



U.S. Department of Homeland Security

# FY 2019 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 2019, DHS received its sixth consecutive Certificate of Excellence in Accountability Reporting (CEAR) from the Association of Government Accountants (AGA) for its FY 2018 Agency Financial Report, along with a best-in-class award for *Receptiveness to Prior Year's CEAR Recommendations*. 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 Fiscal Year (FY) 2019 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 2019, the Department's Performance and Accountability Reports consist of the following three reports:

- DHS Agency Financial Report | Publication date: November 15, 2019.
- DHS Annual Performance Report | Publication date: February 3, 2020 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, 2020.

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

## Message from the Secretary

November 14, 2019



I am pleased to present the Department of Homeland Security's (DHS) Agency Financial Report for Fiscal Year (FY) 2019. 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.

The U.S. Department of Homeland Security and its homeland security mission are born from the commitment and resolve of Americans across the United States in the wake of the September 11<sup>th</sup> attacks. In those darkest hours, we witnessed true heroism, self-sacrifice, and unified resolve against evil. We rallied together for our common defense, and we pledged to stand united against the threats attacking our great Nation, fellow Americans, and way of life. Together, we are committed to relentless resilience, striving to prevent future attacks against the United States and our allies,

responding decisively to natural and manmade disasters, and advancing American prosperity and economic security long into the future.

In the many years since the September 11<sup>th</sup> attacks, the Department has marshaled this collective vision to face new and emerging threats against the Homeland. To do so, we are instilling a “culture of relentless resilience” across the United States to harden security for the threats on the horizon, withstand attacks, and rapidly recover. We are raising security baselines across the world, addressing systemic risks, and building redundancies for critical lifelines that enable our prosperity and way of life. Perhaps most importantly, we are forging partnerships to strengthen public, private, and international cooperation and crowd-sourcing solutions that outpace the intentions of our adversaries.

As the complex threat environment continues to evolve and loom, the Department will embody the relentless resilience of the American people to ensure a safe, secure, and prosperous Homeland.

We are championing a Resilience Agenda for DHS that focuses on:

- **Champion “Relentless Resilience” for All Threats and Hazards:** DHS will remain resolute against today’s threats and hazards by keeping pace with our adversaries and preparing for those of tomorrow by identifying and confronting systemic risk, ensuring the Nation’s citizens remain resilient, building redundancy and resilience into community lifelines, and raising the baseline of our security across the board—and across the world.
- **Reduce the Nation’s Risk to Homeland Security Dangers:** DHS will mitigate risks to the Homeland by interdicting threats, hardening assets to eliminate vulnerabilities, and enhancing rapid recovery efforts to reduce potential consequences from physical attacks, natural disasters, and cyber incidents.
- **Promote Citizen Engagement and Strengthen and Expand Trusted Partnerships:** Homeland security is a whole-of-society endeavor, from every federal department and agency to every American across this Nation. We will work together and empower

partners to leverage national capacity and capabilities, improve training exercises, and develop contingency plans that make America safe, secure, and resilient against all threats and all hazards.

- **Uphold Privacy, Transparency, Civil Rights, and Civil Liberties:** DHS will continue to implement safeguards for privacy, transparency, civil rights, and civil liberties when developing and adopting policies and throughout the performance of its mission to ensure that homeland security programs uphold privacy, civil rights, and civil liberties.
- **Ensure Mission-Driven Management and Integration:** As a unified Department, DHS will leverage the collective capabilities of its operational Components to identify opportunities for jointness and integration. Through a comprehensive and collaborative approach, DHS will ensure its operators and employees have the necessary tools, resources, and authorities to execute its mission.

To be a resilient organization, our business processes must be rock solid. Functions such as budgeting, financial management, internal control, and acquisition need to work seamlessly to enable our front-line operators with the tools needed to do their jobs. DHS continues to aggressively push forward to improve its management and operations, facing and over-coming many of the challenges of unifying so many disparate organizations.

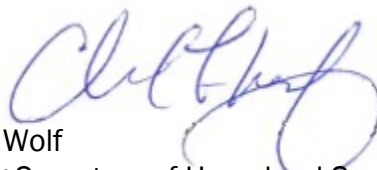
DHS is the only federal agency required by law to obtain an opinion on internal controls over financial reporting. The Department's maturing internal control program and its comprehensive enterprise approach to remediation are driving continuous progress, as evidenced by the ability to reduce material weaknesses. With remaining internal control weaknesses in Financial Reporting and Information Technology Controls and Financial System Functionality, DHS is executing a multi-year strategy and plan to achieve an unmodified internal control audit opinion.

DHS remains committed to improving performance measurement and accountability, and I am able to provide reasonable assurance, based on our internal controls evaluations, 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>.

None of these efforts are possible without the efforts and sacrifice of our men and women. Whether is our front-liners or those supporting our missions, the Department workforce continues to excel at safeguarding our assets, our nation, and values.

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

Sincerely,



Chad Wolf  
Acting Secretary of Homeland Security

## Table of Contents

<b>About this Report</b> .....	<b>i</b>
<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.....	18
Secretary’s Assurance Statement .....	23
<b>Financial Information</b> .....	<b>33</b>
Message from the Chief Financial Officer.....	34
Introduction.....	35
Financial Statements .....	36
Notes to the Financial Statements.....	44
Required Supplementary Stewardship Information .....	116
Required Supplementary Information.....	121
Independent Auditors’ Report.....	125
<b>Other Information</b> .....	<b>152</b>
Tax Burden/Tax Gap.....	153
Combined Schedule of Spending .....	154
Summary of Financial Statement Audit and Management Assurances .....	158
Payment Integrity.....	160
Fraud Reduction .....	180
Reduce the Footprint.....	182
Civil Monetary Penalty Adjustment for Inflation .....	183
Other Key Regulatory Requirements.....	190
Office of Inspector General’s Report on Major Management and Performance Challenges Facing the Department of Homeland Security.....	191
<b>Acronym List</b> .....	<b>213</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 Sheet, Statement of Net Cost, Statement of Changes in Net Position, Statement of Budgetary Resources, and Statement of Custodial Activities.

The ***Management Assurances*** 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 220,000 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 web site at <http://www.dhs.gov/organization>.

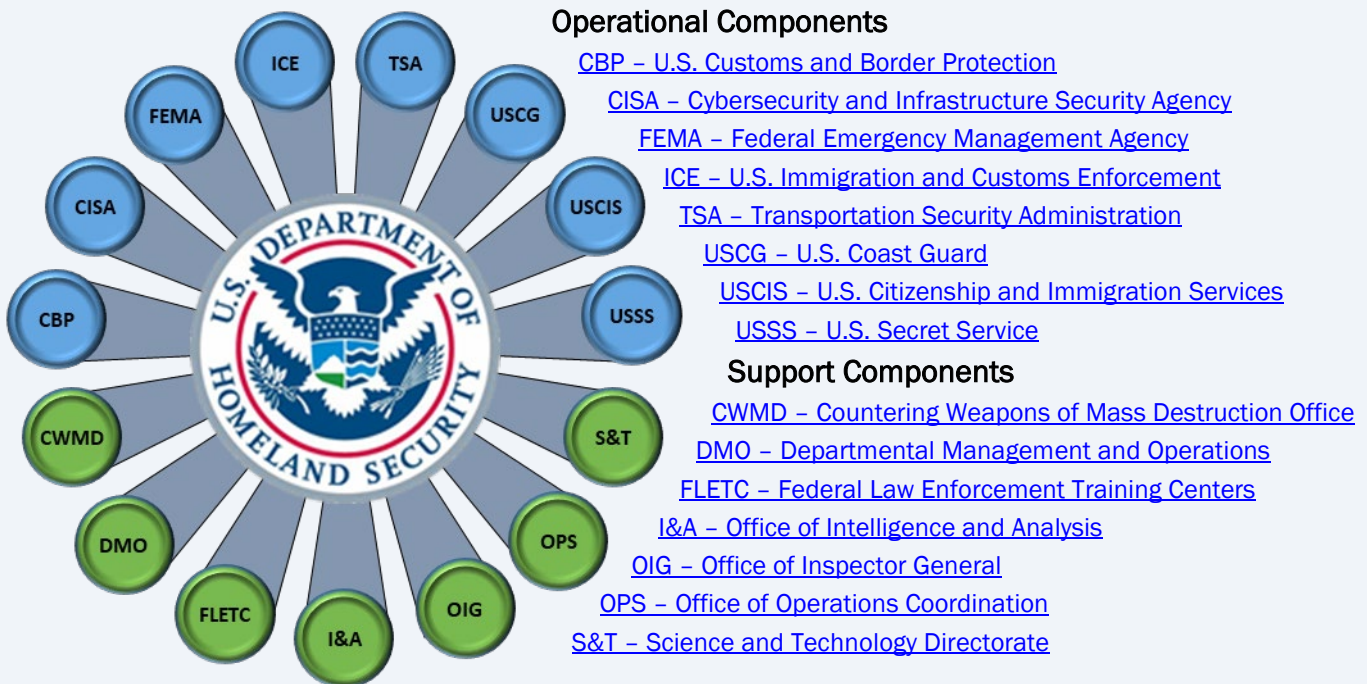


Figure 1: DHS Components

## Performance Overview

The Performance Overview provides 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 2019-2021 Annual Performance Report with the FY 2021 Congressional Budget and can be accessed at: <http://www.dhs.gov/performance-accountability>. Previous reports can be found at this link as well.

The Department has a robust performance framework that drives performance management and enables the implementation of performance initiatives. Strategic plan goals are implemented by our mission programs. A mission program is a group of activities acting



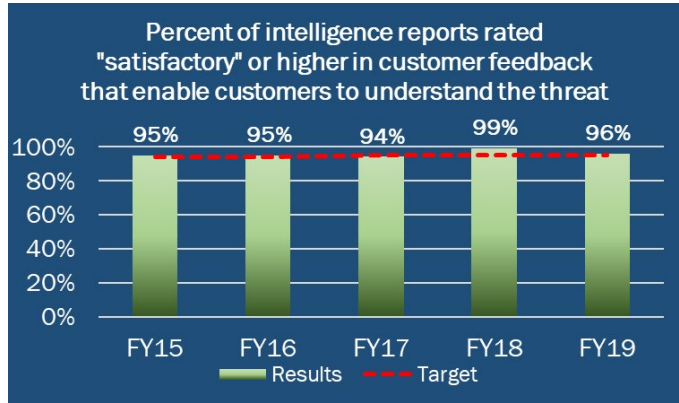
together to accomplish a specific high-level outcome external to DHS and includes operational processes, skills, technology, human capital, and other resources. Mission programs have performance goals, performance measures, and performance targets.

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

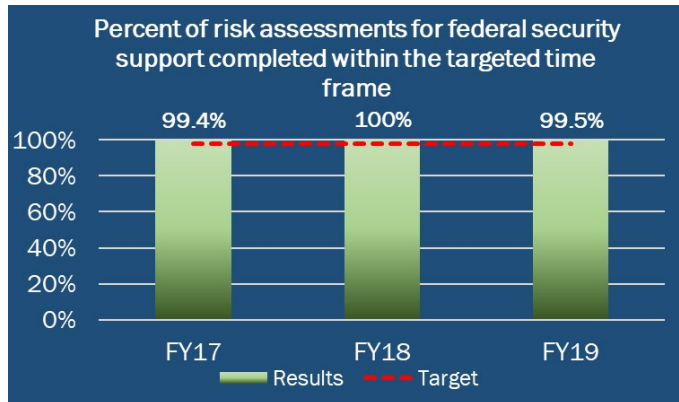
One of the Department’s top priorities is to protect Americans from terrorism and other homeland security threats by preventing nation-states and their proxies who engage in terrorist or criminal acts that threaten the homeland. In recent years, terrorists and criminals have increasingly adopted new techniques and advanced 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 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 2019, 1,239 out of 1,290 DHS evaluations were rated as satisfactory or higher resulting in a 96 percent satisfaction rate, meeting the target. Trends over time show high satisfaction with reports.



**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 percent of [Special Event Assessment Ratings](#) (SEAR) completed within the targeted timeframe as voluntarily requested from state and local authorities for events taking place within their jurisdictions. These events are assessed using the SEAR methodology providing a rating scale that defines five levels of risk, with a SEAR-1 rating being the highest. These risk assessments are used by federal agencies as criteria to determine their level of support to state and local events and are the primary

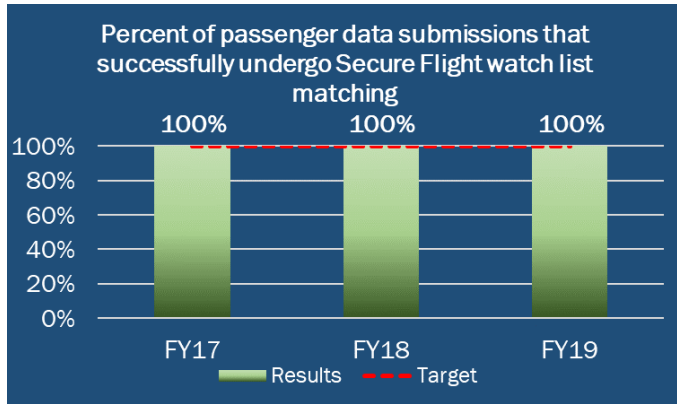


Management’s Discussion and Analysis



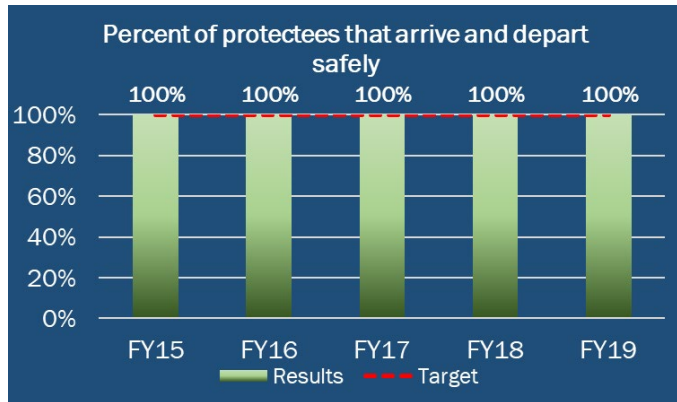
The DHS Office of Operations Coordination, Special Events Program (SEP) is the sole federal entity that coordinates the identification, risk assessment, information sharing, and support for special events. SEP engages in direct outreach to local, state, and federal event planners and manages the National Special Events Data Call which resulted in the submission of over 17,000 events for 2019.

federal awareness mechanisms for special events occurring across the nation. OPS provided risk assessment ratings on-time 99.5 percent of the time, which is above target but slightly down compared to last year’s 100 percent result. With growing demand, success over the past three years can be attributed to standardized processes for adjudicating submissions, dedicated staff, and successful development and application of methodology and technology tools.



**Percent of passenger data submissions that successfully undergo Secure Flight watch list matching (TSA):** 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.

Vetting individuals against high-risk watch lists disrupts current and emerging homeland security threats. In FY 2019, this measure achieved 100 percent, meeting the target, and has maintained this level of performance for the past three 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 gauges the percent of travel stops where the [USSS](#) protectees arrive and depart safely. Protectees include 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. 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 the USSS, including the: Airspace Security Branch; Counter Sniper Team; Emergency Response Team; Counter Surveillance Unit; Counter Assault Team; Hazardous Agent Mitigation and

**Did you know?**

Because of the assassination of President William McKinley on September 14, 1901, Congress requested USSS Protection of U.S. Presidents.




Medical Emergency Response Team; and the Magnetometer Operations Unit. Using advanced countermeasures, USSS executes security operations that deter, minimize, and decisively respond to identified threats and vulnerabilities.

### Looking Forward

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

- *DHS recently released and is implementing the Department of Homeland Security Strategic Framework for Countering Terrorism and Targeted Violence*: This framework highlights key insights and actions to be taken, including: understanding the interconnection between terrorism and targeted violence; conducting an annual assessment that will explain the state of the threat to the Homeland; providing an extended assessment of the dangers posed by domestic terrorists; understanding how preventive tools can be brought to bear against these threats, regardless of the varying ideological or non-ideological drivers; and the importance of transparency, the protections of civil rights and civil liberties, and the protection of data in a digital age. DHS's Strategic Framework for Countering Terrorism and Targeted Violence is intentionally forward-looking in its understanding of technology's role—as a factor that can exacerbate problems, but also one that can provide new solutions to combat the threats we confront. This strategy is designed to implement the White House's 2017 National Security Strategy and 2018 National Strategy for Counterterrorism, as well as related national policy guidance.
- *DHS is conducting studies to combat terrorism*: These studies include focused examinations on enhancing the use of social media/open source information, considering methods to leverage artificial intelligence for data integration and discoverability, and continuing to improve situational awareness and information sharing through tools and partnerships with our law enforcement and federal, state, and local partners.
- *Deploy improvements to airport scanning and detection*: Since aviation security continues to present a high-risk environment for exploitation by terrorists, the Department will continue 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 recently began the multi-year deployment of [computed tomography scanners](#) that apply sophisticated algorithms for the detection of explosives and create three-dimensional images that can be viewed and rotated for thorough visual image analysis by TSA officers.



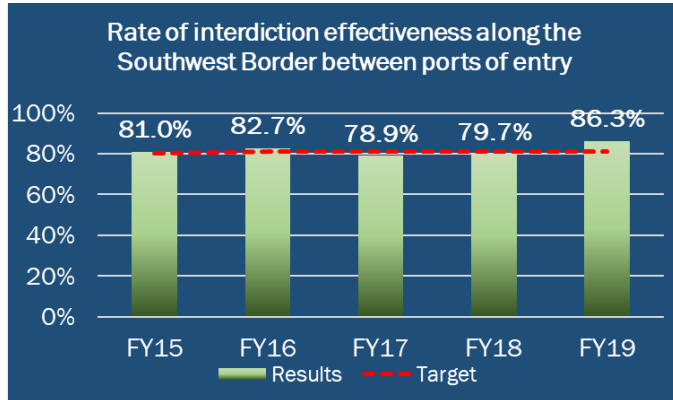
The USSS secured the Salute to America Independence Day celebration on July 4th, 2019, coordinating with many agencies across the National Capital Region. The event occurred at the Lincoln Memorial in Washington, DC, and required extensive planning to keep the public and USSS protectees safe, including the development of a comprehensive and strategic operational security and safety plan that addressed the current threat environment and vulnerabilities posed in today's world.

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

Secure borders are essential to our national sovereignty. Those who enter the country illegally or overstay their authorized period of admission potentially compromise the security of our nation by disregarding our national sovereignty, threatening our national security,

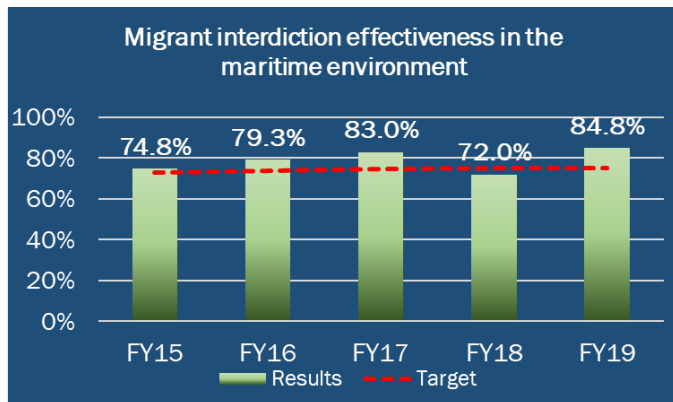
## Management's Discussion and Analysis

compromising our public safety, exploiting our social welfare programs, and ignoring lawful immigration processes. 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 at apprehending detected illegal border crossers or confirming that illegal entrants return to the country from which they entered. It is an important indicator of the effectiveness of law enforcement response, an element of Border Patrol's Operational Control of U.S. borders. In FY 2019, the results for this

measure were greater than historical results due largely to the unprecedented increase in the number of individuals crossing the border who made no attempt to evade apprehension. In addition, mass illegal migration activity created an unprecedented border security and humanitarian crisis in FY 2019 and led to a variety of successful administrative activities striving to reduce the flow. The FY 2019 results were also influenced by efforts of the Border Patrol working to increase Operational Control between ports of entry, and the assistance of [National Guard](#) personnel and CBP's Office of Field Operations. It is expected that the results for this measure in the future will be similar to historical results.



**Migrant interdiction effectiveness in the maritime environment (U.S. Coast Guard):** This measure reports the percent of detected migrants of all nationalities who were interdicted by the [U.S. Coast Guard](#) and partners via maritime routes. The U.S. Coast Guard 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. In FY 2019, this

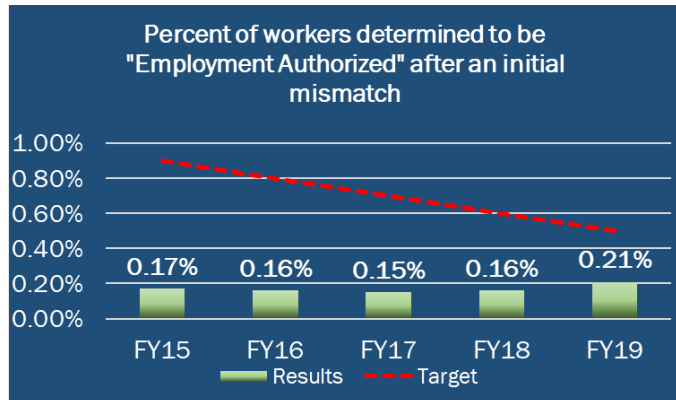
measure achieved a record 84.8 percent, which is above target and represents the highest interdiction rate in the past five years. The FY 2019 reported interdiction rate is significantly higher than FY 2018 due to a major improvement in the reporting processes of our partner nations rather than an actual spike in the number of migrants utilizing maritime routes that were interdicted.





In August 2019, the U.S. Coast Guard Cutter WILLIAM TRUMP interdicted 146 Haitian migrants off Haiti, embarking them from an overloaded 40-foot vessel due to safety of life at sea concerns. This is the second largest U.S. Coast Guard migrant interdiction in 2019, and the largest migrant interdiction by a Fast Response Cutter (FRC) to-date. This highlights the use of the FRC in this mission set in the Caribbean.

**Percent of workers determined to be "Employment Authorized" after an initial mismatch (USCIS):** This measure assesses the accuracy of the [E-Verify](#) process by assessing the percent of employment verification requests that are not positively resolved at time of initial review. In FY 2019, this measure achieved 0.21 percent easily 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 2020 U.S. Border Patrol Strategy and the Operational Control \(OPCON\) framework](#): This strategy articulates the three essential elements of OPCON: 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 plan expands the OPCON concept to include a path for measuring and assessing performance and improving Border Patrol’s ability to clearly articulate status and progress. The [FY 2020-2021 OPCON Agency Priority Goal](#) is a tool that will support implementation of this important strategy.
- [Remove those who have entered the country illegally](#): The [Office of Enforcement and Removal Operations](#) and the [Office of the Principal Legal Advisor](#) 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. Future efforts include: expansion of temporary and emergency detention

**Did you know?**

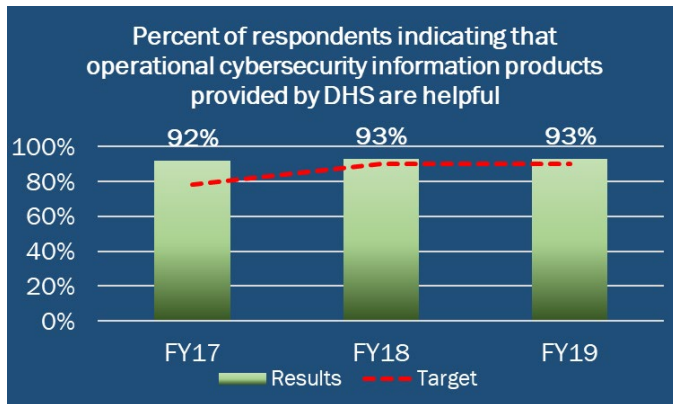
The 287(g) Jail Enforcement Model Program is one of ICE’s safest and most efficient methods for identifying, arresting, and removing immigration law violators through partnerships with state and local law enforcement agencies.

capacity; efforts to implement a family case management program; increasing digital content to improve the public's understanding of program efforts; investments in enhanced video teleconference technology; engagement in cross-training with the Department of Justice, Office of Immigration Litigation, to facilitate the timely and efficient completion of federal litigation activities; and work with the Department of Justice's Executive Office for Immigration Review to establish priority dockets and processing for expediting cases.

### Goal 3: Secure Cyberspace and Critical Infrastructure

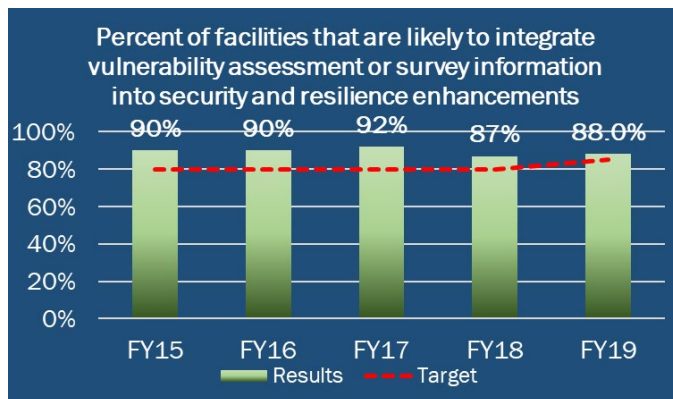
Increased connectivity of people and devices to the Internet and to each other has created an ever-expanding attack surface that transcends borders and penetrates almost every American home. As a result, cyberspace has become an active threat domain in the world and a dynamic threat to the Homeland. Nation-states and their proxies, transnational criminal organizations, and cyber criminals use sophisticated and malicious tactics to undermine critical infrastructure, steal intellectual property and other innovations, engage in espionage, and threaten our democratic institutions. Moreover, the interconnectivity of critical infrastructure systems raises the possibility of cyber-attacks inflicting devastating effects.

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



**Percent of respondents indicating that operational cybersecurity information products provided by DHS are helpful (CISA):** This measure assesses whether the products that the DHS [National Cybersecurity and Communications Integration Center \(NCCIC\)](#) provides are helpful for its customers. NCCIC's website feedback form enables recipients of products to submit feedback about the content of each product. DHS uses the feedback to determine how various

organizations measure the value of operational cybersecurity information and to improve the exchange of information and intelligence. In FY 2019, a total of 4,169 out of 4,446 respondents reported that NCCIC products were helpful, achieving 93 percent, which meets the target and is consistent compared to the last two years.



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. In FY 2019, a total of 372 out of 423 respondents indicated they will integrate vulnerability information into security enhancements. Current year's results are consistent with the five-year trend. Providing facilities with vulnerability information allows them to understand and reduce risk to the nation's critical infrastructure.



For months prior to the 2018 midterm elections, DHS provided risk & vulnerability assessments to state & local governments to help them harden their election registration and reporting systems against cyber-attacks. Leading up to the election day, DHS worked with state and local officials to provide them with the necessary information to make security enhancements to their election infrastructure. The DHS-provided risk and vulnerability assessments helped election officials to better understand vulnerabilities to their systems to prioritize actions and investments to make the election more secure.

**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 will continue to advance federal cybersecurity through a follow-on [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,
- **Enhance resilience of critical infrastructure:** Nation-state adversaries work to identify and exploit technology for maximum injury to American critical infrastructure and systems. Cyber-attacks for financial gain have become ever more common, requiring improved cyber hygiene at every level. CISA is focusing efforts in the following areas: supply chain disrupters; 5G wireless; soft target; government network protection; industrial control systems; and election security.

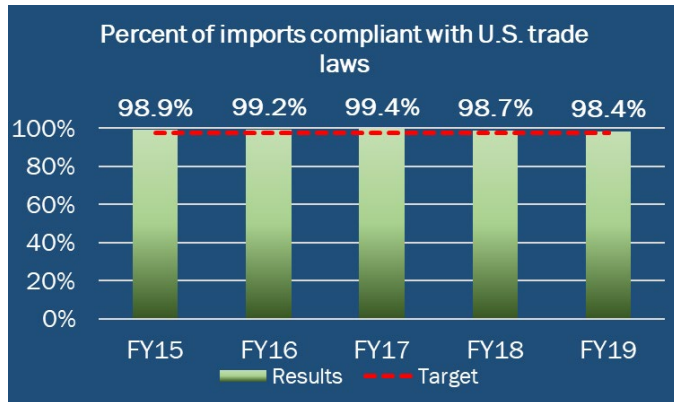
**Did you know?**

The DHS National Cybersecurity Assessments and Technical Services team provides free cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's election cyber infrastructure.

**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.



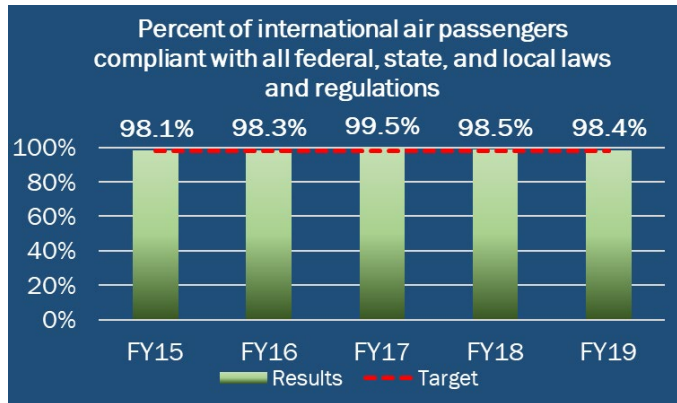
**Percent of imports compliant with U.S. trade laws (CBP):** This measure reports the percent of imports that are compliant with [U.S. trade laws including customs revenue laws](#). Ensuring all imports are legally compliant and that their entry records contain no major discrepancies facilitates lawful trade. In FY 2019, this measure achieved 98 percent results which meets the target and is slightly down compared to last year’s result. Any discrepancies discovered from the compliance

measurement process are addressed through billing and collection, and if broader risks are apparent, further action is taken.



CBP oversees and processes more than 33 million declared imports through automated systems each year, averaging more than one shipment per second every day. Leveraging partnerships and legal authorities and emphasizing legitimate trade, revenue collection and advanced enforcement capabilities enable 98% compliance with U.S. trade laws. CBP operations significantly impact the U.S. economy—for every dollar invested in regulatory compliance, technology transformation and enforcement of import laws, an estimated \$96 is gained in the American economy—benefiting producers, manufactures and government.

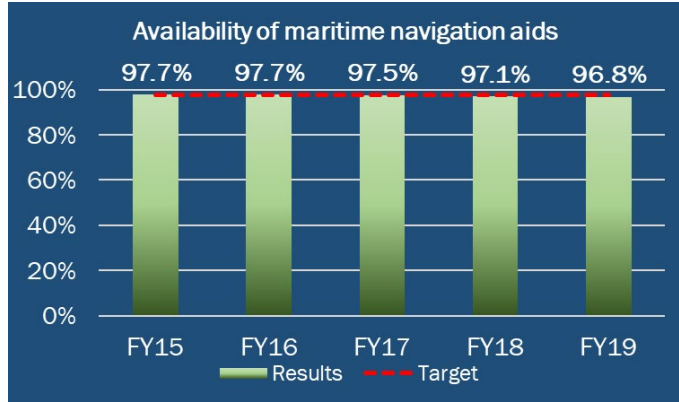
**Percent of international air passengers compliant with all federal, state, and local laws and regulations (CBP):** This measure shows CBP’s success at maintaining a high level of security in the [international air environment](#) by measuring the degree of compliance with all federal, state, and municipal laws and regulations which CBP is charged with enforcing at the ports of entry (international airports). The laws and regulations include those CBP has direct jurisdiction over, such as agriculture,



immigration, and customs, as well as those of other government agencies that CBP is tasked by Congress to enforce. Examples include Food and Drug Administration pharmaceutical regulations, Consumer Product Safety Commission product safety alerts, Center for Disease Control health and safety alerts, and confiscation of alcoholic beverages from minors on behalf of state authorities. In FY 2019, this measure achieved 98.4 percent which is above target and consistent over the past 5 years. CBP continues to meet targets for air passenger compliance with laws, rules, and regulations through passenger outreach efforts on the CBP website pages "[For U.S. Citizens/Lawful Permanent Residents](#)", "[Know Before You Visit](#)", "[Electronic System for Travel Authorization](#)", "[Electronic Visa Update System](#)", "[Visa Waiver Program](#)", including "[For Canadian Citizens and Mexican Nationals](#)", and "[Trusted Traveler Programs](#)".

**Availability of maritime navigation aids (U.S. Coast Guard):**

This measure indicates the hours that short-range federal [Aids to Navigation](#) are available as defined by the International Association of Marine Aids to Navigation and Lighthouse Authorities in December 2004. A short-range Aid to Navigation is counted as not being available from the initial time a discrepancy is reported until the time the discrepancy is corrected. In FY 2019, this measure achieved 96.8 percent which is slightly below target and down compared to last year’s result and has slightly declined over the past five years. Several factors continue to hinder meeting the target the past two years which include ongoing repairs in the Mid-Atlantic, Florida, Puerto Rico, and the Gulf Coast due to 2017 storm damage from Hurricanes Harvey, Irma, and Maria as well as late-2018 damage due to Hurricane Florence. The U.S. Coast Guard will continue with their risk-based prioritization of navigational aid repairs.

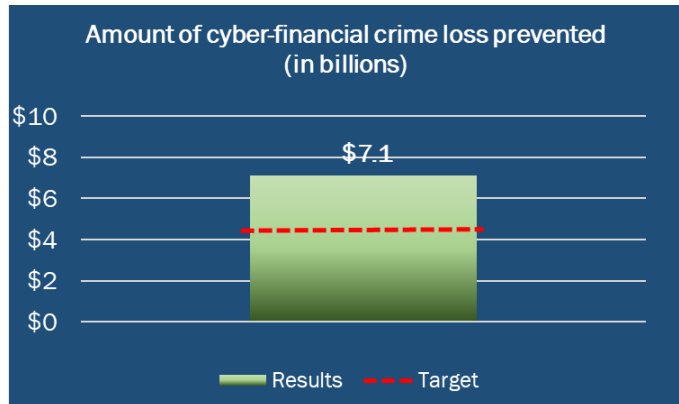


**Did you know?**

The U.S. Coast Guard ensures that over 20,000 bridges and causeways spanning the navigable waters of the U.S. do not unreasonably obstruct navigation.

**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 [U.S. Secret Service](#). This is the first fiscal year that the cyber and traditional financial loss measures were combined to show a comprehensive view of our efforts to combat financial crimes. 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 to reduce financial losses to the public attributable to cyber financial crimes. In FY 2019, this measure achieved \$7.10 billion in loss prevention greatly exceeding the target of \$4.5 billion due to one very large case closure. This single case involved \$4.3 billion in loss prevented associated with the Deepwater Horizon explosion and oil spill in the Gulf.



**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:** CBP collects approximately \$50 billion in duties, taxes, and other fees while processing more than \$2.5 trillion in imports. In addition, CBP processes more than 350 million travelers each year at 328 ports of entry and more than 700 enforcement actions daily. The rapidly changing and ever-increasing level of trade and travel presents ongoing challenges to ensuring security while delivering



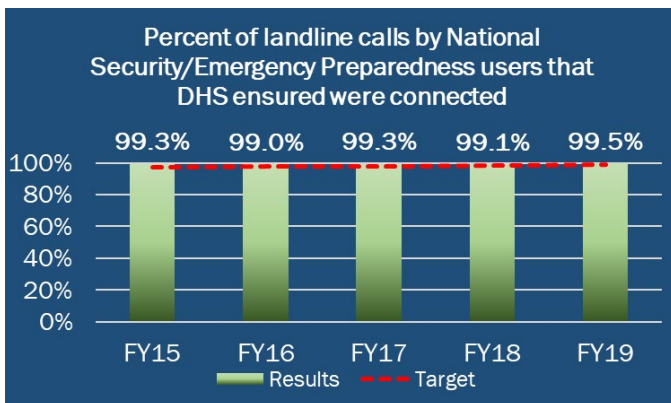
service expected by trade partners and the traveling public. CBP will continue to focus on developing and implementing high-impact solutions [Information Technology (IT) and non-IT] to process each trade transaction at faster speeds, and to find non-intrusive methods for processing international travelers while ensuring safety and maintaining civil rights and liberties.

- ***Safeguard the nation's financial system:*** Economic prosperity depends on global trust in the U.S. dollar and reliable financial institutions and payment systems as critical enablers of global commerce. The [USSS Electronic Crimes Task Force](#) (ECTF) network is a strategic alliance of law enforcement, other federal agencies (e.g., Treasury), academia, and the corporate sector, dedicated to investigating, disrupting, and deterring homeland security-related cybercrime, as well as cyber-related high consequence events that might affect the financial infrastructure. The ECTF is currently leveraging state-of-the-art forensic equipment and laboratories to keep pace with heightened capabilities of cyber criminals and the growing complexity of cybercrimes. The ECTF leadership is continuously looking at new technology to stay abreast of our adversaries. Furthermore, to improve oversight of our nation's financial systems, the USSS Office of Investigations will: expand investigative purview; conduct high-impact investigations; expand the ECTF; develop specialized expertise; increase collaboration; and provide training to key foreign partners.

## 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 responding 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 landline calls by National Security/Emergency Preparedness users that DHS ensured were connected (CISA):


This measure gauges the landline 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 2019, this measure achieved 99.5 percent call completion which is above target and the highest call completion rate over the past five years. In FY 2019, there were more than 600,000 calls made using GETS. By ensuring effective emergency communications, DHS

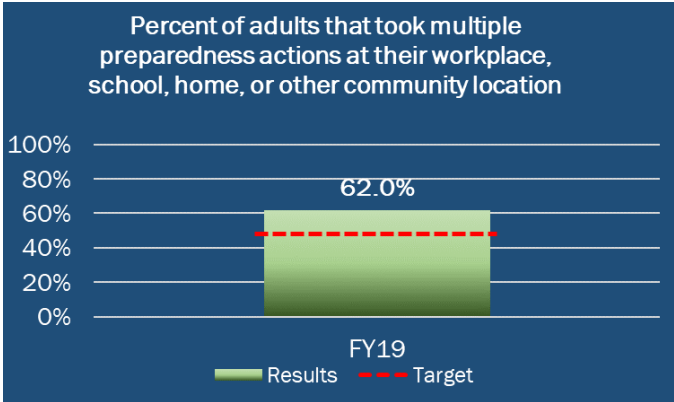
contributes to a national effective emergency response effort which helps strengthen national preparedness and resilience.

**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 first year for this measure reporting results. This measure reports the share of all respondents to [FEMA’s annual National Household Survey \(NHS\)](#) 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 2019, this measure achieved 62.0 percent which is above target and future trends will be reported in DHS’s Annual Performance Reports. The NHS surveyed approximately 5,000 adults in the United States identifying residents who took three or more of the surveyed preparedness actions including attending a local meeting or training, talking with others, making an emergency plan, seeking preparedness information, participating in a drill, or gathering supplies to last at least three days. These efforts help motivate communities and individuals to act and to serve as a contributing factor to the increase in preparedness actions.

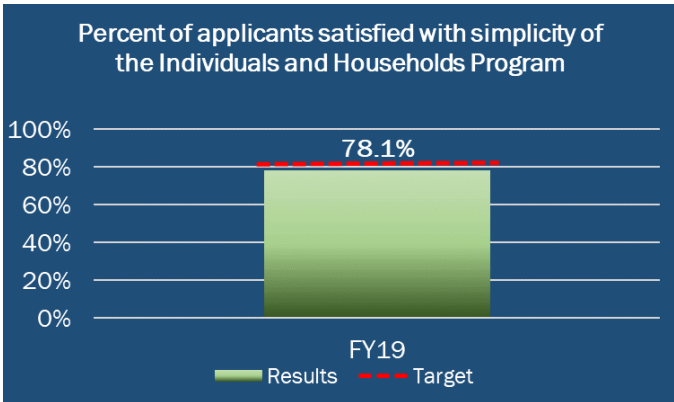


CISA partnered with the National Council of Statewide Interoperability Coordinators to develop 25 State Interoperability Markers. States and territories use these markers to conduct a self-assessment, resulting in a national view of communications interoperability. This information will help states and territories identify gaps to inform strategic and financial planning. In addition, the data enables CISA to tailor technical communications assistance to states and territories.




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

This is the first 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 2019, this measure achieved 78.1 percent which is below target and



Management’s Discussion and Analysis

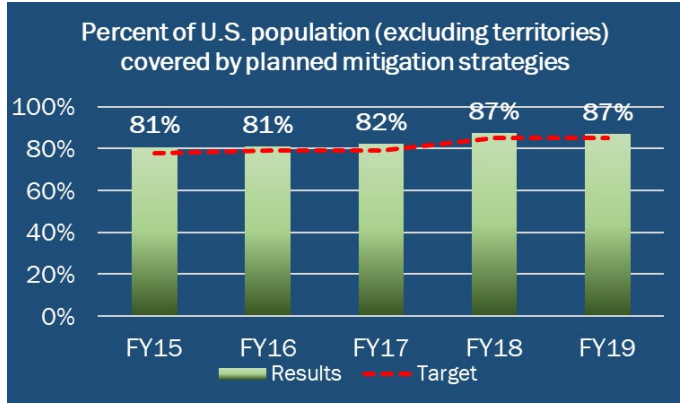


The Disaster Recovery Reform Act provides separate maximum grant amounts under the Individual and Households Program for Other Needs Assistance and Housing (excluding accessibility-related items and rental assistance) retroactive to August 1, 2017. Since March 2019 more than \$74 million has been provided to over 11,200 applicants in retroactive assistance. Retroactive payments will continue until all eligible cases have been reviewed.

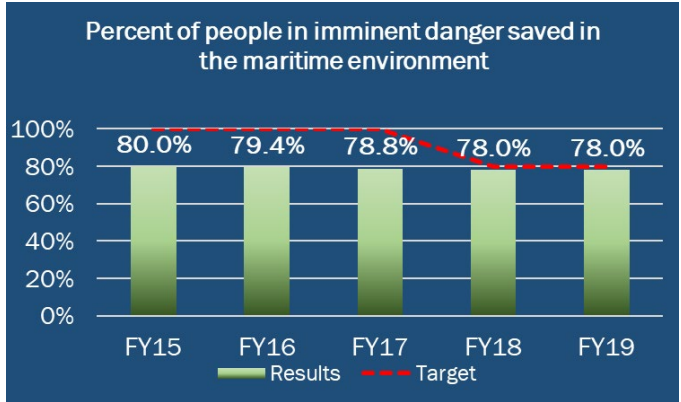
future results will be reported in DHS’s Annual Performance Reports. After a detailed analysis of the survey results, it was determined that the primary issue was the ease of use of disaster assistance information. FEMA will work to clarify disaster information to simplify the application process for the survivor.

**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 2019, this measure achieved 87 percent which is above target and consistent with last year’s result. The process of creating a Hazard Mitigation Plan allows communities to build partnerships, increase awareness, identify comprehensive approaches to focus their resources, and communicate



internally to identify potential sources of grant funding to support strategies. FEMA regional planning staff work directly with states and jurisdictions to support timely submission of plans for review and approval. In FY 2019, regional staff focused technical assistance on assisting communities with producing higher quality risk assessments.



**Percent of people in imminent danger saved in the maritime environment (U.S. Coast Guard):** 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 [U.S. Coast Guard](#). The number of lives lost before and after the U.S. Coast Guard is notified and the number of persons missing at the end of search operations are factored into this result. In FY 2019, this measure achieved 78 percent which is below target but is

consistent with the last five years’ results. This measure has only a 2.0 percent variance from a low of 78.0 percent to a high of 80 percent. Several factors hinder successful response including untimely distress notification to the U.S. Coast Guard, incorrect distress site location reporting, severe weather conditions at the distress site, and distance to the scene. Target adjusted in FY 2018 to be in-line with historical results.



## Looking Forward

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

- Outcome-Driven Community Response:** The *2017 Hurricane Season FEMA After-Action Report* identified the need to create a new operational prioritization and response tool. To that end, FEMA has championed the [Community Lifelines](#) decision tool, to enable the continuous operation of government functions and critical business concerns essential to human health, safety, and economic security. The Lifelines tool assists affected populations in addressing concerns about safety and security; food, water, and shelter; health and medical; energy (power and fuel); communications; transportation; and hazardous materials. FEMA is also initiating efforts to reduce the complexity of FEMA to lessen the administrative and bureaucratic burden tied to the delivery of assistance and to improve the survivor and grantee experience.
- Train and equip first responders:** Most effective strategies for emergency management are federally-supported but executed by the immediate authority of a local jurisdiction. As disasters unfold, individuals and municipal agencies serve as the first responders to triage the incident and stabilize the situation. DHS will continue to promote community-building initiatives to improve the strength of local networks and reinforce practical skills of first responders and disseminate key skills including basic first aid, home maintenance, and emergency planning methods. In addition, DHS's Science and Technology (S&T) Directorate continues to drive advances in immediate response capabilities as well as long-term recovery capabilities. With S&T's recent reorganization, future focus on emerging needs will be incorporated into their research and development plans for equipping first responders with tools to improve their job.

### Did you know?

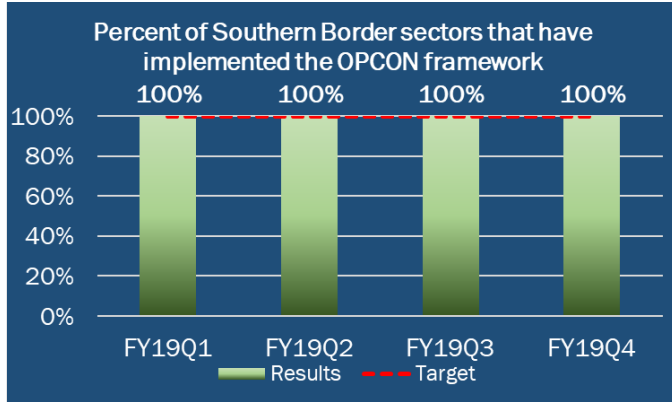
FEMA's National Watch Center maintains uninterrupted, all-hazards situational awareness. Working closely with regional & interagency partners, the men & women of the Watch Center provide national-level reporting, and 24/7 capability to immediately initiate a coordinated national disaster response.

## Agency Priority Goals

Agency Priority Goals (APGs) are one of the tenets of the Government Performance and Results Act Modernization Act of 2010 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 Office of Management and Budget (OMB) web site [performance.gov](https://www.performance.gov).

### **APG: Enhance Southern Border Security**

DHS's FY 2018-2019 APG, *Enhance Southern Border Security*, was initiated to improve security along the southwest border between ports of entry. The goal focused on beginning implementation activities associated with the [Operational Control](#) (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. A follow-on FY 2020-2021 APG will continue to articulate progress in Southern Border implementation efforts while expanding initial implementation of OPCON to the Northern Border.



**Key Measure: Percent of Southern Border sectors that have implemented the OPCON framework**

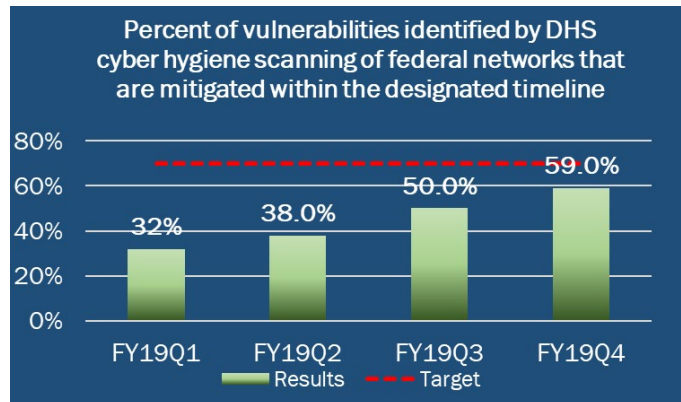
With the submission of FY 2019 Master Concepts of Operations (CONOPs) from each sector in October 2018, and subsequent approval by Headquarters in December 2018, CBP achieved its original goal. By developing the FY 2019 CONOPs, the Border Patrol acclimated sector staff to writing yearly plans with the intent of

improving OPCON implementation in their sectors. This will be critical for the development of FY 2020 CONOPs, when sector plans will reference the OPCON baseline scores, and will use measures in the OPCON framework, to discern measurable impacts from their efforts during FY 2020. The CONOPs establish traceability for how operations in the field impact OPCON. The FY 2020-2021 OPCON APG will continue to advance the implementation of OPCON to enhance border security.

**APG: Strengthen Federal Cybersecurity**

DHS’s Cybersecurity FY 2018-2019 APG focused 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 was to mitigate 70% of significant (critical and high) vulnerabilities identified through DHS scanning. In FY 2019, 59 percent of vulnerabilities were mitigated within the designated timeframe. The [FY 2020 – 2021 Cybersecurity APG](#) will continue to advance efforts to mitigate risks the federal network. 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 and ensure the successful implementation of activities to enhance the security of the federal network.

**Key Measure: Percent of significant (critical and high) vulnerabilities identified by DHS cyber hygiene scanning of federal networks that are mitigated within the designated timeline (CISA):** This measure calculates the percent of significant (critical and high) vulnerabilities identified through cyber hygiene scanning that are mitigated within the specified timeline. For critical vulnerabilities the timeline is 15 days and for high vulnerabilities the timeline is 30 days. DHS provides cyber hygiene scanning to agencies to aid in identifying and prioritizing vulnerabilities based on their severity for agencies to make risk-based decisions regarding their network security. Identifying and mitigating the most serious vulnerabilities on a network in a timely manner is a critical component of an effective cybersecurity program. FY 2019, this measure achieved 59 percent



which is below target, but has made significant progress the last half of the year. During the last half of the year, the Binding Operational Directive (BOD) 15-01 was replaced with BOD 19-02 on April 29 formally establishing mitigation timelines of 15 days for critical vulnerabilities and 30 days for high vulnerabilities. Since BOD 19-02's implementation, the compliance rate has increased substantially, and DHS expects performance to continue to improve in FY 2020.

### **Performance Measure 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, and the Reports Consolidation Act of 2000 (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.

DHS has implemented a multi-pronged approach to effectively mitigate risks and reinforce processes that enhance the Department's ability to report complete and reliable data for performance measure reporting. This approach consists of: 1) an annual measure improvement and change control process using a standard form for consistency; 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, third-party, review team. A full description of our processes, as well as a full accounting of each measure's description, scope, data source(s), data collection methodology, and data reliability checks can be found in our forthcoming FY 2019-2021 Annual Performance Report, or our previous reports, located at <http://www.dhs.gov/performance-accountability>.



## Financial Overview

The Department’s principal financial statements—Balance Sheet, Statement of Net Cost, Statement of Changes in Net Position, Statement of Budgetary Resources, and Statement of Custodial Activity—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. KPMG LLP performed the audit of the Department’s principal financial statements.

## Financial Position

The Department prepares its Balance Sheet, Statement of Net Cost, and Statement of Changes in Net Position on an accrual basis, in accordance with 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 2019	FY 2018	\$ Change	% Change
Fund Balance with Treasury	\$ 108,971	\$ 105,095	\$ 3,876	4%
Property, Plant, and Equipment	24,673	23,146	1,527	7%
Other Assets	24,455	20,445	4,010	20%
<b>Total Assets</b>	<b>158,099</b>	<b>148,686</b>	<b>9,413</b>	<b>6%</b>
Federal Employee and Veterans’ Benefits	65,107	61,864	3,243	5%
Debt	20,596	20,541	55	0%
Accounts Payable	4,464	4,440	24	1%
Deferred Revenue and Advances	3,001	4,737	(1,736)	-37%
Insurance Liabilities	3,389	1,658	1,731	>100%
Accrued Payroll	2,889	2,432	457	19%
Other Liabilities	13,463	10,218	3,245	32%
<b>Total Liabilities</b>	<b>112,909</b>	<b>105,890</b>	<b>7,019</b>	<b>7%</b>
Total Net Position	45,190	42,796	2,394	6%
<b>Total Liabilities and Net Position</b>	<b>\$ 158,099</b>	<b>\$ 148,686</b>	<b>\$ 9,414</b>	<b>6%</b>

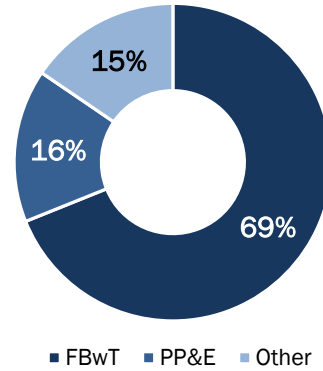
Results of Operations (\$ in millions)	FY 2019	FY 2018	\$ Change	% Change
Gross Cost	\$ 80,818	\$ 82,051	\$ (1,233)	-2%
Less: Revenue Earned	(15,655)	(16,373)	718	-4%
Net Cost Before Gains and Losses on Assumption Changes	65,163	65,678	(515)	-1%
Gains and Losses on Assumption Changes	924	1,143	(219)	-19%
<b>Total Net Cost</b>	<b>\$ 66,087</b>	<b>\$ 66,821</b>	<b>\$ (734)</b>	<b>-1%</b>

**Assets – What We Own and Manage**

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

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

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



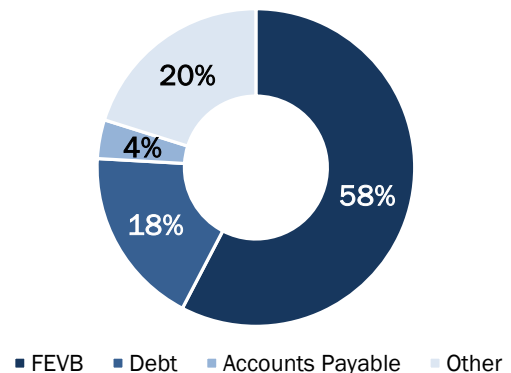
*Other Assets* includes items such as investments, accounts receivable, cash and other monetary assets, taxes, duties and trade receivables, direct loans, and inventory and related property.

As of September 30, 2019, the Department had \$158.1 billion in assets, representing a \$9.4 billion increase from FY 2018. The majority of this change is due to an increase in USCG funding for the acquisition, procurement, construction, rebuilding, and improvement of vessels, aircraft, shore facilities and military housing, aids to navigation systems and facilities, and command, control, communications and computer systems and related equipment, as well as an increase in funding in support of ICE's expanded law enforcement activity and CBP's customs and border protection activities.

**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 and related interest payable 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 pay its debt; therefore, legislation will need to be

## Management's Discussion and Analysis

enacted to provide funding to repay the Treasury or cancel the debt. This is discussed further in Note 15 in the Financial Information section.

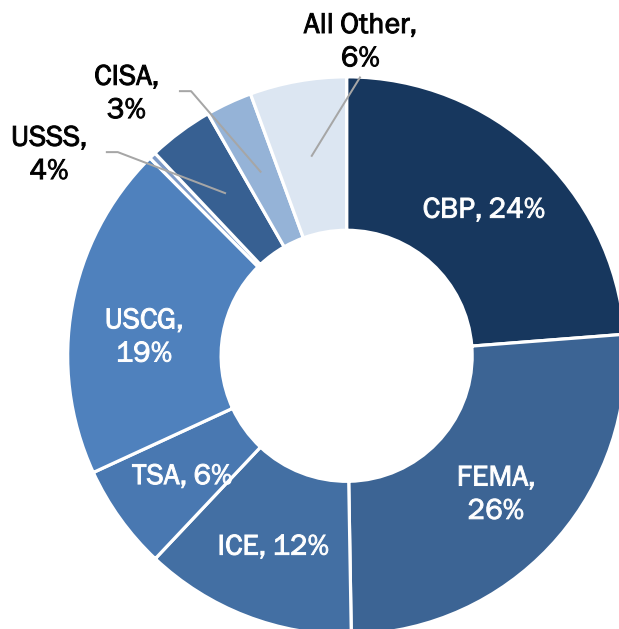
*Insurance Liabilities* represent an estimate of NFIP claim activity based on the loss and loss adjustment expense factors inherent to the NFIP insurance underwriting operations, including trends in claim severity and frequency.

*Other Liabilities* include amounts owed to other federal agencies and the public for goods and services received by the Department, amounts received by the Department for goods or services that have not been fully rendered, unpaid wages and benefits for current DHS employees, and amounts due to the Treasury's general fund, environmental liabilities, refunds and drawbacks, and other.

As of September 30, 2019, the Department reported approximately \$112.9 billion in total liabilities. Total liabilities increased by \$7 billion in FY 2019 mostly due to numerous changes in actuarial assumptions related to the Department's FEVB, as well as an increase in cash collections due to the General Fund by CBP based on current year import activity on goods imported.

### 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 \$45.2 billion. Total net position increased \$2.4 billion from FY 2018, in large part because there was an increase in appropriations for border security and USCG procurement, construction and improvements which were offset by a reduction in actual expenditures in FY 2019.



\*USCIS negative net cost balance is due from excessive revenue from H1-B and L-1 visa fee collections.

### 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 \$65.2 billion in FY 2019. DHS recognized decreased costs in FY 2019 due to a decrease in disaster events.

During FY 2019, the Department earned approximately \$15.7 billion in exchange revenue. Exchange revenue arises from transactions in which the Department and the other party receive value and

that are directly related to departmental operations. The Department also collects



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

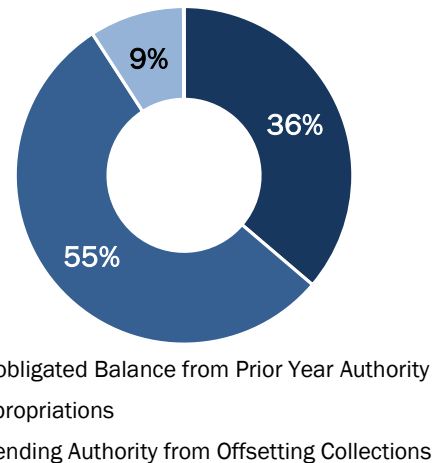
### Budgetary Resources

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 2019	FY 2018	\$ Change	% Change
Unobligated Balance from Prior Year Authority	\$ 50,768	\$ 23,900	\$ 26,868	>100%
Appropriations	76,512	110,725	(34,213)	-31%
Spending Authority from Offsetting Collections	12,738	14,038	(1,300)	-9%
Borrowing Authority	67	6,110	(6,043)	-99%
<b>Total Budgetary Authority</b>	<b>\$ 140,085</b>	<b>\$ 154,773</b>	<b>\$(14,688)</b>	<b>-9%</b>

The Department’s budgetary resources were approximately \$140.1 billion for FY 2019. The authority was derived from \$50.8 billion in authority carried forward from FY 2018, appropriations of \$76.5 billion, approximately \$12.7 billion in collections, and \$67 million in borrowing authority. Budgetary resources decreased approximately \$14.6 billion from FY 2018. This is due to decrease in supplemental appropriations and borrowing authority related to disaster recovery.

Of the total budget authority available, the Department incurred a total of \$92 billion in obligations from salaries and benefits, purchase orders placed, contracts awarded, or similar transactions.



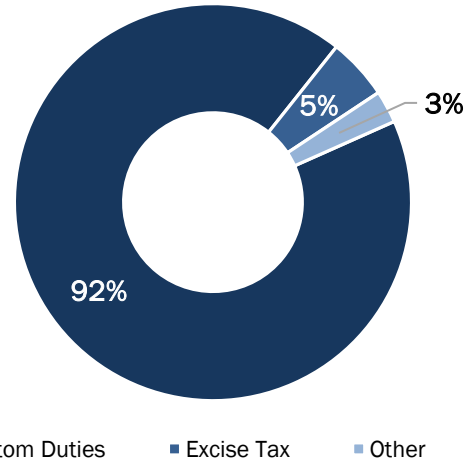
### Custodial Activities

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 2019	FY 2018	\$ Change	% Change
Cash Collections from Duties	\$ 71,902	\$ 41,584	\$ 30,318	73%
Excise Tax	3,889	3,809	80	2%
Other	2,058	1,892	166	9%
<b>Total Cash Collections</b>	<b>\$ 77,849</b>	<b>\$ 47,285</b>	<b>\$ 30,564</b>	<b>65%</b>

## Management's Discussion and Analysis

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 \$77.8 billion. Total cash collections increased \$30.5 billion from FY 2018. This is due to increased collections related to several duty increases enacted by Executive Orders and/or as a result of U.S. Trade investigations including but not limited to steel and aluminum imports and various imported products.



Custom duties collected by CBP account for 92 percent of total cash collections. The remaining 8 percent is comprised of excise taxes, user fees, and various other fees.

### Other Key Regulatory Requirements

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

## Secretary's Assurance Statement

November 14, 2019



The Department of Homeland Security management team is responsible for meeting the objectives of the Federal Managers' Financial Integrity Act of 1982 (FMFIA) 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, 2019 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 Appendix A of OMB Circular A-123 and Government Accountability Office (GAO) Standards for Internal Control. 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 Systems Functionality, where areas of material weaknesses have been identified and remediation is in process, as further described in the *Management Assurances* section of the Agency Financial Report.

In addition, the areas of material weaknesses related to Information Technology (IT) Controls and Systems Functionality stated above affects the Department's ability to fully comply with the Federal Financial Management Improvement Act of 1996 (FFMIA) financial management system requirements, and therefore the Department is also reporting a noncompliance with FFMIA. In addition, a few Components identified certain financial management systems do not substantially comply with Federal accounting standards and application of the United States Standard General Ledger at the transaction level.

As a result of our assessments conducted, I am pleased to report that the Department has made progress in enhancing its internal controls and financial management program and continues to plan for additional improvements going forward.

Sincerely,

A handwritten signature in blue ink, which appears to read "Chad Wolf". The signature is fluid and cursive.

Chad Wolf  
Acting Secretary of Homeland Security



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

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



**Homeland  
Security**

The Honorable 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, 2019, 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, 2019, the DHS's internal control over financial reporting is effective except for material weaknesses identified in Financial Reporting and Information Technology Controls and System Functionality, based on criteria established in the *Standards for Internal Control in the Federal Government*. Specifically, management of DHS identified areas of material weaknesses in Financial Reporting and Information Technology Controls and System Functionality. Specifically:

1. *Financial Reporting*: Ineffective controls over the journal entry process, review of actuarial liability assumptions, service provider monitoring, and other conditions.
2. *IT Controls and System Functionality*: Ineffective controls in financial management systems, insufficient design of controls over information produced by entity, and ineffective monitoring of service provider organizations.

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

The Honorable Joseph V. Cuffari  
Page 2

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,



Acting Secretary

## Management Assurances

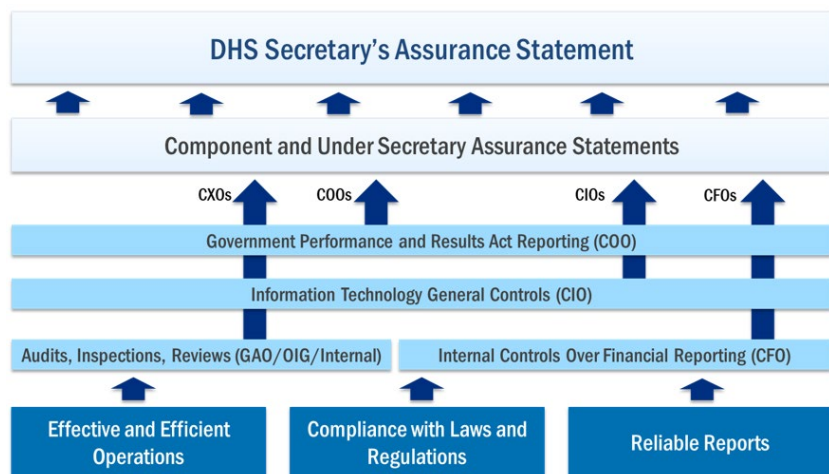
DHS management is responsible for establishing, maintaining, and assessing internal controls to provide reasonable assurance that the objectives of the Federal Managers’ Financial Integrity Act of 1982 (31 United States Code 3512, Sections 2 and 4) and the Federal Financial Management Improvement Act of 1996 (Pub. L. 104-208), as prescribed by the GAO Standards for Internal Control in the Federal Government known as the Green Book, are met. In addition, the DHS Financial Accountability Act (Pub. 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 of internal control in the Federal Government. 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.

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, establishing requirements to assess, correct, and report on the effectiveness of internal controls. OMB Circular A-123 implements the FMFIA and Green Book requirements. FMFIA also requires the Statement of Assurance to include assurance on whether the agency’s financial management systems comply with government-wide requirements. The financial management systems requirements are directed by Section 803(a) of the FMFIA and Appendix D to OMB Circular A-123, *Compliance with the Federal Financial Management Improvement Act of 1996*.

In accordance with 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 financial 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.

Furthermore, DHS is building on the enterprise risk management framework per OMB Circular A-123 and have established a Department-wide Enterprise Risk Management (ERM) working group to facilitate and promote Component development and maturation of ERM capability. In FY 2018, the Department developed an agency risk profile. As continuation, Components were asked to update and continue to implement ERM at Component-levels. 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.

#### **Department of Homeland Security Financial Accountability Act**

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 we meet the overall objectives.

Using GAO Standards for Internal Control and 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 four-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 assessments are performed to validate that neither material weakness conditions exist, nor will there be audit surprises. This assessment and reporting strategy supports 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 2018, management reported two areas of material weaknesses - financial reporting and IT controls and system functionality. DHS made significant improvements in remediating areas of material weaknesses and planned to resolve financial reporting in FY 2019 through targeted remediation at USCG. USCG designed and implemented a Journal Entry process that focused on management review controls as well as documenting and implementing acceptable documentation to support journal entries. However, Management did not formally test these areas to provide reasonable assurance that risks have been sufficiently mitigated. Refer to the table below for areas contributing to the financial reporting material weakness and appropriate corrective actions planned in FY 2020.

**Table 1: Internal Control over Financial Reporting Corrective Actions**

Area of Material Weakness	Component	Year Identified	Target Correction Date
	USCG, USSS, AII <sup>1</sup>	FY 2003	FY 2020
<b>Financial Reporting</b>	<p>Areas of material weakness exist that are attributed to financial reporting, which include the following:</p> <ul style="list-style-type: none"> <li>• <i>Journal Entry / On-Top-Adjustments:</i> USCG did not sufficiently test the JV/OTA process as part of its annual assessment process. In FY 2020, USCG will continue to train process owners and improve execution of the designed journal entry process and continue to document and test underlying and compensating controls that would prevent and detect errors on a timely basis. In addition, ineffective IT system controls have contributed to this area. Refer to IT Controls and System Functionality material weakness and corrective action for more details.</li> <li>• <i>Actuarial Liabilities:</i> Controls over validating and documenting actuarial assumptions were not operating effectively. While Standard Operating Procedures exist, controls were not fully executed.</li> <li>• <i>Other:</i> Several deficiencies aggregated to an area of material weakness, classified as other. These include lack of monitoring of service providers and inability to record trading partner activity at the initiation of the transaction event due to system limitations.</li> </ul>		
<b>Corrective Actions</b>	<ul style="list-style-type: none"> <li>• <i>Journal Entry / On-Top-Adjustments:</i> USCG will test the Journal Entry and 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 the entries.</li> <li>• <i>Actuarial Liabilities:</i> USCG and USSS will continue to refine its processes and ensure are fully executed and monitored.</li> <li>• <i>Other:</i> DHS is in the process of implementing G-Invoicing<sup>2</sup> which will help reduce the risk of system limitations. For service monitoring controls, refer to IT Controls and System Functionality material weakness and corrective action for more details.</li> </ul>		

Areas of material weakness over IT controls and system functionality remains; Components continue to fix known issues and have not yet been able to sufficiently demonstrate control effectiveness through testing. Corrective Actions for IT controls and system functionality is in the following table. The Department remains dedicated to fully remediating significant IT system security and functionality weaknesses. A summary of corrective actions is provided in the table below.

**Table 2: Internal Control over Financial Reporting Corrective Actions**

Area of Material Weakness	Component	Year Identified	Target Correction Date
	All DHS Components	FY 2003	FY 2020
<b>IT Controls and System Functionality</b>	<p>Areas of material weakness exist that are attributed to the IT controls and system functionality deficiencies, which include the following:</p> <ul style="list-style-type: none"> <li>• <i>Financial System Requirements:</i> The Department internal control assessment identified IT Controls as a material weakness due to inherited control deficiencies surrounding general computer and application controls. 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. In addition, the Department’s financial systems do not fully comply with the FFMA.</li> </ul>		

<sup>1</sup> The “Other” area of material weakness in financial reporting contributes DHS-wide. Areas, Journal Entry/On-Top-Adjustment and Actuarial Liability, within financial reporting are only attributed to USCG and USSS.

<sup>2</sup> G-Invoicing is the government’s long-term sustainable solution for Buy/Sell transactions and will manage the receipt and acceptance of General Terms and Conditions Agreements, Orders, and Performance.

Area of Material Weakness	Component	Year Identified	Target Correction Date
	All DHS Components	FY 2003	FY 2020
	<ul style="list-style-type: none"> <li>• <i>System Functionality and Information Produced by Entity (IPE):</i> Ineffective IT control and inadequate application controls (functionality) impact the ability for management to fully rely on system generated data and reports, commonly referred to as IPEs. Currently, these deficiencies are directly associated with financial system requirement deficiencies. In FY 2020, in addition to fixing long-standing IT control weaknesses, DHS will implement a risk-based strategy for identifying and testing IPEs as well as test functionality for systems that have sufficient IT controls.</li> <li>• <i>Service Provider Monitoring:</i> The Department did not maintain effective internal controls related to service organizations, including evaluating and documenting roles of service organizations, performing effective reviews of service organization control reports, and addressing service provider risk in absence of SOC reports.</li> </ul>		
<b>Corrective Actions</b>	<p>Key contributing Components fixed prior year identified issues in FY 2019 while non-key contributing Components continued to implement the find, fix, test strategy. Remediated controls will be tested in FY 2020, which will be reflected in each Component’s IT Commitment Letters signed by both the respective CFO and CIO. The IT Commitment Letters require each Component to commit to testing as well as provide commitment to passing results for each system and control in scope. Once OCFO obtains final Component commitments, this will enable the Department to gauge by FY 2020 Q1 if target correction date can be achieved.</p>		

**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.

We assess our financial management systems annually for compliance with the requirements of Appendices A and D to OMB Circular A-123 and other federal financial system requirements. In addition, we assess available information from audit reports and other relevant and appropriate sources, such as FISMA compliance activities, to determine whether our financial management systems substantially comply with FFMIA. We also assess improvements and ongoing efforts to strengthen financial management systems and the impact of instances of noncompliance on overall financial management system performance.

Based on the results of our overall assessment, areas of material weaknesses related to Information Technology Controls and Systems Functionality affects the Department’s ability to fully comply with financial management system requirements, and therefore the Department is also reporting a noncompliance with FFMIA. The Department is actively engaged to correct the areas of material weaknesses through significant compensating controls while undergoing system improvement efforts. The outcome of system improvement efforts will efficiently enable the Department to comply with government-wide requirements and reduce manual compensating controls.



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

Area of	Component	Year Identified	Target Correction Date
Non-Compliance	All DHS Components	FY 2003	FY 2020
<b>FFMIA Non-compliance</b>	<p>DHS does not substantially comply with FFMIA primarily due to lack of compliance with financial system requirements as disclosed as material weakness in IT Controls and System functionality. 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.</p> <p>In FY 2018, the Department updated the targeted correction date to FY 2020. The target correction date took into consideration reduction of the financial reporting material weakness that would also compensate for inadequate system functionality as well as the Department’s target to substantially reduce the severity of IT controls by end of FY 2020. Based on rigorous testing conducted in FY 2017 through FY 2018, key contributing Components committed to fixing prior year identified issues in FY 2019 which ultimately delayed the Department in meeting its goals. Remediated controls will be tested in FY 2020, which will be reflected in each Component’s IT Commitment Letters signed by both the respective CFO and CIO. The IT Commitment Letters require each Component to commit to testing as well as provide commitment to passing results for each system and control in scope. Once OCFO obtains final commitments, this will enable the Department to gauge by FY 2020 Q1 if target correction date can be achieved.</p>		
<b>Corrective Actions</b>	<p>The DHS CFO, CIO, and Components will support the Components in the design and implementation of internal controls in accordance with DHS 4300A, Sensitive Systems Handbook, Attachment R: Compliance Framework for CFO Designated Financial Systems. In addition, DHS CFO and Components will continue to design, document, and implement compensating controls to reduce the severity of system security internal controls and functionality limitations. Once OCFO obtains final Component commitments, this will enable the Department to gauge by FY 2020 Q1 if target correction date can be achieved.</p>		

### **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 (DQP) 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 its respective DATA Act reporting processes and controls over consolidation and variance resolution of data submitted to DHS Headquarters. In FY 2019, DHS developed 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.

### **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 efforts.

DHS has established a Joint Program Management Office (JPMO) to oversee Financial Systems Modernization (FSM) program management, priorities, risk, cost, and schedule. Our approach to modernizing financial management systems across the Department includes:

- Expanding business intelligence and standardizing data across Components to quickly provide enterprise-level reporting;
- Targeting investments in financial systems modernization in a cost-effective manner and minimizing duplication in infrastructure in accordance with emerging technologies and guidance;
- Prioritizing essential system modernizations for the Components with the most critical need and projected greatest return on investment for efficiency and business process improvements; and
- Strengthening existing system controls – DHS is not depending on FSM efforts to achieve a “clean” internal control opinion or FFMIA compliance. We are addressing IT control weaknesses in high-impact CFO designated systems through a holistic, multi-year remediation and internal control strategy, including compensating and complimentary controls.

In March 2017, it was determined that DHS would transition the CWMD, TSA, and USCG FSM initiatives out of their current shared service provider environment at the Department of

## Management's Discussion and Analysis

Interior (DOI) and into a DHS-managed solution. This solution delivers a standardized baseline for this trio of components, with increased functionality and integration for CWMD. In October of 2018, TSA and USCG resumed implementation efforts while CWMD has been upgraded to the latest solution. 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.

Progress continues as USSS and CWMD have completed upgrades to the next version of their current accounting software, as we actively work to implement upgrades at TSA and USCG. Other significant system modernization efforts in various stages of implementation include FEMA's financial system, flood insurance, and grants management modernization as well as CBP's custodial revenue system, Automated Commercial Environment (ACE).

### **Other Regulatory Matters**

The Department is required to comply with several other legal and regulatory financial requirements, including the Improper Payment Information Act (IPIA, as amended), the Debt Collection Improvement Act, and the Prompt Payment Act. The results of IPIA are reported in the Other Information section. In addition, the Department does not refer a substantial amount of debts to Treasury for collection. In FY 2019, DHS paid vendor timely 93% of the time versus the government-wide goal of 98%. On-time invoice payment reduction was primarily due to delays in invoice processing due to the funding lapse in FY 2019.