



# Homeland Security

## U.S. Department of Homeland Security FY 2020 Agency Financial Report

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

# Certificate of Excellence in Accountability Reporting



In May 2020, DHS received its seventh consecutive Certificate of Excellence in Accountability Reporting (CEAR) from the Association of Government Accountants (AGA) for its Fiscal Year (FY) 2019 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.

# About this Report



The Department of Homeland Security (DHS) Agency Financial Report for FY 2020 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 2020, the Department's Performance and Accountability Reports consist of the following three reports:

- DHS Agency Financial Report | Publication date: November 16, 2020.
- DHS Annual Performance Report | Publication date: February 1, 2021 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, 2021.

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

## Message from the Secretary

November 13, 2020



I am pleased to present the Department of Homeland Security's (DHS) Agency Financial Report for Fiscal Year (FY) 2020. This report provides an assessment of the Department's detailed financial status and demonstrates how the resources entrusted to us were used to support our homeland security mission.

COVID-19 has proven to be one of the most significant threats our Nation has faced in years. Since the beginning of the pandemic, the resiliency of our public health system, national security, and economy have been tested on a daily basis. Still, even with these challenges, the men and women of DHS have risen to the occasion time and again. The selflessness and dedication to deliver on our mission—even during a pandemic—are a testament to the values we hold dear at DHS.

Today, more than ever, the Department is focused on its mission to ensure we safeguard the American people, that we are watchful in identifying threats, and that we respect and honor our partners as we work together to ensure the safety and security of our people.

As we confront all these challenges, we continue to assure the public that the resources entrusted to the Department are used to support our mission and to respond to our Nation's needs. In Fiscal Year 2020, DHS received and executed significant funding to support the COVID-19 relief effort. These funds provided American communities with critical support—including personal protective equipment, temporary medical facilities, and lost wages assistance. At the same time, DHS continued to deliver all our other essential missions—including disaster relief, border security and enforcement, transportation security, and cyber security. The performance and financial data in this report provides a more detailed summary of our results.

On March 27, 2020, the CARES Act was signed into law to provide fast and direct economic assistance for American workers, families, and small businesses, and to preserve jobs for our American industries. DHS has been at the center of this unprecedented response by working with other federal agencies, state, local, tribal, and territorial governments to execute a whole-of-America response to the pandemic. This recovery and economic support constitute the largest relief assistance program in American history. As DHS continues providing relief and assistance to the American people, we want to ensure the resources entrusted to the Department are safeguarded and subjected to the highest standards.

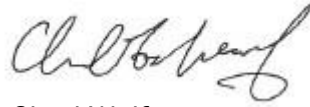
DHS remains committed to improving performance measurement and accountability, and based on our internal control evaluations, I am able to provide reasonable assurance that the performance and financial information reported for the Department in our performance and accountability reports are complete and reliable, except those noted 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>.

## Message from the Secretary

As the complex threat environment continues to evolve, the Department will embody the relentless resilience of the American people to ensure a safe, secure, and prosperous Homeland. However, none of these efforts are possible without the efforts and sacrifice of our men and women. Whether it's those on the front-line or those supporting our missions, the Department's workforce continues to excel at safeguarding our assets, Nation, and values.

I look forward to the Department's accomplishments in the years to come.

Sincerely,

A handwritten signature in black ink, appearing to read "Chad Wolf". The signature is fluid and cursive, with a large, sweeping "W" and "F".

Chad Wolf  
Acting Secretary of Homeland Security

Table of Contents

<b>Message from the Secretary</b> .....	<b>ii</b>
<b>Management’s Discussion and Analysis</b> .....	<b>1</b>
Our Organization .....	2
Performance Overview .....	2
Financial Overview.....	24
Secretary’s Assurance Statement .....	31
<b>Financial Information</b> .....	<b>42</b>
Message from the Chief Financial Officer.....	43
Introduction.....	45
Financial Statements .....	46
Notes to the Financial Statements.....	54
Required Supplementary Information.....	134
Independent Auditors’ Report.....	138
<b>Other Information</b> .....	<b>167</b>
Tax Burden/Tax Gap.....	168
Combined Schedule of Spending .....	169
Summary of Financial Statement Audit and Management Assurances .....	173
Payment Integrity.....	175
Gone Act.....	195
Real Property .....	196
Civil Monetary Penalty Adjustment for Inflation .....	197
Other Key Regulatory Requirements.....	204
Office of Inspector General’s Report on Major Management and Performance Challenges Facing the Department of Homeland Security.....	205
<b>Acronym List</b> .....	<b>238</b>
<b>Acknowledgements</b> .....	<b>239</b>

# Management's Discussion and Analysis



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

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

The **Performance Overview** section provides a summary of each homeland security mission, 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 Activities.

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.

## Our Organization

DHS has a fundamental duty 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 as one team, with one mission, we are one DHS—keeping America safe.

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. For the most up to date information on the Department's structure and leadership, visit our website at <http://www.dhs.gov/organization>.



Figure 1: DHS Operational and Support Components

## Performance Overview

The Performance Overview provides an overview of our performance 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 2020-2022 Annual Performance Report with the FY 2022 Congressional Budget Justification and will be available at: <http://www.dhs.gov/performance-accountability>. All previous reports can be found at this link as well.



## DHS Performance Framework

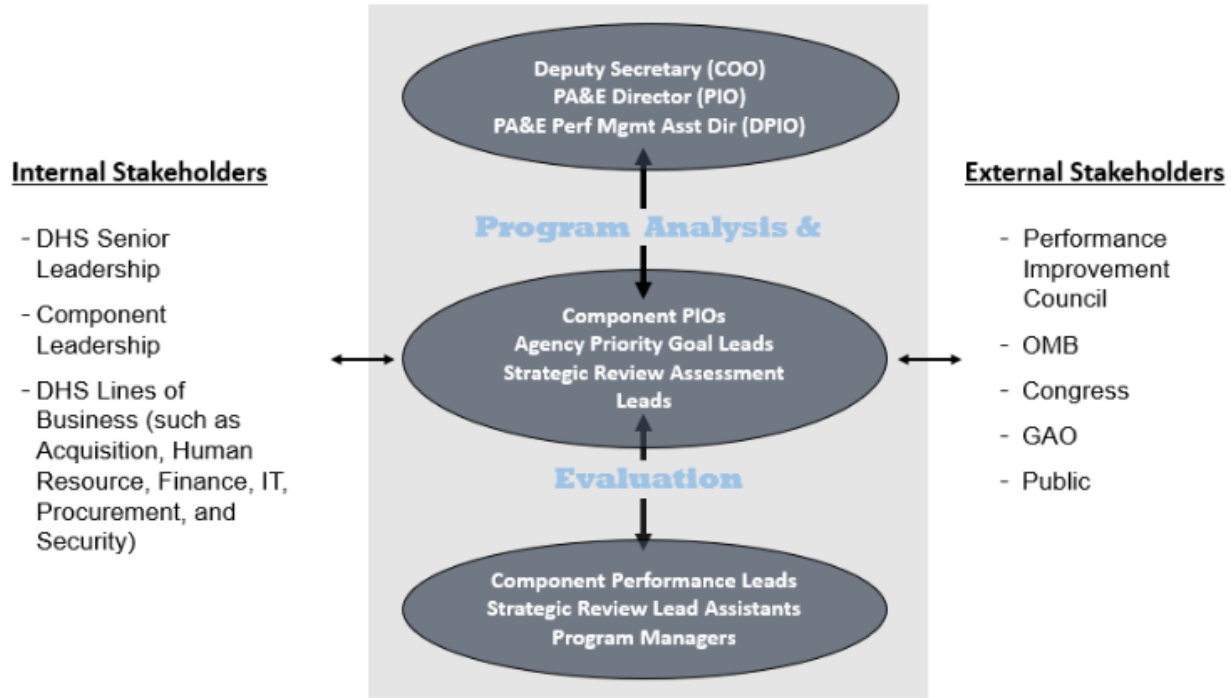
The Department has a robust performance framework that drives performance management and enables the implementation of performance initiatives. This framework consists of core concepts and initiatives to assess program implementation progress, measure results, and drive the delivery of value to external 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 2: DHS Performance Management Framework**

### Performance Community

The DHS performance community is led by the Chief Operating Officer, 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).



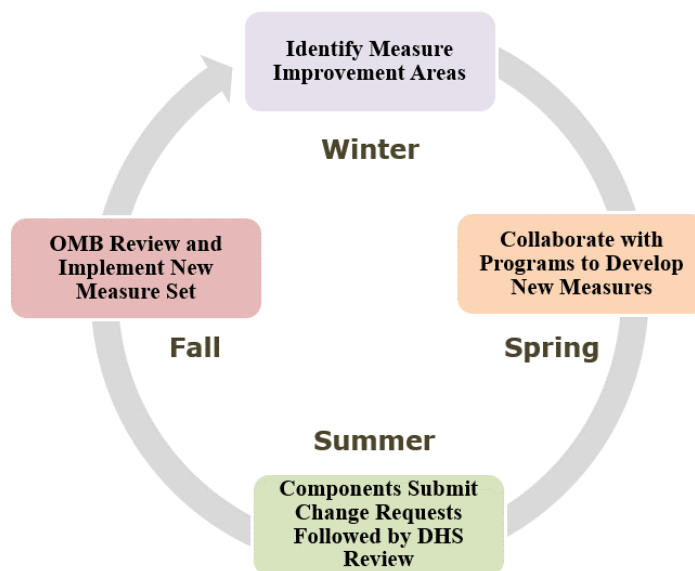
**Figure 3: DHS Organizational Performance Community**

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 communicate 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 planning and managing Assessment Team efforts annually and refining and delivering key findings from the review process. Program managers across DHS Components are contributors to the Strategic Review assessment, along with generating ideas for performance measures, producing measures 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 4: DHS Annual Measure Improvement Process**

While measure 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 place<sup>1</sup>.

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

---

<sup>1</sup> Note: Circular A-11, PART 6, THE FEDERAL PERFORMANCE FRAMEWORK FOR IMPROVING PROGRAM AND SERVICE DELIVERY, Section 240.26 Definitions. Data limitations. In order to assess the progress towards achievement of performance goals, the performance data must be appropriately valid and reliable for intended use. Significant or known data limitations should be identified to include a description of the limitations, the impact they have on goal achievement, and the actions that will be taken to correct the limitations. Performance data need not be perfect to be valid and reliable to inform management decision-making. Agencies can calibrate the accuracy of the data to the intended use of the data and the cost of improving data quality. At the same time, significant data limitations can lead to bad decisions resulting in lower performance or inaccurate performance assessments. Examples of data limitations include imprecise measurement and recordings, incomplete data, inconsistencies in data collection procedures and data that are too old and/or too infrequently collected to allow quick adjustments of agency action in a timely and cost-effective way.

## Management's Discussion and Analysis

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; 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 and management 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 ongoing 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:

- 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 2020 DHS conducted its seventh 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*, GPRA, and GPRAMA.

The SR serves multiple purposes for Components, DHS, and OMB to: 1) assess progress of our mission 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; and 6) drive a focused conversation with OMB on significant issues to inform their management and budget activities.

## DHS Summary of Key Performance Measures

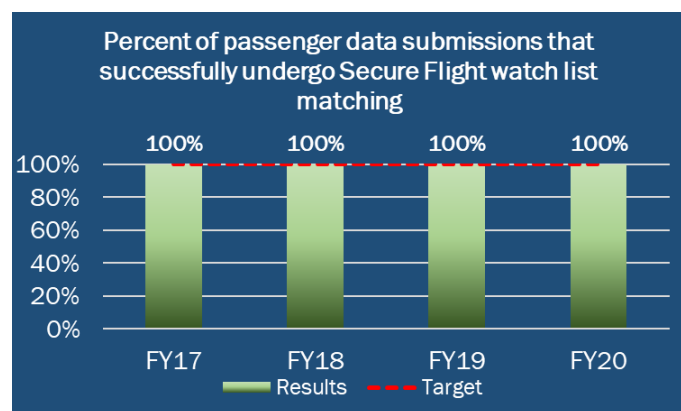
Strategic plan goals are implemented by our mission programs which are groups of activities acting together to accomplish a specific high-level outcome external to DHS and include operational processes, skills, technology, human capital, and other resources. Mission programs have performance goals, performance measures, and performance targets. Below are a select set of measures that describe how our mission programs drive to deliver on the DHS mission.

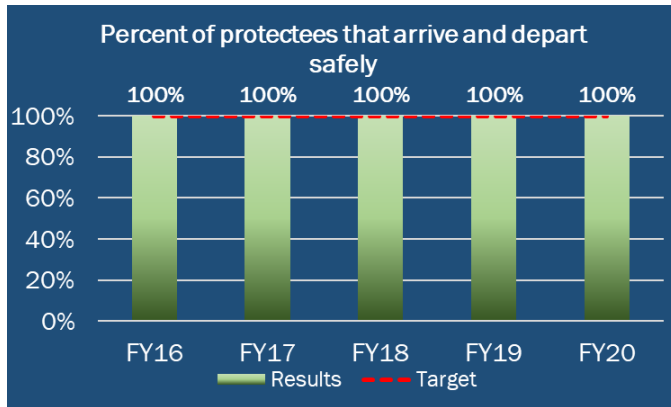
### Goal 1: Counter Terrorism and Homeland Security Threats

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 activity 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 and this measure ensures the traveling public that all domestic air passengers have undergone checking against these watch lists. This measure reports the percent of qualified message submissions received from the airlines that are successfully matched by the [Secure Flight](#) automated vetting system against the existing high-risk watch lists. A qualified message submission from the airlines contains passenger data sufficient to allow successful processing in the Secure Flight automated vetting system. In FY 2020, this measure achieved 100 percent, meeting the target, and has maintained this level of performance for the past four years. DHS will continue to report this measure as it conveys an underlying critical layered process to ensure security in the aviation environment.





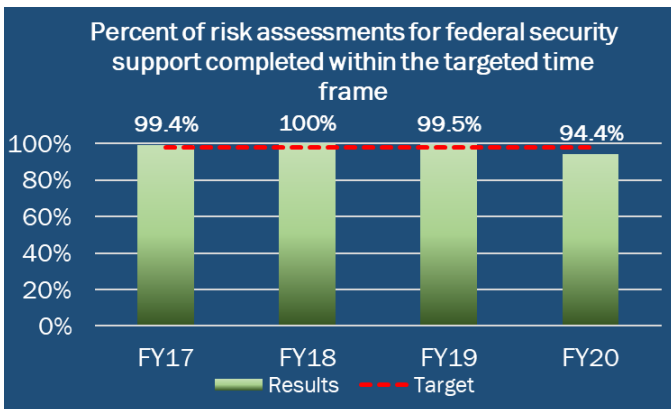
**Percent of protectees that arrive and depart safely (USSS):** This measure reflects the effectiveness of efforts to ensure safe travel (arrive and depart safely) for the President and Vice President of the United States and their immediate families, former presidents, their spouses, and their minor children under the age of 16, major presidential and vice-presidential candidates and their spouses, and foreign heads of state. This measure gauges the percent of travel stops where the [USSS](#) protectees arrive and depart safely. The performance target is always 100 percent and the USSS has maintained a 100 percent performance record for the past five years. To achieve these results takes a coordinated effort across several specialized resources within USSS. Using advanced countermeasures, the USSS executes security operations that deter, minimize, and decisively respond to identified threats and vulnerabilities to keep protectees safe.



The Office of Protective Operations (OPO) implemented Events Management, an IT system where OPO can efficiently develop and assess the strategic operational posture of its assets and personnel globally.

This system enables fast and informed decision-making in emergent situations, resulting in improved coordination for USSS' protective operations. As of July 2020, this tool has led to a significant return on investment with a time savings equivalent of 4 full-time employees per year.

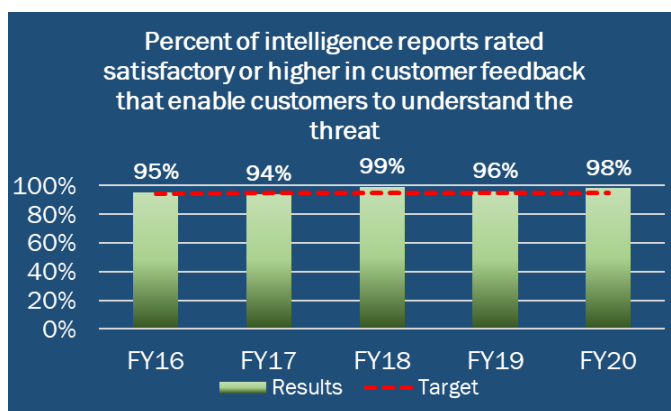
**Percent of risk assessments for federal security support of large public/community special events completed within the targeted time frame (OPS):** This measure indicates the timeliness of risk assessments that are used by federal agencies as criteria to determine their level of support to state and 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 94.4 percent of the time, seeing a decline in overall performance based on historical trends. During the first quarter of FY 2020, technical issues and a significant increase in National Special Events Data Call events from the previous year resulted in assessments not being completed within the targeted time frame. This, coupled with an unexpected second quarter surge, impacted service delivery. The technology used for inputs has been updated to improve performance in FY 2021 as well as addressing issues related to surge activity.

**Percent of intelligence reports rated satisfactory or higher in customer feedback that enable customers to understand the threat (I&A):**

This measure gauges the extent to which the DHS Intelligence Enterprise is satisfying customer needs related to anticipating emerging threats. This measure encompasses reports, produced by all DHS Component intelligence programs, which are provided to federal, state, and local customers. In FY 2020, DHS evaluations were rated as satisfactory or higher resulting in a 98 percent satisfaction rate, meeting the target. Trends over time show a high stakeholder satisfaction with reports.



Trends over time show a high stakeholder satisfaction with reports.

**Looking Forward**

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

- **Unmanned Aerial Systems (UAS):** Terrorists are using unmanned aerial systems (i.e., drones) to conduct surveillance and potentially launch terrorist attacks; drug smugglers are using them to monitor border patrol officers and to deliver drugs in remote areas; and criminals and nation states are using them to spy on sensitive facilities. The threat is real, and they can be used for a wide array of dangerous purposes. To address this, the Department has taken a proactive approach across several of our Components to include:
  - S&T is investing in research and development activities to better understand how UAS advances can be applied to protect the American people, increase operational efficiencies, and improve command and control decision-making, especially when combined with [counter-UAS \(CUAS\) technologies](#).
  - CBP, CISA, USCG, and others are working to implement CUAS technologies to: enhance situational awareness of the land and sea borders, at and between Ports-of-Entry; enhance the ability to share, query, and analyze law enforcement information/data to enable law enforcement investigations; deploy improved tools to advance the safety and effectiveness of DHS personnel; improve the detection and tracking of low-altitude airborne threats; enhance capabilities to integrate border security sensor and intelligence sources, perform data analytics, and share the resulting actionable intelligence with partners across the homeland security enterprise.
- **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 creating three-dimensional images that TSA officers can manipulate to enable thorough image analysis. As part of the Administrator’s Intent 2.0, TSA seeks to leverage

Did you **know?**

TSA training goes way beyond the airport checkpoints. The agency also instructs Federal Air Marshals and canine teams, and it offers programs in leadership and other advanced skills to all its personnel. On average, TSA employees complete millions of courses per fiscal year, with almost 20 thousand students attending in-residence classes.

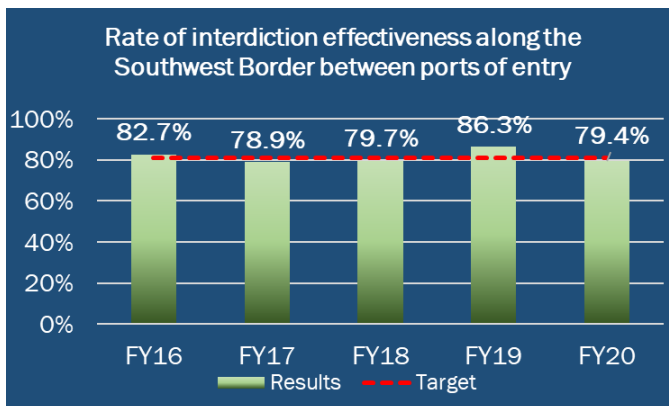
## Management's Discussion and Analysis

innovations in artificial intelligence, identity management, machine learning and screening automation across the TSA enterprise to advance TSA's security mission across both the TSA enterprise and the Transportation Systems Sector. See [TSA's Administrator's Intent](#) for more information.

- **Countering Weapons of Mass Destruction:** The Department of Homeland Security works every day to prevent terrorists and other threat actors from using weapons of mass destruction to harm Americans. The Countering Weapons of Mass Destruction Office (CWMD) leads Department efforts and coordinates with domestic and international partners to safeguard the United States against chemical, biological, radiological and nuclear (CBRN) and health security threats. CWMD's Capability and Operational Support program coordinates with partners in all levels of government to help communities build capabilities and prepare for CBRN and public health events. The CWMD Federal Assistance program further aligns and reinforces operational programs and activities across the Weapons of Mass Destruction threat space through consistent and persistent engagement. The CWMD Research and Development program manages efforts to identify, explore, develop, and demonstrate science and technologies that address gaps in the detection architecture. Finally, the CWMD Procurement, Construction and Improvements program provides resources necessary for the planning, operational development, procurement, deployment, operational test and evaluation, and improvement of assets that help the Department combat weapons of mass destruction.

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

Secure borders are essential to our national sovereignty. DHS continues to implement a border security approach 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 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 Operational Control (OPCON) over the U.S. border. Results for this measure have varied significantly the past three years. In FY 2019, the results for this measure were greater than historical results

due largely to the unprecedented mass illegal migration and the nontypical encounter where most of these people voluntarily surrendered to Border Patrol Agents. Known illegal entries decreased to 405,036 in FY 2020 from 859,501 in FY 2019. 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. In late March 2020, Border

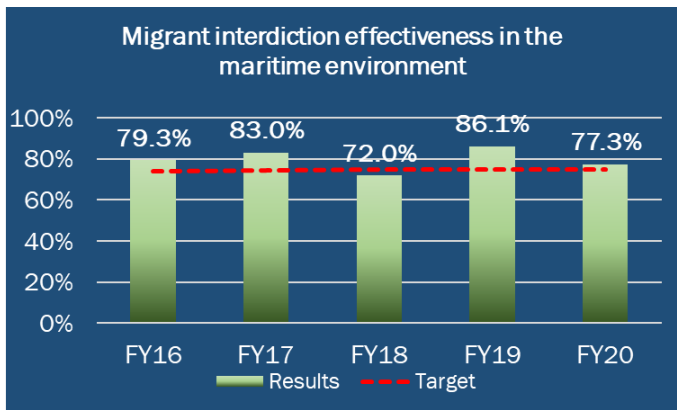


Patrol began implementing the federal regulation entitled *Suspending Introduction of Persons from a Country Where a Communicable Disease Exists* (85 Fed Reg 17060), which provides for persons subject to the order to be expelled from the U.S. as expeditiously as possible under Title 42 of the U.S. Code, instead of being subject to processing under Title 8. Title 42 actions accounted for about 30.2% of FY 2020 response efforts from March through the end of the fiscal year. Going forward, the Border Patrol will continue to shift resources to locations that commanders determine to be the best use of personnel and surveillance technology to meet estimated targets.

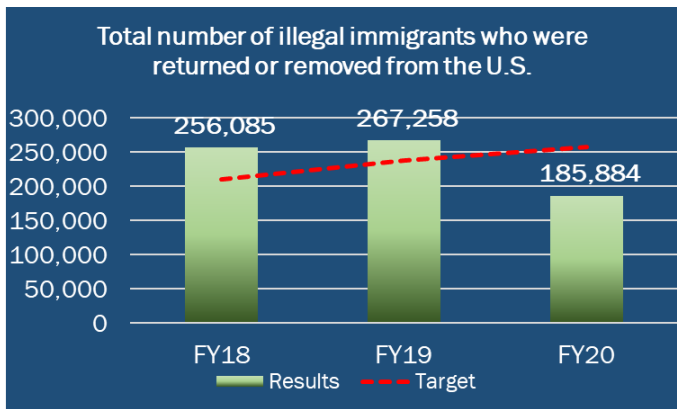
Did you **know?**

The Director of the Centers for Disease Control and Prevention (CDC), under the authority of the *Public Health Service Act*, directed CBP to prohibit the entry of persons originating from or who traveled through countries in which COVID-19 cases exist beyond a certain threshold.

**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. Most partner nation interdictions involve Haitian nationals who typically travel on larger conveyances with more migrants onboard. While the migrant interdiction rate has fluctuated over the past five years, the FY 2020 results are consistent with the overall average.

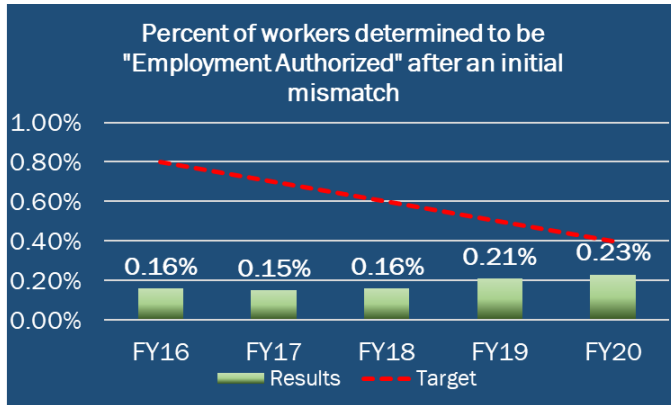


**Total number of illegal immigrants who were returned or removed from the United States (ICE):** This measure describes the total number of illegal immigrants returned and/or removed from the United States by ICE Enforcement and Removal Operations (ERO). The measure includes both immigrants who have entered the country illegally, but do not already have prior criminal conviction, along with those who have had a prior criminal conviction. This measure provides a complete picture of all the returns and removals accomplished by the program to ensure illegal immigrants do not remain in the United States. The decrease in removal actions is, in part, driven by less overall migration due to the pandemic, as well as other policy-related factors such as the effects of



## Management's Discussion and Analysis

Migrant Protection Protocols and humanitarian efforts impacting arrests. COVID-19 in conjunction with CDC guidance not to exceed 70% detention capacity also impacted removals.



**Percent of workers determined to be "Employment Authorized" after an initial mismatch (USCIS):** This measure provides a feedback mechanism to indicate the accuracy of E-Verify system reporting the number of cases in which adjudicating officials in the program find an alien "employment authorized" after an initial automated mis-match decision. Ensuring the accuracy of E-Verify processing 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. This measure assesses the accuracy of the [E-Verify](#) process by assessing the percent of employment verification requests that are not positively resolved during the initial review. This measure, which aims to be below the target (i.e., a less than measure) achieved 0.23 percent, meeting its target but slightly up compared to last year's result. 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. USCIS continues to increase the records available for electronic matching, which strengthens the program against identity fraud.

### Looking Forward


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

- **Implement the OPCON framework** which is the first goal in the [2020 U.S. Border Patrol Strategy](#). The OPCON Agency Priority Goal describes through quarterly public reporting on [performance.gov](#) progress in implementing this framework to enhance border security through three elements: Situational Awareness – collecting and assessing information and integrating that intelligence into our operations; Impedance and Denial – stopping illegal crossings or slowing them down to allow additional response time; and Response and Resolution – rapidly responding to threats determined in the areas of highest risk. This APG builds on foundational work previously done to develop the elements of OPCON and deploy the framework to all Southern Border Sectors and Stations. Efforts now are underway to develop Southwest Border sector strategies and data collection and build out the performance measures for the OPCON framework that will be used for the Northern Border. The [FY 2020-2021 OPCON Agency Priority Goal](#) is a tool to advance and report on the progress of the use of OPCON to ensure border security.
- **Remove those who have entered the country illegally:** [ERO](#) and the [Office of the Principal Legal Advisor](#) (OPLA) work to remove those who have entered the country illegally. While workload, technology, staffing, and interagency collaboration are challenges, these two programs are actively working to implement correction actions to maximize their effectiveness. To manage this workload, OPLA, ERO, and the Department of Justice (DOJ) are working together to improve processing while simultaneously addressing OPLA staffing models to align with court docket demands, DOJ Executive Office for Immigration

Review staffing, and the expansion of court facilities to address case backlog. ERO and OPLA will continue to work with communities to better support 287(g) type programs to get deportable immigrants into the process of being given a final order for removal.

- **Immigration Benefits and Fraud:**

Immigration Benefit Fraud is the willful misrepresentation of a material fact on a petition or application to gain an immigration benefit, often involving sophisticated schemes and multiple co-conspirators. USCIS has taken recent steps to address this to include: continuous immigration vetting for applicants filing Form N-400 (Application for Naturalization) until delivery of a benefit, including social media checks to identify publicly available social media information to identify



**Fraud Detection and National Security**  
VIGILANCE. INTEGRITY. PARTNERSHIP.

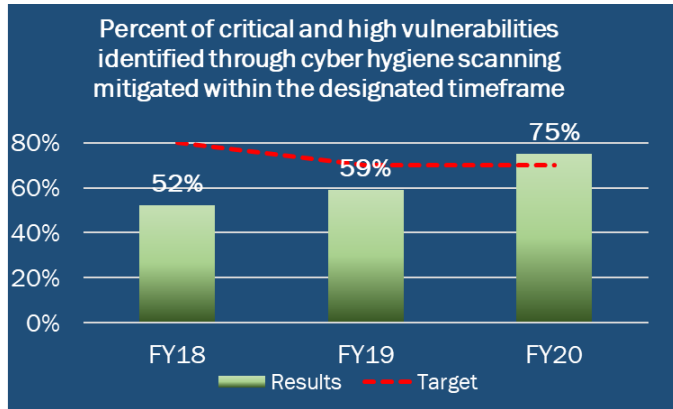
The USCIS Fraud Detection and National Security Directorate (FDNS) has vastly increased coordination with the Current and Emerging Threats Center by providing rapid responses to unclassified and classified requests for information. Topics have included at least 24 Immigration Systems Research Reports (ISRR) related to COVID-19 fraud, unauthorized test kits, and threats with an immigration nexus. Additional topics of intensive ISRR reporting have included Romanian Transnational Organized Crime and threats and criminal activity coming from Venezuela.

potential fraud, public safety, or national security concerns linked to persons requesting immigration benefit requests from USCIS to include primary applicants and their dependent family members. USCIS launched a new online tip form to help the public report suspected immigration benefit fraud and abuse. The online form is now available on the USCIS public website and has streamlined reporting by replacing three email boxes previously used to collect tips. It facilitates more efficient handling and provides the agency with the information needed to investigate and address benefit fraud and abuse.

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

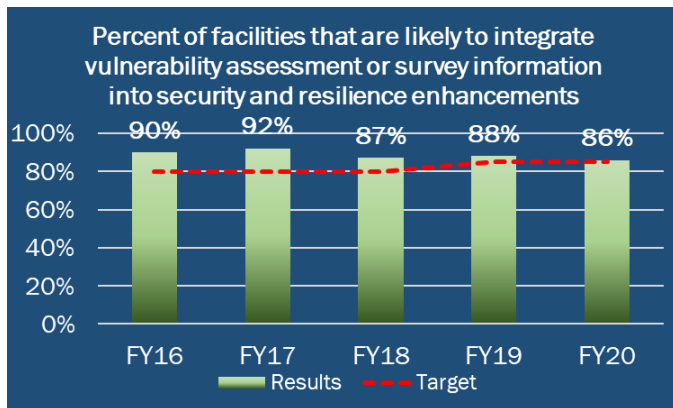
Increased connectivity of people and devices to the Internet and to each other has created an ever-expanding attack surface that transcends borders and penetrates almost every American home. In addition, the Federal Government depends on reliable and verifiable information technology systems and computer 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 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 agencies to aid in identifying and prioritizing vulnerabilities based on their severity for agencies to make risk-based decisions regarding their network security. For critical vulnerabilities, mitigation is required within 15 days from point of initial detection, and for high vulnerabilities mitigation is required within

30 days. Cyber hygiene scanning prioritizes vulnerabilities based on their severity as a means for agencies to make risk-based decisions regarding their network security. Identifying and mitigating vulnerabilities on a network in a timely manner is a critical component of an effective cybersecurity program, as it is critical to maintaining operational availability and the integrity of systems. With Binding Operational Directive 19-02 in effect since April 2019, federal agencies are demonstrating progress in addressing vulnerabilities within required timelines. This is evidenced by the increase in FY 2020 to 75.0 percent, significantly up from 2019. See the [Agency Priority Goals](#) section for more information on cybersecurity.



**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 maintained 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 civilian network:** CISA will gain appropriate visibility into the federal enterprise to assist in the safeguarding of systems and assets against a spectrum of risks. CISA continues to advance federal cybersecurity through its [FY 2020-2021 Agency Priority Goal](#) to mitigate, within 30 days, 75 percent of critical and high, configuration-based vulnerabilities identified through high value asset assessments, by September 30, 2021. Looking forward, CISA looks to enhance additional authorities to gain visibility into the federal enterprise and take action to safeguard

systems, instill a singleness of purpose to managing cybersecurity risks and protecting federal networks between DHS and agency network defense operators, to increase and improve tools and services to make federal networks more defensible and secure; and then to synthesize risk posture data and assessments to reduce exposure to threats.

- National Risk Management Center (NRMC)**: Critical infrastructure are those assets, systems, and networks that provide functions necessary for our way of life. From generating electricity to supplying clean water, there are [16 critical infrastructure sectors](#) that form a complex, interconnected ecosystem including communications, energy, transportation, emergency services, and water. Since the nation's critical infrastructure is largely owned and operated by the private sector, managing risk is a priority shared by industry and government. As the Department's planning, analysis, and collaboration center, the [NRMC](#) is working to bring 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 develop and improve their capability roadmap that will baseline current capabilities; identify critical infrastructure capability gaps and 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.

**CISA Gears Up For  
2020 Election Security**



#PROTECT2020  
cisa.gov

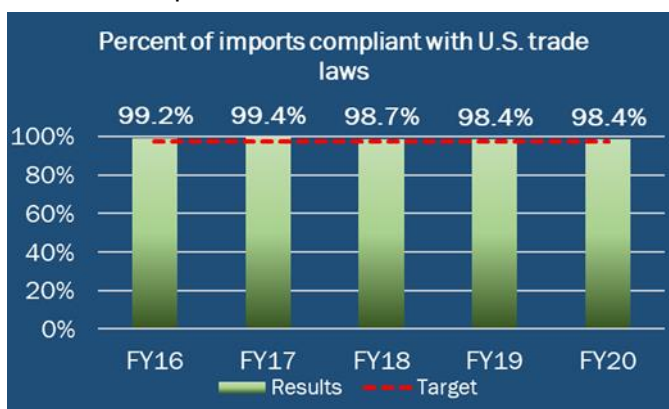
The Cybersecurity Program has worked closely with state and local election authorities to aid in their security improvements ahead of the 2020 election. CISA conducted numerous vulnerability assessments across the election stakeholder community, then briefed and distributed a unique report (highlighting key trends, vulnerabilities, and weaknesses) to several hundred election stakeholders. CISA has also worked closely with over 40 states on training exercises that simulate threat scenarios, including foreign disinformation campaigns and cyber-attacks on election infrastructure to bolster state and local incident-response plans.

**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.

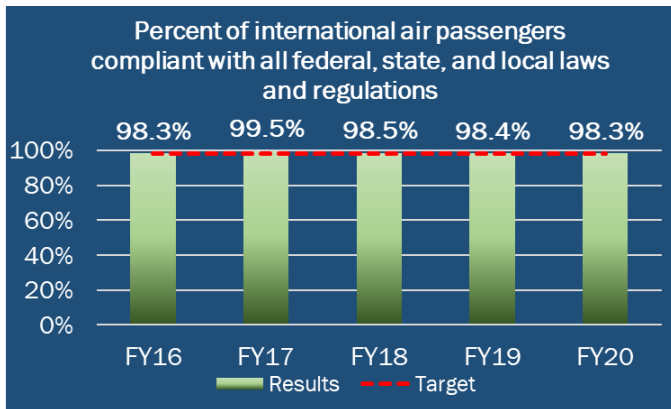
The following measures highlight some of our efforts to preserve and uphold the nation's prosperity and economic security. Up to five years of data is presented if available.

**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](#). 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 laws and regulations. In carrying out this task, CBP encourages importers to become familiar with applicable



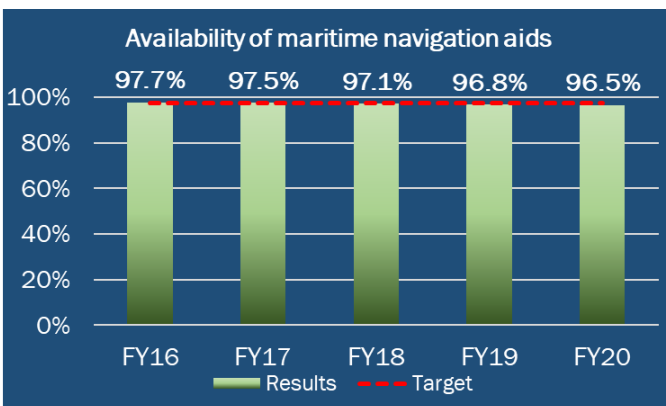
## Management's Discussion and Analysis

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 2020 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.



**Percent of international air passengers compliant with all federal, state, and local laws and regulations (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 2020, 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 year, compliance remained 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](#).

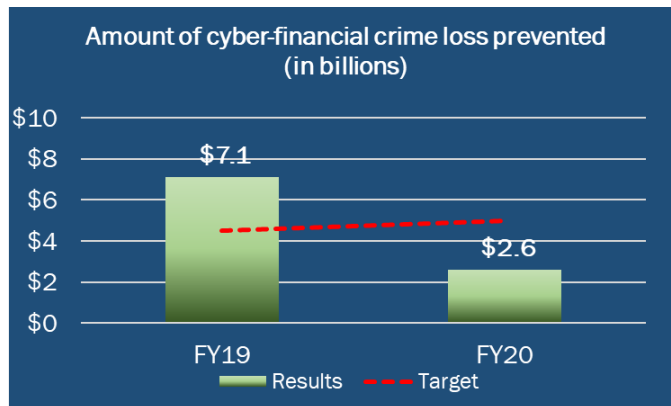


**Availability of maritime navigation aids (USCG):** This measure indicates the hours that short-range federal [Aids to Navigation](#) (ATON) are available as defined by the International Association of Marine Aids to Navigation and Lighthouse Authorities in December 2004. As the Road Signs of the Sea, maritime navigational aids ensure safety of maritime traffic and the safe passage of trillions of dollars of economic activity. In FY 2020, this measure achieved 96.5 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 is exploring solutions to mitigate this risk.

**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](#). 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. The measure reflects USSS’ efforts, in conjunction with partners, to reduce financial losses to the public attributable to cyber-financial crimes. In FY 2020, this measure achieved \$2.60 billion in loss prevention. The disparity from FY 2019 is the result of a very large case closure in FY 2019 (more than \$4 billion) and the impact of COVID-19 in FY 2020. The USSS relies on partnerships with a variety of other law enforcement agencies to investigate highly complex cyber-financial criminal investigations; however, due to COVID-19, investigations have been impacted and the U.S. court system has slowed. In addition, as a result of the pandemic, the USSS has continually adapted to safeguard the integrity of the financial system and has swiftly reacted to fraudulent activity associated with the pandemic and the *Coronavirus Aid, Relief, and Economic Security (CARES) Act* (P.L. 116-136) . In FY 2020, the pace of USSS investigations did not decrease, and these investigations resulted in 1,620 arrests.



**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 balance security with delivering service expected by trade partners and the traveling public. Looking forward, CBP is investing in advanced analytics to provide predictive and prescriptive analyses to better target those trying to circumvent the systems. In addition, CBP continues to enhance the Automated Commercial Environment (ACE)—the single system used by all government agencies to process cargo imports and exports, and collect duties, taxes, and fees. Other areas of focus include refinements to the Automated Targeting System, fed by ACE inputs, to advance homeland security while facilitating trade. Lastly, CBP and TSA are looking to expand partnerships and leverage parallel operational processes (e.g., facial recognition; baggage screening) to reduce duplication, delays and redundant processing for travelers, leveraging technology development and acquisition to the benefit of both organizations.

CBP launched the U.S.–Mexico–Canada Agreement (USMCA) Center July 1, 2020, to coordinate implementation of the USMCA, which replaced the North American Free Trade Agreement (NAFTA). Staffed with CBP experts from operational, legal, and audit disciplines, and in collaboration with Canadian and Mexican customs authorities, the USMCA Center is a cornerstone of CBP’s USMCA implementation plan. It will serve as a central communication hub for CBP and the private sector, ensuring a smooth and efficient transition from NAFTA to USMCA.



The USSS led the investigation against Aleksey Burkov, who was sentenced to 9 years in June 2020. Burkov is notorious to international law

enforcement as the owner of Cardplanet, a database of payment card numbers stolen through network intrusion. Burkov also ran a site for cybercriminals to advertise stolen goods, like the personal information of potential fraud victims. With their training and expertise, USSS agents prevented \$75M in potential loss with this successful investigation.

- **Combating cybercrime and safeguarding the nation's financial system:**

Cybercrime is 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, developing the Electronic Crimes Task Force modernization plan to

strengthen and expand the existing network of task forces to address growing cybercriminal threats and 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 developing 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 is addressing online trafficking in counterfeit and pirated goods, exploring expanded use of verifiable digital trademarks.
- USCG plans include the enhancement of the security of the service's cyber networks, bolstering new efforts on offensive cyber capabilities, to help safeguard the maritime domain and related infrastructure.

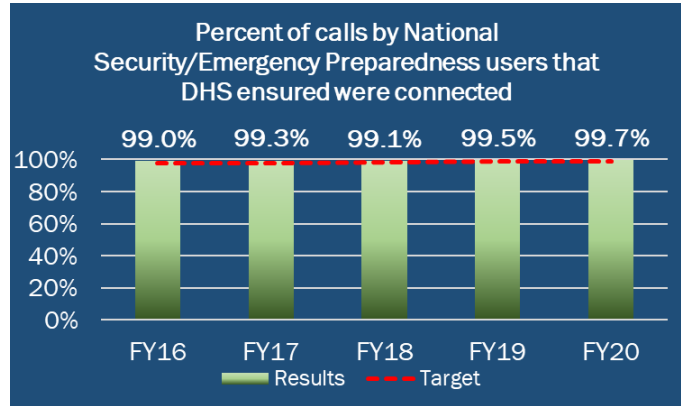
### **Goal 5: Strengthen Preparedness and Resilience**

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 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.



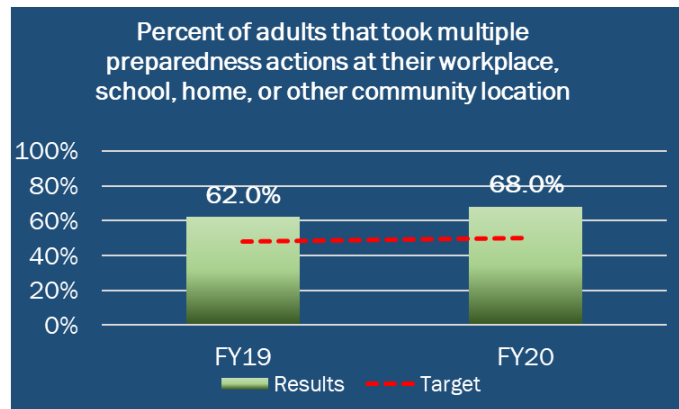
**Percent of calls by National Security/Emergency Preparedness users that DHS ensured were connected (CISA):** By ensuring the connection of calls for first responders and government officials during a disaster, DHS contributes to a national effective emergency response effort. This measure gauges the 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 2020, this measure achieved 99.7 percent call completion which is above target and in-line with results over the past five years. Due to COVID-19, there was an approximately 25 percent increase in call volume using GETS. By ensuring effective emergency communications, DHS contributes to a national effective emergency response effort which helps strengthen national preparedness and resilience.



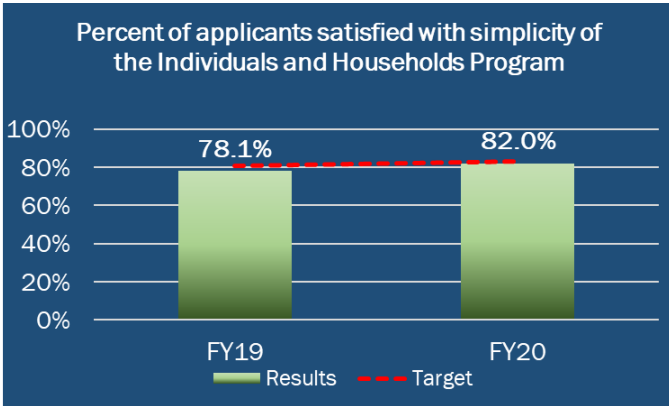
**Did you know?**

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.

**Percent of adults that took multiple preparedness actions at their workplace, school, home, or other community location in the past year (FEMA):** This is the second year for this measure reporting results. This measure indicates how many Americans have taken action to prepare for an emergency and provides feedback regarding the effectiveness of efforts to encourage this activity. This measure reports the share of all respondents to [FEMA’s annual National Household Survey](#) who answered affirmatively to questions assessing whether they had taken more than one preparedness action in the past year, whether taking these actions at their workplace, school, home, or other community location. Many Americans will experience a disaster or emergency at some point and FEMA emphasizes the importance of a national approach to preparedness and will use results from this measure to assess the agency’s effectiveness. In FY 2020, this measure achieved 68 percent which is above target. These efforts help motivate communities and individuals to act and to serve as a contributing factor to the increase in preparedness actions.

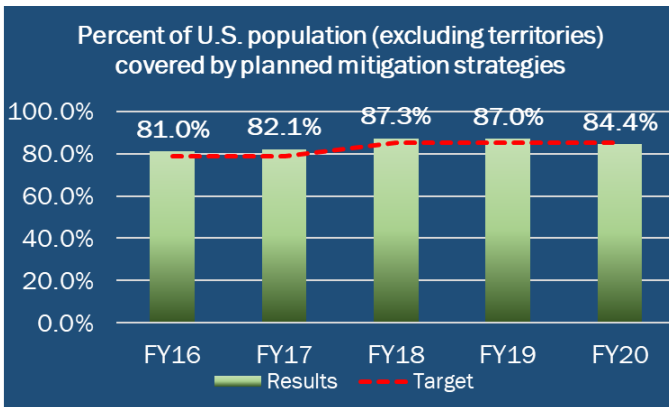


Management’s Discussion and Analysis



**Percent of applicants satisfied with simplicity of the Individuals and Households Program (FEMA):** This is the second year for this measure reporting results. This measure provides information on disaster survivors’ impressions about the simplicity of the procedures required to receive disaster relief from the [Individuals and Households Program](#) (IHP). The program collects survivors’ impressions of their interactions with IHP using standard surveys, administered by telephone, at three

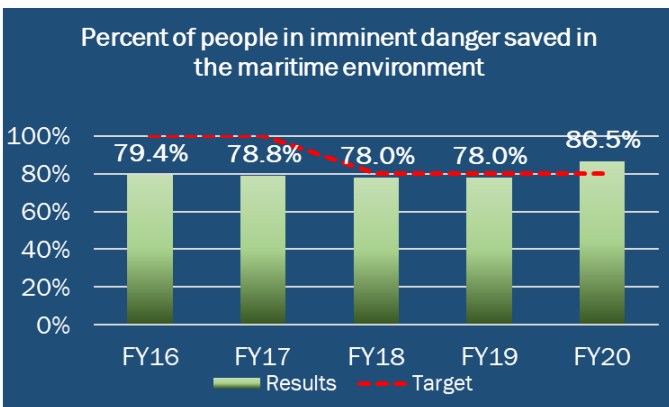
touchpoints of their experience with FEMA. Managers use insights derived from survey results to help identify procedural improvements. Feedback from disaster survivors will ensure that the program provides clear information and high-quality service in critical, public-facing agency activities. In FY 2020, this measure achieved 82 percent, narrowly missing the target. After a detailed analysis of the survey results, it was determined that the primary issue was the ease of use of disaster assistance information. FEMA’s Individual Assistance (IA) program developed an internal Strategic Plan to improve survivor-centric operations. IA is also deploying a new survey in fiscal year 2021 which is intended to help identify specific causes of applicant dissatisfaction. This will help IA target specific areas for staff training to improve the customer experience.



**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](#). The population of each community with approved or approvable local Hazard Mitigation Plans is used to calculate the percent of the national population. In FY 2020, this measure achieved 84.4 percent which is below target. The COVID-19

pandemic has hindered the plan development and approval process. Regional planners are encountering delays in plan submission as the staff of states and local communities have reallocated their time and resources to provide an adequate response to manage the emergency. The community resources needed to coordinate and execute plan development activities will

continue to be diverted in support of the COVID-19 response, causing plan coverage to lapse for some jurisdictions.




**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 2020, the USCG achieved 86.5 percent which is above target and is the 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.

- COVID-19 Implications:** FEMA has provided front-line support for the U.S. response to the pandemic. FEMA released the COVID-19 Pandemic Operational Guidance for the 2020 Hurricane Season, which outlines how FEMA plans to adapt to response and recovery operations in a COVID-19 environment. At the same time, FEMA guidance also has implications moving forward, such as the mix of personnel required for COVID-19 response beyond the current hurricane season. This guidance also helps to shape a shared understanding with regard to roles and expectations among local and regional emergency managers and FEMA. The pandemic also impacts current and future requirements for response and recovery logistics and products, such as determining eligible work and costs for non-congregate sheltering in response to a Presidentially declared emergency or major disaster, processing a Fire Management Assistance Grant, how to manage communications, training, and the use of virtual tools 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 or loss by rendering aid in the maritime environment to persons in distress and property has always been 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.



The Response and Recovery program published the COVID-19 Pandemic Operational Guidance (CPOG) to help emergency managers and public health officials best prepare for response and recovery operations. The program hosted seven webinars on CPOG, reaching 2,500 participants. About 85% of participants considered adjusting existing plans to account for the COVID-19 constraints in preparation for the upcoming hurricane season. Several regions mentioned that the CPOG prepared them to meet survivor needs by reinventing their processes.

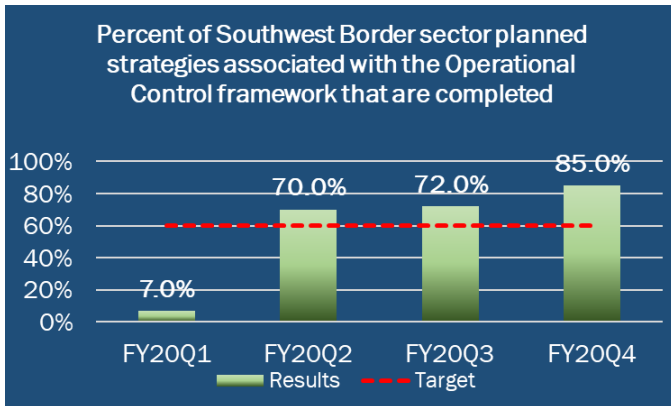
### Agency Priority Goals

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](https://www.performance.gov).

**APG: Enhance Southern Border Security**

**Goal Statement:** Improve security along the U.S. borders between ports of entry with emphasis on the Southwest Border. By September 30, 2021, 90% of Southwest Border sector strategies associated with the Operational Control framework will have been completed.

DHS's FY 2020-2021 APG, *Enhance Southern Border Security*, is a follow-on APG to continue to improve security along the Southwest Border between ports of entry. The goal is focused on improving on previous work to enhance the [OPCON](#) framework between ports of entry in Border Patrol Sectors along the Southwest Border. This framework relies on the interconnectedness of the three pillars of OPCON: Situational Awareness; Impedance and Denial; and Law Enforcement Resolution. Implementation of the OPCON framework aligns strategies, tools, and tactics across the Southern Border to enhance border security.



**Key Measure: Percent of Southwest Border sector planned strategies associated with the Operational Control framework that are completed:**

This measure gauges the percent of planned strategies that were executed by the nine Southwest Border sectors of the Border Patrol, as part of the sector Concept of Operations (CONOPs) Plans associated with the Operational Control (OPCON) framework. A planned strategy is defined in the OPCON Planning Guidance as the ways and means by which

each sector plans to mitigate or address their highest priority capability gaps using operations, technology deployments, and partnerships. Sectors submit their CONOPs at the start of the fiscal year to describe how each will work to improve elements of operational control through specific strategies. Quarterly reports provide progress updates regarding execution of sector strategies, along with initial sector data on measures associated with the OPCON framework. This measure is valuable in demonstrating sectors' early efforts to operationally use the OPCON framework to improve security along the Southwest Border. The results for this measure exceeded the annual target with the bulk of the implementation in the 2<sup>nd</sup> quarter.

**APG: Strengthen Federal Cybersecurity**

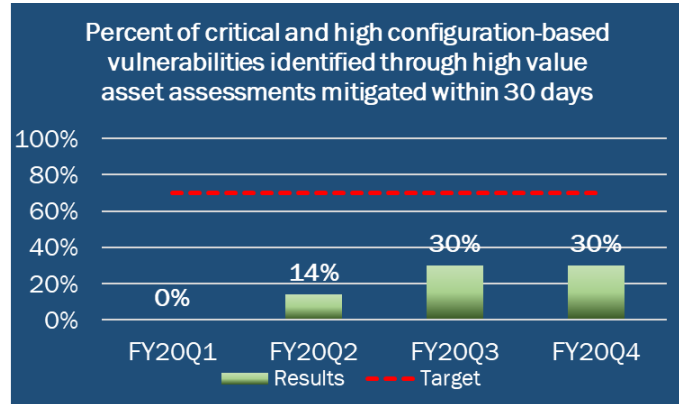
**Goal Statement:** Protect federal networks by defending against threats and assisting agencies in managing risk. By September 30, 2021, 75% of critical and high configuration-based vulnerabilities identified through high value asset assessments will be mitigated within 30 days.

DHS's [Cybersecurity FY 2020-2021 APG](#) focuses on strengthening the defense of the federal civilian network. Cybersecurity threats to federal networks continue to grow and evolve. Continuous scanning, intrusion prevention, and vulnerability assessments have allowed DHS to augment existing agencies' capabilities with additional tools and information to assist them in taking timely and appropriate risk-based actions to defend their networks. Through the increased dissemination of cyber threat and vulnerability information in near real time to federal agencies, the goal is to mitigate 70% of significant (critical and high) vulnerabilities identified through DHS scanning.

**Key Measure: Percent of critical and high configuration-based vulnerabilities identified through high value asset assessments mitigated within 30 days:**

This measure reports the percent of critical and high configuration-based vulnerabilities identified in High Value Assets (HVA) assessments that have been mitigated within 30 days. HVA assessments are performed across the Federal Government to identify vulnerabilities associated with the most sensitive Information Technology (IT) systems and data.

Configuration-based vulnerabilities are those that can be more quickly mitigated by agencies and departments through such actions as changing security settings, software or configuration changes, patching software vulnerabilities, and adjusting user account privileges. Agencies and departments report monthly to the program on the status of mitigating these configuration-based vulnerabilities. DHS will also continue to engage with senior agency leadership and appropriate information technology and security experts to apply cybersecurity programs and agency cybersecurity practices to ensure the successful implementation of activities to enhance the security of the federal network.



## 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—report the financial position and results of operations of the Department, including long-term commitments and obligations. The statements have been prepared pursuant to the requirements of Title 31, United States Code, Section 3515(b), in accordance with U.S. generally accepted accounting principles and the formats prescribed by OMB. These statements are in addition to the financial reports used to monitor and control budgetary resources, which are prepared from the same books and records. The statements should be read with the realization that they are for a component of the Federal Government, a sovereign entity.

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.

### 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's efforts in preparedness and readiness have facilitated a rapid, whole-of-government response in confronting COVID-19, keeping Americans safe, and helping detect and slow the spread of the virus. 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 CARES Act to support our essential missions and to respond to our nations' needs, including personal protective equipment, temporary medical facilities, and lost wages assistance. FEMA continues to work with the state and territorial governments (including the District of Columbia) that have chosen to participate in the Lost Wages Assistance Program to provide up to six weeks of assistance to eligible individual claimants that were unemployed or partially underemployed due to COVID-19 disruptions.

FEMA activated the National Response Coordination Center (NRCC) in the wake of the Coronavirus outbreak in the United States. 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 has been monitoring 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 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. DHS CWMD's early involvement in the COVID-19 screening process helped ease the burden on CDC medical professionals who would be tasked with medical screening. Working within CWMD, the Department's Chief Medical Officer has deployed public health and medical experts to the Nation's hot spots and is coordinating DHS vaccine planning.

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 2020	FY 2019	\$ Change	% Change
Fund Balance with Treasury	\$ 131,013	\$ 108,971	\$ 22,042	20%
Property, Plant, and Equipment	26,561	24,673	1,888	8%
Other Assets	25,435	24,455	980	4%
<b>Total Assets</b>	<b>183,009</b>	<b>158,099</b>	<b>24,910</b>	16%
Federal Employee and Veterans' Benefits	69,814	65,107	4,707	7%
Debt	20,596	20,596	-	0%
Accounts Payable	5,274	4,464	810	18%
Deferred Revenue and Advances	3,163	3,001	162	5%
Insurance Liabilities	2,830	3,389	(559)	-16%
Accrued Payroll	3,404	2,889	515	18%
Other Liabilities	28,350	13,463	14,887	>100%
<b>Total Liabilities</b>	<b>133,431</b>	<b>112,909</b>	<b>20,522</b>	18%
Total Net Position	49,578	45,190	4,388	10%
<b>Total Liabilities and Net Position</b>	<b>\$ 183,009</b>	<b>\$ 158,099</b>	<b>\$ 24,910</b>	16%

Results of Operations (\$ in millions)	FY 2020	FY 2019	\$ Change	% Change
Gross Cost	\$ 127,215	\$ 80,818	\$ 46,397	57%
Less: Revenue Earned	(14,874)	(15,655)	781	-5%
<b>Net Cost Before Gains and Losses on Assumption Changes</b>	<b>112,341</b>	<b>65,163</b>	<b>47,151</b>	72%
(Gains) and Losses on Assumption Changes	3,061	924	2,137	>100%
<b>Total Net Cost</b>	<b>\$ 115,402</b>	<b>\$ 66,087</b>	<b>\$ 49,315</b>	75%

**Assets – What We Own and Manage**

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

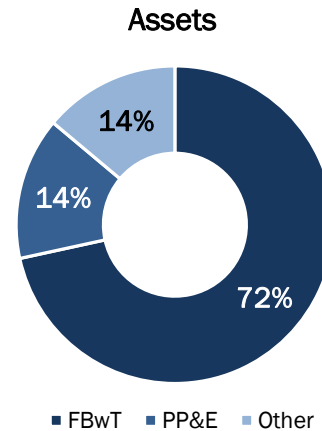
The Department’s largest asset is *Fund Balance with Treasury (FBwT)*, which consists primarily of appropriated, revolving, trust, deposit, receipt, and special funds remaining at the end of the fiscal year.

*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.

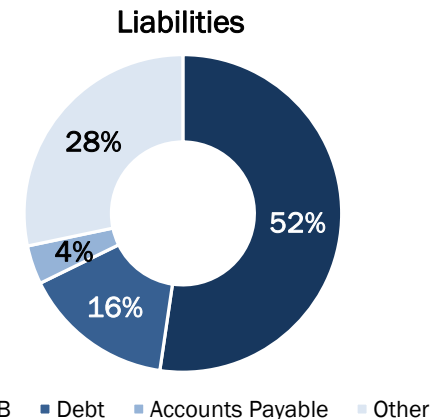
As of September 30, 2020, the Department had \$183 billion in assets, representing a \$24.9 billion increase from FY 2019. The majority of this change is due to an increase in Fund Balance with Treasury resulting from additional supplemental appropriations received under the CARES Act (see Note 31 in 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 Veterans’ Benefits (FEVB)*. 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 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.

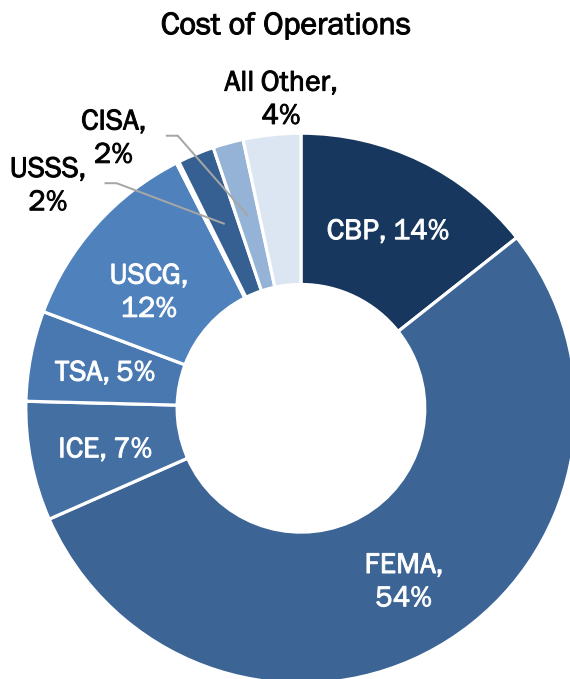


*Other Liabilities* include amounts owed to other federal agencies and the public for goods and services received by the Department, amounts received by the Department for goods or services that have not been fully rendered, unpaid wages and benefits for current DHS employees, and amounts due to the Treasury’s general fund, environmental liabilities, refunds and drawbacks, and other. This includes grants provided by FEMA to participating states, territories, and the District of Columbia for lost wage assistance.

As of September 30, 2020, the Department reported approximately \$133.4 billion in total liabilities. Total liabilities increased by \$20.5 billion in FY 2020 mostly due to FEMA’s Lost Wages Assistance Program in addition to FEMA’s grants payable activity related to disasters including fires, hurricanes and COVID 19 (see Note 18 in the Financial Information section).

**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 \$49.6 billion. Total net position increased \$4,.4 billion from FY 2019, 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 \$112.3 billion in FY 2020. DHS recognized increased costs of \$47.1 billion in FY 2020 due to costs associated with disaster responses to COVID-19, hurricanes, and wildfires.

During FY 2020, the Department earned approximately \$14.9 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

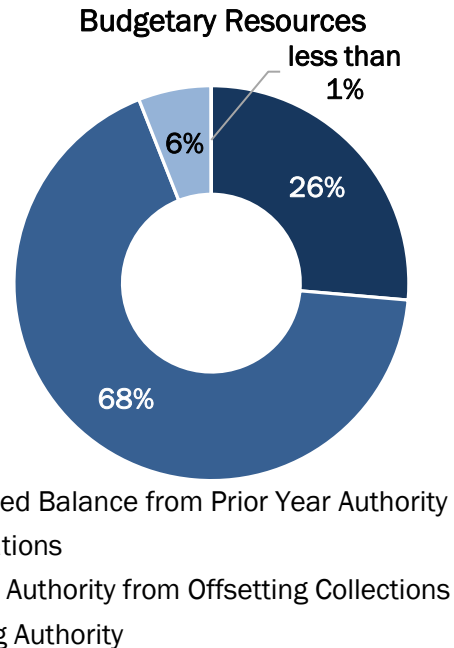
operations. The Department also collects non-exchange duties, taxes, and fee revenue on behalf of the Federal Government. This non-exchange revenue is presented in the Statements of Custodial Activity or Statements of Changes in Net Position, rather than the Statements of Net Cost.

## Budgetary Resources

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 2020	FY 2019	\$ Change	% Change
Unobligated Balance from Prior Year Authority	\$ 51,848	\$ 50,768	\$ 1,080	2%
Appropriations	133,025	76,512	56,513	74%
Spending Authority from Offsetting Collections	11,732	12,738	(1,006)	-8%
Borrowing Authority	33	67	(34)	-51%
<b>Total Budgetary Authority</b>	<b>\$ 196,638</b>	<b>\$ 140,085</b>	<b>\$ 56,553</b>	<b>40%</b>

The Department’s budgetary resources were \$196.6 billion for FY 2020. The authority was derived from \$51.8 billion in authority carried forward from FY 2019, appropriations of \$133 billion, approximately \$11.7 billion in collections, and \$33 million in borrowing authority. Budgetary resources increased approximately \$56.6 billion from FY 2019. This is mainly due to additional supplemental appropriation for COVID-19. Of the total budget authority available, the Department incurred a total of \$160.5 billion in obligations from salaries and benefits, purchase orders placed, contracts awarded, or similar transactions.



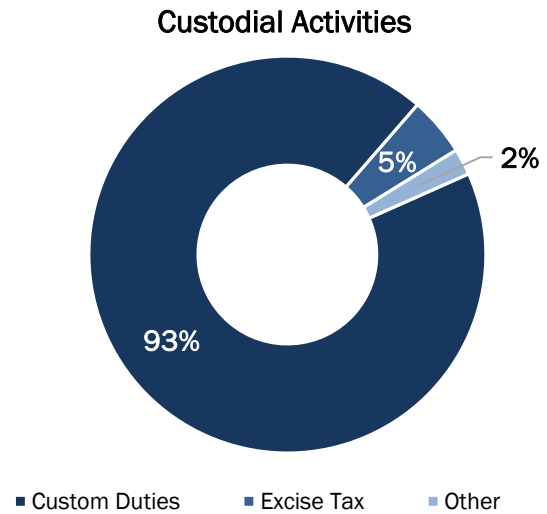
## Custodial Activities

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

Cash Collections (\$ in millions)	FY 2020	FY 2019	\$ Change	% Change
Cash Collections from Duties	\$ 74,401	\$ 71,902	\$ 2,499	3%
Excise Tax	3,967	3,889	78	2%
Other	1,706	2,058	(352)	-17%
<b>Total Cash Collections</b>	<b>\$ 80,074</b>	<b>\$ 77,849</b>	<b>\$ 2,225</b>	<b>3%</b>

Custodial activity includes the revenue collected by the Department on behalf of others, and the disposition of that revenue to the recipient entities. Non-exchange revenue is either retained by the Department to further its mission or transferred to Treasury’s general fund and other federal agencies. The Department’s total cash collections is \$80 billion. Total cash collections increased \$2.2 billion from FY 2019. This increase is mainly due to tariffs placed on products from certain countries.

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.



**Supplementary 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 2020) in human capital, research and development, and non-federal physical property are shown below.

**Investments in Research and Development**

Investments in research and development represent expenses incurred to support the search for new or refined knowledge and ideas. The intent of the investment is to apply or use such knowledge to improve and develop new products and processes with the expectation of maintaining or increasing national productive capacity or yielding other future benefits. S&T, CWMD, and USCG have made significant investments in research and development this fiscal year (in millions):

Components	FY 2020
S&T	\$ 827
CWMD	51
USCG	7
<b>Total Research &amp; Development</b>	<b>\$ 885</b>

**Investments in Human Capital**

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

Components		FY 2020
	FEMA	\$ 86
	S&T	3
<b>Total</b>	<b>Human Capital</b>	<u>\$ 89</u>

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

Components	FY 2020
TSA	\$ 191
<b>Total Non-Federal Physical Property</b>	<u>\$ 191</u>

**Other Key Regulatory Requirements**

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

## Secretary's Assurance Statement

November 13, 2020



The Department of Homeland Security management team 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 control inclusive of financial management systems that protect the integrity of federal programs. These objectives are satisfied by managing risks and maintaining effective internal control over three internal control objectives: effectiveness and efficiency of operations; reliability of reporting; and compliance with applicable laws and regulations. The Department conducted its assessment of risk and internal control in accordance with the Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. Based on the results of the assessment, the Department can provide reasonable assurance that internal control over operations, reporting, and compliance were operating effectively as of September 30, 2020, 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 control over financial reporting. The Department conducted its assessment of the effectiveness of internal control 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 control over financial reporting was designed and operating effectively, except for Financial Reporting and Information Technology Controls and Information Systems, where areas of material weaknesses have been identified and remediation is in process.

Due to financial management system limitations at select Components, the Department does not fully comply with government-wide requirements, including federal accounting standards and application of the United States Standard General Ledger at the transaction level. In addition, the area of material weakness related to Information Technology Controls and Information Systems stated above affects the Department's ability to substantially comply with the *federal Financial Management Improvement Act of 1996* (FFMIA) financial management system requirements. Therefore, the Department is reporting a noncompliance with FFMIA and Section 4 of FMFIA.

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 black ink, appearing to read "Ch. O. ...".

Acting Secretary of Homeland Security

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

November 13, 2020

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

Dear Inspector General Cuffari:

The United States Department of Homeland Security (DHS) internal control over financial reporting is 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 accounting principles generally accepted in the United States of America. An entity's internal control 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 accounting principles generally accepted in the United States of America, and that receipts and expenditures of the entity 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 entity's assets that could have a material effect on the financial statements.

Management of DHS is responsible for designing, implementing, and maintaining effective internal control over financial reporting. Management assessed the effectiveness of the DHS's internal control over financial reporting as of September 30, 2020, based on criteria established in the *Standards for Internal Control 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, 2020, the DHS's internal control over financial reporting is effective except for areas of material weaknesses in Financial Reporting and Information Technology Controls and Information Systems. Specifically:

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

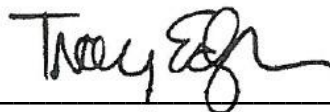
DHS has made progress in improving its internal controls and financial management program. Management commits to implementing corrective actions to resolve the remaining areas of material weakness.

Best Regards,



---

Chad F. Wolf  
Acting Secretary



---

Troy D. Edgar  
Chief Financial Officer

## Management Assurances

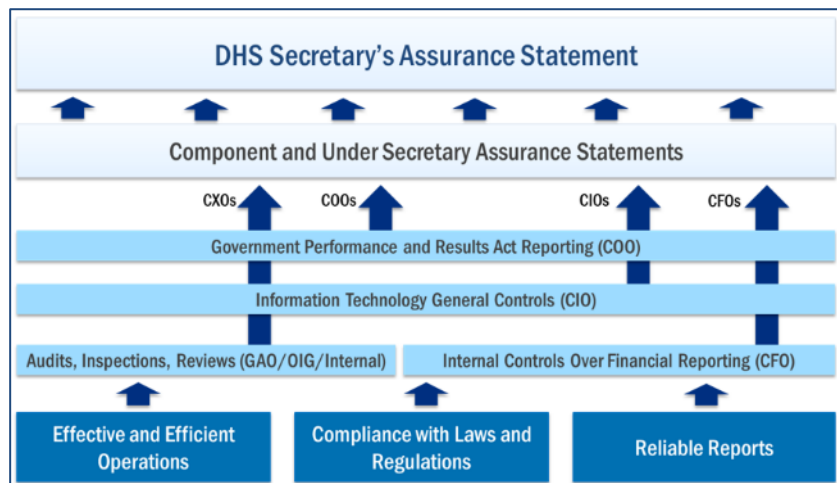
DHS management is responsible for establishing, maintaining, and assessing internal controls to provide reasonable assurance that the objectives of the *Federal Managers’ Financial Integrity Act of 1982* (31 United States Code 3512, Sections 2 and 4) and the *Federal Financial Management Improvement 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 the 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 FFMIA 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, inspections, and investigations performed by the Department’s Office of Inspector General (OIG) and GAO. Using available information, each Component performs an analysis on the



pervasiveness and materiality over any identified deficiencies to determine their impact and uses the result as the basis for the respective Component assurance statement signed by the Component Head. The Secretary provides assurances over the Department's internal controls in the annual assurance statement considering the state of internal controls at each Component.

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 update the Department's risk profile annually beginning in FY 2021.

#### **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 test 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 2019, management reported two areas of material weaknesses: 1) financial reporting and 2) IT controls and system functionality. In FY 2020, 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 2021.

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

Area of Material Weakness	DHS Component(s)	Year Identified	Target Correction Date
	All	FY 2003	FY 2021
Financial Reporting	<p>Multiple deficiency areas exist that are attributed to the financial reporting area of material weakness, which include the following:</p> <ul style="list-style-type: none"> <li>• <b>Journal Entry / On-Top Adjustments and Beginning Balances</b> (Contributing Component(s): CBP, FEMA, MGMT, &amp; USCG) <ul style="list-style-type: none"> <li><u>Deficiency Details</u> <ul style="list-style-type: none"> <li>○ USCG determined that controls over the journal entry / on-top adjustment process and beginning balances were not operating effectively in FY 2020 and could not provide reasonable assurance that risks had been sufficiently mitigated. In addition, ineffective IT system controls have contributed to this area, due to system risk around the integrity of data and automated controls. Refer to the IT Controls and Information Systems area of material weakness and corrective actions for more detail.</li> <li>○ Process deficiencies related to reviews, validations, and USSGL accounts used regarding manual journal entries were noted at CBP, FEMA, and MGMT.</li> </ul> </li> <li><u>Planned Corrective Actions</u> <ul style="list-style-type: none"> <li>○ USCG will test the journal entry / on-top adjustment process as part of its annual assessment. In addition, USCG will continue to improve its procedures and supporting documentation to better explain and support the respective entries.</li> <li>○ Process improvements for manual journal entries will be developed, implemented, and assessed in accordance with Component remediation plans.</li> </ul> </li> </ul> </li> <li>• <b>Other</b> (Contributing Component(s): All) <ul style="list-style-type: none"> <li><u>Deficiency Details</u> <ul style="list-style-type: none"> <li>○ Several deficiencies aggregated to substantiate inclusion into this area of material weakness. These include 1) lack of monitoring of service providers, 2) ineffective controls over system generated data and reports, commonly referred to as information produced by the entity (IPE), and 3) inability to record trading partner activity at the initiation of the transaction event due to system limitations.</li> </ul> </li> <li><u>Planned Corrective Actions</u> <ul style="list-style-type: none"> <li>○ For service provider monitoring controls, DHS continues to build improvements utilizing a risk-based management program to provide monitoring and oversight of service providers.</li> <li>○ DHS will utilize a similar risk-based strategy for identifying and assessing IPE going forward with anticipation that this will be a multi-phased effort.</li> <li>○ DHS is in the process of implementing G-Invoicing which will help reduce the risk of system limitations.</li> </ul> </li> </ul> </li> </ul>		

**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"> <li>• <b>Financial System Requirements</b> (Contributing Component(s): All) <ul style="list-style-type: none"> <li><u>Deficiency Details</u> <ul style="list-style-type: none"> <li>○ The Federal Information Security Management Act (FISMA) mandates that federal agencies maintain IT security programs in accordance with OMB and National Institute of Standards and Technology guidance. The Department internal control assessment identified IT controls as a material weakness due to deficiencies surrounding general security and application controls. As a result of the noted deficiencies, the Department’s financial systems are unable to fully comply with the FFMIA.</li> </ul> </li> <li><u>Planned Corrective Actions</u> <ul style="list-style-type: none"> <li>○ Components will continue to implement the find, fix, test strategy in FY 2021. The IT Commitment Letters, signed by both the respective CFO and the Chief Information Officer (CIO) leadership, require each Component to commit to testing as well as provide commitment to passing results for each system and control in scope.</li> <li>○ The DHS CFO, CIO, and Component leadership will support the Components in the design and implementation of internal controls in accordance with DHS policy requirements defined for CFO Designated Financial Systems.</li> </ul> </li> </ul> </li> <li>• <b>System Functionality / Information Derived from Systems</b> (Contributing Component(s): All) <ul style="list-style-type: none"> <li><u>Deficiency Details</u> <ul style="list-style-type: none"> <li>○ Ineffective IT security control and inadequate application / functionality controls impact the ability for management to fully rely on system generated data and reports without putting the processes utilizing this information at risk. Currently, these deficiencies are directly associated with financial system requirement deficiencies.</li> </ul> </li> <li><u>Planned Corrective Actions</u> <ul style="list-style-type: none"> <li>○ Components will continue to improve and enhance IT security, as noted above for Financial System Requirements. As IT security enhances reliability, DHS will also work to incorporate the find, fix, test strategy to gain coverage over application / functionality controls.</li> <li>○ In FY 2021, in addition to fixing long-standing IT control weaknesses, DHS will implement a risk-based strategy for identifying and testing IPE and/or information derived from systems. DHS will also establish an approach to assess the key functionality of systems that have sufficient IT security controls established.</li> </ul> </li> </ul> </li> <li>• <b>Service Provider Monitoring</b> (Contributing Component(s): All) <ul style="list-style-type: none"> <li><u>Deficiency Details</u> <ul style="list-style-type: none"> <li>○ The Department did not maintain effective internal control related to service organizations, including evaluating and documenting roles of service organizations, performing effective reviews of service organization control (SOC) reports, and addressing service provider risk in absence of SOC reports.</li> </ul> </li> <li><u>Planned Corrective Actions</u> <ul style="list-style-type: none"> <li>○ For service provider monitoring controls, DHS continues to build improvements utilizing a risk-based management program to provide monitoring and oversight of service providers.</li> </ul> </li> </ul> </li> </ul>		

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

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

DHS assesses financial management systems annually for compliance with the requirements of Appendix D to OMB Circular A-123 and other federal financial system requirements. In addition, available information from audit reports and other relevant and appropriate sources, such as FISMA compliance activities, is reviewed to determine whether DHS financial management systems substantially comply with FFMIA. Improvements and ongoing efforts to strengthen financial management systems are considered as well as the impact of instances of non-compliance on overall financial management system performance.

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

**Table 3: FFMIA Non-compliance Details and Corrective Actions**

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

### **Digital Accountability and Transparency Act of 2014**

Pursuant to OMB Circular A-123, Appendix A, *Management of Reporting and Data Integrity Risk*, the Department issued its *Digital Accountability and Transparency Act of 2014* (DATA Act) Data Quality Plan on March 15, 2019. The plan describes the organizational structure, operating environment, internal controls processes, and systems used to generate and evaluate the data published to USAspending.gov. The plan includes DHS's processes for compiling, reviewing, and monitoring the quality of data provided to USAspending.gov. In addition, the plan describes the processes to assess the level of data quality, methods for increasing the data quality, and the data risk management strategy. The outcomes of this plan align with the Administration's goal for greater transparency, ultimately benefiting citizens and holding government accountable for its stewardship over its assets.

In prior years, Components assessed 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. In FY 2020, DHS utilized a risk assessment process to identify high risk data elements and tested the accuracy, completeness, and timeliness of the recorded transactions against source documents. Deficiencies were identified during testing and aggregated to a level of control deficiency, where management can provide reasonable assurance over the submitted data. 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 addition, to continue making improvements and enhancements to the Department's DATA Act reporting processes and controls, an enhanced Component corrective action plan process was implemented 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.

## Management's Discussion and Analysis

- 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 Management Systems Solution, 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 remains on schedule to go-live in October 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, 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 2021 for FEMA as well as ICE and its customer Components<sup>2</sup>.

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 directive<sup>3</sup> 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.

---

<sup>2</sup> ICE serviced Components include: S&T, Management Directorate, CISA, and USCIS

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

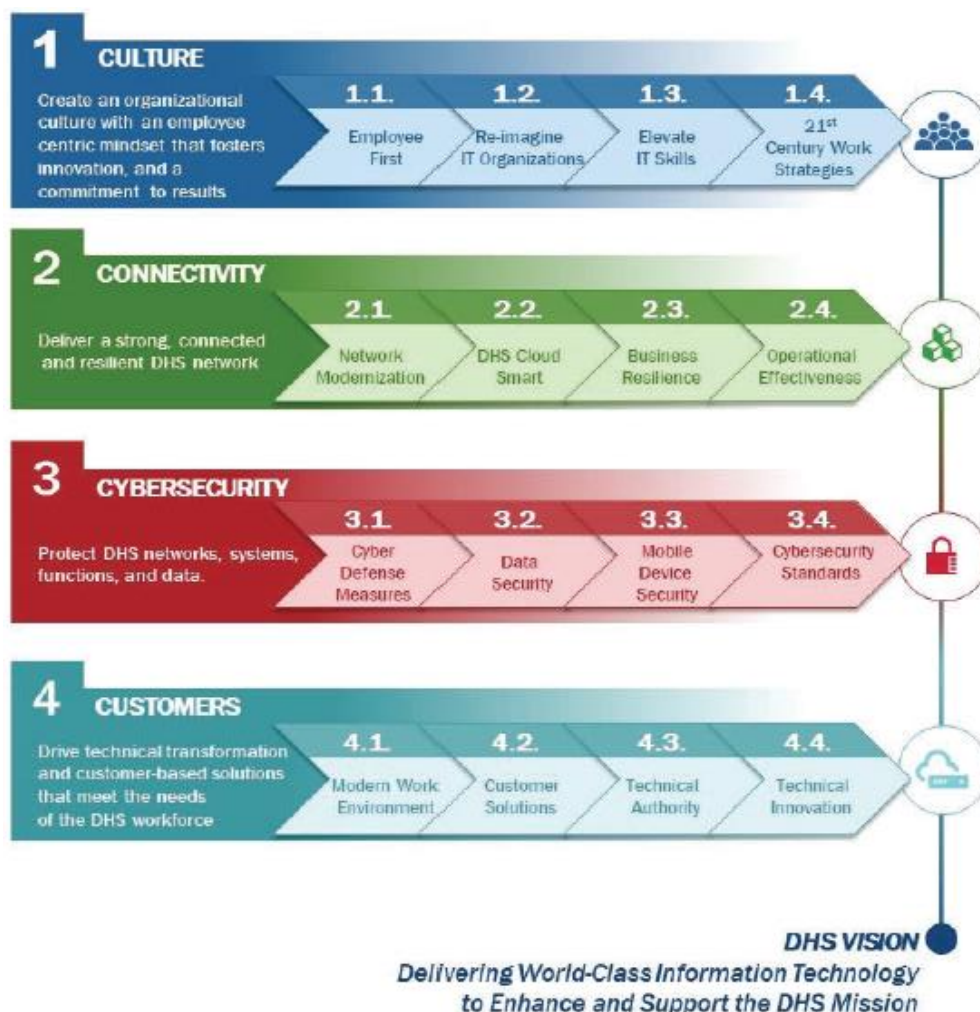


Figure 5: DHS IT Strategic Plan – Goals

Specifically related to modernization, the 2019-2023 DHS IT Strategic Plan outlined initiatives to adopt cloud-based computing<sup>4</sup> 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.

DHS is in the process of optimizing its data centers with the Data Center and Cloud Optimization Support Services initiative. This initiative includes a three-pronged strategy to improve service availability, reliability, and cost-effectiveness. To execute these strategies, DHS is implementing a plan to consolidate two enterprise data centers, migrate applications to the cloud, and purchase colocation services. As of May 2020, nearly 40% of DHS systems in an alternate data center had either been consolidated or migrated to the cloud. In addition, DHS achieved 68% overall data center closures, exceeding the original initiative closure requirements.

<sup>4</sup> 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.