective Components. Component Performance Leads are the critical liaison between DHS PA&E and Component leadership and program managers for all performance management initiatives. They assist with

<sup>1</sup> A mission program is a group of activities acting together to accomplish a specific high-level outcome external to DHS and includes operational processes, skills, technology, human capital, and other resources. In addition, all mission programs uphold privacy, civil rights, and civil liberties throughout their performance. The Support Components and their related offices deliver needed capability and capacity to strengthen the enterprise. In addition, they provide specific assistance and guidance to other DHS Components and external organizations.



communicating guidance and initiatives, provide advice to programs on measure development, collect and review measure results, and coordinate with their leadership on performance management initiatives. Strategic Review (SR) Assessment Leads are responsible for SR Team efforts annually and delivering key findings from the review process. Program Managers across DHS Components are key contributors to the SR assessment, generating ideas for performance measures, producing measure data, and using information to manage and improve operations. The DHS Performance Community meets quarterly to discuss the implementation of key initiatives and share best practices.

### **Improving our Measures**

PA&E initiates an annual measure improvement process to enhance our set of publicly reported measures. Although the Department has many enduring measures in the Annual Performance Plan (APP) that convey activities of our core mission areas, measures must be dynamic in order to gauge changing priorities and initiatives and more effectively convey the results of our mission programs. Measure improvement ideas are derived from multiple sources:

- DHS and Component Strategic Plans
- Administration and leadership priorities and initiatives
- Government Accountability Office (GAO) and OIG recommendations
- Office of Management and Budget (OMB) suggestions to achieve greater visibility into program performance and connections to resources
- President's Management Agenda and Customer Service initiatives
- Measure gaps identified from Strategic Review findings
- Elevation of existing internal data to publicly reported information
- Budgetary changes
- Review of existing measures to ensure consistency with current operations and guidance

**Figure 3: DHS Annual Measure Improvement Process**





PA&E works with Components each spring to help them develop and document measures and their targets on the Performance Measure Definition Form (PMDF), which is the change control document and artifact of the measure improvement process. The PMDF is used to propose new measures, make changes to existing measures, and to retire measures from our measure sets.

Once measure changes are approved by DHS and OMB, measures are entered into the Performance Management (PM) system and Components begin collecting and reporting data from the beginning until the end of the fiscal year.

The results of this process constitute our publicly reported measures associated with our performance budget deliverables each year that are incorporated in the [Annual Performance Report](#), the Overview chapter of each Component's Congressional Budget Justification ([see the DHS Budget](#)), and the Future Years Homeland Security Program (FYHSP) Report.

### **Internal Controls for Measure Verification and Validation**

The Department recognizes the importance of complete, accurate, timely, and reliable performance data that is shared with leadership and external stakeholders. Performance data are considered reliable if transactions and other data that support reported performance measures are properly recorded, processed, and summarized to permit the preparation of performance information in accordance with criteria stated by management. OMB Circular A-136, *Financial Reporting Requirements*, OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*, and the *Reports Consolidation Act* of 2000 (Public Law (P.L.) No. 106-531) further delineate this responsibility by requiring agencies to ensure completeness and reliability of the performance data they report by putting management assurance procedures in place.<sup>2</sup>

DHS implemented a multi-pronged approach to effectively mitigate risks and reinforce processes that enhance the Department's ability to report complete and reliable data for performance measure reporting. This approach consists of:

- An annual measure improvement and change control process described in the previous section using the PMDF
- The PM system information technology repository for performance measure information
- Measure verification and validation assessments by an independent review team
- The Performance Measure Checklist for Completeness and Reliability

### **Quarterly Performance Reporting**

Component program managers work with Component performance staff to collect, review, and enter results, forecasts of the likelihood of meeting measure targets, and meaningful explanations in the PM System on a quarterly basis, or as specified in the measure's data collection methodology. Information is shared quarterly with the DHS PIO and DPIO, posted on a DHS intranet site, and available to all DHS senior leaders and program managers to support their

---

<sup>2</sup> Note: Circular A-11, PART 6, THE FEDERAL PERFORMANCE FRAMEWORK FOR IMPROVING PROGRAM AND SERVICE DELIVERY, Section 240.26 Definitions. Data limitations. In order to assess the progress towards achievement of performance goals, the performance data must be appropriately valid and reliable for intended use. Significant or known data limitations should be identified to include a description of the limitations, the impact they have on goal achievement, and the actions that will be taken to correct the limitations. Performance data need not be perfect to be valid and reliable to inform management decision-making. Agencies can calibrate the accuracy of the data to the intended use of the data and the cost of improving data quality. At the same time, significant data limitations can lead to bad decisions resulting in lower performance or inaccurate performance assessments. Examples of data limitations include imprecise measurement and recordings, incomplete data, inconsistencies in data collection procedures and data that are too old and/or too infrequently collected to allow quick adjustments of agency action in a timely and cost-effective way.



on-going program management activities. Additionally, many Components have their own internal processes and reports by which they regularly review performance data for management and decision making.

### **Performance Public Reporting**

The Department follows the OMB Circular A-11 and A-136 requirements to produce the following performance and accountability reports to communicate key financial and performance information to stakeholders:

- DHS Agency Financial Report (this report);
- DHS Annual Performance Report; and
- DHS Report to our Citizens (Summary of Performance and Financial Information).

When published, all three reports are located on our DHS.gov public website at [Performance & Financial Reports](#).

DHS also integrates performance information in our performance budget deliverables to Congress. The Overview Chapter of the Congressional Justification (referred to as the Strategic Context) contains program descriptions and their associated measures by Component. We include our measures in the Executive Summary section of the FYHSP Report to Congress to again emphasize the connection between funding and performance. The last avenue for performance public reporting is through the Agency Priority Goals discussed below.

### **Agency Priority Goals**

Agency Priority Goals (APGs) provide a tool for senior leadership to drive the delivery of results on key initiatives over a two-year period. PA&E collaborates with Components and OMB to develop APG plans and provide quarterly progress reports to the public at the OMB web site [performance.gov](#). For the FY22-FY23 cycle, the Department has implemented two APGs on improving cybersecurity and reducing the burden of paperwork.

### **Performance Reviews**

Performance Reviews are a means for senior leadership to be engaged in the management of efforts to deliver results relevant to stakeholders. Meetings may be held with APG Goal Leads, senior leaders, subject matter experts, and performance leadership and staff to discuss current results, progress, and challenges on APGs and other performance initiatives to drive improvement.

### **Strategic Review**

Per OMB Circular A-11, DHS conducts an annual SR assessment of progress each spring that examines program execution accomplishments and challenges, risks, and next steps to improve. The Strategic Review integrates numerous government-wide organizational initiatives into the assessment methodology including the Program Management Improvement Accountability Act (PMIAA), Enterprise Risk Management (ERM), and the Foundations of Evidence-based Policy Making Act (Evidence Act). The review serves multiple purposes for the Components, DHS, and OMB:

- Assesses the effectiveness of programs and capabilities
- Identifies next steps and opportunities for improvement
- Develops initial evidence-building questions
- Makes key findings available to inform planning, budgeting, and management decisions
- Facilitates best practices of a learning organization





## Management's Discussion and Analysis

- Drives a focused conversation with OMB on significant issues and informs management and budget activities

PA&E manages the process to produce the Strategic Review findings. Component Assessment Teams, led by a Senior Executive Service leader, gauge program progress, and recommend a rating using a variety of qualitative and quantitative evidence. Assessment Team Leads present written findings and oral briefings to the PIO and other Department leadership. The Headquarters Review Team conducts a cross-cutting review of assessment results, and progress ratings are agreed upon in concert with the PIO, DPIO, and senior program leadership. PA&E prepares a Summary of Findings to inform targeted discussions with OMB. Findings are also used to inform the Department's Planning, Programming, Budgeting, and Execution (PPBE) cycle, and are published in the APR to inform stakeholders.



## DHS Summary of Key Performance Measures

Strategic plan goals are implemented by our programs which are groups of activities acting together to accomplish a specific high-level outcome external to DHS and include operational processes, skills, technology, human capital, and other resources. Programs have performance goals, performance measures, and performance targets. Below are a select set of measures organized by the goals contained in [DHS’s FY 2020-2024 Strategic Plan](#), and that describe how our programs work to deliver on the DHS mission.

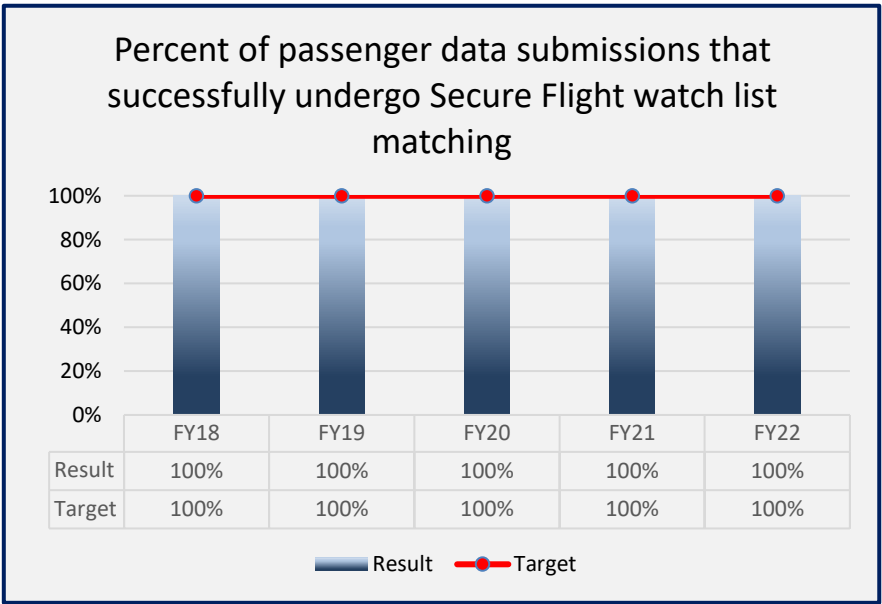
### Goal 1: Counter Terrorism and Homeland Security Threats

One of the Department’s top priorities is to protect Americans from terrorism and other homeland security threats by preventing nation-states and their proxies who engage in terrorist or criminal acts from threatening the homeland. Terrorists and criminals are constantly adopting new techniques and sophisticated tactics to circumvent homeland security and threaten the safety, security, and prosperity of the American public and our allies. The rapidly evolving threat environment demands strategies and tactics to ensure an initiative-taking response by DHS and its partners to identify, detect, and prevent attacks against the United States. Focused activities associated with this goal include information sharing, aviation security, and protection of national leaders and events.

The following measures highlight some of our efforts to counter terrorism and homeland security threats. Up to five years of data is presented if available.

**Percent of passenger data submissions that successfully undergo Secure Flight watch list matching (TSA):** Vetting individuals against high-risk watch lists strengthens the security of the transportation system by ensuring that individuals on the No-Fly List are prevented from boarding an aircraft and informs the traveling public that all covered domestic and international air

passengers have undergone checking against these watch lists. This measure reports the percent of qualified message submissions received from the airlines that are successfully matched by the Secure Flight automated vetting system against the existing high risk watch lists. A qualified message submission from the airlines contains passenger data sufficient to allow successful processing in the Secure Flight automated vetting system. Secure Flight receives an average 2 million passenger submissions per day from commercial airline operators. In FY 2022 this measure achieved



100%, meeting the target, and has maintained this level of performance since 2010. DHS will continue to report this measure as it conveys an underlying critical layered process to ensure security in the aviation environment and transportation system.

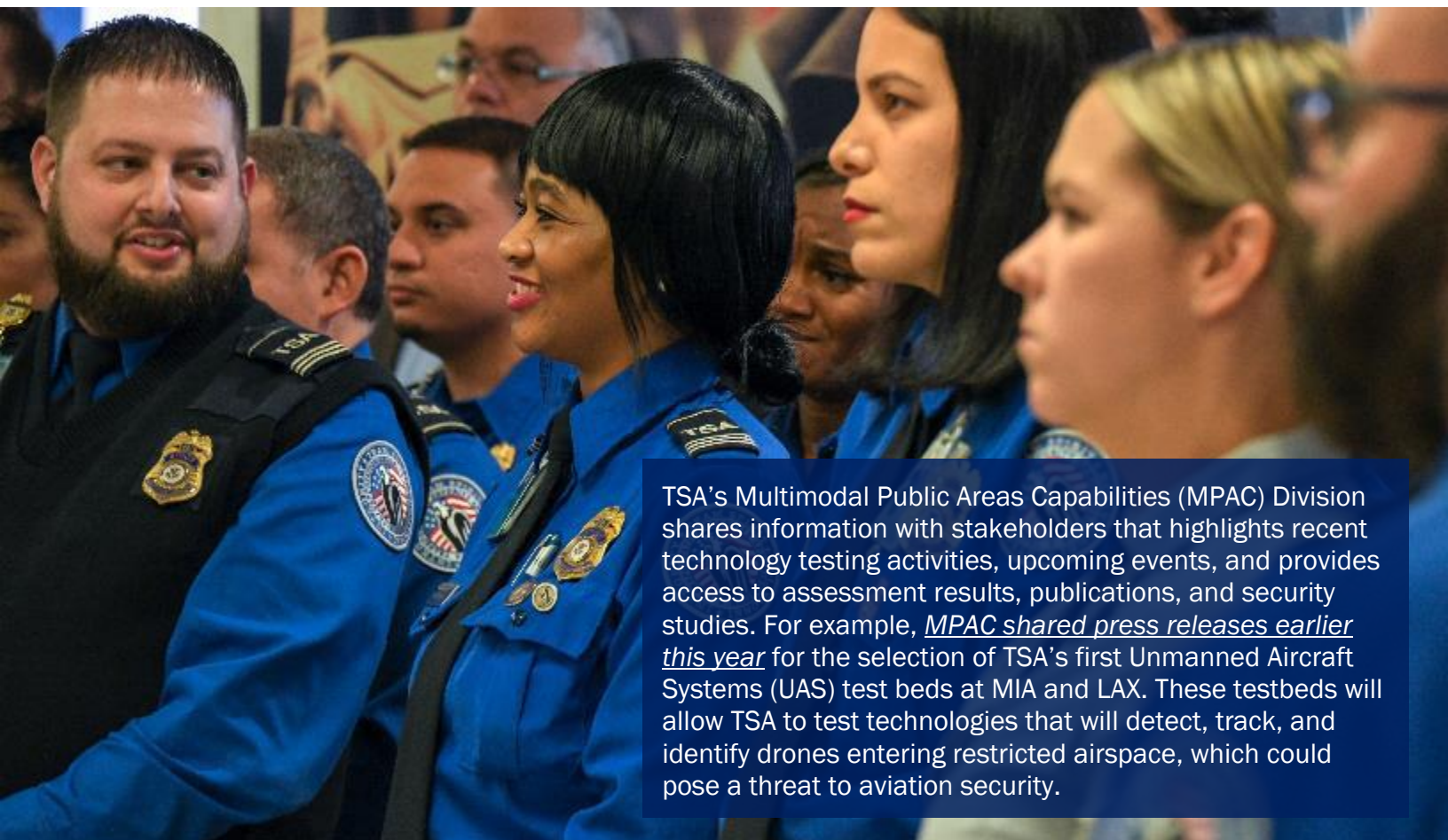
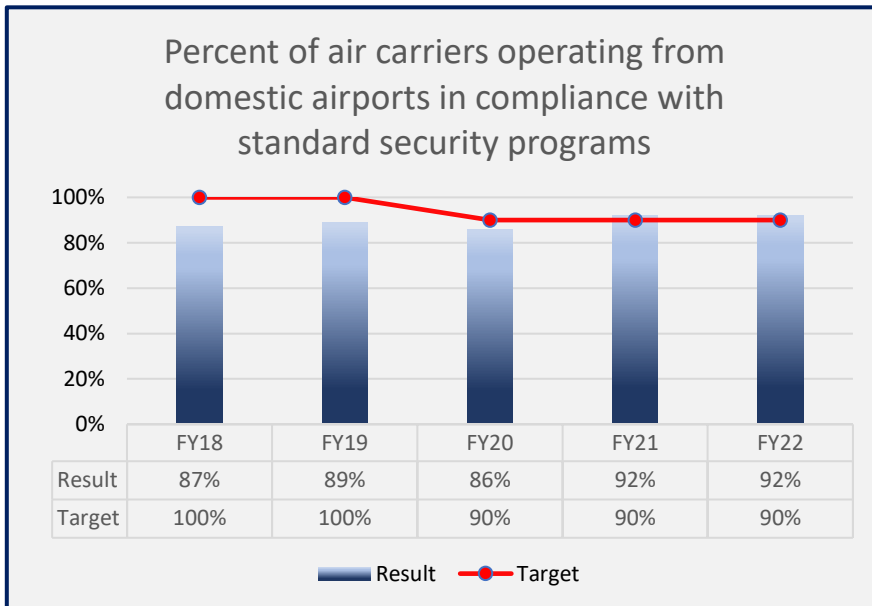


## Management’s Discussion and Analysis

### Percent of air carriers operating from domestic airports in compliance with standard security indicators (TSA):

TSA verifies air carrier compliance from domestic airports with standardized security through a robust inspection program on one or more aspect of operations such as catering, cargo acceptance, and aircraft searches, which allows for improved collaboration, information sharing, and facility awareness of emerging security risks. Inspections are conducted in accordance with the Compliance Implementation

Plan that identifies three types of inspections (comprehensive, targeted, and supplemental). In FY 2022, there were 33,680 inspections conducted, resulting in 2,768 findings nationwide. TSA continues to engage with regulated parties to reduce vulnerabilities and findings. Joint testing and regular visits with airline officials are conducted to address areas of concern as well. TSA



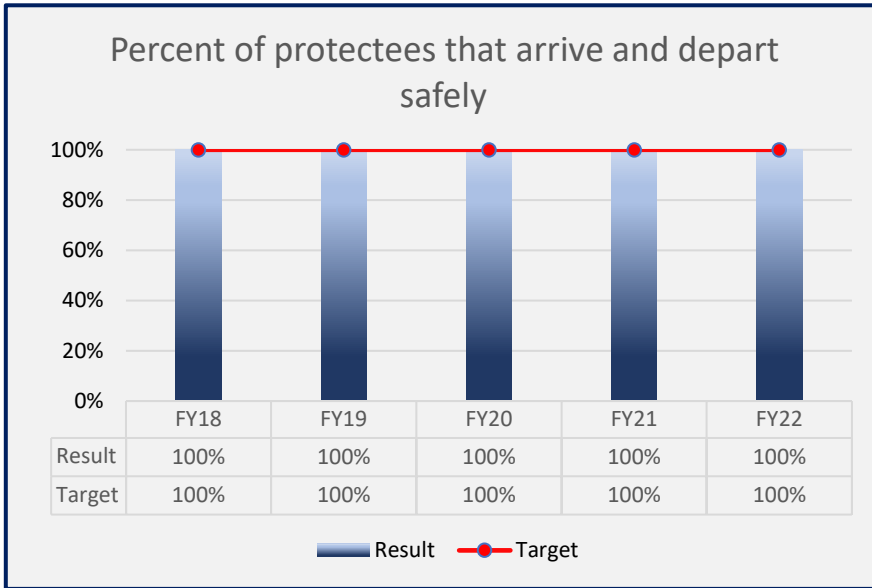
TSA’s Multimodal Public Areas Capabilities (MPAC) Division shares information with stakeholders that highlights recent technology testing activities, upcoming events, and provides access to assessment results, publications, and security studies. For example, *MPAC shared press releases earlier this year* for the selection of TSA’s first Unmanned Aircraft Systems (UAS) test beds at MIA and LAX. These testbeds will allow TSA to test technologies that will detect, track, and identify drones entering restricted airspace, which could pose a threat to aviation security.



will continue to deliver critical and complex aviation guidance and clarification to industry partners to ensure overall adequacy, effectiveness, and efficiency of security programs.

**Percent of protectees that arrive and depart safely (USSS):** This measure reflects the effectiveness of efforts to ensure safe arrivals and departures for the President and Vice President of the United States and their immediate families, former presidents, their spouses, and their minor children under the age of 16, major presidential and vice-presidential candidates and their spouses, and foreign heads of state. In FY 2022, USSS ensured safe arrival and departure for all 4,867 protective visits. The target for this measure is always 100% and the USSS has achieved 100% of safe arrivals and departures for more than the past five years. To achieve these results takes a coordinated effort across several specialized resources within USSS and coordination with federal, state, and local partners. Using advanced countermeasures, the USSS executes security operations

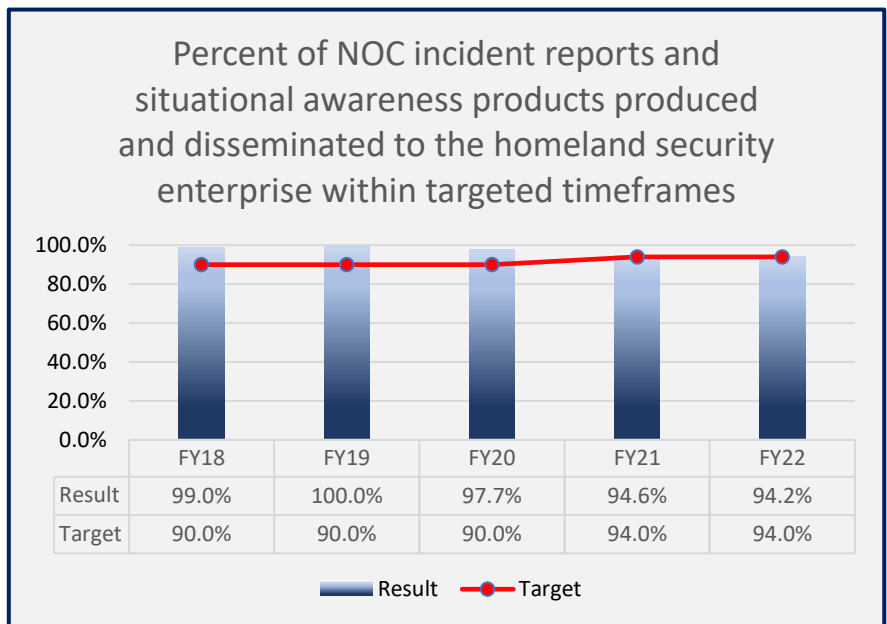
that deter, minimize, and decisively respond to identified threats and vulnerabilities to keep protectees safe.



that deter, minimize, and decisively respond to identified threats and vulnerabilities to keep protectees safe.

**Percent of National Operations Center incident reports and situational awareness products produced and disseminated to the homeland security enterprise within targeted timeframes (OPS):** This measure evaluates the percent of Situational Awareness (SA) Products disseminated within targeted timeframes.

These products serve as the basis for senior leader decision-making and promote SA across the homeland security enterprise. To augment SA, facilitate coordination, and provide decision support, the National Operations Center (NOC) utilizes a web-based DHS Common Operating Picture (COP). The COP can be accessed through various Briefing Display Systems within the NOC, or through any computer using the Homeland Security Information Network (HSIN). The NOC Watch Team creates a geographically located icon on the COP and an overall written situation summary to provide SA on the event to decision makers and the



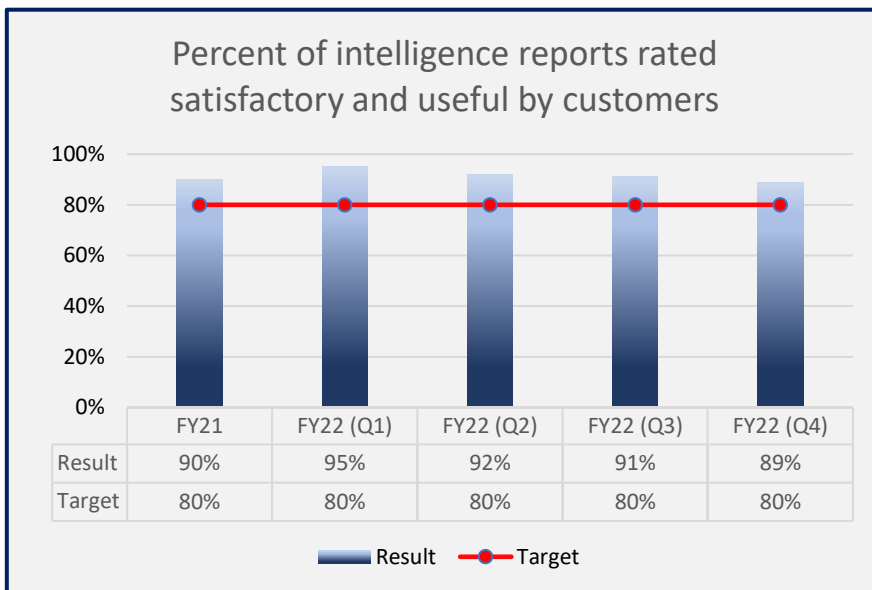
to provide SA on the event to decision makers and the



## Management’s Discussion and Analysis

homeland security enterprise. In FY 2022, OPS disseminated 94.2% of NOC incident reports and SA products to the homeland security enterprise within targeted timeframes.

**Percent of intelligence reports rated satisfactory and useful by customers (I&A):** This measure gauges the extent to which finished intelligence products are satisfying customers’ needs. An intelligence report is a product of analytical judgement applied to address an intelligence question produced by DHS or through partnerships with other agencies where the analytic conclusions have been drafted, reviewed, and disseminated to customers. Providing intelligence on topics of concern equips the homeland security enterprise with the timely intelligence and information it needs to keep the homeland safe, secure, and resilient. In FY 2022, I&A received 258 customer feedback forms, 230 of which provided usefulness ratings of “Very Satisfied” or “Somewhat Satisfied” with I&A’s intelligence reports.



The Secret Service provided protection for the President and other world leaders at the Summit of the Americas in Los Angeles in FY 2022. The President, Vice President, as well as 22 Heads of State attended the summit. This multi jurisdictional security event concluded without protective incident, ensuring the safety of all protectees and attendees.



### Looking Forward

A few near-term efforts to advance the Department's capability and capacity in these areas are provided below.


- **DHS has taken a tactical and preemptive approach to address the threat posed by the pace of technological advance for unmanned aerial systems (UAS). [Terrorists continue to use UAS](#) (i.e., drones) to conduct surveillance and potentially launch terrorist attacks which are a real threat across many domains. Drug smugglers have used these systems to monitor border patrol officers and to deliver drugs in remote areas. Criminals**

and nation-states are using them to spy on sensitive facilities. Threats continue to evolve, and unmanned aerial systems can support a wide array of emerging threats. To address this, the Department has taken a tactical and preemptive approach across several Components. Notable examples include but are not limited to:

- CBP partnered with S&T to establish a center focused on the exploitation of aviation and maritime drones. The Center for Air and Marine Drone Exploitation, a first of its kind in federal law enforcement, provides support for all CBP components to help protect covered facilities and operations. While CBP continues to provide counter-UAS (C-UAS) capabilities during Special Event Assessment Rating events and DHS-identified mass gathering events, a major next step for CBP is a funding proposal to continue expanding their air domain awareness and C-UAS capabilities.

### DID YOU KNOW?

The Coast Guard is a leader in countering UAS threats within DHS and protects the public at major waterfront events, like the Macy's Thanksgiving Day Parade and San Francisco Fleet Week. This year, the Coast Guard protected nearly 3 million spectators at public events nationwide.



S&T's Silicon Valley Innovation Program (SVIP) has successfully provided innovative autonomous small Unmanned Aircraft Systems (sUAS) to CBP agents on the Southwest border. The sUAS features software and sensors that enable a unique launch and recovery system that can be operated from a moving vehicle.



## Management's Discussion and Analysis

- USCG partnered with S&T to field initial [C-UAS capabilities](#). As USCG continues to mature its C-UAS capabilities to meet this rapidly evolving threat, they plan to make significant updates and revisions to internal program guidance for patrols, boardings, escorts, and fixed security zones to enhance the ability of the field to respond to C-UAS and active shooter and active threat situations.
- CISA also plans to establish a [small unmanned aircraft system](#) Security Program Office to further support and enhance the Department's UAS-related programs.
- **DHS is seeking technological advantages and leveraging partnerships to advance aviation security.** TSA and S&T continue to collaboratively explore innovative approaches to aviation security. The two agencies have partnered with Duke University to develop a prototype hybrid x-ray system that combines multi-view transmission (e.g., CT) with x-ray diffraction (XRD) tomography. XRD technology will improve material recognition and threat identification, which means an increased ability to detect currently unidentifiable threats. S&T will also be supporting TSA with modeling and simulation studies to better define requirements for the checked baggage program. In the future, the goal is to improve checked baggage alarm rates while managing down-stream resource constraints.

### DID YOU KNOW?

In 2022, I&A released a mobile app that puts intelligence in the hands of its frontline customers. "DHS Intel" features push notifications, threat area filters, and an advanced keyword search capability, providing swift, secure, and simplified access to DHS and partner generated products.



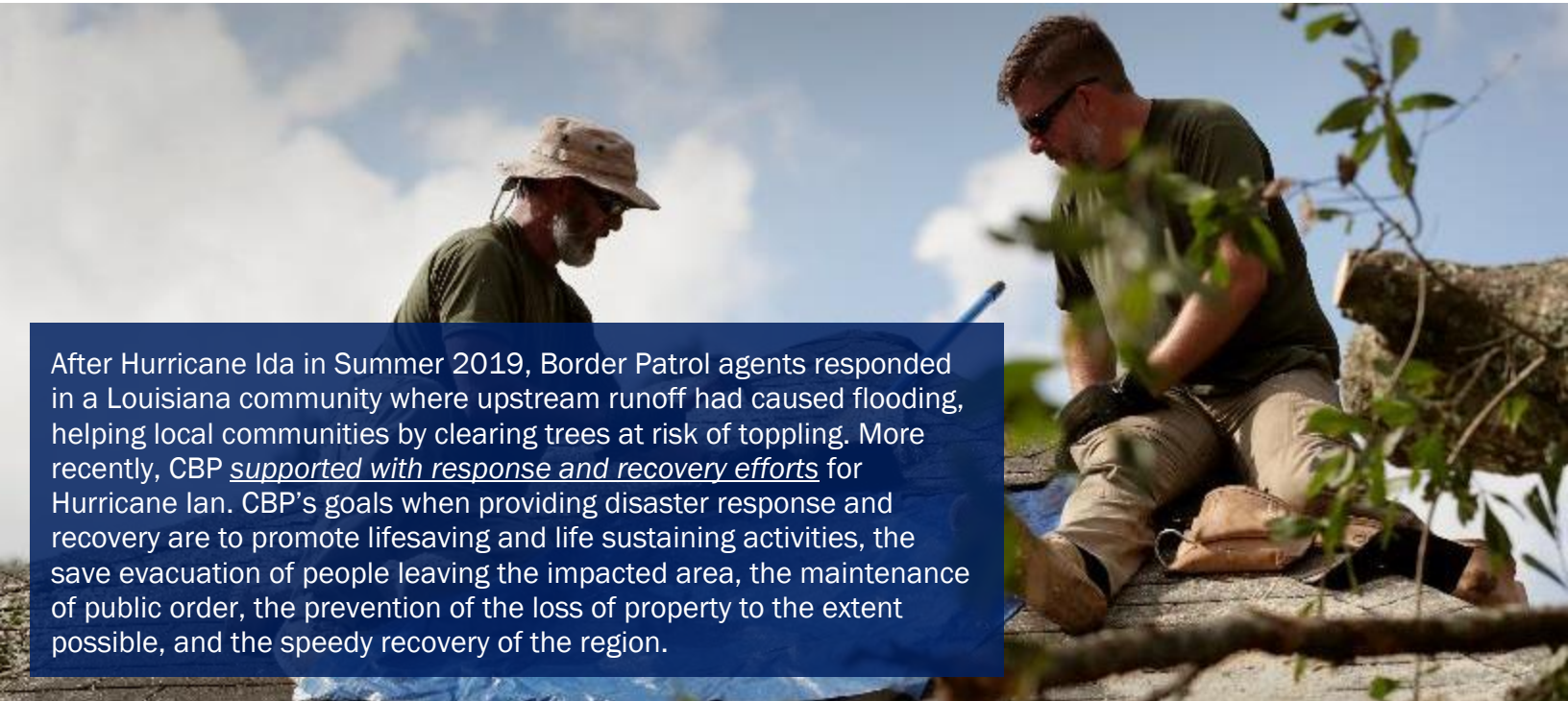
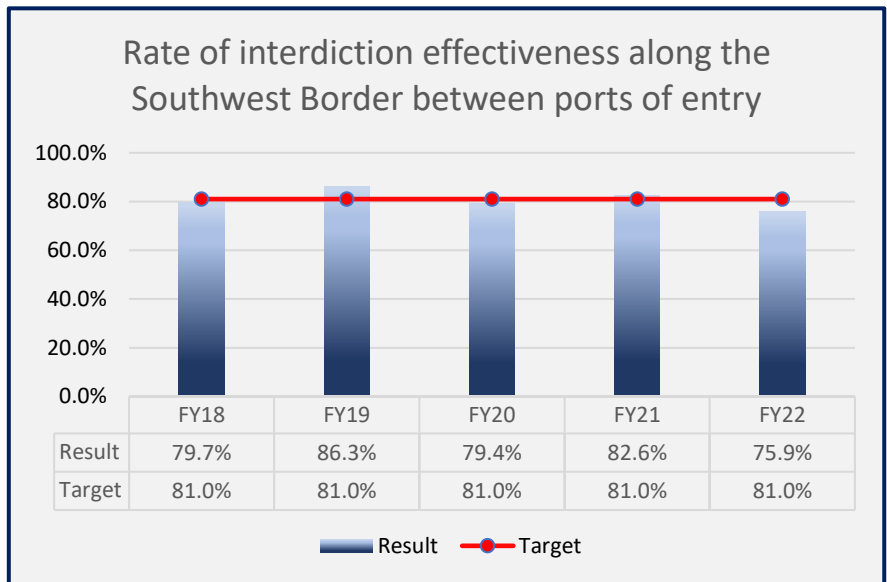


### Goal 2: Secure U.S. Borders and Approaches

Secure borders are essential to our national sovereignty. DHS continues its efforts to secure and maintain control of our land and maritime borders. Concentration is also focused on Transnational Criminal Organizations (TCO) and preventing the impact of these organizations operating both domestically and internationally. Efforts also continue to pursue and appropriately prosecute those illegally in the interior of the country, and to ensure that we properly administer immigration benefits and employ only those who are authorized to work.

The following measures highlight some of our efforts to secure U.S. borders and approaches. Up to five years of data is presented if available.

**Rate of interdiction effectiveness along the Southwest Border between ports of entry (CBP):** The Border Patrol uses this measure as an important indicator of the effectiveness of law enforcement and response efforts to apprehend detected illegal border crossers, and as a key indicator of the status of security over the U.S. Border. Results for this measure have varied significantly in recent years. Illicit cross-border activity has increased, necessitating operational adjustments to



After Hurricane Ida in Summer 2019, Border Patrol agents responded in a Louisiana community where upstream runoff had caused flooding, helping local communities by clearing trees at risk of toppling. More recently, CBP supported with response and recovery efforts for Hurricane Ian. CBP’s goals when providing disaster response and recovery are to promote lifesaving and life sustaining activities, the save evacuation of people leaving the impacted area, the maintenance of public order, the prevention of the loss of property to the extent possible, and the speedy recovery of the region.

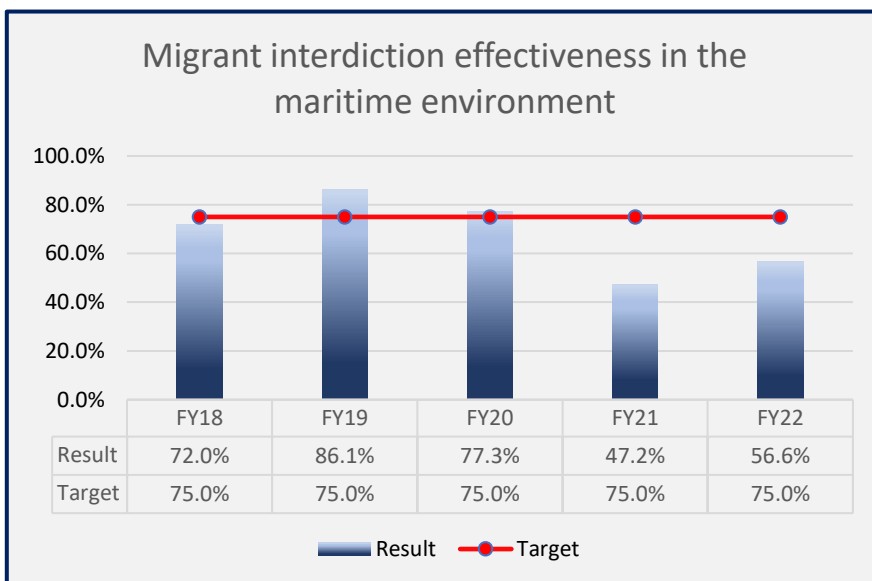




## Management’s Discussion and Analysis

facilitate humanitarian efforts. While many of the people processed by CBP are members of family units or unaccompanied children, a growing number remain evasive and often are guided by criminal organizations. While CBP anticipates further increases in the daily volume of cross-border traffic, application of Title 42 authority also continues to lower the interdiction effectiveness rate, entailing that people subject to the order be expelled as expeditiously as possible from the U.S. due to the ongoing pandemic. Going forward, the Border Patrol will continue to shift resources to locations that are determined to be the best use of personnel and surveillance technology to meet estimated targets.

**Migrant interdiction effectiveness in the maritime environment (USCG):** This measure communicates the effectiveness of the maritime law enforcement program to interdict migrants of all nationalities attempting to enter the United States through maritime borders not protected by the Border Patrol. This measure reports the percent of detected migrants of all nationalities who were interdicted by the USCG and partners via maritime routes. The USCG conducts patrols and coordinates with other federal agencies and foreign countries to interdict migrants at sea, denying them entry via maritime routes to the United States, its territories, and possessions. There is currently a significant increase in migrant flow in the



The Coast Guard is responsible for coordinating lifesaving missions across much of the Pacific and Atlantic Oceans. When combined, these U.S. search and rescue regions encompass an area that is eight time larger than the continental United States.





maritime environment, and it is expected this trend will continue. Assets have been surged to address this increase, especially in the Caribbean. The additional assets have led to more interdictions, but the increased flow of migrants led to an overall lower interdiction effectiveness rate. USCG will continue to adjust patrol patterns to meet the changes in the migrant flow.

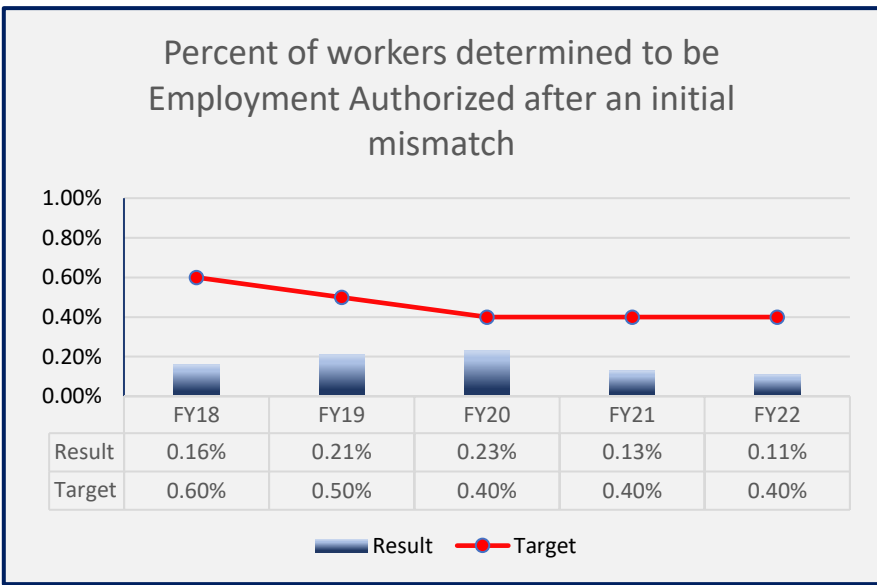
**DID YOU KNOW?**

In 2021, the Coast Guard responded to 11,427 pollution incidents, mitigated the impacts of 990,464 gallons of oil discharged within the Coastal Zone, and prevented the discharge of 8,234,524 gallons of oil into U.S. waters.

**Percent of workers determined to be Employment Authorized after an initial mismatch (USCIS):**

This measure assesses the accuracy of E-Verify by the percent of employment verification requests that are not confirmed as work authorized during the initial review.

E-Verify confirms employment eligibility of new hires by electronically matching information provided by employees on the I-9 Form, Employment Eligibility Verification, against records available to the Social Security Administration and DHS. The report shows the number of cases in which examiners in the program find an individual employment authorized after an initial mismatch. Ensuring the accuracy of E-Verify reflects the program’s intent to minimize negative impacts imposed upon those entitled to employment in the U.S. while ensuring the integrity



of immigration benefits by effectively detecting and preventing unauthorized employment. A lower result indicates that the system is effective in confirming employment eligibility and does

Since its inception in 2009, the USCIS Citizenship and Integration Grant program (CIGP) has awarded over \$100 million through over 500 competitive grants to immigrant serving organizations nationwide. The CIGP has helped more than 300,000 immigrants prepare for citizenship through its support and high quality services.





## Management's Discussion and Analysis

not require manual intervention. USCIS continues to increase the records available for electronic matching, which strengthens the program against identity fraud.

### *Looking Forward*

A few near-term efforts to advance the Department's capability and capacity in these areas are provided below.

- **Border security operations continue to be a top priority for DHS.** CBP prioritizes keeping terrorists and their weapons from entering the U.S. while welcoming all legitimate travelers and commerce. Cross-border flows of people are at historical highs, and as changes in the composition of cross-border flows have expanded the non-interdiction tasks for CBP's agents, CBP has remained agile and identified workforce management solutions to address critical gaps in recruiting, retention, capacity, and capability. For example, CBP continues to implement the Border Patrol Processing Coordinator position to better enable agents to focus their time on core law enforcement competencies. Looking ahead, CBP plans to supplement this approach by continuing to develop incentives, professional development opportunities, and training that [attracts new talent](#) and augments the retention of skilled, experienced agents. To further enhance Border Security Operations, CBP also plans to fuse performance data and resource

## DID YOU KNOW?

In 1789, the U.S. Customs Service was established to aid in the protection of the nation's supply chains and financial systems. Congress authorized the Collector of Customs to acquire boats and boatsmen, and a fleet of vessels began to patrol the coastal waters of the U.S, the forerunners of today's CBP Air and Marine Operations (AMO).



HSI has a Cyber Crimes Unit which houses the Computer Intrusion Response Program and is devoted to protecting American businesses and infrastructure by detecting, investigating, and countering network intrusion attempts.



deployment information into a geospatial depiction that eases explanations and promotes decision making regarding Operational Advantage. To support its public and private partnerships, CBP will also continue maturing its ability to use evidence and evaluation to identify efficiencies and best practices related to technology and programs, and to provide further evidence of CBP's efficacy in these areas.

- **DHS is responding with agility to ensure national security and to protect the increased number of people and goods that cross our nation's borders every day.** ICE's Enforcement and Removal Operations (ERO) and the Office of the Principal Legal Advisor (OPLA) work to remove those who pose a threat to national security, public safety, and border security. While workload, technology, staffing, and interagency collaboration continue to pose challenges, these two programs persist in implementing corrective actions to maximize their effectiveness. For example:
  - OPLA is frequently called upon to provide guidance on time-sensitive issues and to address significant litigation and frequent court decisions. As the demands of OPLA's mission grow in relation to the increase in cross-border flows, they persist in managing a docket of well over a million cases with the Executive Office for Immigration Review (EOIR), among other significant activities like providing legal advice to clients on complex, novel, and emerging issues related to the COVID-19 pandemic or supporting Operation Allies Welcome. To address resource

## DID YOU KNOW?

ICE's Law Enforcement Support Center (LESC) continues to provide smart and effective services and support that strengthen national security and public safety. In FY 2022, the LESL processed over one million queries and nearly 40,000 phone calls in support of federal, state, local, international, and tribal law enforcement agencies.

In July 2022, CBP signed a joint statement with Bahrain to launch a full Global Entry partnership with the Government of the Kingdom of Bahrain. CBP now has 15 Global Entry partner countries. Despite the pandemic, Global Entry surpassed 10 million applicants in FY 2022. That number exceeds the previous records of approximately 3 million applicants prior to the pandemic in 2019.



U.S. Customs and Border Protection

Welcome to the USA



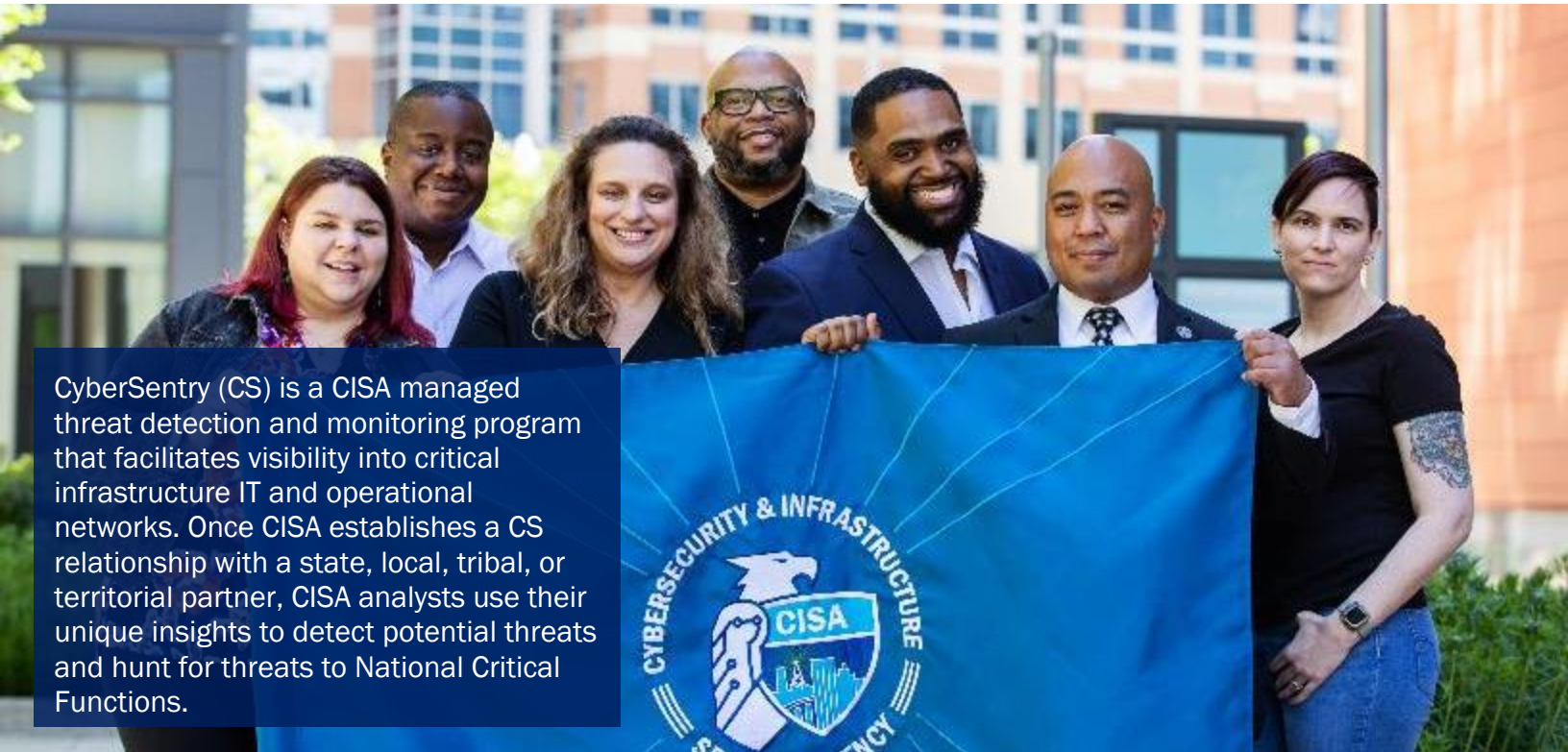


challenges relative to EOIR's expansion, OPLA will seek appropriations at a level sufficient to ensure that they can fully cover each immigration court and provide necessary facilities. OPLA will also continue to prioritize immigration court docket coverage so the government appears in cases of public safety, national security, or where there would be an injustice if the agency was not represented.

- In response to the surge of new refugee and asylum cases across the Southwest Border (SWB), ICE-ERO has also been faced by resource challenges. Despite this, ERO continues to vet well over a million queries and issue several thousand immigration detainers annually on priority noncitizens posing public safety risks. ERO has also improved many of the services it provides to people in ICE custody. For example, ERO increased accessibility by translating vital documents into languages spoken by noncitizens and provided language services for the deaf and hard of hearing, including in-person and video relay sign language services. ERO also expanded Virtual Attorney Visitation (VAV) to allow legal representatives to meet with clients virtually and confidentially using video technology. In the same spirit, ERO also plans to modernize IT resources to improve data quality and access for all agencies in the immigration lifecycle, improve operational efficiencies, and strengthen capabilities for data tracking and sharing. ERO also plans to secure funding to develop a workforce capable of meeting the demands of its growing mission.

**Goal 3: Secure Cyberspace and Critical Infrastructure**

Increased connectivity of people and devices to the Internet and to each other has created an ever-expanding attack surface that transcends borders and penetrates almost every American home and institution. In addition, the Federal Government depends on reliable and verifiable information technology systems and computer networks for essential operations. As a result, malicious cyber attackers target government systems to steal information, disrupt and deny



CyberSentry (CS) is a CISA managed threat detection and monitoring program that facilitates visibility into critical infrastructure IT and operational networks. Once CISA establishes a CS relationship with a state, local, tribal, or territorial partner, CISA analysts use their unique insights to detect potential threats and hunt for threats to National Critical Functions.



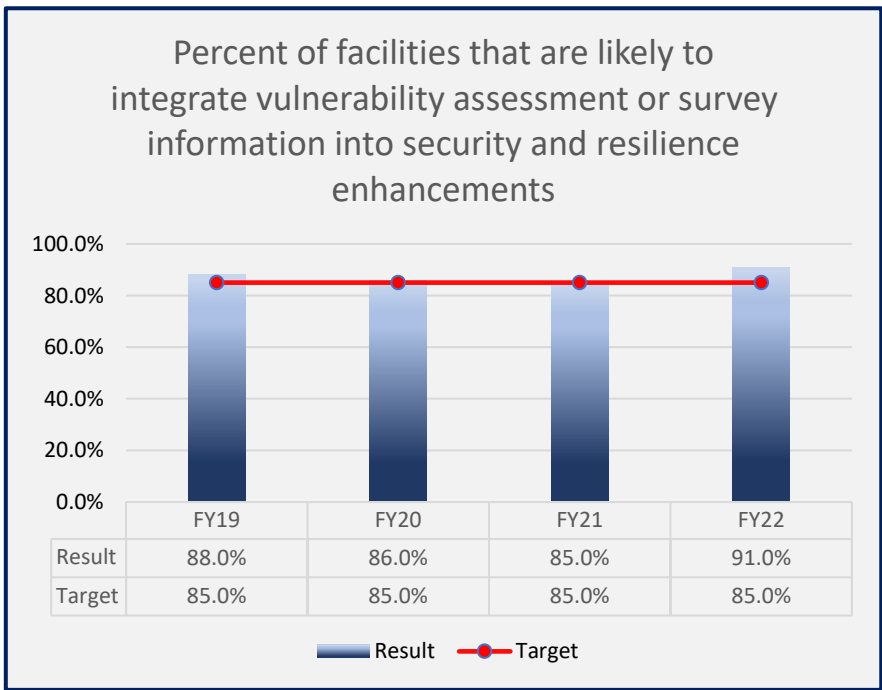
access to information, degrade, or destroy critical information systems, or operate a persistent presence capable of tracking information or conducting a future attack. Serving as the designated federal lead for cybersecurity across the U.S. Government, DHS promotes the adoption of common policies and best practices that are risk-based and responsive to the ever-changing cyber threat environment. Additionally, DHS collaborates with federal interagency counterparts to deploy capabilities for intrusion detection, unauthorized access prevention, and near real-time cybersecurity risk reports. In deploying these capabilities, DHS prioritizes assessments, security measures, and remediation for systems that could significantly compromise national security, foreign relations, the economy, public confidence, or public health and safety.

The following measures highlight some of our efforts to secure federal cyberspace and critical infrastructure. Up to five years of data is presented if available.

**Percent of facilities that are likely to integrate vulnerability assessment or survey information into security and resilience enhancements (CISA):** This measure demonstrates the percent of facilities that are likely to enhance their security and resilience by integrating [Infrastructure Protection vulnerability assessment](#) or survey information. Security and resilience enhancements can include changes to physical security, security force, security management,

**DID YOU KNOW?**  
 CISA’s Joint Cyber Defense Collaborative (JCDC) released its first joint cyber defense plan in 2022 focused on protecting critical U.S. infrastructure and used communication tools to share threat information with partners amid growing Russia Ukraine tensions. This effort informed CISA’s *Shield’s Up Campaign* to help all organizations prepare for, respond to, and mitigate the impact of malicious cyber activity.

information sharing, and protective measures. Providing facility owners and operators with vulnerability information allows them to understand and reduce risk to the Nation’s critical infrastructure. The program maintains a strong positive response on integrating assessment and survey information despite limitations in delivering assessments and follow-ups due to social distancing requirements during the pandemic. The current year’s results are consistent with the five-year trend.

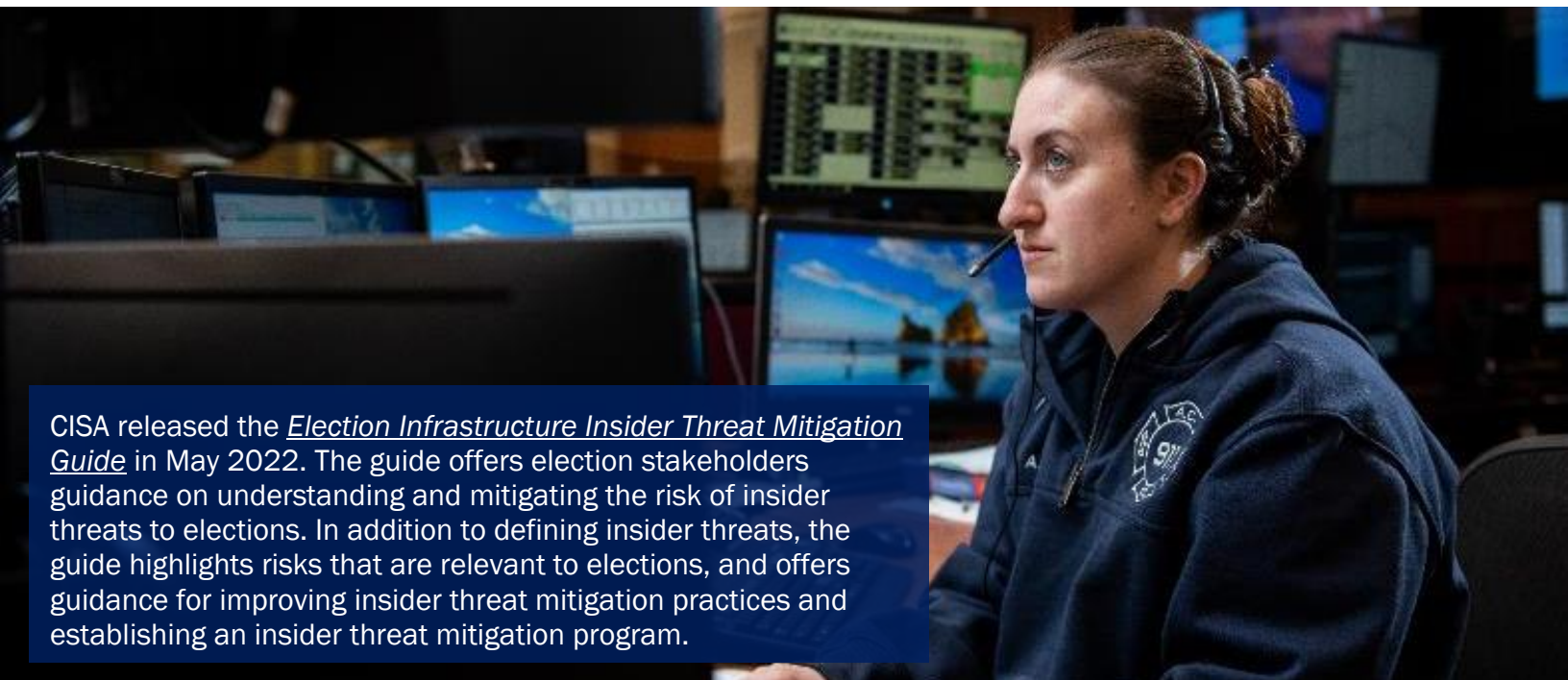
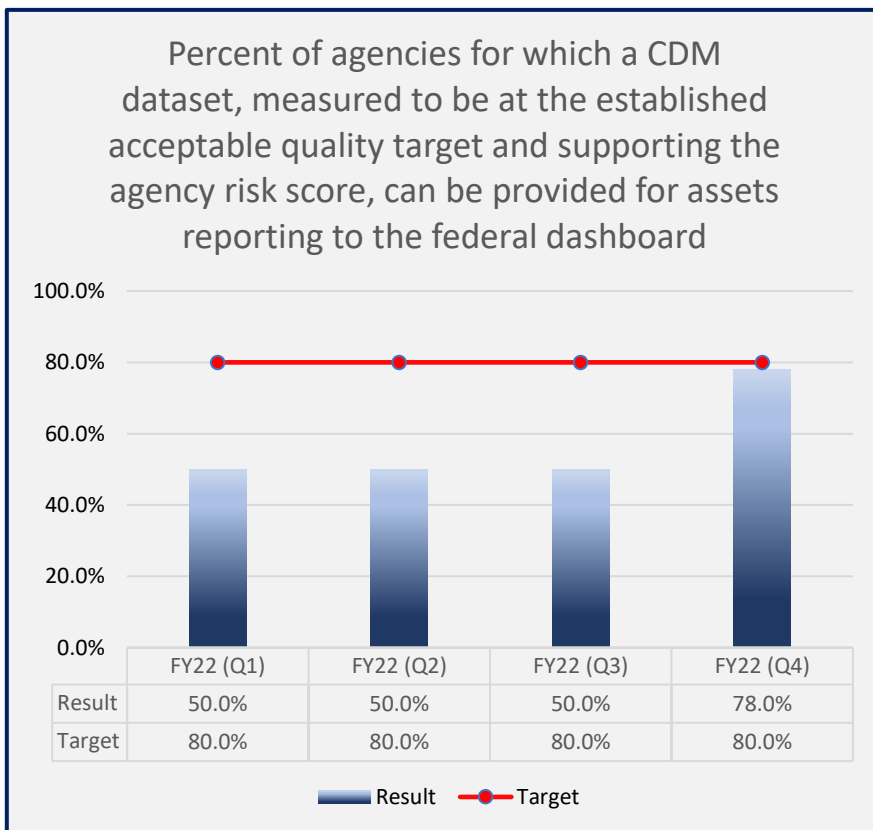




## Management’s Discussion and Analysis

**Percent of agencies for which a Continuous Diagnostic and Mitigation (CDM) dataset, measured to be at the established acceptable quality target and supporting the agency risk score, can be provided for assets reporting to the federal dashboard (CISA):**

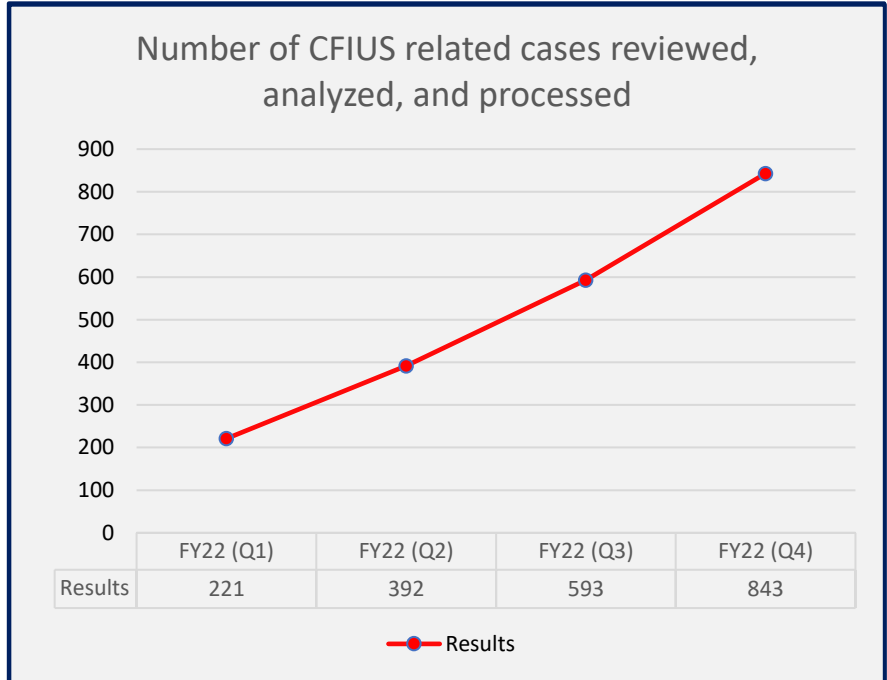
This measure is an indicator of a federal agency’s ability to provide reliable asset management information to the Federal Dashboard that can subsequently be used to determine cyber risk. More specifically, this measure reports the percent of participating Federal Civilian Executive Branch (FCEB) agencies that have completed a series of required engineering reviews with CDM engineers, demonstrating that the agency’s CDM Asset Management solution set is ready for a data quality assessment, and ultimately achieving an acceptable score for the level of data quality leveraged to support a reliable AWARE score and is used to convey results for its associated Agency Priority Goal on Cybersecurity.



CISA released the *Election Infrastructure Insider Threat Mitigation Guide* in May 2022. The guide offers election stakeholders guidance on understanding and mitigating the risk of insider threats to elections. In addition to defining insider threats, the guide highlights risks that are relevant to elections, and offers guidance for improving insider threat mitigation practices and establishing an insider threat mitigation program.



**Number of Committee on Foreign Investment in the United States (CFIUS) related cases reviewed, analyzed, and processed (CISA):** CISA plays an integral role within DHS supporting CFIUS, an interagency committee that reviews mergers, acquisitions, or takeovers that could result in foreign control of a United States business. These reviews are designed to determine the effects of such transactions on the national security of the United States. As a priority program for DHS, this new measure was developed and is being implemented for FY 2023



to demonstrate progress in this area of CISA’s work. This measure was baselined in FY 2022, and the results have been provided here for the reader’s awareness.

**Looking Forward**

A few near-term efforts to advance the Department’s capability and capacity in these areas are provided below.

- **Attracting, retaining, training, and providing a talented cybersecurity workforce is an increasingly vital part of the DHS mission.** DHS Components, in coordination with the DHS Office of Human Capital, are prioritizing cyber hiring and leveraging additional hiring authorities and incentives to meet the challenge of hiring and retaining top cyber talent. For example, DHS implemented the Cybersecurity Talent Management System (CTMS) in November 2021, a new personnel system that will enable DHS to recruit, develop, and retain our Nation’s top cybersecurity professionals more effectively. CISA is also exploring other alternatives like retention pay incentive programs, tuition reimbursement, and student loan payoff programs to attract and retain talented personnel. The agency will also continue to invest in its workforce through learning and evaluation training, cyber-skill training, leadership training, and diversity, equity, inclusion, and accessibility training.
- **DHS safeguards the federal enterprise network, systems, and assets against a spectrum of risks, and has advanced the security of federal networks overall.** CISA works with SLTT partners to provide guidance and recommendations on how to reduce their cyber-attack surface. As CISA continues to mature how it engages with its SLTT partners and other

**DID YOU KNOW?**

Partners can use the *Secure Tomorrow Series*, a strategic foresight capability, to identify emerging risks that could affect infrastructure in 5+ years. With the toolkit, partners can analyze, prioritize, and manage risks drivers to steer towards a preferred future.





## Management’s Discussion and Analysis

stakeholders, the delivery of [CyberSentry](#) – a software and hardware-based solution pilot program – will help define gaps in stakeholder networks and offer real-time insight into operational technology and critical infrastructure networks for targeted improvements.

### **Goal 4: Preserve and Uphold the Nation’s Prosperity and Economic Security**

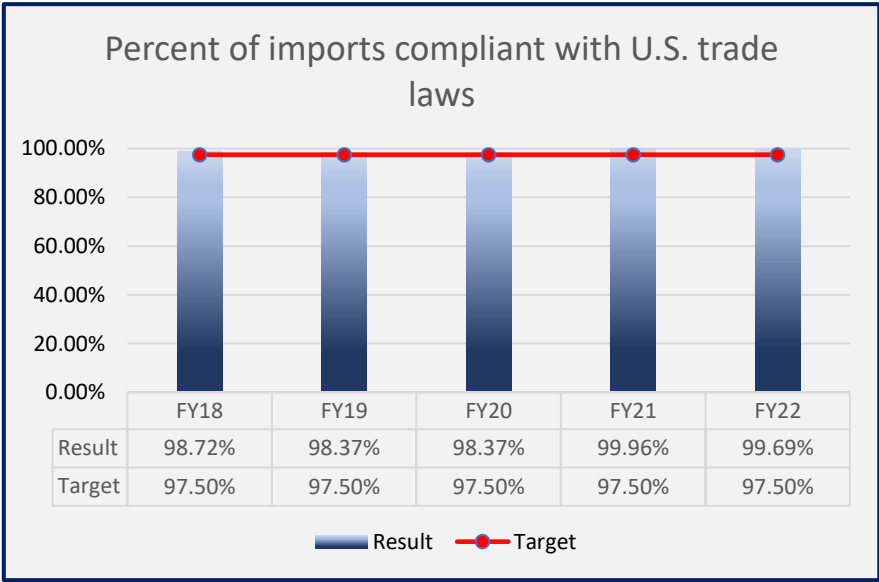
America’s prosperity and economic security are integral to homeland security and are achieved through our international trade operations, maritime natural resources, ice breaking for commercial cargo, aids to navigations for boats/ships, and protection of the nation’s financial systems.

The following measures highlight some of our efforts to preserve and uphold the nation’s prosperity and economic security. Up to five years of data is presented if available.

**Percent of imports compliant with U.S. trade laws (CBP):** This measure reports the percent of imports that are compliant with [U.S. trade laws including customs revenue laws](#), based on statistical sampling of entry records. Ensuring all imports are legally compliant and that their entry records contain no major discrepancies facilitates lawful trade. CBP, the importing community, and our federal partners have a shared

**DID YOU KNOW?**

CISA’s [Interoperable Communications Technical Assistance Program Service Offerings Guide \(TA SOG\) Version 7.0](#) serves as an overview of the technical assistance programs that CISA offers to state, local, tribal, and territorial partners across the country.

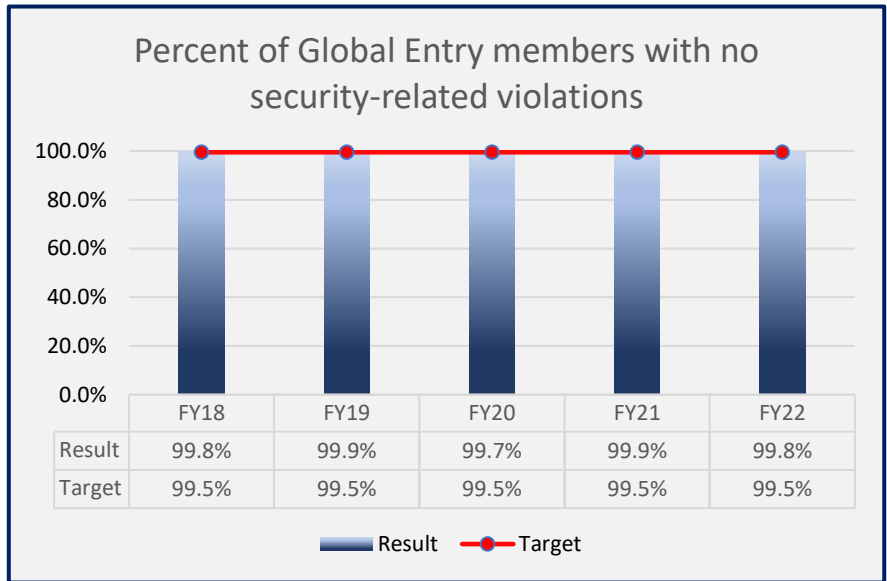


While COVID 19 presented a new opportunity for individuals to commit fraud, USSS continues to prevent losses to the public through pandemic related fraud investigations. For example, [in August 2022](#), USSS returned approximately \$286 million in fraudulently obtained Economic Injury Disaster Loans to the Small Business Administration.

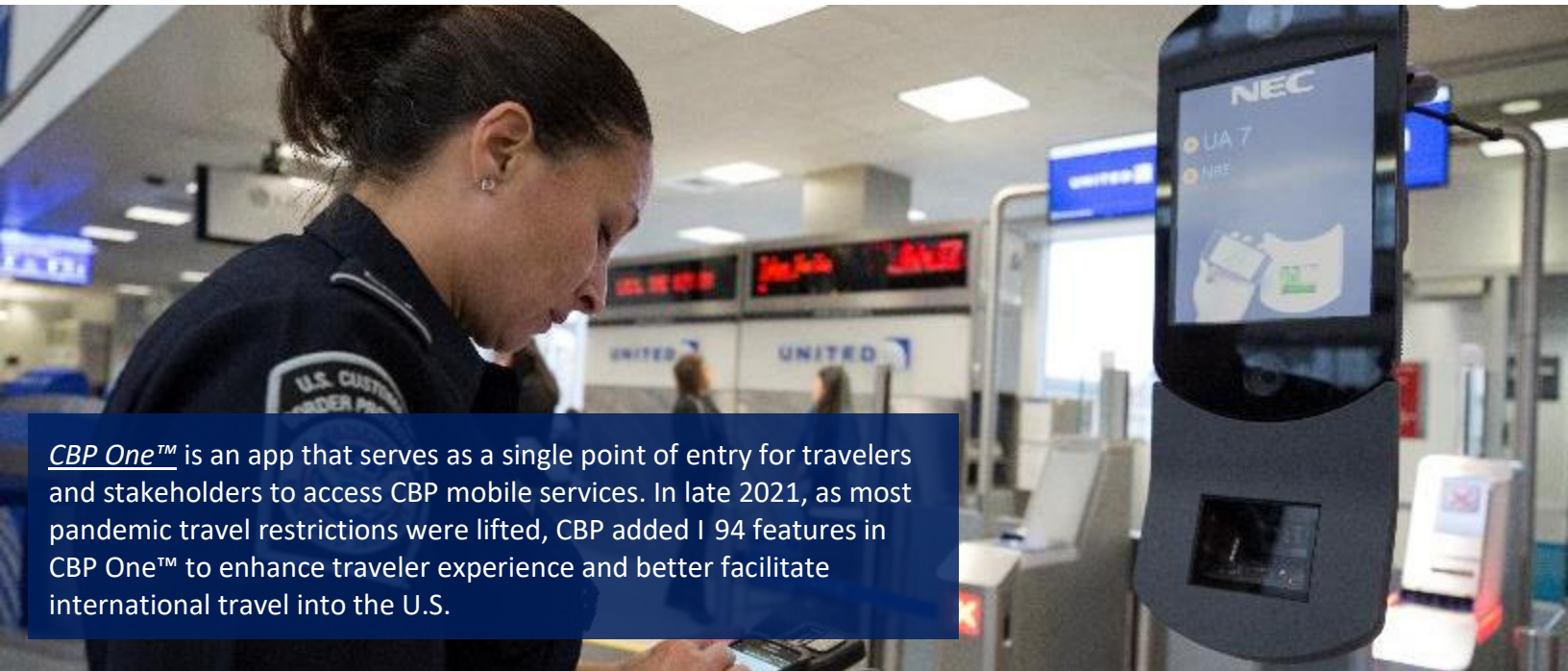


responsibility to maximize compliance with laws and regulations. In carrying out this task, CBP encourages importers to become familiar with applicable laws and regulations and work together with the CBP Office of Trade and Office of Field Operations to protect American consumers from harmful and counterfeit imports by ensuring the goods that enter the U.S. marketplace are genuine, safe, and lawfully sourced. This long-standing measure shows a consistently high compliance rate with FY 2022 results in-line with recent trends. While the expansion of e-commerce has led to greater trade facilitation, its overall growth has facilitated a concomitant increase in online trafficking in counterfeit and pirated goods that are typically shipped through international mail and express courier services and account for approximately 90 percent of counterfeit seizures.

**Percent of Global Entry members with no security-related violations (CBP):** This measure shows CBP’s success at maintaining a high level of security in the [international air environment](#) by measuring the degree of compliance with all federal, state, and municipal laws and regulations that CBP is charged with enforcing at the ports of entry (international airports) by Global Entry trusted traveler passengers. During typical non-pandemic times, CBP officers welcome almost a million international travelers daily. In



screening both foreign visitors and returning U.S. citizens, CBP uses a variety of techniques to assure that global tourism remains safe and strong. In FY 2022, the Travel program continued



**CBP One™** is an app that serves as a single point of entry for travelers and stakeholders to access CBP mobile services. In late 2021, as most pandemic travel restrictions were lifted, CBP added 194 features in CBP One™ to enhance traveler experience and better facilitate international travel into the U.S.

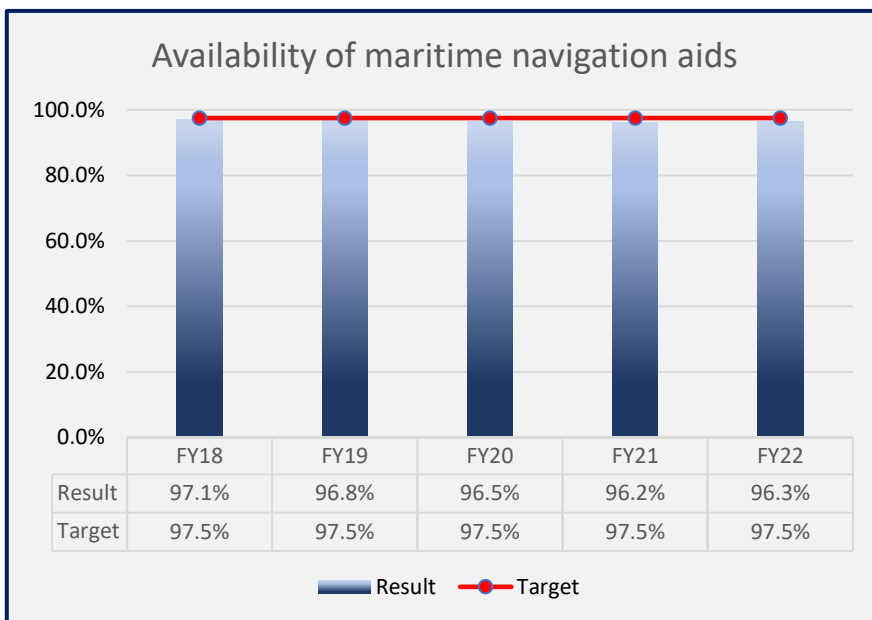


## Management's Discussion and Analysis

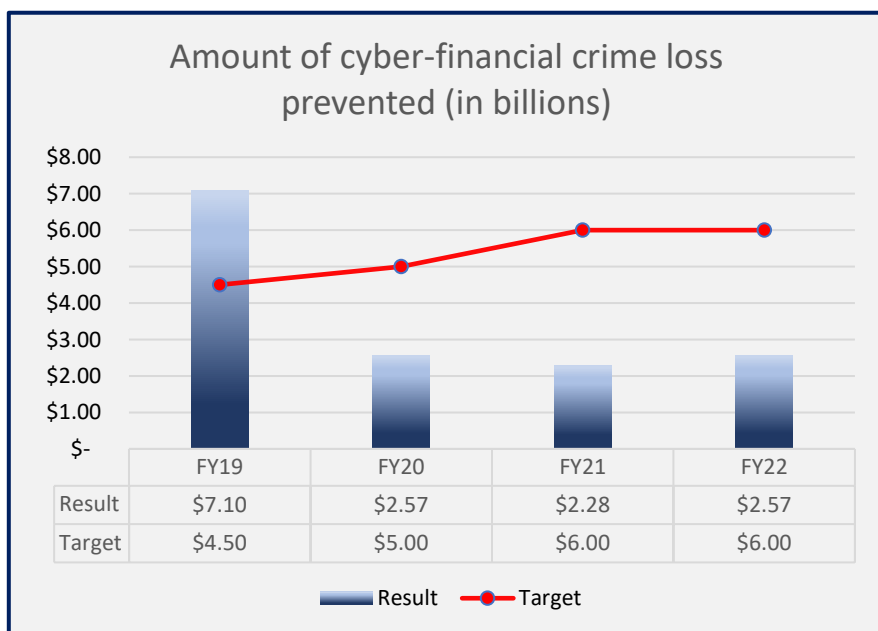
its outstanding performance in safeguarding international travel. While COVID-19 and associated requirements continued to impact the volume of travel into the United States, compliance remains strong. The Travel program is constantly looking at new technologies to receive traveler data in advance of arrival at a port of entry, which enhances security and allows for better facilitation of the entry process into the United States. The program also has a strong outreach program through their public-facing websites: [Know Before You Visit](#), [Trusted Traveler Programs](#), [For U.S. Citizens/Lawful Permanent Residents](#), [Electronic System for Travel Authorization](#), [Electronic Visa Update System](#), and [Visa Waiver Program](#).

### Availability of maritime navigation aids (USCG):

This measure indicates the hours that short-range federal [Aids to Navigation](#) (ATON) are available as defined by the International Association of Marine Aids to Navigation and Lighthouse Authorities in December 2004. As the Road Signs of the Sea, maritime navigational aids ensure safety of maritime traffic and the safe passage of trillions of dollars of economic activity. While ATON damage from hurricanes over the past several years has, for the most part, been addressed, resource availability continues to impact overall availability. The USCG continues to explore solutions to address this challenge.



**Amount of cyber-financial crime loss prevented (in billions) (USSS):** This measure is an estimate of the direct dollar loss to the public prevented due to cyber-financial investigations by the [USSS](#)



and their law enforcement partners. The dollar loss prevented is based on the estimated amount of financial loss that would have occurred had the offender not been identified nor the criminal enterprise interrupted. Since the onset of the global pandemic, USSS has dedicated significant resources to investigating crimes targeting pandemic relief funds. During FY 2021 and FY 2022 there were many responses to notifications of fraudulently obtained pandemic relief funds. USSS is working with data systems



owners to better capture and record the loss prevented associated with these crimes, which is currently not being reported in this metric. USSS is planning to incorporate this data into future reporting.

**Looking Forward**

A few near-term efforts to advance the Department's capability and capacity in these areas are provided below.

- **Cybercrime continues to be the fastest-growing mode for crime occurring across the country and touches a large share of the U.S. population.** To address this evolving threat, USSS protects the integrity of our nation's financial systems from a broad range of fraud, network intrusions, and other cyber-enabled attacks, regularly preventing billions in fraud loss. To amplify the impact of this mission and to share cybercrime prevention information with stakeholders, USSS partners with [the National Computer Forensics Institute](#) (NCFI) to train and equip SLTT law enforcement officers, prosecutors, and judges with the tools necessary to combat the evolving world of cyber and electronic crime. Looking ahead, USSS plans to seek re-authorization to train SLTT law enforcement officers and add authorities to train other Cyber Fraud Task Force (CFTF) partners. ICE-HSI also plays a key role in protecting the United States against cyber and financial crime. For example, HSI established cyber groups of criminal investigators, computer forensic

**DID YOU KNOW?**

USCG monitors terrorist risk posed to the Nation's vital Marine Transportation System, safeguarding \$5.4 trillion of annual economic activity. In response to heightened risk, USCG elevates operations and advises industry and the public, recommending actions to mitigate risk via USCG's Maritime Security Level.



The USCG's Great Lakes Center of Expertise (GLCOE) is the newest scientific research center that will lead research and testing of freshwater oil spill response technology. The Great Lakes are the largest body of surface freshwater on the planet that supply drinking water to over 40 million people in the U.S. and Canada and support a \$7 billion fishing industry. The GLCOE seeks to improve methods of detection, containment, and removal in freshwater and ice conditions, which differ from saltwater density, water circulating patterns, and ecosystems where response technologies were developed.



specialists, and cyber operations officers at domestic offices nationwide to look at exploitation on the dark web such as marketplace, ransomware, child endangerment, and victimization. Moving forward, HSI's [Cyber Crimes Center](#) is working to retain their cyber workforce and create targeted recruitment efforts to expand specialized cyber and forensics skills.

- **DHS promotes values of free and fair trade, the rule of law, and respect for human dignity.** [The Uyghur Forced Labor Prevention Act \(UFLPA\)](#) was enacted on December 23, 2021, to strengthen the existing prohibition against the importation of goods made wholly or in part with forced labor into the United States, and to end the systematic use of forced labor in the Xinjiang Uyghur Autonomous Region. Among its mandates, the UFLPA charged the Forced Labor Enforcement Task Force (FLETF), chaired by DHS, to develop a strategy for supporting the enforcement of Section 307 of the Tariff Act of 1930, as amended (19 U.S.C. § 1307). On June 17, 2022, this interagency task force, with input from CBP, ICE, and DHS's Office Strategy, Policy, and Plans, [published a strategy](#) to prevent the importation of goods mined, produced, or manufactured with forced labor in the People's Republic of China. Ending forced labor is a moral, economic, and national security imperative. DHS and its FLETF partners remain steadfast in their duty to address this global challenge. Combating trade in illicit goods produced with forced labor, including government-sponsored forced labor of convict labor, protects against unfair competition for compliant U.S. and international manufacturers and promotes American values of free and fair trade, the rule of law, and respect for human dignity. As one example of the impact of FLETF's strategy, CBP is considering revisions to its regulations to provide well-defined requirements for importers for better prohibition of goods made with forced labor, with the goal of deterring and discouraging the use of forced labor. CBP is also exploring novel approaches like increases in technology, overtime, and contractor support to



CBP played a key role in the implementation of two Executive Orders (E.O. 14066 and E.O. 14068) on Russian sanctions, prohibiting the importation of certain Russian goods into the United States. A range of Russian products are now prohibited from importation into the U.S. The range of products spans energy products such as crude oil, petroleum energy products, liquefied natural gas, and coal products, to more typical consumer products such as fish, alcohol, and non industrial diamonds.



address initial capacity gaps as the agency works to hire and prepare funding proposal for additional personnel in support of UFLPA requirements.

**Goal 5: Strengthening Preparedness and Resilience**

Preparedness is a shared responsibility across federal, state, local, tribal, and territorial governments; the private sector; non-governmental organizations; and the American people. Some incidents will overwhelm the capabilities of communities, so the Federal Government must remain capable of helping them to respond to natural and man-made disasters. Following disasters, the Federal Government must ensure an ability to direct resources needed to support local communities’ immediate response and long-term recovery assistance. The United States can effectively manage emergencies and mitigate the harm to American communities by thoroughly preparing local communities, rapidly responding during crises, and supporting recovery.

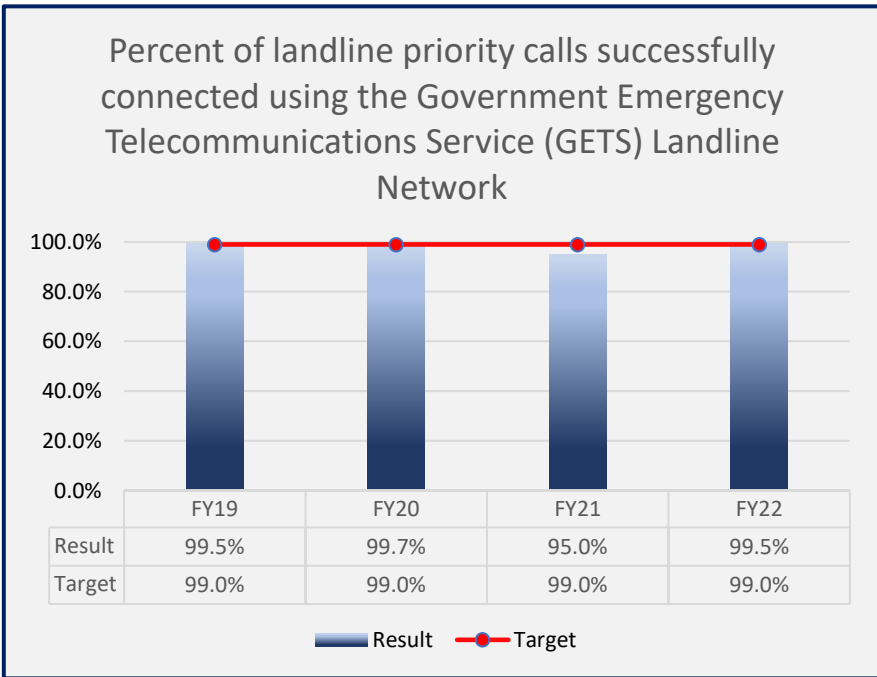
**DID YOU KNOW?**

CISA has a school safety program that supports schools by developing and deploying actionable and tailorable guidance, resources, and tools for K 12 communities on school safety issues, threats, and hazards to educate stakeholders, build awareness, and promote vigilance. For more information, see [CISA’s K 12 School Security Guide Product Suite](#).

The following measures highlight some of our efforts to strengthen preparedness and resilience. Up to five years of data is presented if available.

**Percent of landline priority calls successfully connected using the Government Emergency Telecommunications Service (GETS) Landline Network (CISA):**

By ensuring the connection of calls for first responders and government officials during a disaster, DHS contributes to a national effective emergency response effort. This measure gauges the reliability and effectiveness of the [Government Emergency Telecommunications Service \(GETS\)](#) to ensure accessibility by authorized users at any time, most commonly to ensure call completion during times of network congestion caused by all-hazard scenarios, including terrorist attacks or natural disasters (e.g., hurricane or earthquake). In FY 2022, this measure achieved 99.5%.

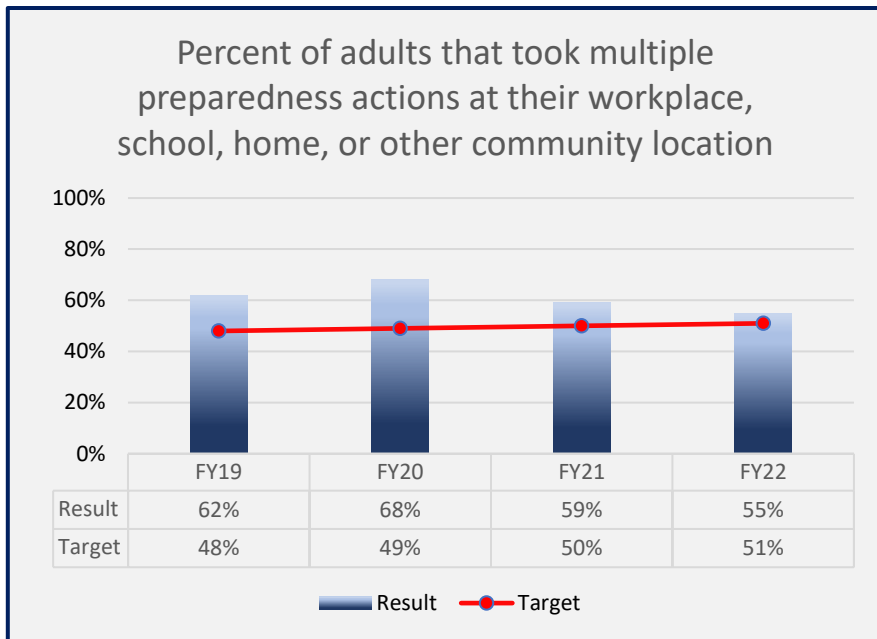


**Percent of adults that took multiple preparedness actions at their workplace, school, home, or other community location (FEMA):**



## Management’s Discussion and Analysis

those risks, and helping people understand how to prepare to meet disasters when they arrive. Programs and initiatives such as preparedness actions, capacity building, youth preparedness,

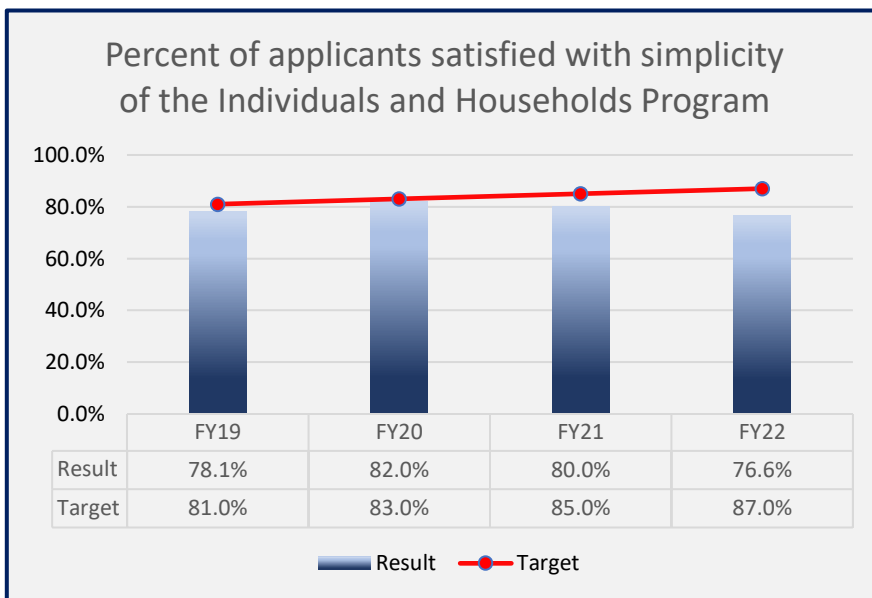


citizen responder, financial resilience, and messaging help ensure the nation has a variety of tools and resources to help build a culture of preparedness. Results are compiled from the National Households Survey. In FY 2022, 55% of the households that provided a response to the National Households Survey reported they did three or more preparedness actions in the last year. FEMA continues efforts on social media for taking preparedness actions, and partners in nation-wide campaigns like National Preparedness Month.

FEMA continues to play a critical role in ensuring the public has a variety of tools and resources to promote and sustain a ready and prepared nation.

### Percent of applicants satisfied with simplicity of the Individuals and Households Program (FEMA):

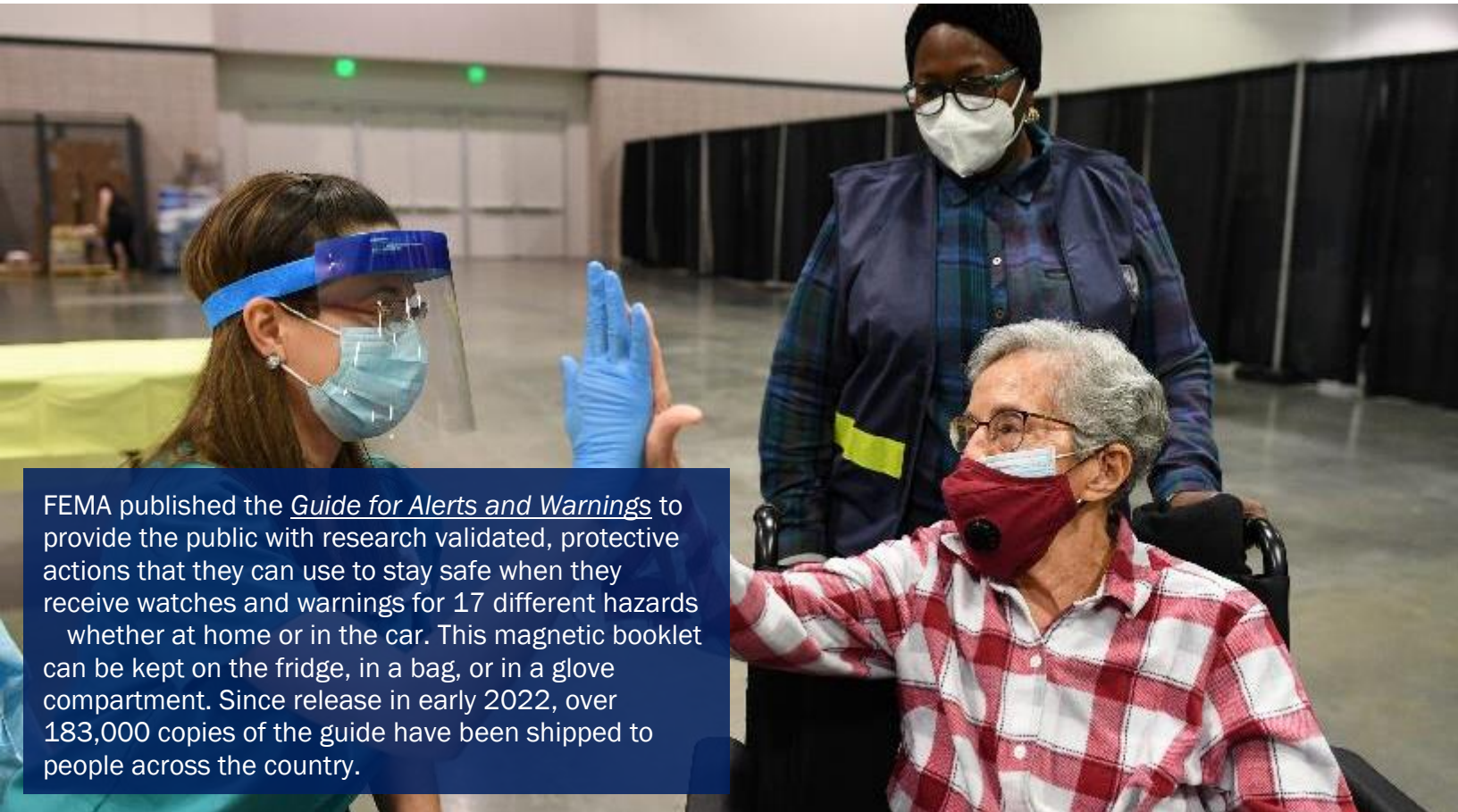
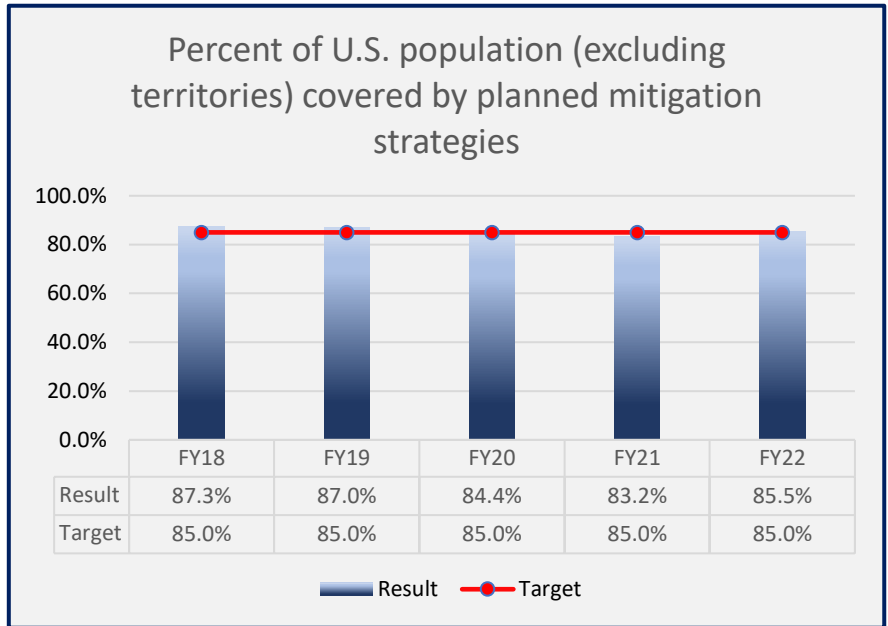
This measure uses surveys to assess applicant impressions of the simplicity of the procedures required to receive disaster relief from the [Individuals and Households Program’s](#) (IHP) assistance and services. The program collects survivors’ impressions of their interactions with IHP using standard surveys, administered by telephone, at three touchpoints of their experience with FEMA. In FY 2021, FEMA deployed the first email survey to Individual Assistance disaster survivors, and continued this through FY 2022. While FEMA did not meet its target of 87% in FY 2022, these results did not hinder FEMA’s ability to execute its mission. Looking ahead, FEMA is working to release a simpler, more intuitive application process that will allow applicants to select their specific Individuals and Households needs, easily see their progress within the application process, navigate instructions that highlight sections where required information is





missing, and review and edit all the information submitted in their entire application from a single screen before submission.

**Percent of U.S. population (excluding territories) covered by planned mitigation strategies (FEMA):** This measure reports the percent of U.S. population (excluding territories) covered by approved or approvable local [Hazard Mitigation Plans](#). To ensure plan coverage did not lapse in some areas, FEMA prioritized hazard mitigation plan review and approvals, continued investment in mitigation through FEMA’s Hazard Mitigation Assistance Grants, and provided training and technical assistance to SLTT partners. In FY 2022, this measure achieved 85.5%.



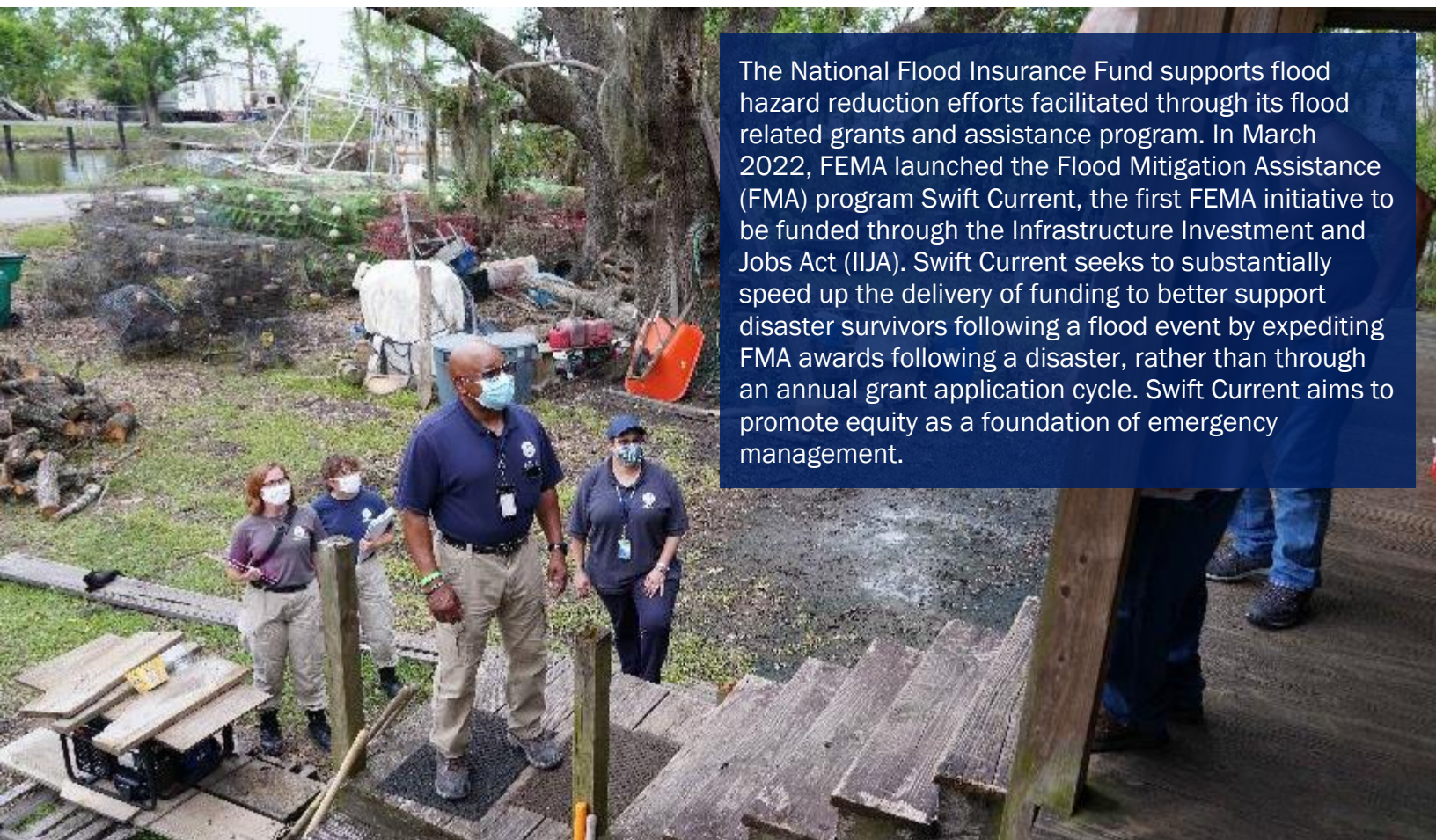
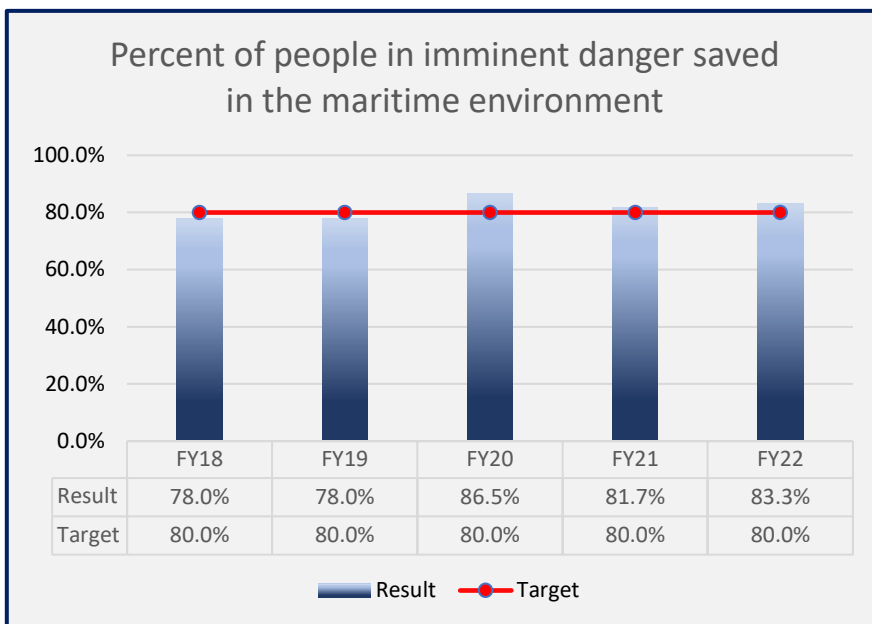
FEMA published the *Guide for Alerts and Warnings* to provide the public with research validated, protective actions that they can use to stay safe when they receive watches and warnings for 17 different hazards whether at home or in the car. This magnetic booklet can be kept on the fridge, in a bag, or in a glove compartment. Since release in early 2022, over 183,000 copies of the guide have been shipped to people across the country.





## Management’s Discussion and Analysis

**Percent of people in imminent danger saved in the maritime environment (USCG):** This is a measure of the percent of people who were in imminent danger on the oceans and other waterways and whose lives were saved by the [USCG](#). The number of lives lost before and after the USCG is notified and the number of persons missing at the end of search operations are factored into this result. In FY 2022, the USCG achieved 83.3%, which is the second highest result in the past five years, and is the third year in a row that USCG has surpassed its performance target for this measure.



The National Flood Insurance Fund supports flood hazard reduction efforts facilitated through its flood related grants and assistance program. In March 2022, FEMA launched the Flood Mitigation Assistance (FMA) program Swift Current, the first FEMA initiative to be funded through the Infrastructure Investment and Jobs Act (IIJA). Swift Current seeks to substantially speed up the delivery of funding to better support disaster survivors following a flood event by expediting FMA awards following a disaster, rather than through an annual grant application cycle. Swift Current aims to promote equity as a foundation of emergency management.



### Looking Forward

A few near-term efforts to advance the Department's capability and capacity in these areas are provided below.

- **Climate change represents a profound crisis for the nation, making natural disasters more frequent, more intense, and more destructive.** FEMA is engaging with federal and SLTT partners to address this evolving challenge. In partnership with the White House Office of Science, Technology and Policy (OSTP) and the National Oceanic and Atmospheric Administration (NOAA), FEMA released a [report outlining the opportunities for expanding and improving climate information services for the public](#). FEMA is also planning for how the agency will address climate change in the future and has established steering committees to develop internal cohesion and improved understanding of shared interests and goals among applicable FEMA programs. A notable example is the [Climate Adaption Enterprise Steering Group](#) (CAESG), chartered to develop a holistic, unified agency approach to consider and address the impacts of climate change across all of FEMA's programs and operations. Moving forward, FEMA will continue to educate the workforce and emergency management community on concepts related to climate change, future conditions, climate adaptation, and resilience. FEMA will also continue to support community resilience and sustainability by promoting community adoption of codes and standards and will support risk-based decision making by providing technical assistance to SLTTs and communities on how to use available and future data and resources to support community resilience.
- **USCG Search and Rescue:** [Search and Rescue \(SAR\)](#) is one of USCG's oldest missions. Minimizing the loss of life, injury, or property damage by rendering aid in the maritime environment to persons in distress and property has always stood as a USCG priority.



The Coast Guard founded the Automated Mutual Assistance Vessel Rescue (AMVER) System in 1958, which tracks approximately 7,000 ships a day for search and rescue across the globe. The Coast Guard manages the AMVER Program and coordinates commercial ships to save people in distress at sea.



USCG SAR response involves multi-mission stations, cutters, aircraft, and boats linked by communications networks. Managing the SAR program has become increasingly challenging due to a decreasing number of designated SAR professionals at key billets throughout the USCG. As such, the USCG continues to direct time and energy to advocate for improvements in the National SAR System, Marine Environmental Response, and Emergency Management programs, to strengthen the USCG's ability to lead in crisis. USCG continues to develop and implement the SAR Continuous Improvement Program to support the SAR community by applying consistent processes to identify, validate, and share information on program strengths, innovations, and areas for improvement. The SAR mission maintains a high degree of focus on the progression of search and rescue tools for locating people in distress, and the potential SAR response challenges in the polar regions as maritime and aeronautical traffic increases.

**DID YOU KNOW?**

FEMA's United States Fire Administration in partnership with the U.S. Department of Transportation's National Highway Traffic Safety Administration (NHTSA) is performing a study with the International Association of Fire Fighters (IAFF) on fire, Emergency Medical Services (EMS), and law enforcement response to fires and other emergencies involving electric vehicles.

**Agency Priority Goals**

Please see our Annual Performance Report (APR) for an update on our FY 2023-2024 APGs. The APR will be available in February 2023 in conjunction with the FY 2024 Budget Submission. The APR will be available at the following link: <https://www.dhs.gov/performance-financial-reports>.



## Financial Overview

The Department's principal financial statements — Balance Sheets, Statements of Net Cost, Statements of Changes in Net Position, Statements of Budgetary Resources, Statements 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, pursuant to the requirements of 31 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 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.

This section is presented as an analysis of the principal financial statements. Included in this analysis is a year-over-year 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.

### ***COVID-19 Activity***

In response to the national public health and economic threats, serious and widespread health issues and economic disruptions caused by COVID-19, DHS has continued to facilitate a speedy, whole-of-government response in confronting COVID-19, keeping Americans safe, helping detect and slow the spread of the virus, and making the vaccine available to as many people as possible.

Throughout the pandemic, DHS has worked with the White House, the Department of Health and Human Services (HHS), the Centers for Disease Control (CDC), and state, local, tribal and territorial governments to fight the COVID-19 pandemic and protect the public. Functioning critical infrastructure is particularly important during the COVID-19 response for both public health and safety as well as community well-being. Today, the Department continues to provide financial assistance through FEMA and under the Other Needs Assistance (ONA) provision of the Individuals and Households Program (IHP) to individuals and households with disaster-related funeral expenses. Under the Coronavirus Response and Relief Supplemental Appropriations Act, 2021, and the American Rescue Plan Act of 2021, FEMA will provide financial assistance for funeral costs specifically related to COVID-19 for funeral expenses at 100 percent federal cost share. In response to the unprecedented pandemic, TSA launched the “[Stay Healthy. Stay Secure.](#)” campaign, which details proactive and protective measures TSA has implemented at security checkpoints to make the screening process safer for passengers and our workforce by reducing the potential of exposure to the coronavirus. Additionally, the DHS workforce protection command center works to ensure that protective procedures are in place for the front-line workforce, who may regularly encounter potential disease carriers, and is in close coordination with federal health partners and component health and safety officials.

Additional activities information and financial impact can be found in the financial information section under Note 31, COVID-19 Activity, as well as on our website at [www.dhs.gov/coronavirus](http://www.dhs.gov/coronavirus).

### ***Financial Position***

The Department prepares its Balance Sheets, Statements of Net Cost, and Statements of Changes in Net Position on an accrual basis, in accordance with U.S. generally accepted accounting principles; meaning that economic events are recorded as they occur, regardless of when cash is received or disbursed.



## Management's Discussion and Analysis

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.

Financial Position (\$ in millions)	FY 2022	FY 2021	\$ Change	% Change
Fund Balance with Treasury	\$ 158,759	\$ 163,044	\$ (4,285)	-3%▼
General Property, Plant, and Equipment, Net	32,754	27,893	4,861	17%▲
Other Assets	28,290	26,201	2,089	8%▲
<b>Total Assets</b>	<b>219,803</b>	<b>217,138</b>	<b>2,665</b>	<b>1%▲</b>
Debt	20,533	20,618	(85)	<0%▼
Federal Employee and Veteran Benefits Payable	16,940	75,570	(58,630)	-78%▼
Accounts Payable	5,593	5,434	159	3%▲
Insurance Liabilities	5,848	3,436	2,412	70%▲
Other Liabilities	21,986	25,512	(3,526)	-14%▼
<b>Total Liabilities</b>	<b>70,900</b>	<b>130,570</b>	<b>(59,670)</b>	<b>-46%▼</b>
Total Net Position	148,903	86,568	62,335	72%▲
<b>Total Liabilities and Net Position</b>	<b>\$ 219,803</b>	<b>\$ 217,138</b>	<b>\$ 2,665</b>	<b>1%▲</b>

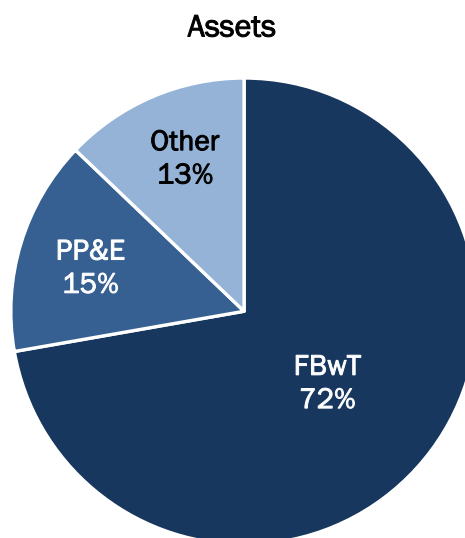
Results of Operations (\$ in millions)	FY 2022	FY 2021	\$ Change	% Change
Gross Cost	\$ 105,853	\$ 104,688	\$ 1,165	1%▲
Less: Revenue Earned	(16,283)	(14,718)	(1,565)	11%▲
<b>Net Cost Before Gains and Losses on Assumption Changes</b>	<b>89,570</b>	<b>89,970</b>	<b>(400)</b>	<b>0%</b>
(Gains) and Losses on Assumption Changes	1,181	1,573	(392)	-25%▼
<b>Total Net Cost</b>	<b>\$ 90,751</b>	<b>\$ 91,543</b>	<b>\$ (792)</b>	<b>-1%▼</b>

### Assets – What We Own and Manage

Assets represent amounts owned or managed by the Department that can be used to accomplish its mission.

The Department's largest asset is Fund Balance with Treasury (FBWT), 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) is the second largest asset, and include 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. On April 30, 2021, DoD announced that all DoD funded border barrier projects will be terminated and the U.S. Army Corps of Engineers (USACE) was authorized to approve exceptions to this proclamation to avert immediate physical dangers. Following this work and completion of the termination of contracts, the infrastructure and certain border barrier





assets were transferred to the CBP. On March 31, 2022, both DoD and CBP signed ten DD form 1354 (transfer and acceptance of DoD real property) detailing property (both complete and in progress) being transferred between DoD and CBP. Based upon this documentation, CBP recorded the interagency transfer from DoD in April 2022 after review of the property and validation of the value. CBP anticipates receiving additional transfer of border wall assets from USACE in FY 2023 with approximately \$1.6 billion in net book value.

Other Assets includes items such as investments, accounts receivable, cash and other monetary assets, taxes, duties and trade receivables, direct loans, and inventory and related property.

As of September 30, 2022, the Department had \$220 billion in assets, representing a \$3 billion increase from FY 2021. The majority of this change is due to an increase in General PP&E, attributed to the acquisition of the border barrier assets transferred from DoD.

### 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.

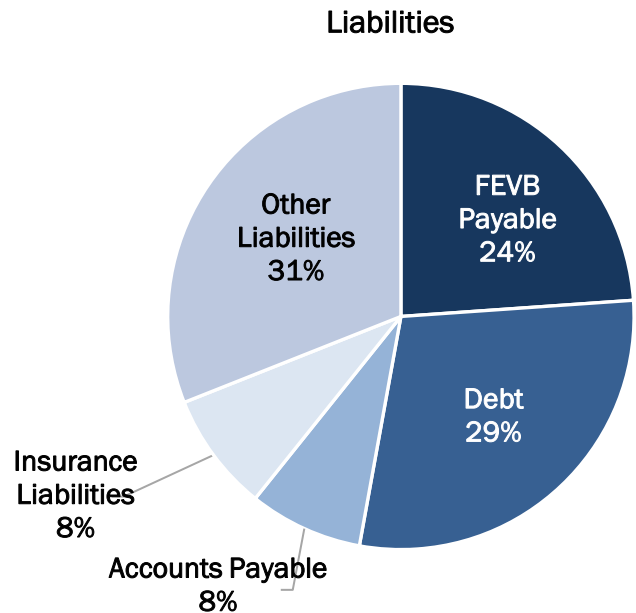
*Debt* is now the Department's largest liability, and results from Treasury loans to fund FEMA's National Flood Insurance Program (NFIP) and Disaster Assistance Direct Loan Program. Given the current premium rate structure, FEMA will not be able to generate sufficient resources from premiums to fully pay its debt. This is discussed further in Note 15 in the Financial Information section.

*Federal Employee and Veteran Benefits (FEVB) Payable* is the Department's second largest liability. In September 2022, per the *National Defense Authorization Act (NDAA) for FY 2021* (P.L. 116-283), DHS transferred the USCG Military Retirement System (MRS) actuarial accrued liability to DoD, and as of September 30, 2022, USCG is no longer the administrative entity. The remaining balance in the Department's FEVB Payable includes amounts owed to current and past personnel for pension and other post-employment benefits. The liability also includes medical costs for approved workers' compensation cases. For more information, see Note 16 in the Financial Information section. This liability is not covered by current budgetary resources, and the Department will use future appropriations to cover these liabilities (see Note 14 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. As a result of estimated claims losses for Hurricane Ian in Southwest Florida and the Carolinas, the Department's Insurance Liabilities increased \$2 billion from FY 2021.

*Other 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. As a result of estimated claims losses for Hurricane Ian in Southwest Florida and the Carolinas, the Department's Insurance Liabilities increased \$2 billion from FY 2021.





## Management’s Discussion and Analysis

*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 wages and benefits for current DHS employees, and amounts due to the Treasury’s general fund, environmental liabilities, refunds and drawbacks, and other.

As of September 30, 2022, the Department reported approximately \$71 billion in total liabilities. Total liabilities decreased by \$60 billion in FY 2022 mostly due to the transfer of USCG’s MRS actuarial accrued liability to DoD.

### **Net Position**

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 and cumulative results of operations 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 discussed in the section below as well as transfers to other agencies decrease net position. The Department’s total net position is \$149 billion. Total net position increased \$62 billion from FY 2021, in large part because of USCG’s transfer of the MRS actuarial accrued liability to DoD.

### **Results of Operations**

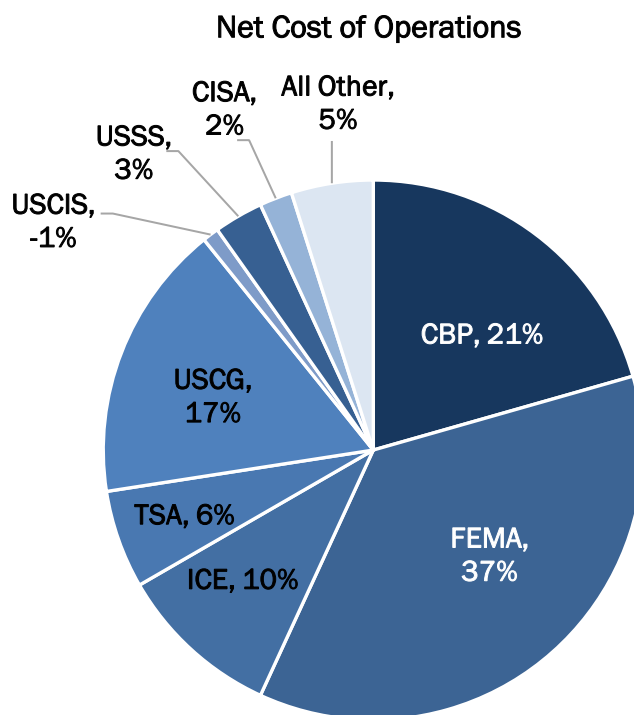
The Department presents net costs by operational Components which carry out DHS’s major mission activities, with the remaining support Components representing “All Other.”

Net cost of operations, before gains and losses, represents the difference between the costs incurred and revenue earned by DHS programs. The Department’s net cost of operations, before gains and losses, was \$90 billion in FY 2022, which is similar to the prior year.

During FY 2022, the Department earned approximately \$16 billion in exchange revenue. Exchange revenue arises from transactions in which the Department and the other party receive value and that are directly related to departmental operations. 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 Statements of Custodial Activity or Statements of Changes in Net Position, rather than the Statements of Net Cost.

### **Budgetary Resources**

The Statement of Budgetary Resources is prepared on a combined basis, rather than a consolidated basis, and provides information about how budgetary resources were made available as well as their status at the end of the period. Budgetary accounting principles require recognition of the obligation of funds according to legal requirements, which in many cases happens prior to the transaction under accrual basis. The recognition of budgetary accounting



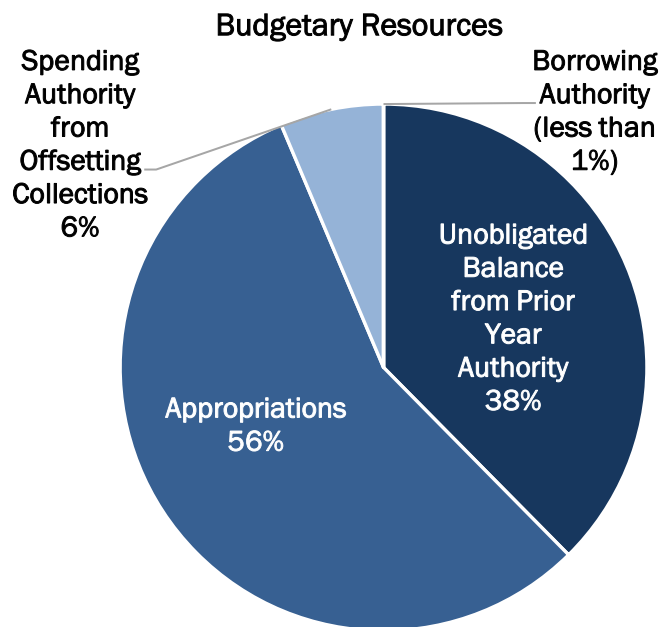
\*USCIS negative net cost balance is due to a new premium fee structure that contributed to increased revenue.



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)				
Unobligated Balance from Prior Year Budget Authority, Net	\$ 65,705	\$ 46,955	\$ 18,750	40%▲
Appropriations	97,949	142,442	(44,493)	-31%▼
Spending Authority from Offsetting Collections	11,097	9,560	1,537	16%▲
Borrowing Authority	4	32	(28)	-88%▼
<b>Total Budgetary Resources</b>	<b>\$ 174,755</b>	<b>\$ 198,989</b>	<b>\$ (24,234)</b>	<b>-12%▼</b>

The Department’s budgetary resources, both discretionary and mandatory, were \$175 billion for FY 2022. The authority was derived from \$66 billion in authority carried forward from FY 2021, appropriations of \$98 billion, approximately \$11 billion in collections, and \$4 million in borrowing authority. Budgetary resources decreased approximately \$24 billion from FY 2021. This is mainly due to a decrease in the amount of appropriations received in FY 2022. Of the total budget authority available, the Department incurred a total of \$133 billion in obligations from salaries and benefits, purchase orders placed, contracts awarded, or similar transactions.



**Custodial Activities**

The Statement of Custodial Activity is prepared using the modified cash basis. With this method, revenue from cash collections is reported separately from receivable accruals, and cash disbursements are reported separately from payable accruals.

Cash Collections (\$ in millions)	FY 2022	FY 2021	\$ Change	% Change
Duties	\$ 104,624	\$ 85,466	\$ 19,158	22%▲
Excise Taxes	4,629	4,773	(144)	-3%▼
Other	2,366	1,905	461	24%▲
<b>Total Cash Collections</b>	<b>\$ 111,619</b>	<b>\$ 92,144</b>	<b>\$ 19,475</b>	<b>21%▲</b>

Custodial activity includes the revenue collected by the Department on behalf of others, and the disposition of that revenue to the recipient entities. Non-exchange revenue is either retained by the Department to further its mission or transferred to Treasury’s general fund and other federal agencies. The Department’s total cash collections is \$112 billion, which is a \$19 billion increase from FY 2021 mainly due to an increase in import activity and collections of customs duties.



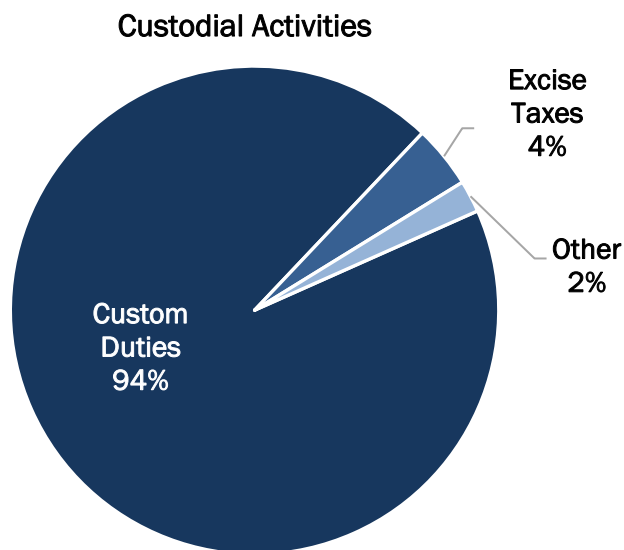


## Management's Discussion and Analysis

Custom duties collected by CBP account for 94% of total cash collections. The remaining 6% is comprised of excise taxes, user fees, and various other fees.

### Stewardship Information

Stewardship investments are substantial investments made by the Federal Government for the benefit of the Nation. When incurred, stewardship investments are treated as expenses in calculating net cost, but due to materiality, they are separately reported to highlight the extent of investments that are made for long-term benefit. The Department's expenditures (including carryover funds expended in FY 2022) in human capital, research and development, and non-federal physical property are shown below.



### Investments in Research and Development

Investments in research and development represent expenses incurred to support the search for new or refined knowledge and ideas. The intent of the investment is to apply or use such knowledge to improve and develop new products and processes with the expectation of maintaining or increasing national productive capacity or yielding other future benefits. S&T major research and development programs include the Wildland Firefighter Respirator (WFFR) that protects firefighters' lungs from toxic gases, a 3D X-Ray that enables DHS personnel to safely detect hidden explosive devices, and a system of ground and aerial autonomous vehicles that allows responders to deliver emergency aid and communicate with civilians in high-risk locations. CWMD, S&T, and USCG investments in research and development this fiscal year (in millions) are as follows:

Components	FY 2022	FY 2021
CWMD	\$ 74	\$ 70
S&T	846	827
USCG	4	8
<b>Total Research &amp; Development</b>	<b>\$ 924</b>	<b>\$ 905</b>

### Investments in Human Capital

Investments in human capital include expenses incurred for programs to educate and train first responders. These programs are intended to increase or maintain national productive capacity as evidenced by the number of responders trained over the course of the programs. FEMA and S&T investments in human capital (in millions) are as follows:

Components	FY 2022	FY 2021
FEMA	\$ 108	\$ 86
S&T	4	3
<b>Total Human Capital</b>	<b>\$ 112</b>	<b>\$ 89</b>



### **Investments in Non-Federal Physical Property**

Investments in non-federal physical property are expenses included in the calculation of net cost incurred by the reporting entity for the purchase, construction, or major renovation of physical property owned by state and local governments, which includes security enhancements to airports. TSA investments in non-federal physical property (in millions) are as follows:

<b>Components</b>	<b>FY 2022</b>	<b>FY 2021</b>
TSA	\$ 128	\$ 188
<b>Total Non-Federal Physical Property</b>	<b>\$ 128</b>	<b>\$ 188</b>

### ***Other Key Regulatory Requirements***

For a discussion on DHS's compliance with the Prompt Payment Act and Debt Collection Improvement Act of 1996, see the Other Information section.

### ***Climate-Related Risks***

For a discussion on DHS's efforts taken or planned to assess, measure, and mitigate any significant climate-related risks, see the Other Information section.



## Analysis of Systems, Controls, and Legal Compliance

### Secretary's Assurance Statement

November 14, 2022



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. These objectives are satisfied 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 controls over operations, internal controls over reporting, and internal controls over compliance were operating effectively as of September 30, 2022, except for the disclosures noted in subsequent sections.

Pursuant to the *DHS Financial Accountability* (FAA), the Department is required to obtain an opinion on its internal controls over financial reporting. The Department conducted its assessment of the effectiveness of internal controls over financial reporting in accordance with OMB Circular A-123 and 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 controls over financial reporting were designed and operating effectively, except for aspects of Financial Reporting, Budgetary Accounting, Insurance Liabilities, and Information Technology Controls and Information Systems, 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 launched a multi-year financial systems modernization program.

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 planning for remediation and additional improvements going forward, as highlighted in the Management Assurances section of the Agency Financial Report.

Sincerely,

Alejandro N. Mayorkas  
Secretary of Homeland Security



**Management's Report on Internal Controls Over Financial Reporting**

November 14, 2022

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 controls 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 accepting accounting principles. An organization's internal controls over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the entity; (2) 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 (3) 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 controls over financial reporting. Management assessed the effectiveness of DHS's internal controls over financial reporting as of September 30, 2022, 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, 2022, DHS's internal controls over financial reporting are effective except for areas of material weakness in Financial Reporting, Budgetary Accounting, Insurance Liabilities, and Information Technology Controls and Information Systems. Specifically:

- 1) *Financial Reporting*: Ineffective monitoring of reports used in financial reporting controls, ineffective service provider monitoring, and other conditions.
- 2) *Budgetary Accounting*: Ineffective controls and monitoring of budgetary resources to include undelivered orders, new obligations incurred, and the reimbursable authority related to unfilled customer order.
- 3) *Insurance Liabilities*: Ineffective design and implementation of controls over the data used in and the review of the valuation approach of the flood insurance liabilities.
- 4) *Information Technology Controls and Information Systems*: Ineffective controls in financial management systems, including those performed by service organizations, and insufficient design of controls over information derived from systems.

Internal controls over financial reporting have inherent limitations. Internal controls over financial reporting constitutes a process that involves human diligence and compliance and is subject to human error. Internal controls over financial reporting can also be circumvented by collusion or improper management override. Because of their inherent limitations, internal controls 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.

Challenges have been faced this year given the transition of the United States Coast Guard from a legacy core accounting system and the late fiscal year impact and FEMA response due to Hurricane Ian. However, the transition to the modernized financial system will have innumerable benefits for the United States Coast Guard financial operations and reporting going forward. In addition, FEMA maintains focus on Hurricane Ian response and supported these efforts financially through grants, disaster loans, and flood insurance payments. 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.

Best Regards,

A handwritten signature in blue ink that reads "Alejandro N. Mayorkas".

Alejandro N. Mayorkas  
Secretary

A handwritten signature in blue ink that reads "Stacy Marcott".

Stacy Marcott  
Senior Official Performing the Duties of the  
Chief Financial Officer



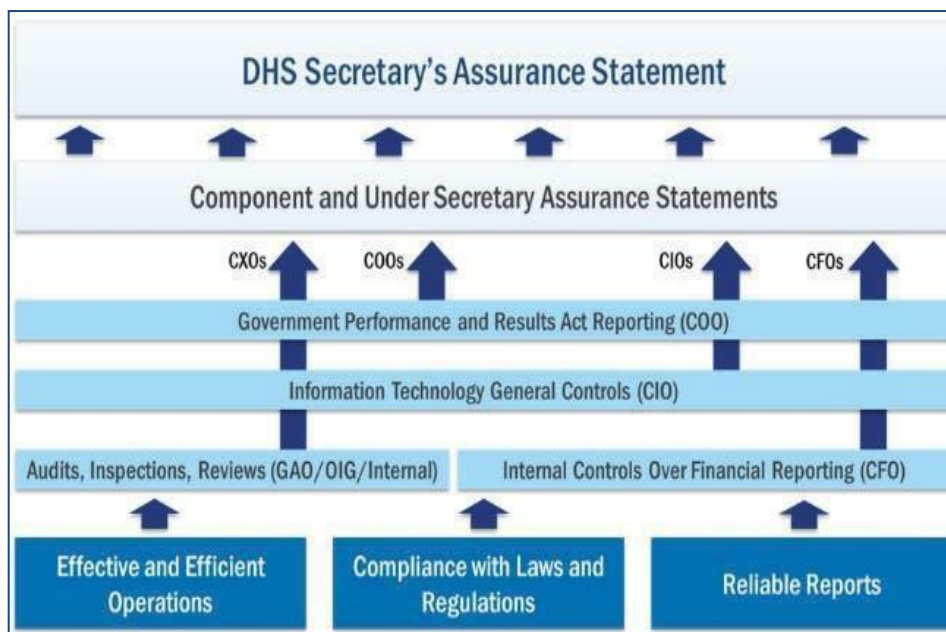
### **Management Assurances**

DHS management is responsible for establishing, maintaining, and assessing internal controls to provide reasonable assurance that the objectives of the Federal Managers' Financial Integrity Act (FMFIA) of 1982 (31 United States Code 3512, Sections 2 and 4) and the Federal Financial Management Improvement Act of 1996 (P.L. 104-208) were achieved. In addition, the DHS Financial Accountability Act (P.L. 108-330) requires a separate management assertion and an audit opinion on the Department's internal control over financial reporting.

The FMFIA requires GAO to prescribe 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. These objectives and related risks can be broadly classified into one or more of the following categories:

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

FMFIA also requires OMB, in consultation with GAO, to establish guidelines for agencies to evaluate their systems of internal control to determine FMFIA compliance. OMB Circular 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. FMFIA also requires the Statement of Assurance to include assurance on whether the agency's financial management systems substantially comply with government-wide requirements. The financial management systems requirements are directed by Section 803(a) of the FMFIA and Appendix D to OMB Circular A-123, Compliance with the Federal Financial Management Improvement Act of 1996.





## Management's Discussion and Analysis

In accordance with OMB Circular A-123, 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 programmatic operations, reliability of reporting, and compliance with laws and regulations. Per OMB Circular 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 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.

DHS is building on the enterprise risk management framework per OMB Circular A-123 and has established a Department-wide Enterprise Risk Management (ERM) working group to facilitate and promote Component development and maturation of ERM capability. DHS Components are at different stages of ERM maturity and some Components have begun embedding the ERM framework into their statement of assurance process. For FY 2022, Components completed operational risk registers to document risks identified and prioritized under the ERM framework. The Department will continue to mature in ERM capability and integrate its internal controls, as appropriate, and will continue to update the Department's risk profile annually.

### **Department of Homeland Security Financial Accountability Act (DHS FAA)**

Pursuant to the DHS FAA, the Department must obtain an opinion over internal control over financial reporting. Annually, the Deputy Secretary issues a memorandum to Component Heads on audit results and approach, asking senior leaders across the organization to fix long-standing issues and properly resource both remediation and assessment efforts. Senior leaders across the organization emulate this top-down approach by committing to annual remediation goals and improving the internal control environment, validated through testing, and finally ensuring that proper resources are available to realize these plans. Senior leaders also track, monitor, and discuss progress against commitments throughout the year to ensure accomplishment of the overall objectives.

Using the GAO Green Book and OMB Circular A-123 as criteria, the Department's internal control over financial reporting methodology is a risk-based, continuous feedback approach centered around four phases: find, fix, test, and assert. Effectiveness of controls and status of each Component's implementation of the internal control strategy are communicated and reported to senior leaders using the Internal Control Maturity Model (ICMM). The ICMM is a five-tiered model that uses tests of design and effectiveness, quality of assessments, and timeliness and efficacy of remediation as primary drivers in demonstrating maturation of the control environment. The Department's goal is to have most Components placed on the Standardized (third) tier, which informs leaders that quality internal control assessments are performed to validate conditions related to areas of material weakness do not exist and that there be minimal, if any, external financial statement audit surprises. This assessment and reporting strategy support sustainment of the financial statement opinion and eventual achievement of an opinion over internal control over financial reporting.

### **Areas of Material Weakness Resolution Status**

In FY 2021, management reported two areas of material weaknesses: 1) Financial Reporting and 2) IT Controls and System Functionality. In FY 2022, DHS continued the ongoing remediating over these known areas of material weaknesses and worked to resolve financial reporting



## Management's Discussion and Analysis

deficiencies through targeted remediation. In FY 2022, the USCG underwent a major financial systems modernization effort that included transitioning to a new financial management system, the Financial Systems Modernization Solution (FSMS), in December 2021. Transition to a modernized financial system will have innumerable benefits for USCG financial operations and reporting going forward. However, challenges with the initial USCG transition to FSMS from the legacy application has had substantial impacts to many of the Component's business processes. As a result, internal control over financial reporting deficiencies were identified and reported in FY 2022. In addition, the late fiscal year landfall of Hurricane Ian has resulted in FEMA response to assist the impacted region. Despite timing challenges, FEMA maintains focus on Hurricane Ian response and continues to support these efforts financially through grants, disaster loans, and flood insurance payments. In FY 2022, DHS management is reporting four areas of material weaknesses: 1) Financial Reporting, 2) Budgetary Accounting, 3) Insurance Liabilities, and 4) IT Controls and System Functionality. DHS has begun remediation of these deficiencies with efforts continuing in FY 2023. Refer to the tables below for areas contributing to the noted areas of material weakness along with appropriate corrective actions planned.





**Table 1: Internal Control over Financial Reporting Deficiency Details and Corrective Actions – Financial Reporting**

Area of Material Weakness	DHS Component(s)	Year Identified	Target Correction Date
	All	FY 2003	FY 2024
Financial Reporting	<p>Multiple deficiency areas exist that are attributed to the Financial Reporting area of material weakness, which include the following:</p> <ul style="list-style-type: none"> <li>• <i>Information Used in Controls</i> (Contributing Component(s): All)  <u>Deficiency Details</u> <ul style="list-style-type: none"> <li>○ Ineffective monitoring over information utilized in DHS internal control over financial reporting processes and control activities.</li> </ul> <u>Planned Corrective Actions</u> <ul style="list-style-type: none"> <li>○ DHS continues to implement a multi-phased, risk-based approach for identifying and assessing Information Used in Controls.</li> </ul> </li> <li>• <i>Service Provider Monitoring</i> (Contributing Component(s): All)  <u>Deficiency Details</u> <ul style="list-style-type: none"> <li>○ 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 Service Organization Control (SOC) reports related to financial services.</li> </ul> <u>Planned Corrective Actions</u> <ul style="list-style-type: none"> <li>○ DHS continues to implement process improvements utilizing a risk-based approach to provide effective monitoring and oversight of service providers.</li> </ul> </li> <li>• <i>Other</i> (Contributing Component(s): All)  <u>Deficiency Details</u> <ul style="list-style-type: none"> <li>○ Deficiencies aggregated to substantiate inclusion into this area of material weakness, including 1) journal entries, 2) funeral assistance grants accruals (FEMA), 3) application controls, 4) intragovernmental trading partner activity reporting due to system limitations (USCG), 5) payment management reporting (USCG), 6) property management reporting (USCG); and 7) military payroll reporting (USCG).</li> </ul> <u>Planned Corrective Actions</u> <ul style="list-style-type: none"> <li>○ Process improvements for journal entries will be developed, implemented, and assessed in accordance with remediation plans. USCG migrated to a new Oracle based financial system in FY 2022 that will significantly reduce the volume and amount of manual journal entries processed by USCG going forward.</li> <li>○ FEMA will strengthen internal controls to identify, analyze, and respond to material changes in programs that may impact financial reporting, including the recording of liabilities in accordance with Federal Financial Accounting Standards, as necessary.</li> <li>○ For efforts associated with application controls, please refer to the IT Controls and Information Systems area of material weakness and corrective actions for more detail.</li> <li>○ DHS is in the process of implementing G-Invoicing which is planned to reduce the risk of system limitations associated with federal trading partners going forward.</li> <li>○ USCG is continuing to partner with the FSMS team to remediated and resolve challenges that were faced due to the system migration in FY 2022. In addition, USCG processes and associated documentation will be updated to accurately reflect the new operational environment with training provided, as necessary.</li> </ul> </li> </ul>		



**Table 2: Internal Control over Financial Reporting Deficiency Details and Corrective Actions – Budgetary Accounting**

Area of Material Weakness	DHS Component(s)	Year Identified	Target Correction Date
Budgetary Accounting	FEMA, USCG, USSS	FY 2022	FY 2023
<p>Multiple deficiency areas exist that are attributed to the Budgetary Accounting area of material weakness, which include the following:</p> <ul style="list-style-type: none"> <li>• <i>Budgetary Resource Management Monitoring</i> (Contributing Component(s): FEMA, USCG, and USSS)               <p><u>Deficiency Details</u></p> <ul style="list-style-type: none"> <li>○ Insufficient FEMA review and approval of the TAFS in order to identify and correct errors for budgetary resources monitoring and associated postings accompanied by insufficient implementation of the SF-132 to SF-133 reconciliation process.</li> <li>○ In FY 2022, USCG was unable to properly oversee budget execution, including the reconciliation and monitoring of budgetary resources to include validating the completeness and accuracy of undelivered orders and review of expenditure activity.</li> </ul> <p><u>Planned Corrective Actions</u></p> <ul style="list-style-type: none"> <li>○ FEMA and USCG will implement additional training to develop the knowledge, experience, and skill of personnel accompanied with enforced accountability.</li> <li>○ USCG will continue to partner with the FSMS team to establish, as necessary, additional system functionality to strengthen and enhance the ability for budgetary resources monitoring going forward.</li> <li>○ USSS continues to execute against prior year corrective actions related to undelivered order status reporting to ensure the accuracy and completeness of undelivered order classification and reporting.</li> </ul> </li> <li>• <i>New Obligations Incurred</i> (Contributing Component(s): USCG)               <p><u>Deficiency Details</u></p> <ul style="list-style-type: none"> <li>○ In FY 2022, USCG was unable to properly oversee budget execution, including the allocation and monitoring of budgetary resources to include validating the completeness and accuracy of undelivered orders for new obligations incurred.</li> </ul> <p><u>Planned Corrective Actions</u></p> <ul style="list-style-type: none"> <li>○ USCG will continue to partner with the FSMS team to establish, as necessary, additional system functionality to strengthen and enhance the ability for incurring and supporting new obligations as well the capacity for budgetary resources monitoring going forward.</li> <li>○ USCG will implement additional training to develop the knowledge, experience, and skill of personnel accompanied with enforced accountability.</li> </ul> </li> <li>• <i>Reimbursable Authority and Unfilled Customer Orders</i> (Contributing Component(s): USCG)               <p><u>Deficiency Details</u></p> <ul style="list-style-type: none"> <li>○ Lack of USCG structure and policy for reimbursable agreements and reimbursable authority related to unfilled customer orders.</li> </ul> <p><u>Planned Corrective Actions</u></p> <ul style="list-style-type: none"> <li>○ USCG will continue efforts to enhance reimbursable agreements and trading partner documentation.</li> </ul> </li> </ul>			



**Table 3: Internal Control over Financial Reporting Deficiency Details and Corrective Actions – Insurance Liabilities**

Area of Material Weakness	DHS Component(s)	Year Identified	Target Correction Date
Insurance Liabilities	FEMA	FY 2022	FY 2023
<p>Multiple deficiency areas exist that are attributed to the Insurance Liabilities area of material weakness, which include the following:</p> <ul style="list-style-type: none"> <li>• <i>Insurance Data and Process Assurances</i> (Contributing Component(s): FEMA)                             <ul style="list-style-type: none"> <li><u>Deficiency Details</u> <ul style="list-style-type: none"> <li>○ Lack of control over the National Flood Insurance Program (NFIP) financial data.</li> <li>○ Inadequate monitoring of NFIP service providers and the Write Your Own program</li> <li>○ Ineffective implementation of controls over the NFIP Claim Payments process.</li> </ul> </li> <li><u>Planned Corrective Actions</u> <ul style="list-style-type: none"> <li>○ FEMA will continue to design and implement policies and procedures within the Federal Insurance Mitigation Administration (FIMA).</li> <li>○ FIMA updated its NFIP legacy rating methodology through the implementation of Risk Rating 2.0 – Equity in Action. Beginning October 1, 2021, new policies were subjected to the new rating methodology and existing policyholders eligible for renewal were able to take advantage of immediate decreases in premiums. By April 1, 2023, all new and renewing policies will have been rated using Risk Rating 2.0.</li> <li>○ FEMA continues to utilize the NFIP PIVOT system to help facilitate and consolidate NFIP core business processes.</li> </ul> </li> </ul> </li> <li>• <i>Valuation of the Flood Insurance Liability</i> (Contributing Component(s): FEMA)                             <ul style="list-style-type: none"> <li><u>Deficiency Details</u> <ul style="list-style-type: none"> <li>○ Insufficient review of the valuation approach of the flood insurance liability.</li> </ul> </li> <li><u>Planned Corrective Actions</u> <ul style="list-style-type: none"> <li>○ FEMA will continue to design and implement policies and procedures within the Federal Insurance Mitigation Administration (FIMA).</li> </ul> </li> </ul> </li> </ul>			



**Table 4: Internal Control over Financial Reporting Deficiency Details and Corrective Actions – IT Controls and Information Systems**

Area of Material Weakness	DHS Component(s)	Year Identified	Target Correction Date
IT Controls and Information Systems	All	FY 2003	FY 2025
<p>Multiple deficiency areas exist that are attributed to the IT controls and system functionality area of material weakness, which include the following:</p> <ul style="list-style-type: none"> <li>• <i>Financial System Requirements</i> (Contributing Component(s): All)               <ul style="list-style-type: none"> <li><u>Deficiency Details</u> <ul style="list-style-type: none"> <li>○ The Federal Information Security Management Act (FISMA) mandates that federal agencies maintain IT security programs in accordance with OMB and National Institute of Standards and Technology guidance. The Department internal control assessment identified IT controls as a material weakness due to deficiencies surrounding general security and application controls. As a result of the noted deficiencies, the Department’s financial systems are unable to fully comply with the FFMA.</li> </ul> </li> <li><u>Planned Corrective Actions</u> <ul style="list-style-type: none"> <li>○ Components will continue to implement the find, fix, test strategy in FY 2023. The IT Commitment Letters, signed by both the respective CFO and the Chief Information Officer (CIO) leadership, require each Component to commit to testing as well as provide commitment to passing results for each system and control in scope.</li> <li>○ The DHS CFO, CIO, and Component leadership will support the Components in the design and implementation of internal controls in accordance with DHS policy requirements defined for CFO Designated Financial Systems.</li> </ul> </li> </ul> </li> <li>• <i>System Functionality / Information Derived from Systems</i> (Contributing Component(s): All)               <ul style="list-style-type: none"> <li><u>Deficiency Details</u> <ul style="list-style-type: none"> <li>○ Ineffective IT security control and inadequate application / functionality controls impact the ability for management to fully rely on system generated data and reports without putting the processes utilizing this information at risk. Currently, these deficiencies are directly associated with financial system requirement deficiencies.</li> </ul> </li> <li><u>Planned Corrective Actions</u> <ul style="list-style-type: none"> <li>○ Components will continue to improve and enhance IT security, as noted above for Financial System Requirements. As IT security enhances reliability, DHS will also work to incorporate the find, fix, test strategy to gain coverage over application / functionality controls.</li> <li>○ In FY 2023, in addition to fixing long-standing IT control weaknesses, DHS will continue to implement a risk-based strategy for identifying and testing IUC and/or information derived from systems. DHS will also establish an approach to assess the key functionality of systems that have sufficient IT security controls established.</li> </ul> </li> </ul> </li> <li>• <i>Service Provider Monitoring</i> (Contributing Component(s): All)               <ul style="list-style-type: none"> <li><u>Deficiency Details</u> <ul style="list-style-type: none"> <li>○ The Department did not maintain effective internal control related to service organizations, including the monitoring of Information Technology General Controls (ITGC) for external systems to ensure adequate reliance. DHS also identified weaknesses related to evaluating and documenting roles of service organizations, performing effective reviews of SOC reports, and addressing service provider risk in absence of SOC reports.</li> </ul> </li> <li><u>Planned Corrective Actions</u> <ul style="list-style-type: none"> <li>○ For service provider monitoring controls, DHS continues to build improvements utilizing a risk-based management program to provide monitoring and oversight of service providers.</li> </ul> </li> </ul> </li> </ul>			



**Federal Financial Management Improvement Act (FFMIA)**

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 United States Standard General Ledger 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.

DHS assesses financial management systems annually for compliance with the requirements of Appendix D to OMB Circular A-123 and other federal financial system requirements. In addition, available information from audit reports and other relevant and appropriate sources, such as FISMA 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 also 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 modernization efforts. The outcome of these efforts will efficiently enable the Department to comply with government-wide requirements and thus reduce the need for manual compensating controls.



**Table 5: Non-compliance Details and Corrective Actions – Federal Financial Management Improvement Act**

Area of Non compliance	DHS Component(s)	Year Identified	Target Correction Date
	All	FY 2003	FY 2025
FFMIA	<p>Multiple deficiency areas exist that are attributed to the FFMIA area of non-compliance, which include the following:</p> <ul style="list-style-type: none"> <li>• <i>Financial System Requirements</i> (Contributing Component(s): All)               <ul style="list-style-type: none"> <li><u>Non-compliance Details</u> <ul style="list-style-type: none"> <li>○ 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.</li> </ul> </li> <li><u>Planned Corrective Actions</u> <ul style="list-style-type: none"> <li>○ Refer to the corrective actions planned for the IT Controls and System Functionality area of material weakness.</li> </ul> </li> </ul> </li> <li>• <i>Federal Accounting and U.S. Standard General Ledger (USSGL) Requirements</i> (Contributing Component(s): CBP, FEMA, ICE, USCG*)               <ul style="list-style-type: none"> <li><u>Non-compliance Details</u> <ul style="list-style-type: none"> <li>○ CBP, FEMA, ICE, and USCG* noted that certain key systems are unable to produce transaction level activity that reconciles at the USSGL-level. USCG also reported a lack of compliance as its financial and mixed systems do not allow for financial statements and budgets to be prepared, executed, and reported fully in accordance with the requirements prescribed by the OMB, Treasury, and the Federal Accounting Standards Advisory Board.</li> </ul> </li> <li>* <i>USCG core accounting system is owned and managed by Management Directorate.</i></li> <li><u>Planned Corrective Actions</u> <ul style="list-style-type: none"> <li>○ DHS CFO and Components will continue to design, document, and implement compensating controls to reduce the severity of legacy system application / functionality limitations.</li> </ul> </li> </ul> </li> </ul>		

**Digital Accountability and Transparency Act of 2014**

Pursuant to OMB Circular A-123, Appendix A, Management of Reporting and Data Integrity Risk, the Department issued its updated Digital Accountability and Transparency Act of 2014 (DATA Act) Data Quality Plan on August 16, 2022. 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](https://www.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 government accountable for its stewardship over its assets.

Components assess the design and operating effectiveness of their respective DATA Act reporting processes and controls over consolidation and 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 2022, Federal Emergency Management Agency (FEMA) and the United States Coast Guard (USCG) experienced challenges associated with their DATA Act reporting. These challenges were compensated by DHS validation pre-check processes as well as regular oversight and metrics reporting. FEMA is in the process of updating necessary DATA Act feeder systems to enhance alignment in reporting the Disaster Emergency Fund Code (DEFC) data element in File C when reporting obligations and gross outlays amounts. The United States Coast Guard (USCG) recently implemented a new financial system and experienced delays in reporting DATA Act file C (financial transaction data).

To continue making improvements and enhancements to the Department's DATA Act reporting processes and controls, an enhanced Component corrective action plan process is maintained that: 1) addresses researching and correcting matching award identification numbers with non-matching obligation amounts; 2) identifies the root causes of timing issue misalignments; and 3) continuously tracks misalignments until corrective actions are completed.

### **Financial Management Systems**

Pursuant to the Chief Financial Officers Act of 1990, the DHS CFO is responsible for developing and maintaining agency accounting and financial management systems to ensure systems comply with applicable accounting principles, standards, and requirements with internal control standards. As such, the DHS CFO oversees and coordinates all the Financial Systems Modernization (FSM) efforts for the Department's core accounting systems.

Foundational tenets for the FSM programs are:

- Increase business process standardization across Components through efforts to define a common set of financial management business processes and then ensure that the Component business process re-engineering and modernization efforts reflect the DHS process standard.
- Implement standard financial data element structures, such as the DHS Accounting Classification Structure and Common Appropriation Structure, across Components to standardize reporting and reduce manual reporting processes and inconsistent data.
- Continue to plan and execute financial system modernization projects by migrating components to modernized platforms with integrated asset and procurement management systems that meet Department and government-wide requirements, reduce the need for manual processes, and strengthen internal controls. FSM projects should leverage existing infrastructure, shared services, and technologies such as cloud-based solutions to the extent possible, following guidance and lessons learned from previous attempts to integrate DHS Components' financial management systems.
- Lastly, after standardization and modernization has occurred, work to consolidate financial operations and transaction processing service centers, where cost effective.

DHS has established the FSM Joint Program Management Office (JPMO) to lead and manage all aspects of the FSM programs, in partnership with DHS Components. In March 2017, it was determined that DHS would transition the CWMD, TSA, and USCG FSM initiatives (known as the Trio) out of their current shared service provider environment and into a DHS-managed solution. This solution, known as the Financial Systems Modernization Solution (FSMS), delivers a standardized baseline for the Trio.

In late 2018, TSA and USCG resumed implementation efforts and the Department completed upgrading CWMD to the latest version of the solution in late 2019. TSA went live on the FSMS



platform in late 2020 and USCG went live in late 2021. Throughout 2022, DHS and USCG worked together to improve system performance, activate interfaces with key USCG feeder systems, and provide support and training to end users. These efforts are ongoing and will continue into 2023.

DHS is leveraging lessons learned from the TSA and USCG implementations, reducing risk in future migrations through deliberative approaches to program management, resource management, business process standardization, risk management, change management, schedule rigor, and oversight. Lessons learned from the Trio implementations will be further leveraged as the JPMO plans for Discovery efforts in FY 2022 for FEMA as well as ICE and its customer Components.<sup>3</sup>

In addition to the ongoing DHS FSM efforts, the DHS Office of Chief Information Officer (OCIO) has rapidly deployed a series of technical solutions to meet emerging priorities across the Department, as well as continuing to steadily introduce key programs for functional integration across the enterprise. In a joint effort with the Office of the Chief Financial Officer (OCFO), DHS OCIO has expanded the IT general control program to assist in the monitoring and management of the IT general controls for the Department.

Additionally, OCIO and OCFO jointly support Components in efforts to strengthen IT general controls, system security, and IT internal control environments. OCIO has expanded the Independent Verification and Validation capabilities of Component IT accountable parties to address remediation and has incorporated key recommendations from various audits and assessments in the OCIO Information Security Performance Plan. OCIO Compliance staff also meet on a regular basis with Component IT staff to address any Federal Information Security Modernization Act (FISMA) Scorecard deficiencies.

OCIO has enhanced the Plan of Action and Milestones (POA&M) monitoring program to ensure the completeness and quality of remediation activity and POA&M management. OCIO continues to develop remedial action plans and demonstrate sustained progress mitigating known vulnerabilities, based on risk, and hold Component IT remediation status meetings prioritizing the weaknesses with the greatest impact to the Department with appropriate Component executives.

For cybersecurity, the DHS Secretary has outlined a bold vision and implemented a roadmap for the Department's cybersecurity efforts to confront the growing threat of cyber-attacks, to drive action in the coming year, and to raise public awareness about key cybersecurity priorities. OCIO has implemented a Unified Cybersecurity Maturity Model framework to align cybersecurity spending and new cybersecurity capability requests to critical cybersecurity domains and current initiatives, further improving alignment between DHS and National Security Strategies. OCIO has prioritized the collaboration with all Components to focus on successful implementation of key cybersecurity initiatives such as Cloud Modernization, Zero Trust Architecture, DHS Supply Chain Risk Management program, DHS Cybersecurity Service Provider program, and hardening Identity and Credential Access Management capabilities within the Department. OCIO has also prioritized the integration of cybersecurity risk into the DHS ERM framework to ensure cybersecurity risk is incorporated into the DHS-wide ERM process. Finally, OCIO has formalized the DHS Chief Information Security Office Council to be the overarching governing body for the integration of cybersecurity operations across the varied Component missions organic to the Department.