



Homeland Security

FY 2021

Agency Financial Report

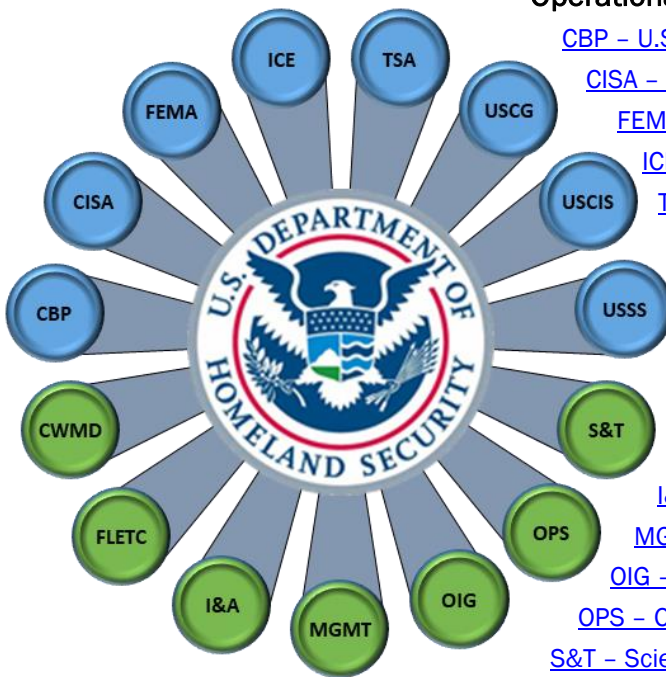


With honor and integrity, we will safeguard the American people, our homeland, and our values.

Connect with DHS

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](#)

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



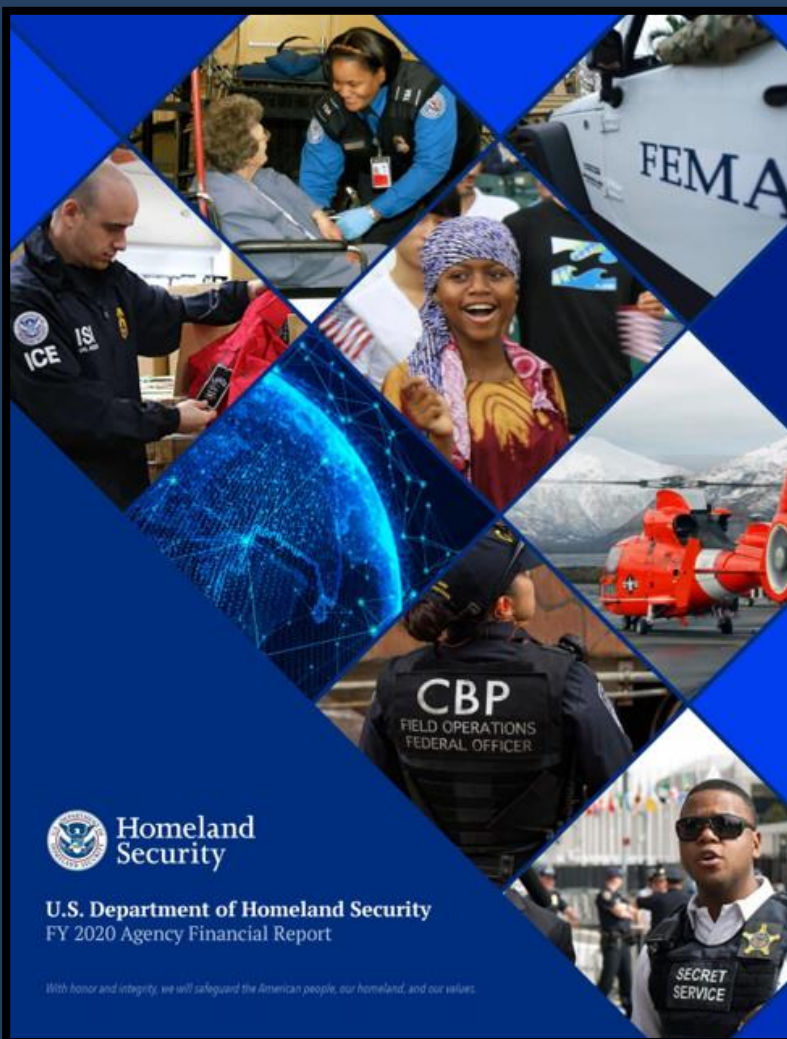
With honor and integrity, we will safeguard the American people, our homeland, and our values.

Certificate of Excellence in Accountability Reporting

In May 2021, DHS received its eighth consecutive Certificate of Excellence in Accountability Reporting (CEAR) from the Association of Government Accountants (AGA) for its Fiscal Year (FY) 2020 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 Excellent Presentation of Performance Results in an Agency Financial Report. This is the second time DHS has been awarded this Best-in-Class Award.

[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 Department of Homeland Security (DHS) Agency Financial Report for FY 2021 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 2021, the Department's Performance and Accountability Reports consist of the following three reports:


- DHS Agency Financial Report | Publication date: November 12, 2021.
- DHS Annual Performance Report | Publication date: February 7, 2022. The DHS Annual Performance Report is submitted with the Department's Congressional Budget Justification.
- DHS Report to our Citizens (Summary of Performance and Financial Information) | Publication date: February 15, 2022.

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





Table of Contents

	Message from the Secretary	iv
	Management’s Discussion and Analysis	1
	Our Organization	3
	Our Strategic Plan	5
	Performance Overview	6
	Financial Overview	32
	Secretary’s Assurance Statement	39
	Financial Information	51
	Message from the Chief Financial Officer	53
	Introduction	55
	Financial Statements	56
	Notes to the Financial Statements	64
	Independent Auditors’ Report	154
	Other Information	180
	Tax Burden/Tax Gap	182
	Combined Schedule of Spending	183
	Summary of Financial Statement Audit and Management Assurances	187
	Payment Integrity	189
	Grants Programs	209
	Civil Monetary Penalty Adjustment for Inflation	210
	Other Key Regulatory Requirements	217
	Office of Inspector General’s Report on Major Management and Performance Challenges Facing the Department of Homeland Security	218
	Appendix A: Acronyms	243
	Appendix B: Acknowledgements	246

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



Message from the Secretary

November 12, 2021



I am pleased to present the Department of Homeland Security's (DHS) Agency Financial Report for Fiscal Year 2021. 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.

Our mission statement - *with honor and integrity, we will safeguard the American people, our homeland, and our values* - is a constant reminder of our call to service. This year, we commemorated the 20th anniversary of the 9/11 terrorist attacks and remembered the victims, their families, and the heroes of that tragic day, some of whom made the ultimate sacrifice to save others. From the first responders who quickly organized rescue operations at Ground Zero, to local citizens banding together to provide relief, America unified in response to the attack that had tried to tear it apart.

Today, our Nation faces a range of diverse threats and challenges, and the Department is addressing them head on. DHS plays a leading role in battling the pandemic, securing the border and implementing our immigration laws, strengthening the Nation's cybersecurity, preventing violent acts of domestic extremism, building greater resilience and preparedness as the effects of climate change prove increasingly dramatic, welcoming our Afghan allies through our role as Lead Federal Agency coordinating Operation Allies Welcome, and so much more. Now the third largest department in the Federal Government, DHS was forged from more than 20 agencies and offices in response to the 9/11 attacks. And, while each agency of DHS has its own distinct history and traditions, we share the same values and the same mission.

As Secretary, I have seen firsthand how the women and men 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: <http://www.dhs.gov/performance-accountability>.

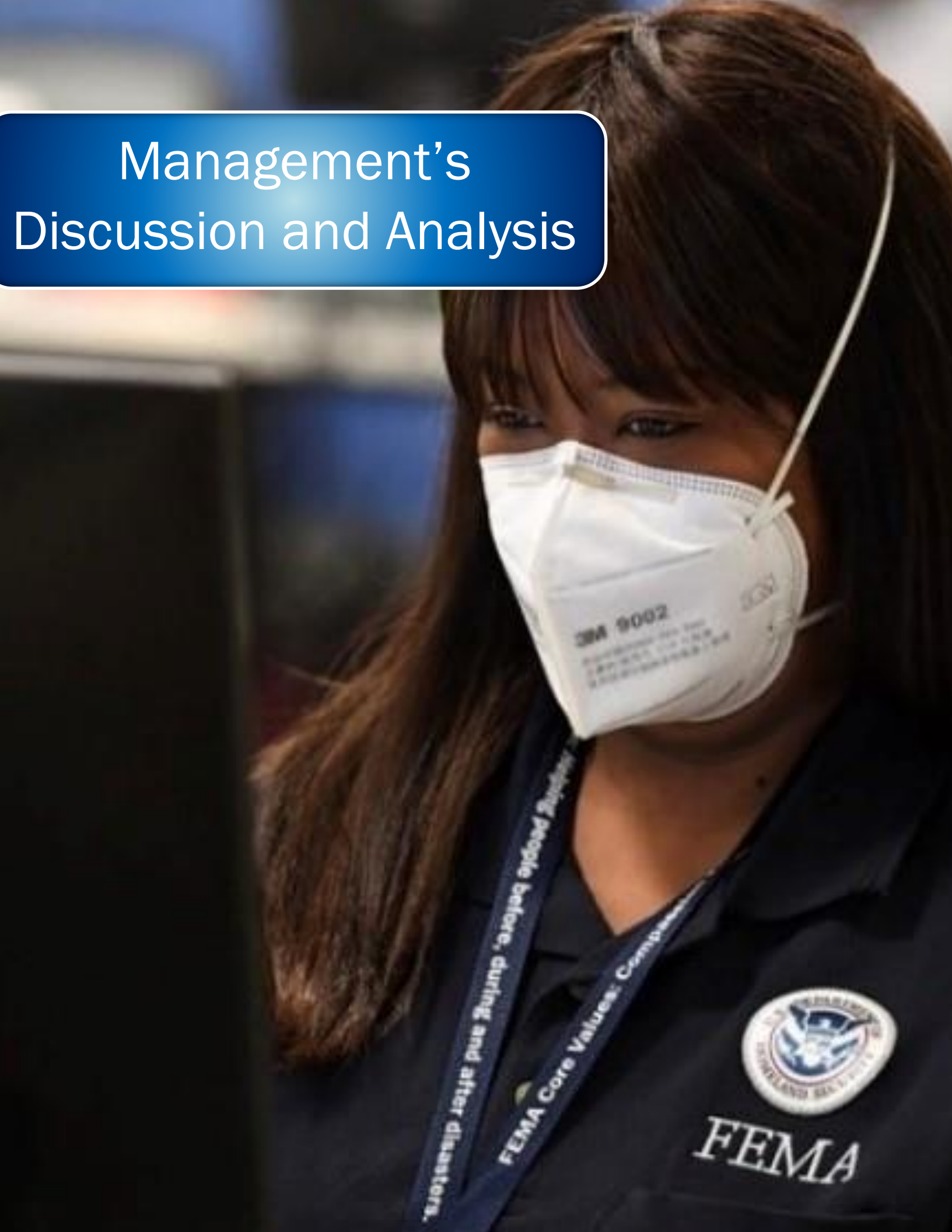
The Department's workforce continues to excel at safeguarding our assets, our Nation, and our values. We have much more to do, and we will succeed because of the immeasurable dedication and talent of the DHS workforce.

I am privileged to support our mission and those who enable it, and I am proud of what we have achieved.

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 Our Strategic Plan section displays the Department’s mission, goals and objectives.

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 Secretary’s Assurance Statement 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
Our Organization	3
Our Strategic Plan	5
Performance Overview	6
Financial Overview	32
Secretary’s Assurance Statement	39



Our 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 to emergency response, from cybersecurity analyst to chemical facility inspector. 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



U.S. Customs and Border Protection

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

CBP is responsible for securing America's borders to protect the United States against threats and prevent the illegal entry of inadmissible persons and contraband, while facilitating lawful travel and trade.



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

CISA leads the national effort to defend critical infrastructure against the threats of today, while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow.



FEMA

[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

[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.



U.S. Immigration and Customs Enforcement

[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 safeguards the Nation's financial infrastructure and payment systems to preserve the integrity of the economy, and protects national leaders, visiting heads of state and government, designated sites, and National Special Security Events.



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; federal employee and federal facility protection; 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 (HSE) 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; and leads the Department's Continuity of Operations, Continuity of Government, and critical infrastructure identification programs to enable the continuation of essential functions.



[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.



Our Strategic Plan (FY 2018 – FY 2022)

Mission: With honor and integrity, we will safeguard the American people, our homeland, and our values.

GOALS	OBJECTIVES
Counter Terrorism and Homeland Security Threats	<ul style="list-style-type: none"> • Collect, Analyze, and Share Actionable Intelligence • Detect and Disrupt Threats • Protect Designated Leadership, Events, and Soft Targets • Counter Weapons of Mass Destruction and Emerging Threats
Secure U.S. Borders and Approaches	<ul style="list-style-type: none"> • Secure and Manage Air, Land, and Maritime Borders • Extend the Reach of U.S. Border Security • Enforce U.S. Immigration Laws • Administer Immigration Benefits to Advance the Security and Prosperity of the Nation
Secure Cyberspace and Critical Infrastructure	<ul style="list-style-type: none"> • Secure Federal Civilian Networks • Strengthen the Security and Resilience of Critical Infrastructure • Assess and Counter Evolving Cybersecurity Risks • Combat Cybercrime
Preserve and Uphold the Nation's Prosperity and Economic Security	<ul style="list-style-type: none"> • Enforce U.S. Laws and Facilitate Lawful International Trade and Travel • Safeguard the U.S. Transportation System • Maintain U.S. Waterways and Maritime Resources • Safeguard U.S. Financial Systems
Strengthen Preparedness and Resilience	<ul style="list-style-type: none"> • Build a National Culture of Preparedness • Respond During Incidents • Support Outcome-Driven Community Recovery • Train and Exercise First Responders



Performance Overview

The Performance Overview provides an overview of our performance management framework, a summary of key performance measures, selected accomplishments, and 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 2021-2023 Annual Performance Report with the FY 2022 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.

DHS Performance Framework

The Department has a robust performance framework that drives performance management and enables the implementation of performance initiatives. This framework consists of core concepts and initiatives to assess program implementation progress, measure results, and drive the delivery of value to external stakeholders. The graphic shows these initiatives that come from both the *Government Performance and Results Act* (GPRA) of 1993, and its companion legislation, the *GPRA Modernization Act of 2010* (GPRAMA).

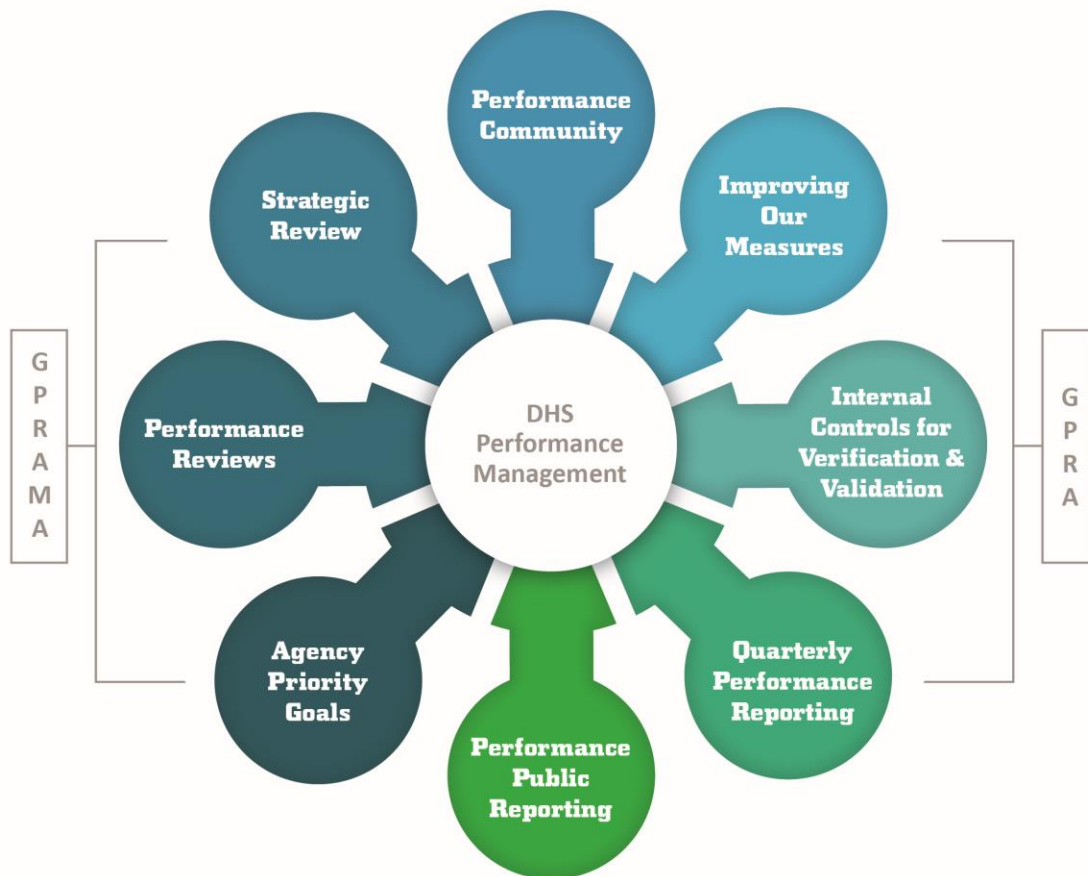


Figure 1: DHS Performance Management Framework



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 located under the DHS Chief Financial Officer (CFO) in the Management Directorate of DHS. The PIO, DPIO, and PA&E Performance Analysts are the liaison 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 the 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 communicating guidance and initiatives, provide advice on measure development concepts, collect and review measure results, and coordinate with Component leadership on performance management initiatives. Strategic Review Lead Assistants play a key role in managing Assessment Team efforts annually and refining and delivering key findings from the review process. Program managers across DHS Components are key contributors to the Strategic Review assessment, along with generating ideas for performance measures, producing measure data, and using the information to manage and improve operations.

Improving our Measures

With the support of leadership and our Components, PA&E initiates the annual measure improvement process to enhance our set of publicly reported measures to more effectively



convey the results delivered to stakeholders. Improvement ideas are derived from several sources:

- Feedback provided by senior leadership to mature our ability to describe the value delivered by DHS;
- Component leadership and program managers' desire to implement measures that are meaningful to current operations and goals;
- Suggestions from PA&E Performance Analysts working to fill gaps and improve quality;
- Suggestions from the Office of Management and Budget (OMB) to achieve greater visibility into program performance and connections to program resources; and
- Recommendations from other external stakeholders such as the Government Accountability Office (GAO) and Congress.



Figure 3: DHS Annual Measure Improvement Process

While measured improvement is iterative, we use the annual process to mature the breadth and scope of our publicly reported set of measures, as shown in the figure above. The process begins in the winter after implementing the new measures in the agency performance plan, to identify gaps that were not filled along with areas where improved measures are desired. Improvement efforts continue into the spring since it can take six to nine months to develop new measure concepts depending on the complexity and scope of data collection. Summer is the Department's review of Component proposals and discussions with OMB continue into the fall.



Internal Controls for Verification and Validation

The Department recognizes the importance of collecting complete, accurate, 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 place¹.

DHS has 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: 1) an annual measure improvement and change control process described in the previous section using the Performance Measure Definition Form; 2) a central information technology repository for performance measure information; 3) a Performance Measure Checklist for Completeness and Reliability used by Components to self-assess and rate their compliance with internal controls over performance information; and 4) annual assessments of the completeness and reliability of a sample of our performance measures by an independent review team.

Quarterly Performance Reporting

Quarterly reporting of the Department's strategic measures is provided by Component program managers, reviewed by Component managers and performance staff, entered into the Performance Management System, and then reviewed by PA&E performance staff. Components use the information to keep their leadership abreast of measure results and progress. PA&E also prepares a Quarterly Performance Report that has visualizations of select measure results over time, along with a trend report for all measures in the strategic and management sets. These reports are shared quarterly with PIO and DPIO, posted on the DHS intranet site, and are available to all DHS senior leaders and program managers to support on-going program management activities. Many Components have their own internal processes and products they use to 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 reports to communicate key financial and performance information to stakeholders:

¹ 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.



- DHS Agency Financial Report (this report);
- DHS Annual Performance Report; and
- DHS Summary of Performance and Financial Information (Citizen's Report).

Combined, these reports comprise our annual performance and accountability reporting requirements. When published, all three reports are located on our public website at [Performance & Financial Reports](#).

Agency Priority Goals

Agency Priority Goals (APGs) are one of the tenets of GPRAMA and provide a tool for senior leadership to drive the delivery of results on key initiatives over a two-year period. Quarterly reports of progress are provided to interested parties through the OMB website [Performance.gov](#) and information on the DHS APGs are presented in our Annual Performance Report.

Performance Reviews

DHS implemented Performance Reviews as a means for senior leadership to engage in the management of efforts to deliver performance results relevant to stakeholders. Meetings are held with APG Goal Leads, senior leaders, subject matter experts, and performance leadership and staff to discuss current results, progress, and challenges being faced by these complex issues.

Strategic Review

The Strategic Review (SR) is a DHS-wide assessment, using evidence, to assess program progress in delivering on our mission. In FY 2021, DHS conducted its eighth annual SR. Twenty-three mission programs were included in the assessment and represent our large operational programs delivering results to external stakeholders. The SR serves as a tool to integrate activities associated with other key legislation such as the *Foundations for Evidence-Based Policymaking Act of 2018*, the *Program Management and Accountability Improvement Act (PMIAA) of 2018*, and *OMB guidance regarding Enterprise Risk Management implementation*.

The SR serves multiple purposes for Components, DHS, and OMB to: 1) assess progress of our program implementation efforts as a means for improvement; 2) facilitate best practices of a learning organization by reflecting annually on where we have been and where we are going; 3) advance the use of risk, program management, and evaluation practices; 4) make key findings available to Component and DHS senior leaders to inform management efforts; 5) provide feedback from execution to planning, programming, and budgeting activities; 6) integrate evidence-building activities into the Strategic Review and other key planning processes; and 7) drive a focused conversation with OMB on significant issues to inform their management and budget activities.



DHS Summary of Key Performance Measures

Strategic plan goals are implemented by our mission 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. Mission programs have performance goals, performance measures, and performance targets. Below are a select set of measures that describe how our mission programs drive to deliver on the DHS mission.

Goal 1: Counter Terrorism and Homeland Security Threats

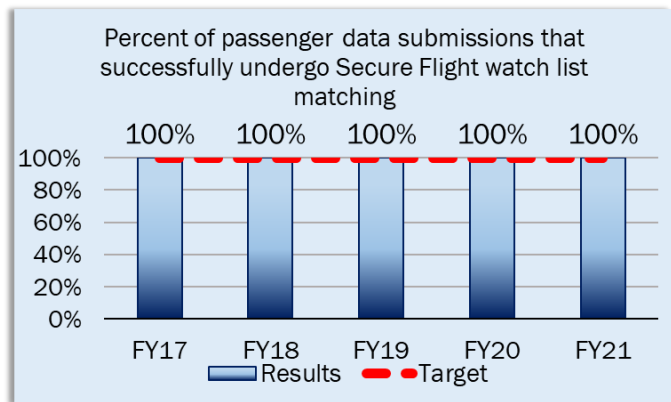
One of the Department's top priorities is to protect Americans from terrorism and other homeland security threats by preventing nation-states and their proxies who engage in terrorist or criminal acts from threatening the homeland. Terrorists and criminals are constantly adopting new techniques and sophisticated 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 a proactive response by DHS and its partners to identify, detect, and prevent attacks against the United States. Focused activities associated with this goal includes 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 sufficient passenger data to allow successful processing in the Secure Flight automated vetting system. In FY 2021, this measure achieved 100 percent, 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.

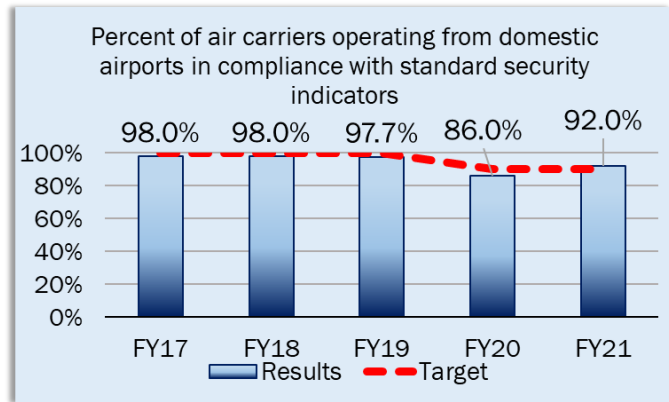




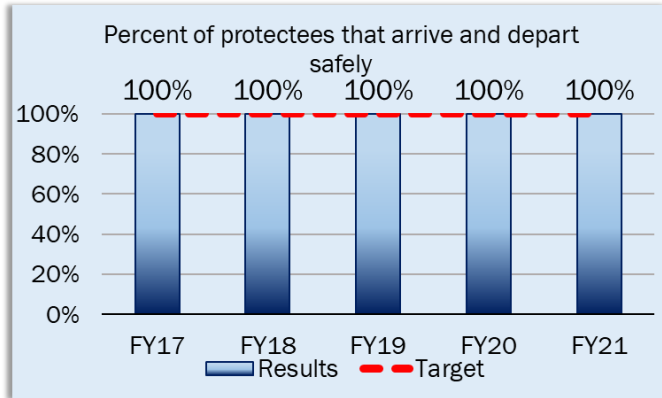
Percent of air carriers operating from domestic airports in compliance with standard security indicators (TSA):

Air carrier inspections can include one or more aspect of operations such as catering, cargo acceptance and aircraft searches and allow for improved collaborations, 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). The plan identifies the timeframe in which each inspection is conducted, based on the air carriers Inspection Frequency Score (IFS). The IFS is determined by a carrier's: 1) Risk register; 2) Compliance history (last 3 years); 3) Enforcement Investigative Reports (EIRs) (Administrative vs Civil Penalty); and 4) Local TSA office assessments/surveys. For FY 2021, a total of 12,077 inspections were conducted with 1,216 Findings, as COVID-19 affected overall planned inspection activity. TSA continually works with TSA-regulated entities implementing Outreach, Action Plans and Joint Testing to enhance security. Inspectors conduct inspections on an annual basis and can include one or more aspect of operations that an air carrier oversees such as catering, cargo acceptance and aircraft searches. The targets were lowered in FY 2020 and FY 2021 due to COVID-19.



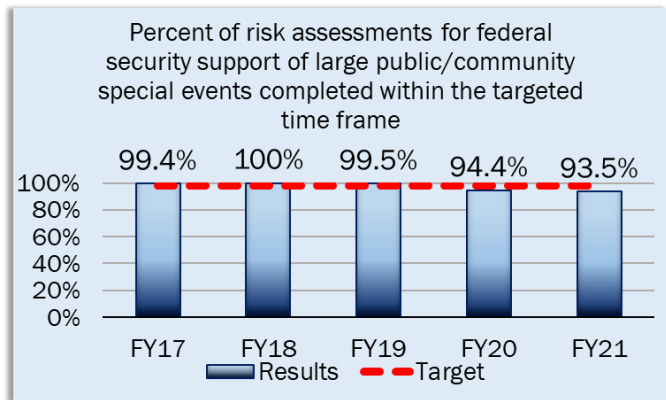
Congress allocated up to \$10M in FY 2018 for TSA to test and analyze perimeter intrusion and detection technologies. TSA's Multimodal Public Areas Capabilities (MPAC) formally partnered with a CAT I and CAT X in September 2019 through Other Transaction Agreements. In FY 2021, MPAC successfully completed the bidding and award phase to choose the installation vendors and began installation of the perimeter intrusion technologies.



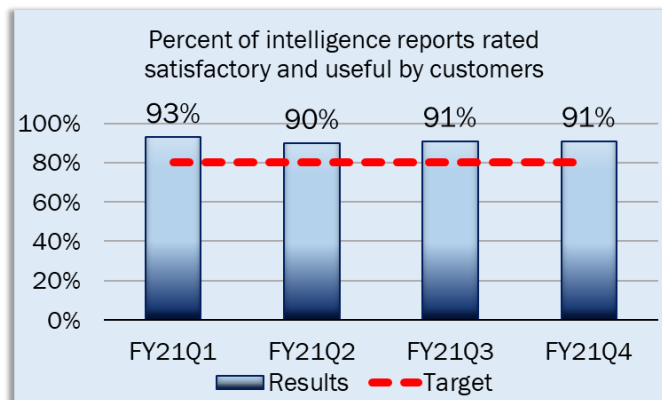
Percent of protectees that arrive and depart safely (USSS): This measure reflects the effectiveness of efforts to ensure safe travel (arrive and depart safely) for the President and Vice President of the United States and their immediate families, former presidents, their spouses, and their minor children under the age of 16, major presidential and vice-presidential candidates and their spouses, and foreign heads of state. In FY 2021, 4,710 protective visits occurred. The target is always 100 percent and the USSS

has achieved 100 percent of safe arrivals and departures for 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.

Percent of risk assessments for federal security support of large public/community special events completed within the targeted time frame (OPS): This measure indicates the timeliness of risk assessments that are used by federal agencies as criteria to determine their level of support to state and local events and is the primary federal awareness mechanism for special events occurring across the Nation. This measure indicates the percent of [Special Event Assessment Ratings](#) completed within the targeted timeframe as voluntarily requested from state and local authorities for events taking place within their jurisdictions.



OPS provided on-time risk assessment ratings 93.5 percent of the time, slightly lowered than previous year. Technology enhancements will support a more robust performance in the future as well as addressing issues related to surge activity.



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 2021, DHS intelligence reports were rated as satisfactory or higher resulting in a 91 percent rating, meeting the target. This was a new measure in the FY 2021 Performance Plan so there is no trend data.

Looking Forward

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

- **Aviation Security:** TSA continues to seek and deploy improvements to airport scanning and detection, with new technology to enhance explosives detection and other threat-detection capabilities at airport checkpoints. TSA has begun installing [computed tomography](#) scanners that apply sophisticated algorithms for the detection of explosives and create three-dimensional images that TSA

DID YOU KNOW?

The TSA "Red Team" covertly tests all aspects of aviation security including the TSA checkpoints at over 450 airports nationwide. In FY 2021, over 1500 tests were conducted. The Red Team awarded over 1,100 recognition awards to screening personnel who successfully prevented simulated attacks.

- officers can manipulate to analyze scanned images thoroughly. Additionally, TSA responded to COVID-19 by improving safety for officers and travelers through increased sanitation; distribution of Personal Protective Equipment to frontline workers; rapid deployment of acrylic shielding at checkpoints; modifying Credential Authentication Technology (CAT) to limit document exchanges; and reducing false alarm rates to require fewer pat-downs. Moving forward, TSA will establish a recapitalization acquisition program to address existing technologies that are near the end of their life while continuing to deploy Computed Tomography, Credential Authentication Technology, and other technology to improve detection capabilities. With regard to personnel and training, TSA plans to hire new Transportation Security Officers to keep pace with increased travel volume (Post-COVID-19).
- **Unmanned Aircraft 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 enable the delivery of drugs in remote areas. Additionally, 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 which includes:
 - A combined effort between CBP, CISA, USCG, and others to implement counter-UAS (CUAS) technologies to: enhance situational awareness along land and sea borders at and between Ports-of-Entry; enhance agencies' ability to share, query, and analyze law-enforcement information/data to advance investigations; deploy



improved tools to promote the safety and effectiveness of DHS personnel; improve the detection and tracking of low-altitude airborne threats; expand capabilities to integrate border-security sensor and intelligence sources; leverage data analytics; and share resulting actionable intelligence with partners across the homeland security enterprise.

- S&T will invest in research and development activities to understand how the department can better apply UAS advances to protect the American people, increase operational efficiencies, and improve command and control decision-making, especially when combined with [CUAS technologies](#).

Goal 2: Secure U.S. Borders and Approaches

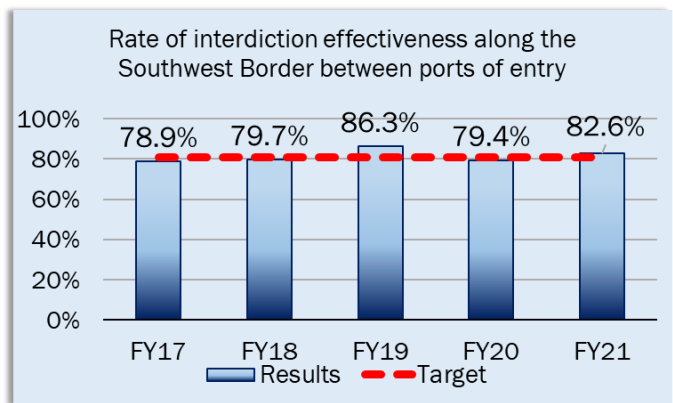
Secure borders are essential to our national sovereignty. DHS continues its efforts to secure and maintain control of our land and maritime borders. Concentration is also focused on Transnational Criminal Organizations and preventing the impact of these organizations

DID YOU KNOW?
 CBP's biometric seamless passenger experience can contribute to the reduction of travel health risks and to the recovery of the travel and tourism industry by mitigating the risk of pathogen transmission.

operating both domestically and internationally. Efforts also continue to pursue, and appropriately prosecute, those illegally in the interior of the country and 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 the past three years.



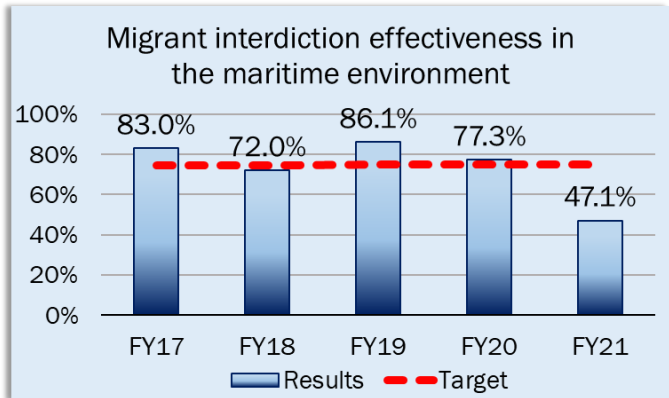
The interdiction rate has increased due largely to the unprecedented mass illegal migration of families and unaccompanied children that voluntarily surrendered to Border Patrol Agents. Improved detection and tracking tools resulted in better awareness of illegal crossing activity, but agents faced challenges to interdict evading groups often guided by criminal organizations. Since late March 2020, Border Patrol has been implementing the federal regulation entitled *Suspending Introduction of Persons from a Country Where a Communicable Disease Exists* (85 Fed Reg 17060), which provides for persons subject to the order to be expelled from the U.S. as expeditiously as possible under Title 42 of the U.S. Code, instead of being subjected to processing under Title 8 due to the ongoing pandemic, additionally lowering the interdiction



effectiveness rate. 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.

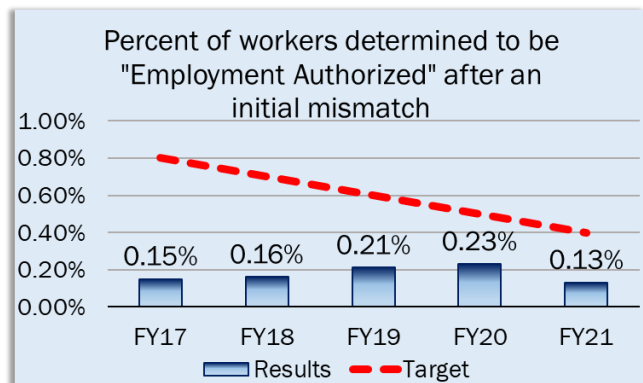
Migrant interdiction effectiveness in the maritime environment (USCG):

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 who were interdicted by the [USCG](#) and partner Nations 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. Over the past two years, an increase in partner Nation reporting efforts has allowed for better data collection and analysis. Partner Nation interdictions make up approximately 50 percent of the migrants interdicted in the maritime domain. There is not one factor that would conclusively indicate why the result is 47.1 percent in FY 2021; however, it is likely due to changing maritime migration patterns to include increased Haitian flow. USCG will continue to adjust patrol patterns to meet the changes in the migrant flow.



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 the system is effective in confirming employment eligibility and does not require manual intervention. USCIS continues to increase the records available for electronic matching, which strengthens the program against identity fraud.



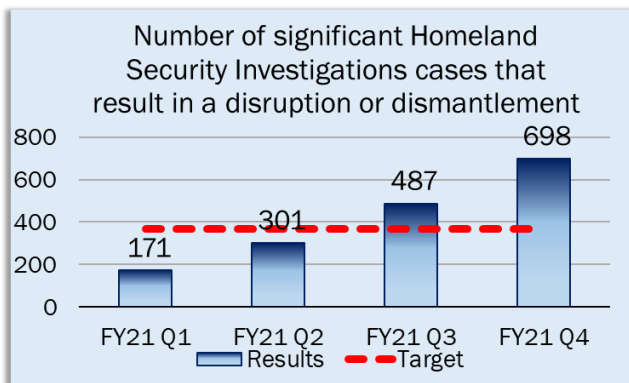


Management's Discussion and Analysis

Number of significant Homeland Security Investigation cases that resulted in a disruption or dismantlement (ICE):

This measure reports on the total cumulative number of significant transnational criminal investigations that resulted in a disruption or dismantlement. To be considered significant, the investigation must involve a high-threat transnational criminal organization engaged in criminal activity related to illicit trade, travel, or finance (both drug-related or non-drug-related); counter-terrorism; national security;

worksite enforcement; gangs; or child exploitation. "Disruption" is defined as impeding the normal and effective operation of the targeted organization. "Dismantlement" is defined as destroying the organization's leadership, financial base and network to the degree that the organization is incapable of operating and/or reconstituting itself. With the adoption of the new "Number of" measures, along with Significant Case Report (SCR) Program training, HSI special agents have a better understanding of HSI's Key Measure and are able to submit multiple disruptions and dismantlement toward SCR designated cases. The factors mentioned above have led to an increase in SCR submissions. Based on the above, HSI was able to meet its target for FY 2021.



Looking Forward

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

- **Border Security Operations:** CBP's top priority lies in keeping terrorists and their weapons from entering the U.S. while welcoming all legitimate travelers and commerce. The Border Security Operations program provides situational awareness; impedance and denial; and law enforcement response and resolution, securing the U.S. border between ports of entry. Since FY 2020, pandemic-driven efforts including the activation of Title 42 authorities, permitted the program to return most illegal crossers immediately on encounter, with no consequence. Changes in the composition of the cross-border flow have expanded non-interdiction tasks for agents, underscoring the critical importance of the program's new Border Patrol Processing Coordinator position. In addition, Border Patrol will continue employing best-available technology to improve situational awareness.
- **Homeland Security Investigations (HSI):** Homeland Security Investigations combats Transnational Criminal Organizations (TCOs) and the exploitation of systemic vulnerabilities in trade and immigration to thwart foreign terrorists and other criminals and organizations from endangering the American people. HSI continued "[Operation Stolen Promise](#)" in FY 2021, which targets pandemic-related fraud through the disruption of TCOs distributing counterfeit personal protective and medical equipment. In addition, HSI continued to coordinate with the Small Business Administration to combat financial fraud under the Coronavirus Aid, Relief and Economic Security Act. Next steps include an interagency dialog to establish a framework, set lines of responsibility, and avoid



duplicative efforts to develop a whole-of-government strategy to counter criminal and terrorist threats. Lastly, ICE has begun to look at a five-year plan for the Innovation Lab to implement new digital technology and open-source data techniques in support of HSI's efforts.

- **Remove those who have entered the country illegally** 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. The pandemic led to a dramatic increase in litigation challenges requiring intensive OPLA litigation in defense of agency authorities. To manage this workload, OPLA, ERO, and the Department of Justice have increased collaboration to improve processing while simultaneously addressing OPLA staffing models to align with the Executive Office for Immigration Review's docket, staffing, and expansion of court facilities to address case backlog.



In May 2021, U.S. Border Patrol agents from Rio Grande Valley Sector's Kingsville Station used a small unmanned aircraft system (sUAS) to locate a lost undocumented migrant in need of help. The agent operating the drone quickly transmitted the location to a U.S. Border Patrol paramedic, whose immediate response stabilized the patient suffering a diabetic emergency.



- **E-Verify** USCIS' E-Verify program is a web-based system that allows enrolled employers to confirm the eligibility of their employees to work in the United States. The program continued to offer employment verification services seamlessly during the pandemic and adapts to the public health and other needs while working closely with Government and industry partners. E-Verify deployed a new Customer Relationship Management platform that improved case management, workload tracking, outreach and engagement, as well as a Verification Information System data reporting warehouse for constant, accurate and timely reporting. Looking forward, the program plans to complete the retirement of legacy E-Verify components to reduce maintenance costs and enable accelerated process modernization. The program will continue enhancing the document upload capability in E-Verify to streamline manual processing of cases through FY 2022. This capability allows employees to electronically submit documents to resolve data mismatches.

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. 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 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 Department's Cybersecurity and Infrastructure Security Agency (CISA) advised TSA on cybersecurity threats to the pipeline industry, as well as technical countermeasures to prevent those threats, in response to the Colonial Pipeline cyber-attack, DHS's Transportation Security Administration (TSA) announced the issuance of a second Security Directive that requires owners and operators of TSA-designated critical pipelines that transport hazardous liquids and natural gas to implement a number of urgently needed protections against cyber intrusions, including specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems, develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review.

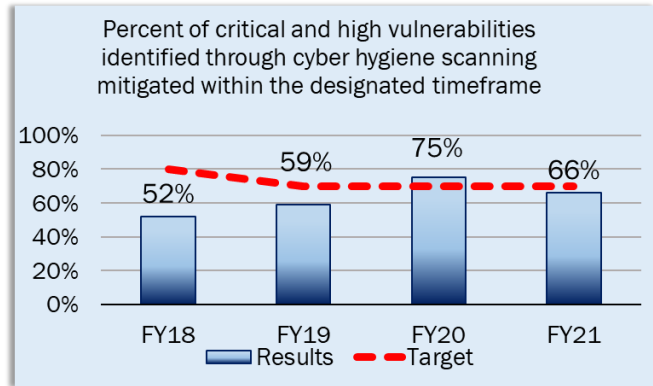
The following measures highlight some of our efforts to secure federal cyberspace and critical infrastructure. Up to five years of data is presented if available.



Percent of critical and high vulnerabilities identified through cyber hygiene scanning mitigated within the designated timeframe (CISA):

DHS provides cyber hygiene scanning to Federal Civilian Executive Branch (FCEB) agencies to aid them in identifying and prioritizing vulnerabilities based upon severity, which in turn enables FCEB agencies to make risk-based decisions regarding their network security posture. For “critical” vulnerabilities, mitigation is required within 15 days from point of initial detection; for

“high” vulnerabilities mitigation is required within 30 days of initial detection. Timely identification and mitigation of network vulnerabilities is a critical component of an effective cybersecurity program, and paramount to maintaining the integrity and operational availability of systems. With Binding Operational Directive 19-02 in effect since April 2019, FCEB agencies have demonstrated improved progress in mitigating “critical” and “high” vulnerabilities within mandated timelines. In turn, the FY 2021 result was 66 percent. Collectively, these mitigation efforts have contributed to an overall trend of improvement for the FCEB Enterprise, and DHS continues to work with agencies on achieving even higher rates of timely mitigation.



WHAT IS 5G?
FASTER.
MORE SECURE.
MORE CONNECTIVE.

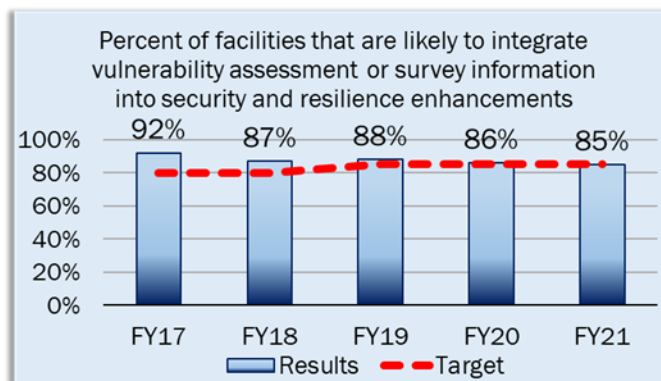
In FY 2021, the NRMCMC's 5G team, in coordination with the National Security Agency (NSA), and the Office of the Director of National Intelligence (ODNI), released the Potential Threat Vectors to 5G Infrastructure paper. This paper identifies and assesses risks and vulnerabilities introduced by 5G and includes a technical review of the types of threats posed by 5G adoption in the United States and sample scenarios of 5G risks.



Management's Discussion and Analysis

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, 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. Current year's results are consistent with the five-year trend.



Looking Forward

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

- **Improve cybersecurity posture of federal enterprise network:** CISA continues to defend and secure the federal enterprise network, systems, and assets against a spectrum of risks. The agency has advanced the security of federal networks. However, strategies are lacking for managing and securing the federal cloud environments and software updates. Insufficient information about specific cyber events impairs the program's ability to assess mission and strategic risks adequately. Looking forward, CISA plans to improve the quality of new hires and the flow of the hiring process to address long-standing needs, increase analytical staffing to improve situational awareness and increase trust with state, local, tribal, and territorial governments and communities; improve shared situational awareness, bi-lateral communications, and increased visibility into critical infrastructure.
- **Infrastructure Security:** CISA coordinates the national effort to secure the Nation's critical infrastructure. The infrastructure security mission is a continuous national effort to identify critical cyber and physical systems and assets, to understand their vulnerabilities—especially against terrorism, and intentional cyber threats, and to take action to reduce risks. There is a need to develop sustained architecture for managing the Sector Risk Management Agencies' structure and responsibilities. The lack of long-

DID YOU KNOW?

The National Defense Authorization Act of 2021 requires that DHS execute National Cyber Exercises. Cyber Storm, the Nation's biennial capstone cybersecurity exercise sponsored by CISA, satisfies this legislative requirement, and Cyber Storm VIII, scheduled for spring 2022, will be the first iteration of the exercise conducted under this legislation.



term authorization for the [Chemical Facility Anti-Terrorism Standards](#) (CFATS) program inhibits the ability for facilities to engage in longer term strategic planning, make large capital investments, and retain talent. Looking forward, the program has engaged the National Security Council on potential successor policy directives to Presidential Policy Directive-21, plans to deliver a National Infrastructure Protection Plan, and is seeking policy solutions for possible chemical facilities of interest and non-regulated facilities. Finally, the program has considered implementing a revised CISA Gateway, which the agency could expand and integrate with common data platforms to deliver multiple services.

- **National Risk Management Center (NRMC):** Critical infrastructures include those assets, systems, and networks that provide functions necessary for our way of life. From generating electricity to supplying clean water, DHS monitors [16 critical infrastructure sectors](#) that form a complex, interconnected ecosystem, including communications, energy, transportation, emergency services, and water. The NRMC works closely with the private sector which owns and operates the nation's critical infrastructure and industry, working together in the governments shared management of risk. As the Department's planning, analysis, and collaboration center, the [NRMC](#) works to convene the private sector, government agencies, and other key stakeholders together to identify, analyze, prioritize, and manage the most significant risks to our critical infrastructure. Moving forward, the NRMC will continue to build a capability roadmap that will baseline current capabilities, identify infrastructure-security capability gaps, outline a 5-year strategy to address those gaps, address the needed authorities to allow for increased coordination and collaboration with the risk community, and develop training programs to serve as a career roadmap for analysts and build a full spectrum of leadership training opportunities.

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 navigation for boats/ships, and protection of the nation's financial systems.

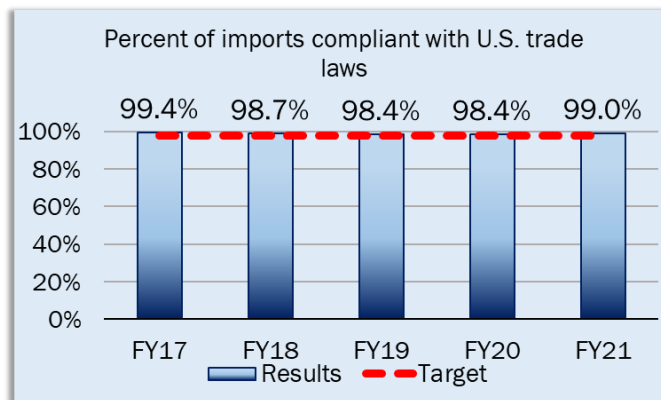
The following measures highlight some of our efforts to preserve and uphold the nation's prosperity and economic security. Up to five years of data is presented if available.



Management’s Discussion and Analysis

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. 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 responsibility to maximize compliance with



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 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 2021 results in-line with recent trends. While the expansion of e-commerce has led to greater trade facilitation, its overall growth has facilitated 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.

WITHHOLD RELEASE ORDER

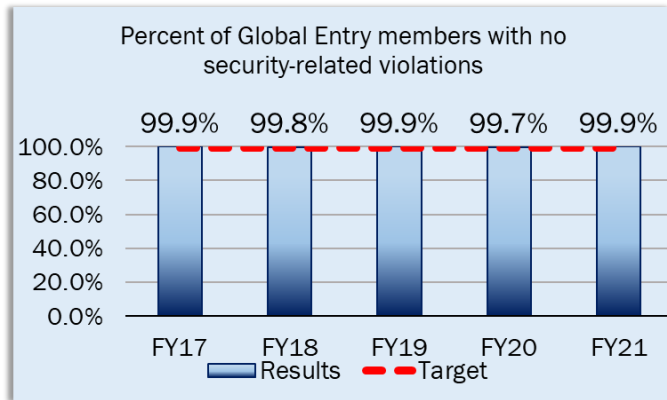
on cotton products and tomato products produced in China’s Xinjiang Uyghur Autonomous Region



U.S. Customs and Border Protection



CBP issued a Withhold Release Order against cotton products and tomato products produced in Xinjiang, China based on information that reasonably indicates the use of detainee or prison labor and situations of forced labor.

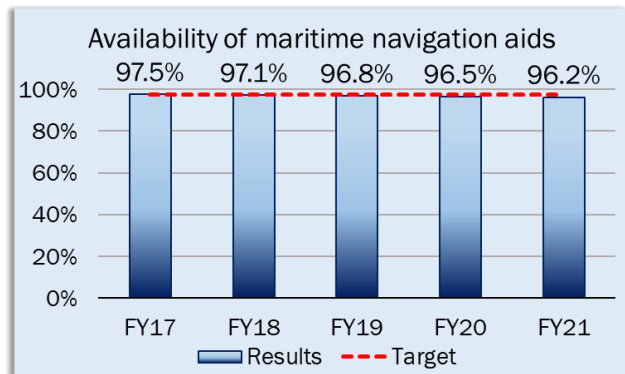


Percent of Global Entry member with no security-related violations (CBP): This measure shows CBP’s success at maintaining a high level of security in the [international air environment](#) by measuring the degree of compliance with all federal, state, and municipal laws and regulations that CBP is charged with enforcing at the ports of entry (international airports). 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 2021, the Travel program continued its outstanding performance in safeguarding international travel. While COVID-19 impacted the volume of travel into the United States this past years, 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. In FY 2021, this measure achieved 96.2 percent which is consistent with recent results but slightly down compared to previous years. While ATON damage from hurricanes over the past several years has, for the most part, been addressed, resource availability continues to impact program success. The USCG continues to explore solutions to mitigate this risk.

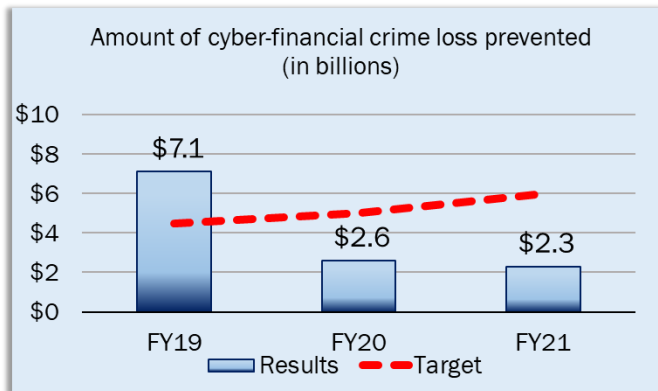




Management's Discussion and Analysis

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. In FY 2021, this measure achieved 2.3 billion in loss prevention. A number of cyber financial investigations related to COVID-19 fraud are still going through the judicial process and have yet to be counted in official statistics. Case closures and judicial processing remain slow due to continued pandemic effects.



Looking Forward

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

- **International trade and travel:** Rapidly growing and diversifying flows of trade and travel present ongoing challenges to balancing security while meeting services for legitimate trade partners and the traveling public. DHS has leveraged the response to COVID-19 to improve operations, execute targeting rules and procedures at all ports of entry. CBP collaborated with partners to monitor international travel rules, tracked affected travelers, denied entry to those prohibited, provided contact-tracing information as needed, expedited medical personnel and equipment through the clearance process, and increased personnel with medical training. CBP operated [eBadge](#) with TSA and commercial service providers to significantly reduce vetting and processing time for badges, credentials, and regular background checks on credentialed workers at a growing number of airports. Looking forward, the department plans to expand current eBadge operations through the development of the Trusted Employer Program, to more airports with improvements in vetting, while developing an eBadge App that allows direct employer completion of employee applications for access to a Travel Operations facility. DHS also plans to establish a Counter-Intelligence Watchlist, or

DID YOU KNOW?

In FY 2021, the Secret Service hosted a virtual Cyber Incident Response Simulation (CIRS) with business executives, federal law enforcement, and public sector officials. The simulation focused on Ransomware, Business Email Compromise, Managed Service Providers, and cryptocurrency. Trainings like these enhance planning, collaboration, and information sharing between private organizations and federal law enforcement agencies.



similar process, to centralize and de-conflict data in support of comprehensive interagency strategies to ensure a whole-of-government approach to Counter-intelligence operations.

- **Combating cybercrime and safeguarding the Nation's financial system:** Cybercrime continues to be the fastest-growing mode for crime occurring across the country and touching a large share of the U.S. population. As such, several DHS Components have efforts underway with plans to address cybercrime or plans to address organizations using cybercrime to support other illegal activities.
 - USSS recently began to implement a policy establishing a Cyber Technical Agent career progression and developing a plan to modernize the Electronic Crimes Task Force to strengthen and expand the existing network of task forces to address growing cybercrime threats as well as expand the Global Investigative Operations Center. To support the expansion of knowledge in cybercrime, there are ongoing efforts to train fellow law enforcement stakeholders on detecting and combatting cybercrimes.
 - ICE continues to develop new tools (e.g., enhanced facial recognition, web scraping, field-deployable DNA testing) used to counter transnational criminal organizations' illicit activities related to financial crimes.
 - CBP continues efforts against online trafficking in counterfeit and pirated goods as well as exploring expanded use of verifiable digital trademarks.
 - USCG plans include enhancing the service's cyber networks security, pursuing new efforts on offensive cyber capabilities, and helping safeguard the maritime domain and related infrastructure.
 - TSA issued new directives that will increase in response to the Colonial Pipeline cybersecurity attack in May, requiring owners and operators of TSA-designated critical pipelines that transport hazardous liquids and natural gas to implement a number of urgently needed protections against cyber intrusions.

DID YOU KNOW?

The Secret Service established its first overseas Electronic Crimes Task Force (ECTF) in Rome, Italy in 2009. This network of public private partnerships is dedicated to fight high tech, computer based crimes.

Goal 5: Strengthen 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



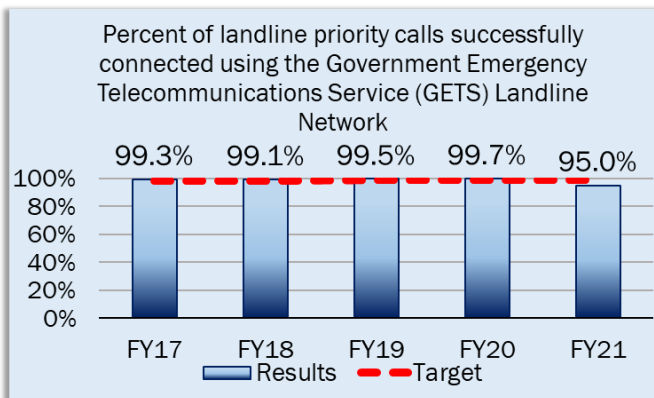
Management's Discussion and Analysis

thoroughly preparing local communities, rapidly responding during crises, and supporting recovery.

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

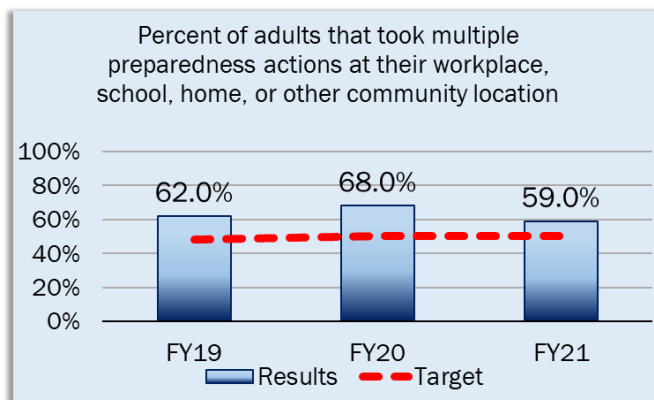
Percent of landline priority calls successfully connected using the Government Emergency Telecommunications Service (GETS) Landline Network (CISA):

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 2021, this measure achieved 95 percent.



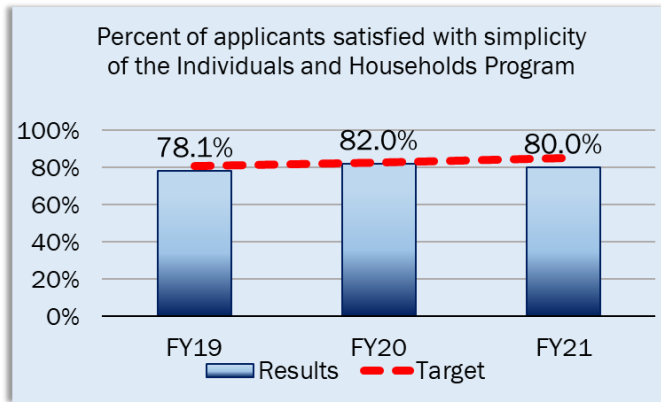
Percent of adults that took multiple preparedness actions at their workplace, school, home, or other community location (FEMA):

This is the third year this measure is reporting results. This measure serves as an indicator of the whole community effort to educate the public regarding their risks, developing methods to mitigate the impacts of 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 surveys distributed to households following such activities. In FY 2021, this measure achieved 59 percent.



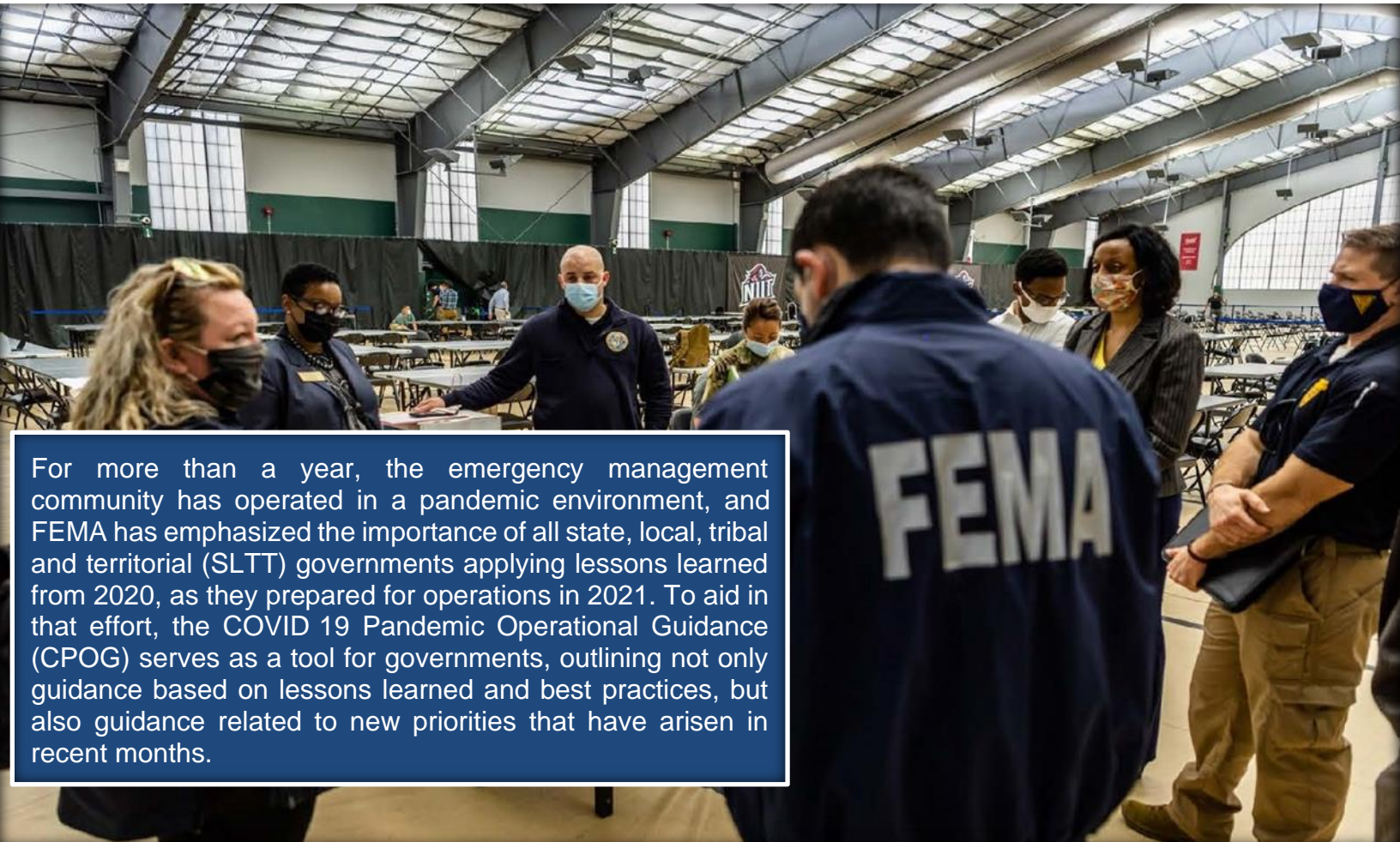
DID YOU KNOW?

In support of the COVID 19 vaccination effort, FEMA Voluntary Agency Liaisons (VALs) coordinated with 15 voluntary agency partners to schedule 2,031 clinical and non clinical volunteers at vaccination sites across the Nation.



Percent of applicants satisfied with simplicity of the Individuals and Households Program (FEMA): This is the third year for this measure reporting results. This measure supports the vision to streamline the disaster survivor experience by using surveys to assess the disaster survivors' overall satisfaction of [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. FEMA will continue email surveys in FY 2022 and expects more responses on disaster survivors' satisfaction. FEMA continues a Holistic Survivor Feedback Strategy with a vision of putting survivors at the center of how FEMA makes decisions. While FEMA did not meet its target of 85 percent, these results did not hinder FEMA's ability to execute its mission. In FY 2021, this measure achieved 80 percent.



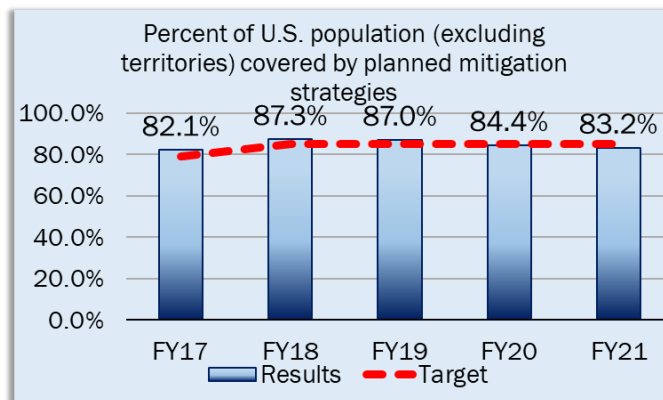
For more than a year, the emergency management community has operated in a pandemic environment, and FEMA has emphasized the importance of all state, local, tribal and territorial (SLTT) governments applying lessons learned from 2020, as they prepared for operations in 2021. To aid in that effort, the COVID 19 Pandemic Operational Guidance (CPOG) serves as a tool for governments, outlining not only guidance based on lessons learned and best practices, but also guidance related to new priorities that have arisen in recent months.

Management's Discussion and Analysis

Percent of U.S. population (excluding territories) covered by planned mitigation strategies (FEMA):

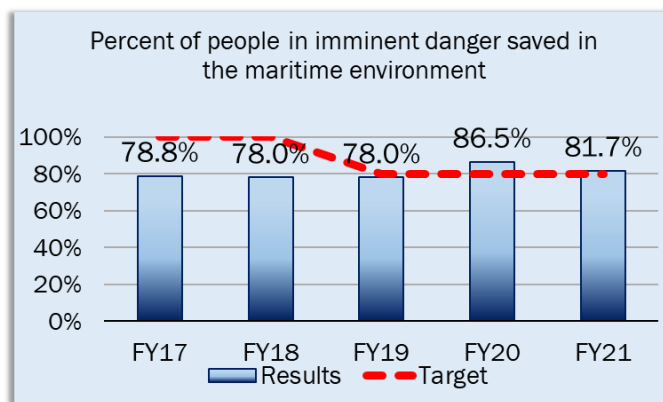
This measure reports the percent of U.S. population (excluding territories) covered by approved or approvable local [Hazard Mitigation Plans](#). During FY 2021, providing technical assistance to communities was difficult as the engagement needed could not always be performed due to COVID. Additionally,

community resources needed to coordinate and execute plan development activities were diverted in support of the COVID response. In FY 2021, this measure achieved 83.2 percent which is below target. In FY 2022, FEMA plans to increase technical assistance to assist communities with producing higher quality risk assessments.



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 2021, the USCG achieved 81.7 percent which is below target but is the



The U.S. Coast Guard Automated Mutual Assistance Vessel Rescue (AMVER) System tracks approximately 7,000 commercial ships a day for search and rescue across the globe. The Coast Guard manages the AMVER Program and coordinates to save people in distress at sea, on average of one person per day!



second highest result in the last five years. In FY 2020, the measure was adjusted to only include cases with lives at risk after the USCG was notified. In addition, COVID-19 may have contributed to the increase as some Districts reported case increases due to a drop in aid from other government agencies, commercial providers, and good Samaritans requiring the USCG to prioritize their own response efforts.

Looking Forward

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

- **Emergency Communications:** Emergency Communications support the deployment of interoperable communications systems for federal, state, local, and tribal government agencies. However, their stakeholders have limited resources and budgets, inhibiting investment in assets to improve capability and capacity. Events and incidents are becoming increasingly complex, necessitating additional planning for incident response and coordination. The inadequate number of engagements with the expanded stakeholder community negatively impacts the ability to identify gaps and define requirements. Looking forward through a concerted effort with partners/stakeholders, Emergency Communications intends to define/develop priorities related to cyber risks to emergency communications and acquire additional funding and personnel to address these gaps. Emergency Communications can ensure a well-coordinated service by assessing current gaps and risks in incident communications. Plans are being made to also develop strategies for reaching expanded communities. Furthermore, plans for developing/ tailoring support for new stakeholders and analyzing existing governance structures are in progress to determine how to better support the expanded community.
- **COVID-19 Implications:** FEMA provided front-line support for the U.S. response to the pandemic through mass vaccination sites and providing coordination across the FEMA regions. The COVID-19 Pandemic Operational Guidance issued during the 2020 Hurricane Season, outlines how FEMA has adapted its response and recovery operations in a COVID-19 environment. At the same time, this guidance has other implications moving forward, for example, providing a workforce mix for any future scenarios similar to the response during this pandemic. The Pandemic Operational Guidance also helps to shape a shared understanding among local and regional emergency managers and FEMA about roles and expectations in such deployments. The pandemic impacts current and future requirements for response and recovery logistics and products, such as

DID YOU KNOW?

The Emergency Communications program supported Statewide Interoperability Coordinators that were indispensable in managing and mitigating COVID 19 telecommunications impacts to support a full telework environment during the unprecedented stress on communications networks nationwide.



determining eligible work and costs for non-congregate sheltering in response to a Presidentially declared emergency or major disaster, processing grants, how to manage communications, and training during such responses, and employing tools requiring limited on-site presence—such as satellite imagery—to assess damage. COVID-19 response will continue for some time, and will have to become increasingly integrated with current operational concepts such as the [Community Lifelines](#) program and developments in the future structure of the Incident Management Workforce.

- **USCG Search and Rescue:** [Search and Rescue \(SAR\)](#) is one of the 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. 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. 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.

Agency Priority Goals

Please see our Annual Performance Report (APR) for an update on our FY 2022-2023 APGs. The APR will be available in February 2022 in conjunction with the FY 2023 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. The majority of noteworthy changes in financial balances are primarily due to COVID-19 related program activity described below (see Note 31, COVID-19 Activity, for additional information).

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 its efforts in preparedness and readiness to facilitate a rapid, 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. Functioning critical infrastructure is particularly important during the COVID-19 response for both public health and safety as well as community well-being. Certain critical infrastructure industries have a special responsibility to continue operations during these unprecedented times. To confront these challenges, DHS received and executed significant funding from the *American Rescue Plan Act* (ARPA), 2021 and the *Consolidated Appropriations Act* (CAA), 2021 to support our essential missions and to respond to our nations' needs, including reimbursing individuals and families for COVID-related funeral expenses, extending the lost wages assistance, and administering vaccine efforts and activities. FEMA continued to work with the state and territorial governments (including the District of Columbia) that chose to participate in the Lost Wages Assistance Program, which provided up to six weeks of assistance to eligible individual claimants that were unemployed or partially underemployed due to COVID-19 disruptions. In FY 2021, FEMA provided financial assistance to individuals and families with funeral expenses for deceased individuals attributable to COVID-19 related deaths. To combat the COVID-19 crisis, the Department focused on vaccine efforts, which included providing test kits to frontline personnel, airport passenger screening, and expanding access to vaccines and support vaccine distribution.

In FY 2020, FEMA activated the National Response Coordination Center (NRCC) in the wake of the Coronavirus outbreak in the United States and continues its operations in FY 2021. The NRCC is a multi-agency center that coordinates the overall federal support for major incidents and emergencies. NRCC also provides a clearinghouse of resources and policies for local and state governments in impacted regions. CISA continues to monitor the evolving virus closely, taking part in interagency and industry coordination calls, and working with critical infrastructure partners to prepare for possible disruptions to critical infrastructure. The Department also took action in furtherance of the public health interests advanced by enforcing the presidential



Management's Discussion and Analysis

proclamations at and between air, land, and seaports of entry, alerting the Centers for Disease Control and Prevention (CDC) partners to any individuals who require enhanced health screening. 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.

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.

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 2021	FY 2020	\$ Change	% Change
Fund Balance with Treasury	\$ 163,044	\$ 131,013	\$ 32,031	24%▲
General Property, Plant, and Equipment, Net	27,893	26,561	1,332	5%▲
Other Assets	26,201	25,435	766	3%▲
Total Assets	217,138	183,009	34,129	19%▲
Federal Employee and Veteran Benefits Payable	75,570	71,835	3,735	5%▲
Debt	20,618	20,596	22	<1%▲
Accounts Payable	5,606	5,408	198	4%▲
Insurance Liabilities	3,436	2,830	606	21%▲
Other Liabilities	25,340	32,762	(7,422)	-23%▼
Total Liabilities	130,570	133,431	(2,861)	-2%▼
Total Net Position	86,568	49,578	36,990	75%▲
Total Liabilities and Net Position	\$ 217,138	\$ 183,009	\$ 34,129	19%▲

Results of Operations (\$ in millions)	FY 2021	FY 2020	\$ Change	% Change
Gross Cost	\$ 104,688	\$ 127,215	\$ (22,527)	-18%▼
Less: Revenue Earned	(14,718)	(14,874)	156	-1%▼
Net Cost Before Gains and Losses on Assumption Changes	89,970	112,341	(22,371)	-20%▼
(Gains) and Losses on Assumption Changes	1,573	3,061	(1,488)	-49%▼
Total Net Cost	\$ 91,543	\$ 115,402	\$ (23,859)	-21%▼



Assets – What We Own and Manage

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

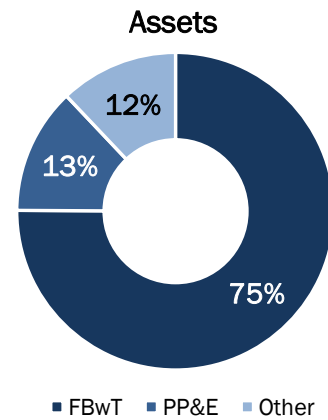
The Department’s largest asset is Fund Balance with Treasury (FBwT), which consists primarily of appropriated, revolving, trust, deposit, receipt, and special funds remaining at the end of the fiscal year.

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.

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.

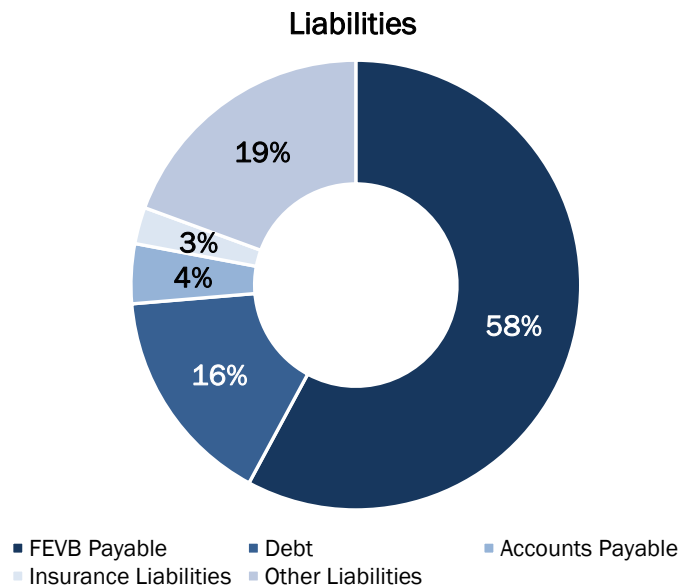
As of September 30, 2021, the Department had \$217 billion in assets, representing a \$34 billion increase from FY 2020. The majority of this change is due to an increase in Fund Balance with Treasury resulting from additional supplemental appropriations received under the American Rescue Plan (see Note 31 in the Financial Information section).



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.

The Department’s largest liability is for Federal Employee and Veteran Benefits (FEVB) Payable. The Department owes these amounts to current and past civilian and military 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).



Debt is the second 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



Management’s Discussion and Analysis

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.

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

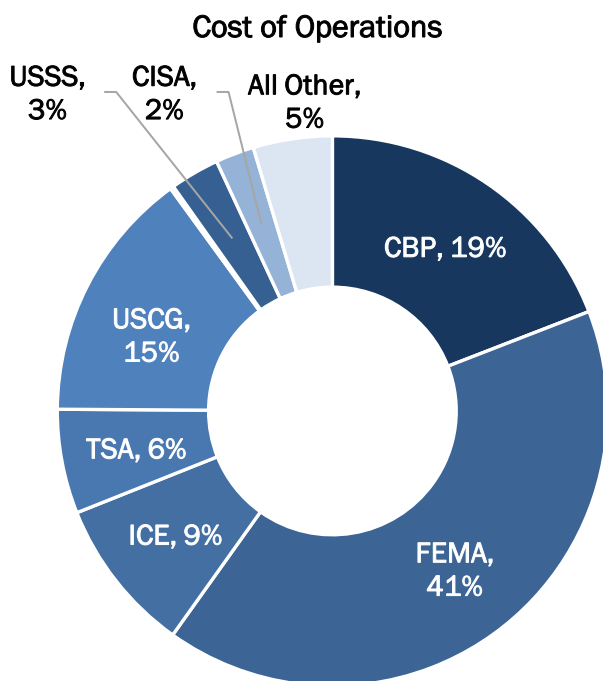
Insurance Liabilities are primarily the result of the Department’s sale or continuation-in-force of flood insurance policies within the NFIP, which is managed by FEMA.

Other Liabilities include amounts owed to other federal agencies and the public for goods and services received by the Department, amounts received by the Department for goods or services that have not been fully rendered, unpaid 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, 2021, the Department reported approximately \$131 billion in total liabilities. Total liabilities decreased by \$2.8 billion in FY 2021 mostly due to FEMA’s payments on Lost Wages Assistance Program which is offset primarily by increases in USCG Actuarial Pensions Liability and CBP Custodial Liability on collection of duties.

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 \$87 billion. Total net position increased \$37 billion from FY 2020, in large part because of the additional supplemental appropriation received by FEMA for COVID-19.

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 2021, which is a decrease of \$22 billion from the prior year. This is mainly due to the large decrease of disaster related costs associated with disaster



responses to COVID-19, hurricanes, and wildfires FEMA incurred in FY 2021 compared to FY 2020.

During FY 2021, the Department earned approximately \$14.7 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 transactions is essential for compliance with legal constraints and controls over the use of federal funds. The budget represents our plan for efficiently and effectively achieving the strategic objectives to carry out our mission and to ensure that the Department manages its operations within the appropriated amounts using budgetary controls.

Sources of Funds (\$ in millions)	FY 2021	FY 2020	\$ Change	% Change
Unobligated Balance from Prior Year Budget				
Authority, Net	\$ 46,955	\$ 51,848	\$ (4,893)	-9% ▼
Appropriations	142,442	133,025	9,417	7% ▲
Spending Authority from Offsetting Collections	9,560	11,732	(2,172)	-19% ▼
Borrowing Authority	32	33	(1)	-3% ▼
Total Budgetary Resources	\$ 198,989	\$ 196,638	\$ 2,351	1% ▲

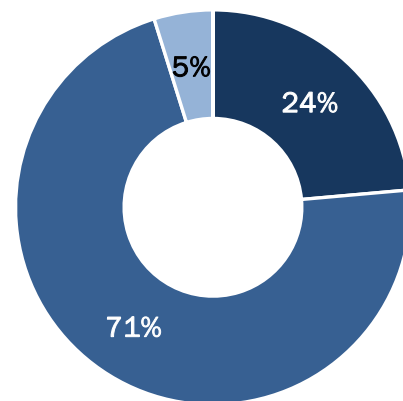
The Department’s budgetary resources, both discretionary and mandatory, were \$199 billion for FY 2021. The authority was derived from \$47 billion in authority carried forward from FY 2020, appropriations of \$142 billion, approximately \$10 billion in collections, and \$32 million in borrowing authority. Budgetary resources increased approximately \$2 billion from FY 2020. This is mainly due to additional supplemental appropriation for COVID-19.

Of the total budget authority available, the Department incurred a total of \$142 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.

Budgetary Resources



- Unobligated Balance from Prior Year Authority
- Appropriations
- Spending Authority from Offsetting Collections
- Borrowing Authority (<1 percent)

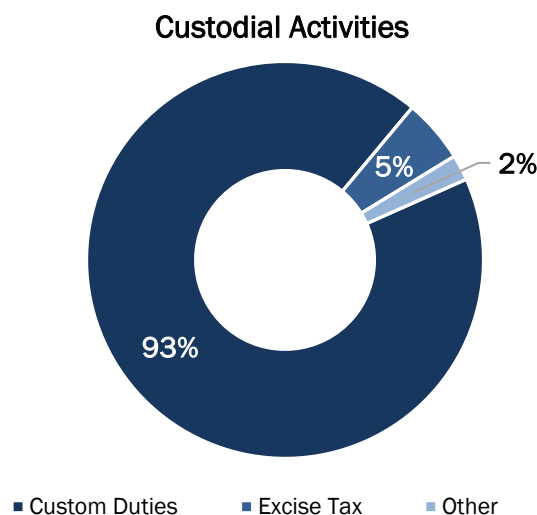


Management's Discussion and Analysis

Cash Collections (\$ in millions)	FY 2021	FY 2020	\$ Change	% Change
Duties	\$ 85,466	\$ 74,401	\$ 11,065	15%▲
Excise Taxes	4,773	3,967	806	20%▲
Other	1,905	1,706	199	12%▲
Total Cash Collections	\$ 92,144	\$ 80,074	\$ 12,070	15%▲

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 \$92 billion, which is a \$12 billion increase from FY 2020 mainly due to an increase in import activity and collections of customs duties.

Custom duties collected by CBP account for 93% of total cash collections. The remaining 7% 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 2021) 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. CWMD, S&T, and USCG have made significant investments in research and development this fiscal year (in millions):

Components	FY 2021	FY 2020
CWMD	\$ 70	\$ 51
S&T	827	827
USCG	8	7
Total Research & Development	\$ 905	\$ 885



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 have made significant investments in human capital (in millions):

Components	FY 2021	FY 2020
FEMA	\$ 86	\$ 86
S&T	3	3
Total Human Capital	\$ 89	\$ 89

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 has made significant investments in non-federal physical property (in millions):

Components	FY 2021	FY 2020
TSA	\$ 188	\$ 191
Total Non-Federal Physical Property	\$ 188	\$ 191

Other Key Regulatory Requirements

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



Secretary's Assurance Statement

November 12, 2021



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, 2021, except for the disclosures noted in the subsequent sections.

Pursuant to the *DHS Financial Accountability Act* (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 was designed and operating effectively, except for aspects of Financial Reporting 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 area of material weaknesses 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,

A handwritten signature in blue ink that reads "Alejandro N. Mayorkas". The signature is fluid and cursive.

Alejandro N. Mayorkas
Secretary of Homeland Security



Management's Report on Internal Controls Over Financial Reporting

November 12, 2021

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 accepted 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, 2021, 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, 2021, DHS's internal controls over financial reporting are effective except for areas of material weaknesses in Financial Reporting 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. *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 also can 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



Management's Discussion and Analysis

compliance with the policies or procedures may deteriorate.

DHS has made progress in improving its internal controls and financial management program. Management commits to implementing corrective actions to resolve the remaining areas of material weakness.

Best Regards,

A handwritten signature in blue ink, appearing to read "Alejandro N Mayorkas", written over a horizontal line.

Alejandro Mayorkas
Secretary

A handwritten signature in blue ink, appearing to read "Stacy Marcott", written over a horizontal line.

Stacy Marcott
Acting Chief Financial Officer



Management Assurances

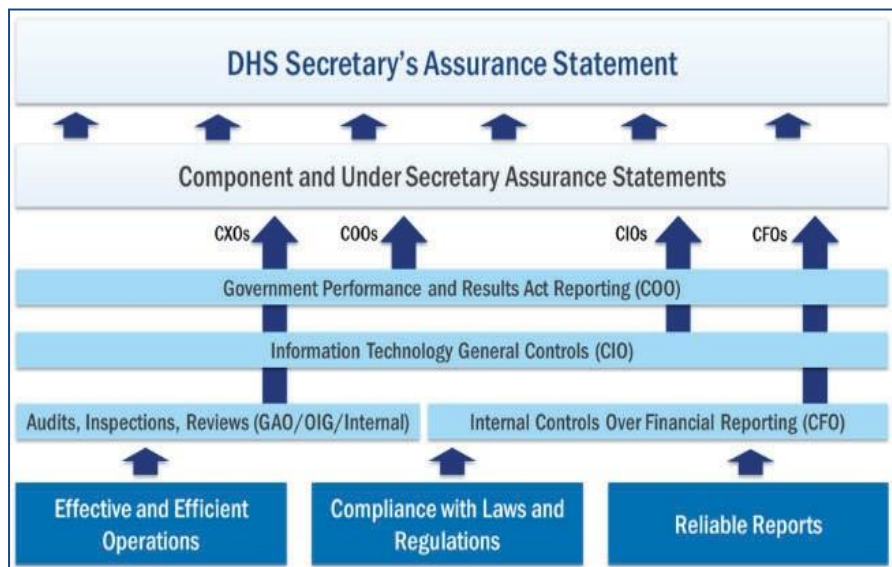
DHS management is responsible for establishing, maintaining, and assessing internal controls to provide reasonable assurance that the objectives of the *Federal Managers’ Financial Integrity Act (FMFIA) of 1982* (31 United States Code 3512, Sections 2 and 4) and the *Federal Financial Management Improvement 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 FFMA and Appendix D to OMB Circular A-123, Compliance with the *Federal Financial Management Improvement Act of 1996*.

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,



Management's Discussion and Analysis

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. 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 testing 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 goal is to have most Components placed on the Standardized (third) tier, which informs leaders that quality internal control assessments are performed to validate that neither material weakness conditions exist, nor will there be 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 Weaknesses Resolution Status

In FY 2020, management reported two areas of material weaknesses: 1) financial reporting and 2) IT controls and system functionality. In FY 2021, DHS made significant improvements in remediating areas of material weaknesses and worked to resolve financial reporting deficiencies through targeted remediation. Refer to the tables below for areas contributing to the financial reporting and IT controls and information systems areas of material weakness along with appropriate corrective actions planned in FY 2022.



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
Financial Reporting	All	FY 2003	FY 2022
<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"> • <i>Information Used in Controls</i> (Contributing Component(s): All) <ul style="list-style-type: none"> <u>Deficiency Details</u> <ul style="list-style-type: none"> ○ Ineffective monitoring over information utilized in DHS internal control over financial reporting processes and control activities. <u>Planned Corrective Actions</u> <ul style="list-style-type: none"> ○ DHS is in the process of implementing a multi-phased, risk-based approach and process for identifying and assessing Information Used in Controls. • <i>Service Provider Monitoring</i> (Contributing Component(s): All) <ul style="list-style-type: none"> <u>Deficiency Details</u> <ul style="list-style-type: none"> ○ 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. <u>Planned Corrective Actions</u> <ul style="list-style-type: none"> ○ DHS continues to build and implement process improvements utilizing a risk-based management program to provide effective monitoring and oversight of service providers. • <i>Other</i> (Contributing Component(s): All) <ul style="list-style-type: none"> <u>Deficiency Details</u> <ul style="list-style-type: none"> ○ Deficiencies aggregated to substantiate inclusion into this area of material weakness, including 1) journal entries, 2) funeral assistance grants accruals, 3) application controls, and 4) inability to record trading partner activity at the initiation of the transaction event due to system limitations <u>Planned Corrective Actions</u> <ul style="list-style-type: none"> ○ Process improvements for journal entries will be developed, implemented, and assessed in accordance with remediation plans. In addition, USCG will be migrating to a new Oracle based financial system in FY 2022 that is planned to significantly reduce the volume and amount of manual journal entries processed by USCG going forward. ○ 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. ○ 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. ○ 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. 			



Table 2: 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 2023
<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"> • <i>Financial System Requirements</i> (Contributing Component(s): All) <p><u>Deficiency Details</u></p> <ul style="list-style-type: none"> ○ 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 FFMIA. <p><u>Planned Corrective Actions</u></p> <ul style="list-style-type: none"> ○ Components will continue to implement the find, fix, test strategy in FY 2022. 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. ○ 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. • <i>System Functionality / Information Derived from Systems</i> (Contributing Component(s): All) <p><u>Deficiency Details</u></p> <ul style="list-style-type: none"> ○ 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. <p><u>Planned Corrective Actions</u></p> <ul style="list-style-type: none"> ○ 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. ○ In FY 2022, 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. • <i>Service Provider Monitoring</i> (Contributing Component(s): All) <p><u>Deficiency Details</u></p> <ul style="list-style-type: none"> ○ 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. <p><u>Planned Corrective Actions</u></p> <ul style="list-style-type: none"> ○ For service provider monitoring controls, DHS continues to build improvements utilizing a risk-based management program to provide monitoring and oversight of service providers. 			



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 3: FFMIA Non-compliance Details and Corrective Actions

Area of Non compliance	DHS Component(s)	Year Identified	Target Correction Date
FFMIA	All	FY 2003	FY 2023
<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"> • <i>Financial System Requirements</i> (Contributing Component(s): All) <ul style="list-style-type: none"> <u>Non-compliance Details</u> <ul style="list-style-type: none"> ○ DHS does not substantially comply with FFMIA primarily due to lack of compliance with financial system requirements as disclosed in the IT Controls and System Functionality area of material weakness. <u>Planned Corrective Actions</u> <ul style="list-style-type: none"> ○ Refer to the corrective actions planned for the IT Controls and System Functionality area of material weakness. • <i>Federal Accounting and U.S. Standard General Ledger (USSGL) Requirements</i> (Contributing Component(s): USCG, CBP, MGMT, and ICE) <ul style="list-style-type: none"> <u>Non-compliance Details</u> <ul style="list-style-type: none"> ○ USCG, CBP, MGMT, and ICE 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. <u>Planned Corrective Actions</u> <ul style="list-style-type: none"> ○ DHS CFO and Components will continue to design, document, and implement compensating controls to reduce the severity of legacy system application / functionality limitations. 			

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 Digital Accountability and Transparency Act of 2014 (DATA Act) Data Quality Plan on July 6, 2021. 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 2021, FEMA



noted a material inadequacy associated with its DATA Act reporting. The inadequacy has been substantially compensated due to DHS validation pre-check processes as well as regular oversight and metrics reporting. Despite the FEMA noted exceptions, DHS has successfully matched over 98.6% percent of financial data (File C) and award data (File D) dollars.

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 October of 2018, TSA and USCG resumed implementation efforts and the Department completed upgrading CWMD to the latest version of the solution in October 2019. In October of 2020, TSA went live on the FSMS platform and USCG is on schedule to go-live in November of 2021.

DHS is leveraging lessons learned from the former shared services implementation, reducing risk in future migrations through deliberative approaches to program management, resource

Management’s Discussion and Analysis

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 Components².

In addition to the DHS FSM efforts, the DHS CIO and Component CIOs met federal mandates to develop IT strategic plans, analyze legacy IT infrastructure requirements, and identify modernization needs. To ensure strategic planning activities are conducted across the Department, DHS issued a directive³ in 2018 to require Component-level CIOs to develop, implement, and maintain IT strategic plans annually. The DHS CIO published the FYs 2019–2023 IT Strategic Plan in March 2019. The DHS IT Strategic Plan identifies an IT vision to “deliver world class IT to enhance and support the DHS mission.” With a focus on rebuilding foundations and driving innovation, the DHS IT Strategic Plan outlines four goals aiming to advance the DHS organizational culture, improve network connectivity & resilience, mature the DHS cybersecurity posture, and transform technology to meet DHS customer needs.

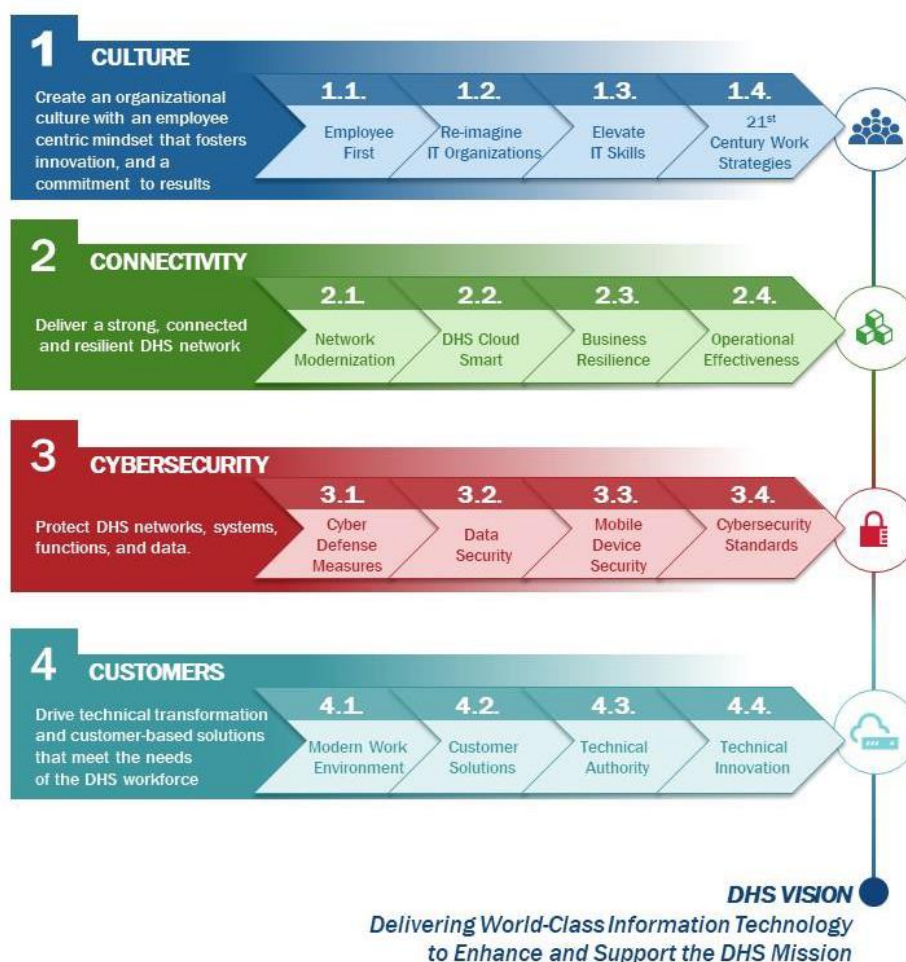


Figure 4: DHS IT Strategic Plan – Goals

² ICE serviced Components include: S&T, Management Directorate, CISA, and USCIS

³ DHS Directive 142-02 Rev. 01, Information Technology Integration and Management, April 12, 2018



Specifically related to modernization, the 2019-2023 DHS IT Strategic Plan outlined initiatives to adopt cloud-based computing⁴ and to consolidate and optimize data centers. To assist in these efforts, DHS established the Cloud Steering Group in May 2018 to oversee the implementation of a federated, enterprise-wide strategy for accelerating the modernization and migration of DHS IT applications and infrastructure to the cloud; and optimization of the remaining data centers by aligning their capabilities and economics, to the extent possible, with the cloud.

⁴ The OMB *Federal Cloud Computing Strategy* defines cloud computing as solutions exhibiting five essential characteristics: on-demand service, broad network access, resource pooling, rapid elasticity, and measured service.