Department of Homeland Security

FY 2017 Agency Financial Report

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

Homeland Security

We are DHS

Certificate of Excellence in Accountability Reporting

In May 2017, DHS received its fourth consecutive Certificate of Excellence in Accountability Reporting (CEAR) from the Association of Government Accountants (AGA) for its FY 2016 Agency Financial Report, along with a best-in-class award for Best Agency Head Message. 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) 2017 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 2017, the Department is using the alternative approach—identified in the Office of Management and Budget's Circular A-136—to produce its Performance and Accountability Reports, which consists of the following three reports:

- DHS Agency Financial Report | Publication date: November 15, 2017.
- DHS Annual Performance Report | Publication date: 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, 2018.

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

Message from the Secretary

November 14, 2017

I am pleased to present the Department of Homeland Security's (DHS) Agency Financial Report for Fiscal Year (FY) 2017. 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 critical mission.

DHS manages risk every day, and in an environment of new and evolving threats, we cannot do more with less. As a result, we strive to ensure that the limited resources we have cover our areas of greatest risk before seeking additional resources to meet agency requirements.

Even with the extremely high operational tempo of the Department, DHS continues to be transparent and accountable to our stakeholders and taxpayers when it comes to how their tax dollars are spent. The Government Accountability Office (GAO) recognized the Department in the 2017 High Risk Series for our significant progress toward addressing GAO's outcomes and meeting criteria to be removed from the GAO High Risk list, demonstrating our continued efforts to transform and integrate our management functions. In 2017, DHS was also recognized by the U.S. Department of the Treasury for demonstrating our full commitment to transparency in achieving compliance with the Digital Accountability and Transparency Act. DHS spending data is available at www.usaspending.gov.

This year, we institutionalized transparent and repeatable processes to guide the Department's resource allocation by mission area rather than Component stovepipes. In one of the largest budget transformations in the Federal Government's history, the Department instituted a Common Appropriations Structure framework, which allows the Department to compare like missions and activities and reduce 76 non-integrated appropriations types to four common appropriations for all Components but the U.S. Coast Guard. The U.S. Coast Guard is transitioning to the Common Appropriations Structure by FY 2019.

For FY 2017, DHS received a clean audit opinion on its financial statements for the fifth consecutive year and continues to strengthen and mature our internal control processes. 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. In FY 2017, with dedicated efforts by all of our Components, but particularly the U.S. Coast Guard, DHS achieved a downgrade of its property, plant and equipment material weakness to a significant deficiency. With the two remaining internal control material weaknesses—Financial Reporting, and Information Technology—DHS is executing a multi-year strategy and plan to achieve an unmodified internal control audit opinion.

DHS remains committed to securing the homeland as well as preparing for and responding to disasters. We will continue to meet these challenges with accountability and transparency — strengthening our risk management, internal controls, and mission-based resourcing to maximize the return on taxpayer investment.

Sincerely,

Elaine C. Duke
Acting Secretary of Homeland Security

Table of Contents

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 the Department of Homeland Security.

The ***Overview*** section describes the Department's organization, missions and goals, and overview of our 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.

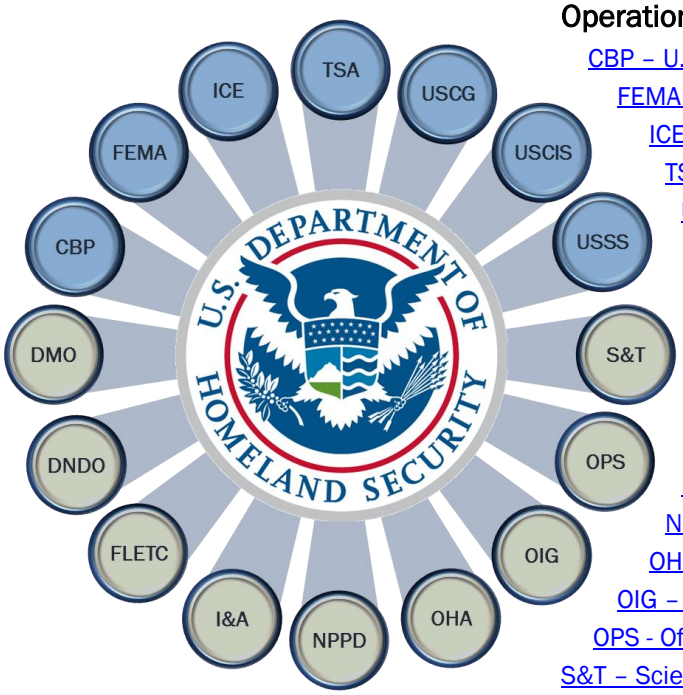
The ***Financial Overview*** section provides a summary of DHS's financial data explaining the major sources and uses of funds and provides a quick look at our Balance Sheet, Statement of Net Cost, Statement of Changes in Net Position, Statement of Budgetary Resources, and Statement of Custodial Activities.

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

The Department of Homeland Security (DHS) has a fundamental duty—to secure the Nation from the many threats we face. This requires the dedication of more than 240,000 employees in jobs that range from aviation and border security to emergency response, from cybersecurity analyst to chemical facility inspector. Our duties are wide-ranging and as one team, with one mission—we are one DHS—keeping America safe.

DHS's operational Components lead the Department's frontline activities to protect our Nation (shaded in blue). The remaining DHS Components (shaded in light green) provide resources, analysis, equipment, research, policy development, and support to ensure the frontline organizations have the tools and resources to accomplish the DHS mission. For more information about the Department's structure, visit our website at http://www.dhs.gov/organization. For information on each of our Components, click on their respective link to the right of the figure below.



Operational Components

CBP – U.S. Customs and Border Protection
FEMA – Federal Emergency Management Agency
ICE – U.S. Immigration and Customs Enforcement
TSA – Transportation Security Administration
USCG – U.S. Coast Guard
USCIS – U.S. Citizenship and Immigration Services
USSS – U.S. Secret Service

Support Components

DMO - Departmental Management and Operations
DNDO – Domestic Nuclear Detection Office
FLETC – Federal Law Enforcement Training Centers
I&A – Office of Intelligence and Analysis
NPPD – National Protection and Programs Directorate
OHA – Office of Health Affairs
OIG – Office of Inspector General
OPS - Office of Operations Coordination
S&T – Science and Technology Directorate

Figure 1: DHS Operational and Support Components

Strategic Alignment Overview

The Department operates under one unified mission: *With honor and integrity, we will safeguard the American people, our homeland, and our values*. The FY 2014-2018 Strategic Plan further details the Department's missions and focus area, which are grouped into four major missions for better alignment within the Financial Section for the Statement of Net Cost

and related footnotes to allow the reader to clearly see how resources are spent towards the common goal of a safe, secure, and resilient Nation.

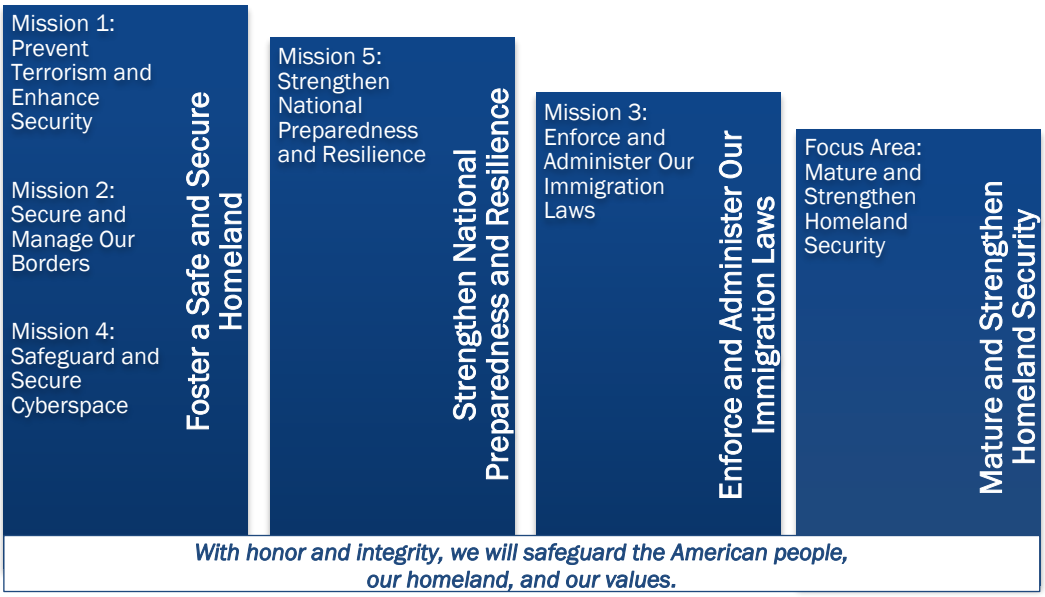


Figure 2: DHS Strategic Plan Alignment for Reporting

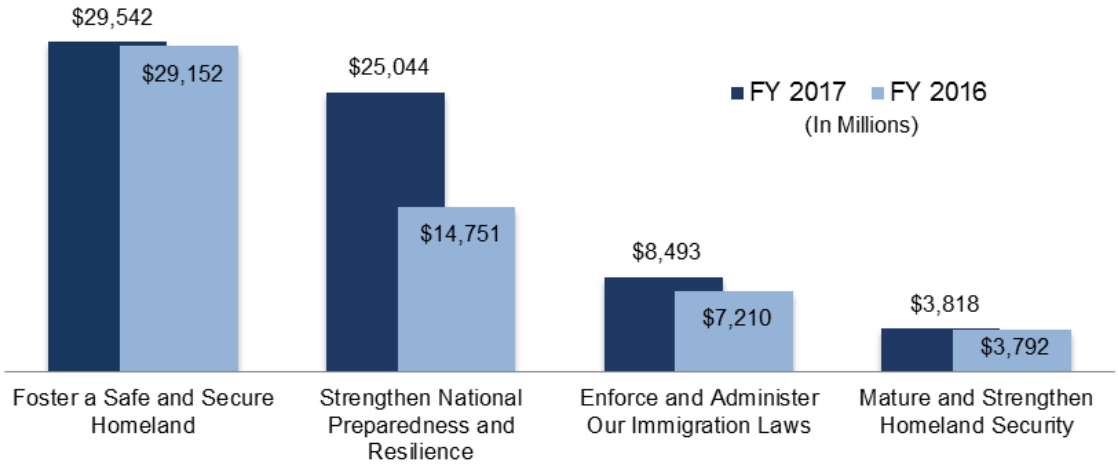


Figure 3: DHS's Net Cost of Operations for Each Major Mission Area

The chart above provides DHS's Net Cost of Operations for each major mission area. Further information about the Department's financial position and results of operations is presented in the Financial Overview section. The Performance Overview that follows provides a summary of performance highlights from a subset of the Department's strategic measures using the structure above.

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 2017-2019 Annual Performance Report with the FY 2019 Congressional Budget and can be accessed at: http://www.dhs.gov/performance-accountability.

The Department created a robust performance framework that drives performance management and enables the implementation of performance initiatives. This approach also facilitates the reporting of results within the Department for a comprehensive set of measures aligned to the missions and goals of the Department. The figure below shows the linkage between our strategic plan, the Department's mission programs, and the measures we use to gauge performance. This approach to measurement ensures that the Department can assess the achievement of our missions as identified in our strategic framework.

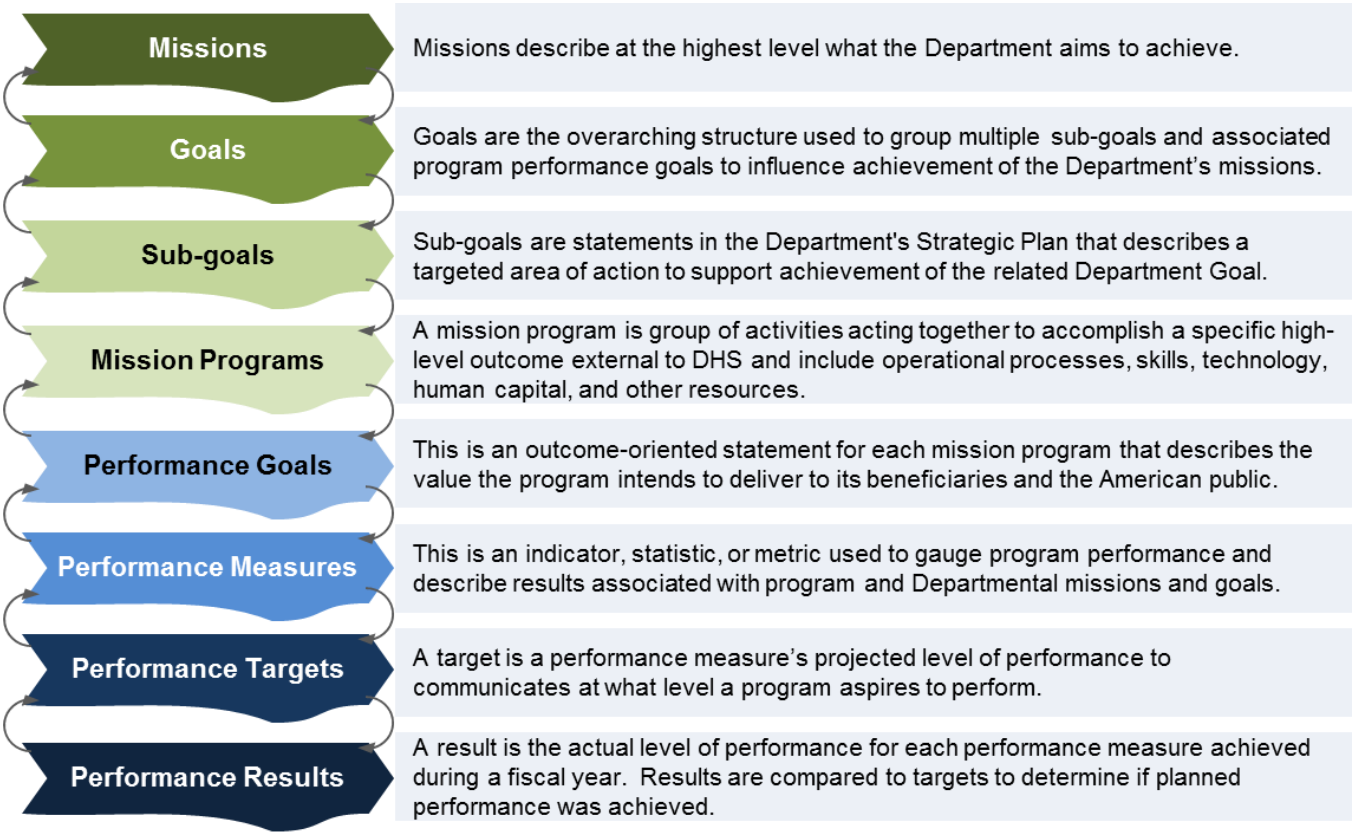


Figure 4: DHS Performance Framework

Foster a Safe and Secure Homeland

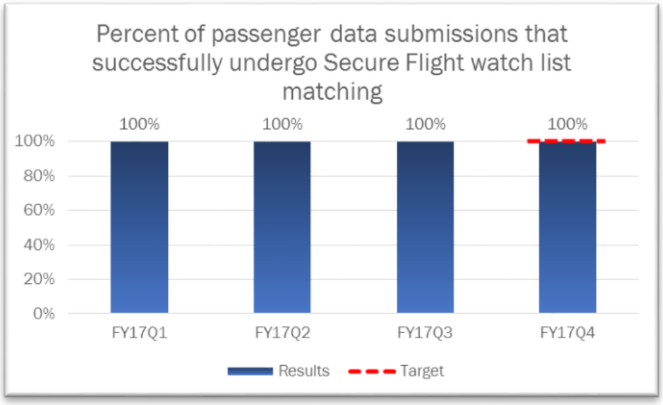
Mission 1: Prevent Terrorism and Enhance Security

Preventing a terrorist attack in the United States remains the cornerstone of homeland security. Our vision is a secure and resilient Nation that effectively prevents terrorism in ways that preserve our freedom and prosperity.

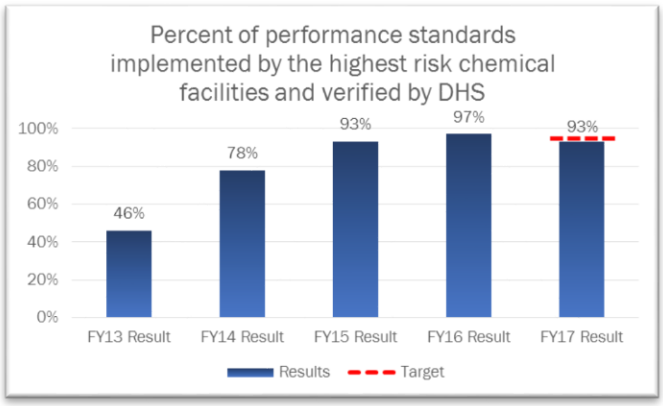
Our goals for this mission are:

- Goal 1.1: Prevent Terrorist Attacks;
- Goal 1.2: Prevent and Protect Against the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities; and
- Goal 1.3: Reduce Risk to the Nation's Critical Infrastructure, Key Leaders, and Events.

The following highlighted measures gauge our efforts to prevent terrorism and enhance security.

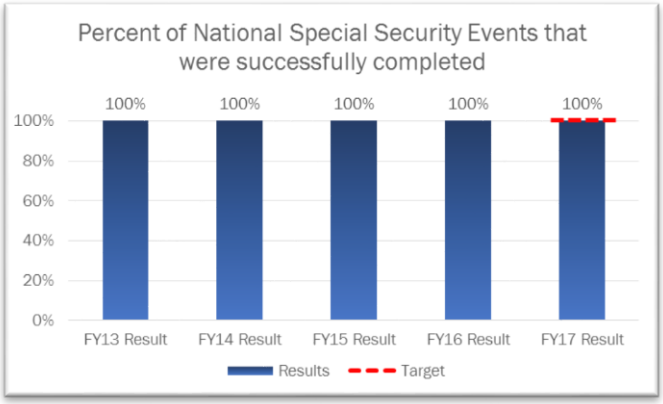


Percent of passenger data submissions that successfully undergo Secure Flight watch list matching (TSA): Vetting individual travelers against high-risk watch lists strengthens the security of the transportation system. This measure reports the percent of qualified message submissions received from the airlines that are successfully matched by the Secure Flight automated vetting system against the existing high-risk watch lists. A qualified message submission from the airlines contains passenger data sufficient to allow successful processing in the Secure Flight automated vetting system. In FY 2017, TSA successfully matched 100 percent of passenger data submissions.



Percent of performance standards implemented by the highest risk chemical facilities and verified by DHS (NPPD): The Chemical Facility Anti-Terrorism Standards (CFATS) program is an important part of our Nation's counterterrorism efforts as the Department works with our industry stakeholders to keep dangerous chemicals out of the hands of those who wish to do us harm. The CFATS program identifies and regulates high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with these chemicals. Initially authorized by Congress in 2007, the program uses a dynamic multi-tiered risk assessment process and requires facilities identified as high-risk to meet and maintain performance-based security standards appropriate to the facilities and the risks they pose. In FY 2017, DHS delivered guidance to the highest risk chemical facilities,

prompting these owners and operators to include 21,412 performance standards in their security plans. Of the 21,412 performance standards, 19,914 have been implemented, achieving a 93 percent result for this measure, narrowly missing its target. Implementing these performance standards improves the overall security of the highest risk chemical facilities. In October 2016, DHS rolled out the Chemical Security Assessment Tool (CSAT) 2.0 system, an updated online portal that helps DHS identify facilities that meet the criteria for high-risk chemical facilities. During FY 2017, the implementation of CSAT 2.0 resulted in significant movement of facilities entering and leaving the program. As a result of these updates, DHS saw an overall decrease in the percentage of performance standards implemented by the highest risk chemical facilities, particularly as more facilities were reviewed and re-tiered using the CSAT 2.0 system. DHS will continue to prioritize the implementation of performance standards across the highest risk chemical facilities.



Percent of National Special Security Events that were successfully completed (USSS): National Special Security Events (NSSE) require a tremendous amount of preplanning and coordination with numerous federal, state, and local jurisdictions. When an event is designated by the Secretary of DHS as an NSSE, the USSS is the lead agency for the design and implementation of the operational security plan. This measure is a percent of the total number of NSSEs completed in a fiscal year where once the event commenced, a security incident inside a USSS protected venue did not preclude the event's agenda from proceeding to its scheduled conclusion. USSS has attained 100 percent success for the past five years.

TSA Pre✓® Reaches Milestone with more than 5 Million Travelers Enrolled

The Transportation Security Administration TSA Pre✓® program reached a milestone in July 2017 of more than 5 million travelers enrolled. TSA Pre✓® now has more than 390 application centers nationwide.

"By growing the trusted traveler population, we help our officers focus on potential threats, which strengthens the security screening process and ultimately provides better security for all travelers," said TSA Acting Administrator Huban A. Gowadia[1]. "We will continue our efforts to further expand the TSA Pre✓® program, with the ultimate goal of providing the most effective security in the most efficient way."

TSA Pre✓®, which is now available at more than 180 U.S. airports, is an expedited screening program that enables low-risk travelers to enjoy a more convenient and efficient screening experience. Travelers using the TSA Pre✓® lane do not need to remove shoes, belts, light jackets, laptops, or 3-1-1 liquids from their carry-on bags.

U.S. citizens and lawful permanent residents may apply for TSA Pre✓® for a cost of $85 for five years. Once approved, travelers will receive a "known traveler number" and will have the opportunity to utilize TSA Pre✓® lanes at select security checkpoints when flying on any of the 37 participating airlines. TSA Pre✓® is also available for U.S. Armed Forces service members, including those serving in the U.S. Coast Guard, Reserves, and National Guard.

[1] David Pekoske was confirmed by the U.S. Senate as the Transportation Security Administration's seventh administrator in August 2017.

Looking Forward

The United States has made significant progress in securing the Nation from terrorism. Nevertheless, the evolving and continuing threat from terrorists remains, as witnessed by events around the globe. The Department and its many partners, which includes international and federal, state, local, tribal and territorial governments, public and private sectors, and communities across the country, have strengthened the homeland security enterprise to better mitigate and defend against these dynamic threats. Below are a few areas that advance our efforts to achieve the Department's mission of preventing terrorism and enhancing security.

TSA Enhancing Security to Mitigate Checkpoint Gaps: TSA continues to advance our ability to assess potential threats from aviation passengers both in the domestic and international domains. We will continue to improve the Threat Image Projection data quality to ensure the security of the traveling public. Ongoing testing and deployment of new technology to identify threats is underway. Based on the results of these tests, plans will be made to enhance our ability to identify and mitigate checkpoint gaps. In addition, specific improvements are being made to enhance airport perimeter and access security and identity vetting.

Chemical Facility Tiering: Tier 1 and 2 facilities are those chemical facilities that pose the highest risk with respect to vulnerability, consequence, and threat factors. The CFATS program identifies and regulates high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with certain chemicals of interest. The challenge is that the number and tier of existing chemical facilities changed in FY 2017 based on a revised methodology enacted at the beginning of FY 2017. These changes in tiering pose a challenge in that the backlog of facilities needing assessments changed dramatically and will have an impact to get all assessments up to date. Moving forward, the Department will look into scheduling and staffing approaches that will prioritize the assessment of all Tier 1 and 2 chemical facilities to achieve an acceptable level of oversight and understanding. DHS anticipates that the tiering for the highest risk chemical facilities will stabilize in FY 2018 as facilities continue to self-report chemicals of interest under the new methodology.

USSS Protecting Critical Infrastructure, Key Leaders, and Events: USSS has numerous efforts underway to meet increasing operational challenges including reducing time to hire, retention initiatives, and technology development. Challenges have been faced with the increased demands on the protective mission in terms of both scope and complexity. Thus the USSS is looking at new and unique methods to address a broad range of areas to include: modernization and support of mission-critical information technology (IT) systems; infrastructure for protective and investigative mission operations; improved staffing and career models to ensure proper work/life balance for agents; new staffing goals and retention initiatives to reduce attrition; and enhancing training infrastructure to meet future needs.

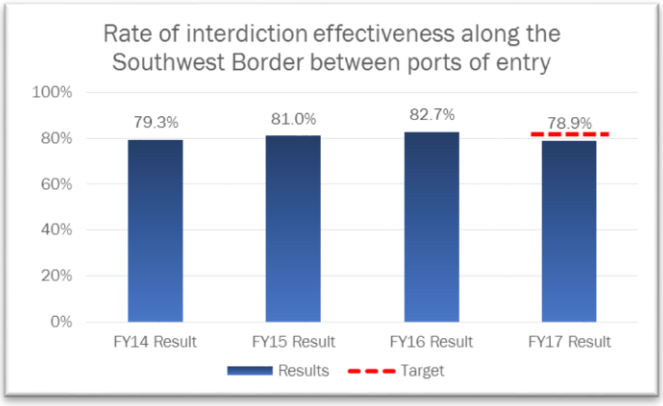
Mission 2: Secure and Manage Our Borders

DHS secures the Nation's air, land, and sea borders to prevent illegal activity while facilitating lawful travel and trade.

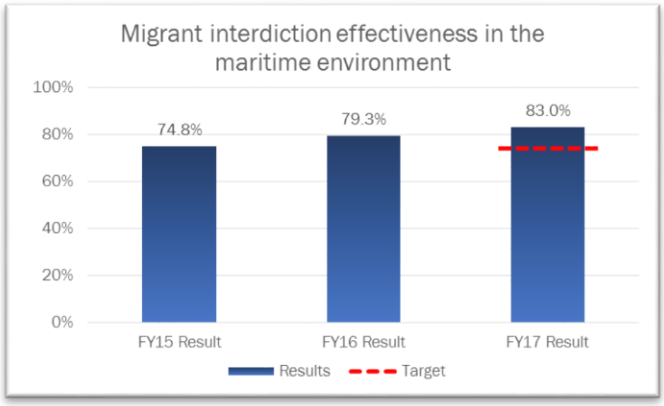
Our goals for this mission are:

- Goal 2.1: Secure U.S. Air, Land, and Sea Borders and Approaches;
- Goal 2.2: Safeguard and Expedite Lawful Trade and Travel; and
- Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations and Other Illicit Actors.

The following highlighted measures gauge our efforts to secure and manage our borders.

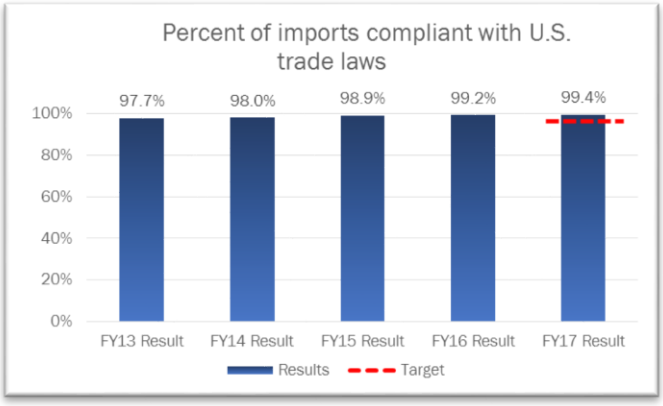


Rate of interdiction effectiveness along the Southwest Border between ports of entry (CBP): As a division of CBP, the Border Patrol has evolved significantly since its inception in 1924; however, its overall mission remains unchanged: protecting our Nation's borders from illegal entry of people, drugs, and contraband. Together with other law enforcement officers, the Border Patrol helps secure our borders between the ports of entry by detecting, tracking, and interdicting illegal flows of people and contraband. This measure reports the percent of detected entrants who were apprehended, or turned back after illegally entering the United States between the ports of entry on the southwest border. The Border Patrol achieves this result by maximizing the apprehension of detected illegal entrants or confirming that illegal entrants return to the country from which they entered; and by minimizing the number of persons who evade apprehension. In FY 2017, this measure achieved 78.9 percent which is a decrease from FY 2016. Concurrently, border detection technology has increased, yielding greater situational awareness of illegal entrants who previously would have gone undetected, however agent staffing shortages reduce the ability to respond. Going forward, the Border Patrol's increased situational awareness will need to be paired with increased response capability. The Department is making investments in recruitment, retention, and relocation programs to address these challenges. Further discussion is located in the "Looking Forward" portion of this section on page 11.



Migrant interdiction effectiveness in the maritime environment (USCG): This measure reports the percent of detected undocumented migrants of all nationalities who were interdicted by the USCG and partners via maritime routes. Thousands of people try to enter this country illegally every year using maritime routes. USCG conducts patrols and coordinates with other federal agencies and foreign countries to interdict undocumented

migrants at sea, denying them entry via maritime routes to the United States, its territories and possessions. Interdicting migrants at sea means they can be quickly returned to their countries of origin without the costly processes required if they successfully enter the United States. In its third year of reporting, the USCG achieved 83.0 percent migrant interdiction effectiveness, up from FY 2016. This increase is primarily due to a reduction in Cuban migrant flow following the termination of the Cuban parole policy[2] in January 2017. The decrease in Cuban migrant flow enabled USCG patrol assets to improve response and have greater interdiction success in the Florida Straits.



Percent of imports compliant with U.S. trade laws (CBP): Ensuring that all imports are compliant and free of major discrepancies allows for lawful trade into the United States and both CBP and the importing/exporting community have a shared responsibility to maximize compliance with laws and regulations. CBP works with our international trade partners through several trade programs to build—and improve upon—a solid and efficient trade relationship to accomplish safer, faster, and more compliant trade. This measure reports the percent of imports that are compliant with U.S. trade laws including customs revenue laws. In FY 2017, 99.4 percent of imports were found to be compliant with U.S. trade laws, meeting this year's target. Results have improved year-over-year for the past five-years.

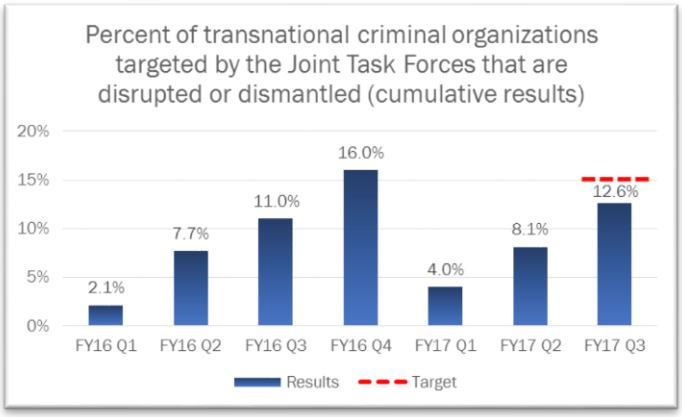
A Unified Effort: Combating Transnational Gang Violence within the Interior Borders of the United States

In February 2017, President Trump signed Executive Order 13773, aimed at targeting transnational criminal organizations (TCO), such as drug cartels or gangs like Mara Salvatrucha (MS -13). The Executive Order is a multifaceted approach in attacking TCOs that pose a threat to national security and/or public safety. U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), remains vigilant in disrupting and dismantling violent gang activity in collaboration with our state, local, and tribal, and foreign law enforcement partners. Due to violence caused by members of MS-13, HSI New York established Operation Matador (OPMAT). OPMAT is a multi-pronged approach in which HSI NY partnered with other DHS components to combat MS-13 in the greater New York City area. OPMAT is primed to disrupt and dismantle MS-13 through five key elements: intelligence gathering; actionable lead development; targeted enforcement; investigation development; and community outreach to at-risk youth in the affected cities. From May 9, 2017 to June 30, 2017, OPMAT has led to 68 arrests of known gang members, 60 of which were established as MS-13 gang members. ICE remains committed in working in a unified approach in combating gang violence and disrupting the MS-13 pipeline.

Priority Goal: Decrease the ability of targeted transnational criminal organizations to conduct illicit activities impacting the southern border and approaches region of the United States. By

[2] On January 12, 2017, DHS eliminated a special parole policy for arriving Cuban nationals commonly known as the "wet-foot/dry-foot" policy, as well as a policy for Cuban medical professionals known as the Cuban Medical Professional Parole Program. It is now Department policy to consider any requests for such parole in the same manner as parole requests filed by nationals of other countries.

September 30, 2017, actions by the DHS Joint Task Forces via synchronized component operations will result in the disruption and/or dismantlement of 15 percent of targeted transnational criminal organizations.



Performance Analysis: Through the execution of coordinated operational plans and investigations, the Joint Task Forces (JTFs) were able to enable the disruption and dismantlement of 12.6 percent (as of the 3rd quarter FY 2017[3]) of their targeted transnational criminal organizations, and is on track to meet its goal of 15 percent for this important work. The JTFs continue to coordinate across organizational boundaries to make positive advances with operations with joint investigations and operations within their functional areas, and are supported by DHS operational components in order to enhance DHS's effort in securing the U.S. Southern Border and Approaches. JTFs facilitated broader discussions with Components and garnered the reallocation of resources, including assets and personnel, to meet operational requirements.

Looking Forward

The protection of the Nation's borders—land, air, and sea—from the illegal entry of people, weapons, drugs, and other contraband while facilitating lawful travel and trade is vital to homeland security, as well as the Nation's economic prosperity. The global economy is increasingly a seamless economic environment connected by systems and networks that transcend national boundaries. The United States is deeply linked to other countries through the flow of goods and services, capital and labor, and information and technology across our borders. As much as these global systems and networks are critical to the United States and our prosperity, they are also targets for exploitation by our adversaries, terrorists, and criminals. Below are a few initiatives that advance our efforts to secure and manage our borders.

Increases in Border Infrastructure and Technology: Executive Order (EO) 13767, *Border Security and Immigration Enforcement Improvements*, requires significant enhancement of border infrastructure and technology. Out year planning has begun to include border barrier system extensions and enhancements and additional assets to include: Integrated Fixed Towers to provide automated, persistent wide area surveillance for the detection, tracking, identification, and classification of illegal entries; Remote Video Surveillance Systems to monitor large spans of the international border; and Cross-Border Tunnel Threat technology to diminish the ability of transnational criminal organizations to gain unobtrusive access into the United States through cross-border tunnels and the illicit use of underground municipal infrastructure.

[3] Final results for this measure will published in the FY 2017-2019 Annual Performance Report in early February 2018 at https://www.dhs.gov/performance-financial-reports.

Border Patrol Staffing: EO 13767 also addresses increasing staff on the border by requiring that DHS hire an additional 5,000 Border Patrol Agents. In response to this directive, CBP's Human Resource Management (HRM) office has developed a multi-year hiring plan to meet the new staffing requirement for Border Patrol. Of the 5,000 planned agent increase, the first surge is planned for 500 agents in FY 2018 and is in addition to the normal attrition hiring conducted by CBP HRM. This initial hiring surge will lay the foundation in increasing operational control in certain key areas along the border. The goal is to increase and maintain a Border Patrol Agent workforce to attain full operational control of the border. This will be an ongoing challenge to find qualified candidates who can pass the protocols to become a Border Patrol Agent, including a polygraph exam, along with ensuring that those who are hired remain in the Border Patrol and do not move to another law enforcement position within the Federal Government or to the private sector.

Biometric Entry Exit: EO 13769, *Protecting the Nation from Foreign Terrorist Entry* into the United States, addresses challenges in screening and vetting protocols and associated technology and procedures with the visa-issuance and management process. One of the efforts to support this Executive Order is the Biometric Entry-Exit System. The Department will utilize the cloud-based Traveler Verification Service system and supporting information technology infrastructure to analyze and verify travelers' identity using biometric data such as facial and fingerprint recognition. This will allow CBP Officers to assist airline partners and other government agencies to verify the identity of travelers entering and exiting the United States. The Department intends to adapt these innovative air environment technological solutions for land and sea environments.

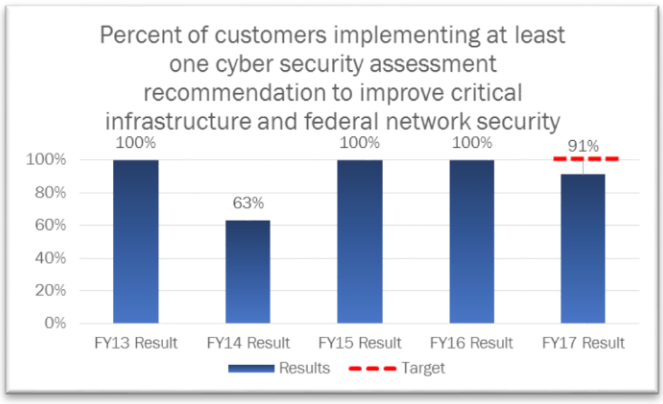
Mission 4: Safeguard and Secure Cyberspace

Our economic vitality and national security depend on a vast array of interdependent and critical cybernetworks, systems, services, and resources. By statute and Presidential Directive: DHS is the lead for the Federal Government to secure civilian government computer systems; works with industry to defend privately owned and operated critical infrastructure; prevents, detects, and investigates cybercrime; and works with state, local, tribal, and territorial governments to secure their information systems.

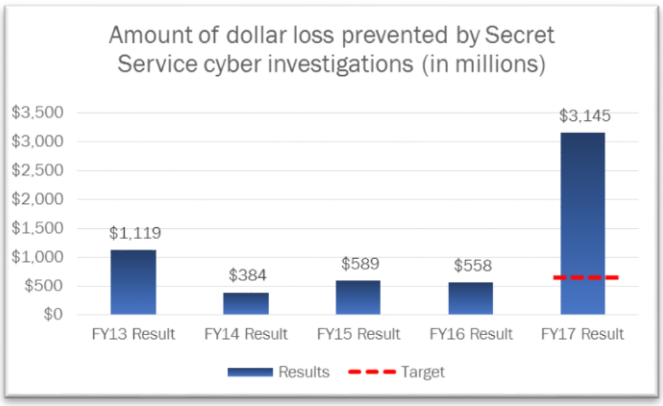
Our goals for this area are:

- Goal 4.1: Strengthen the Security and Resilience of Critical Infrastructure against Cyber Attacks and other Hazards;
- Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise;
- Goal 4.3: Advance Cyber Law Enforcement, Incident Response, and Reporting Capabilities; and
- Goal 4.4: Strengthen the Cyber Ecosystem.

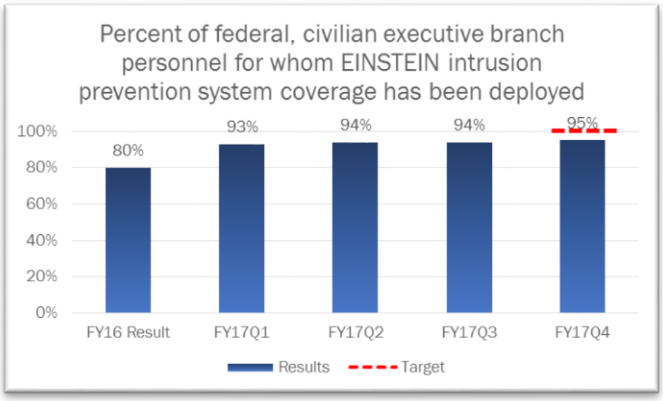
The following highlighted measures gauge our efforts to safeguard and secure cyberspace.



Percent of customers implementing at least one cyber security assessment recommendation to improve critical infrastructure and federal network security (NPPD): This measure demonstrates the percent of assessed asset owners and operators of critical infrastructure that are not only developing a better understanding of their cybersecurity posture, but are also taking action to improve that posture. In FY 2017, 91 percent of organizations who received an assessment also implemented at least one cybersecurity enhancement, down from the last two years. Making enhancements is at the discretion of the customer and may not be implemented for a number of reasons to include funding, internal policies and priorities, organizational maturity, and internal expertise. Note that a small number of organizations are known to have implemented security recommendations during the actual assessment process but these efforts were not necessarily reflected in their survey response. Going forward, the program will review its methodology for this measure to ensure the data collection efforts are targeted to the customers who were involved in the assessment and improvement process.



Amount of dollar loss prevented by Secret Service cyber investigations (in millions) (USSS): The USSS maintains Electronic Crimes Task Forces that focus on identifying and locating domestic and transnational cybercriminals connected to cyber-intrusions, bank fraud, data breaches, and other computer-related crimes. This measure reflects USSS' efforts to reduce financial losses to the public from cybercrimes. In the second quarter of FY 2017, the Secret Service closed an investigation into a network intrusion impacting a major U.S. retailer. This case involved over 4.5 million devices and substantial potential fraud losses totaling well in excess of the annual performance target. The year-to-year results for this performance measure are highly volatile based upon the cases closed in a particular reporting period.



Percent of federal, civilian executive branch personnel for whom EINSTEIN intrusion prevention system coverage has been deployed (NPPD): This measure gauges the intrusion prevention coverage provided by EINSTEIN 3 Accelerated (E3A) that is currently operating on civilian executive branch networks. E3A has the capacity to both identify and block known malicious traffic. This performance measure assesses the extent to which DHS has deployed

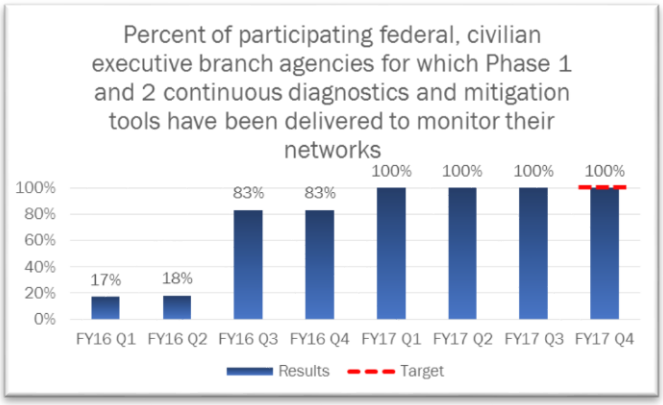
at least one E3A countermeasure to protect federal, civilian executive branch agencies. The FY 2017 result reflects an increase of approximately 525,000 federal civilian personnel protected by E3A intrusion prevention services from the FY 2016 end of year result. As of September 30, 2017, 95 percent of the federal, civilian executive branch personnel and 100 percent of Chief Financial Officer (CFO) Act agency personnel are protected by at least one E3A countermeasure. DHS continues to work with relevant internet service providers, and federal entities to deploy E3A at remaining Small/Micro agencies; however, these agencies have fewer Information Technology (IT) staff, and E3A competes with resources dedicated to day-to-day operations, and other cybersecurity initiatives and requirements.

Malware Impacts to the Nation's Supply Chain

In collaboration with the National Center for Manufacturing Sciences, DHS's NPPD, National Cyber Exercise and Planning Program (NCEPP) designed an exercise to test cyber-elements of the manufacturing sector. The June 27, 2017 exercise was held in Ann Arbor, MI with 20 stakeholder groups. It explored cyber-incident response to their discovery of critical systems infected with malware designed to affect radio frequency identification (RFID) components (e.g., readers, scanners, and tags) that impact the supply chain. During this full-day tabletop exercise, NCEPP facilitators guided exercise participants through three separate scenarios to address the issues. This is important because the complexities associated with RFID tagging systems include an increased potential for the exploitation of vulnerabilities. Participants discovered through this exercise that an abundance of external resources were available to help them about which they were not aware. The exercise also demonstrated that cyber-incident response capabilities varied widely among participating organizations. Surprisingly, larger organizations were more likely to maintain open lines of communications and/or share cyber-threat information than smaller entities. Cyber-exercises of this type aid in addressing the DHS Strategic Goals of strengthening the security and resilience of critical infrastructure against cyber-attacks, and reducing risk to the Nation's most critical infrastructure.

Priority Goal: Improve federal network security by providing federal civilian executive branch agencies with the tools and information needed to diagnose, mitigate, and respond to cybersecurity threats and vulnerabilities. By September 30, 2017, DHS will deliver two phases of continuous diagnostics and mitigation tools to 100 percent of the participating federal civilian executive branch agencies so that they can monitor their networks.

Performance Analysis: The Continuous Diagnostics and Mitigation (CDM) program provides federal agencies with capabilities to identify cybersecurity risks, prioritize those risks, and enable mitigation of the most significant problems first. Thus it is imperative that contracts to implement CDM on the federal network are awarded in a timely manner. As of the end of the first quarter of FY 2017, the program attained its target of 100 percent with 69 agencies participating in Phase 1 (asset management) and 65 agencies participating in Phase 2 (user management) tools. The final award for Phase 2 tools was completed the first quarter of FY 2017 and 100 percent of Phase 1 and Phase 2 have been delivered for installation to participating federal, civilian executive branch agencies. It should be noted that not every non-Defense federal organization is currently participating in



the CDM program and this measure only reflects those agencies that have chosen to participate in the program.

Looking Forward

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyberthreat hazards. Sophisticated cyber-actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes are now being perpetrated through cyberspace, including banking and financial fraud, intellectual property violations, and other crimes, all of which have substantial human and economic consequences. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide-scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend. In light of the risk and potential consequences of cyber-events, strengthening the security and resilience of cyberspace has become an important homeland security mission.

Continuous Diagnostics and Mitigation: The Continuous Diagnostics and Mitigation (CDM) program provides tools, sensors, and dashboards to the 23 Chief Financial Officer (CFO) Act agencies and is in the process of deploying a shared services CDM offering to provide the same capabilities to non-CFO Act agencies. As part of the CDM Program, two dashboards were developed—first the Agency Dashboard and then the Federal Dashboard. Agency Dashboards push agency-specific summary data from federal civilian agencies to the Federal Dashboard user interface. The Federal Dashboard provides the Office of Cybersecurity and Communications (CS&C) with a federal enterprise view of cybersecurity risk. It provides access to security information that will be used in a variety of ways, with new features and methods still under development. DHS is delivering the program in phases with the first two phases in the implementation and deployment stage. A number of agencies have successfully deployed the first phase of the program and have begun to utilize the prioritized vulnerability information provided to address key security weaknesses on their networks. It is anticipated that the deployment of the second phase tools and the contract delivery of the third phase will occur in FY 2018. DHS is planning on measuring the effectiveness of the CDM program through the timely patching of identified critical vulnerabilities on the federal network beginning in 2018. Many challenges are faced in this endeavor, including federal agencies prioritizing the deployment and use of these tools, and having seasoned Chief Information Officer leadership and staff to implement and leverage these tools to enhance federal network security. Also, it should be noted that CDM is not currently a statutorily required program, thus there are agencies who have chosen not to participate. DHS is working to demonstrate the benefits of the program to those non-participatory agencies in order to make the program as robust as possible.

Automated Indicator Sharing: In 2017, DHS made great strides in fulfilling a legislative requirement to share cyberthreat information with both public and private sector partners in near real time, but challenges remain. Being able to distinguish between real threats and those that do not pose harm to information systems is an ongoing challenge for agencies want to focus their response and corrective actions on only those threats that pose real harm. The Automated Indicator Sharing (AIS) program rapidly expanded both the volume of cyberthreat indicators shared and the number of public and private stakeholders participating in the

program FY 2017. The number of indicators shared through AIS increased from 100,394 in FY 2016 to over 1.2 million in FY 2017. Federal partners participation also grew from 7 agencies in FY 2016 to 25 in FY 2017 with all 23 non-defense CFO Act agencies and two additional agencies participating. Within DHS, all of the department's internal security operations centers were able to connect to AIS through the introduction of a web based platform to share indicators within the agency in real time to protect against known threats. Participation in the program was also extended to state governments, critical infrastructure sectors, and trusted allied nations. The number of non-federal participants increased dramatically from 45 in FY 2016 to 90 in FY 2017. The intent is to continue to grow the quantity of information shared by both DHS and participating entities and further expand the number of partners both domestically and internationally.

National Cybersecurity Protection System: The National Cybersecurity Protection System is an integrated system that delivers a range of capabilities to include intrusion detection and prevention, analytics, and information sharing of malicious activity on federal networks. The system currently detects and blocks threats that are already known by DHS from harming the federal network. While preventing known threats is important, the system currently lacks the capability to identify and block previously unknown threats from entering federal networks. To increase the effectiveness of the system, DHS is currently piloting a program to develop the capability to detect previously unknown malicious activity on a network. This capability would establish a baseline for normal network behavior and traffic and alert DHS to any deviations or abnormalities from that baseline. This pilot program has the potential to enable DHS to discover malicious activity and actors that were previously unknown to the information security community and share it with public and private partners in near real time. The impact would be improved situational awareness of cyberthreats and the ability to block our adversaries most sophisticated attack methods. Challenges with this approach are being able to accurately predict the nature of new threats and the impact they may cause. In addition, there is the challenge to respond in an appropriate fashion without directing limited staff resources unnecessarily to threats that would not have been impactful.

Strengthen National Preparedness and Resilience

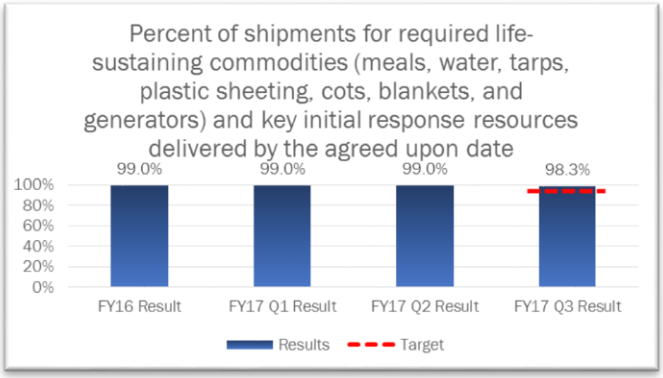
Mission 5: Strengthen National Preparedness and Resilience

Despite ongoing vigilance and efforts to protect this country and its citizens, major accidents and disasters, as well as attacks, may occur. The challenge is to build the capacity of American communities to be resilient in the face of disasters and other threats. Our vision of a resilient Nation is one with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.

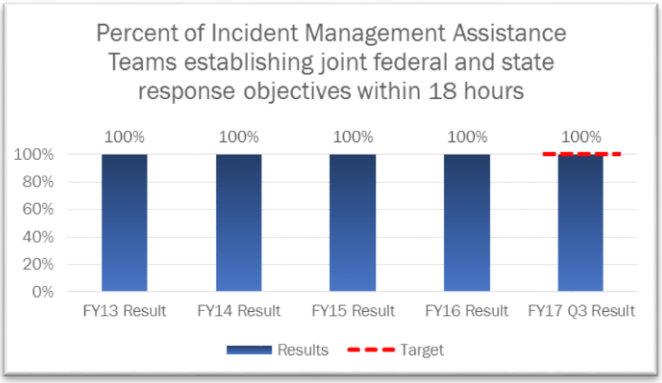
Our goals for this mission are:

- Goal 5.1: Enhance National Preparedness;
- Goal 5.2: Mitigate Hazards and Vulnerabilities;
- Goal 5.3: Ensure Effective Emergency Response; and
- Goal 5.4: Enable Rapid Recovery.

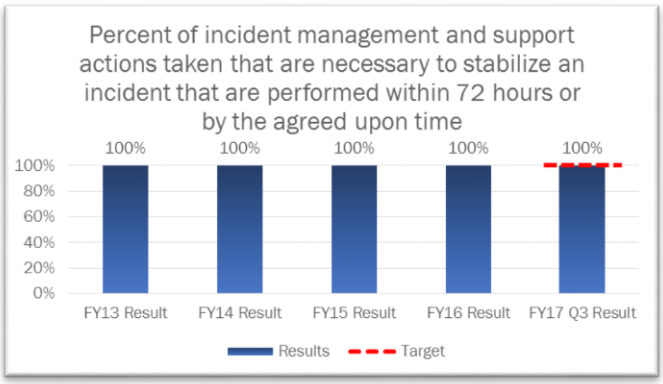
The following highlighted measures gauge our efforts to strengthen national preparedness and resilience. Due to Hurricanes Harvey, Irma, and Maria, FEMA is unable to provide year-end results in time for this report. As such, their 3rd quarter results are provided for context and their final results will be available in the FY 2017-2019 Annual Performance report in early February 2018 at https://www.dhs.gov/performance-financial-reports.



Percent of shipments for required life-sustaining commodities (meals, water, tarps, plastic sheeting, cots, blankets, and generators) and key initial response resources delivered by the agreed upon date (FEMA): This measure evaluates the percent of shipments from FEMA distribution centers or logistics partners that arrive at the specified location by the validated and agreed upon delivery date. Timely delivery of many of these commodities are truly life-saving as well as life-sustaining. For the past two years, FEMA's distribution centers and logistics partners have met expectations.

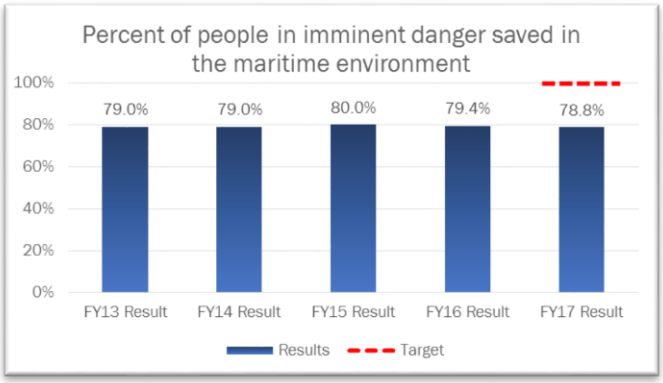


Percent of Incident Management Assistance Teams establishing joint federal and state response objectives within 18 hours (FEMA): This measure gauges the percent of time that Incident Management Assistance Teams (IMATs) have deployed and have established initial joint federal and state response objectives within 18 hours of a request from a state or jurisdiction. IMATs are made up of dedicated and experienced senior-level emergency management professionals that are able to deploy upon a moment's notice when requested by the state. IMATs generally consist of 10 members, with expertise in operations, logistics, planning, and recovery. They are a rapidly deployable asset to anywhere in the region or the country, supporting our states and territories in their emergency response efforts. For the past five years, when called upon, IMATs have establishing joint federal and state response objectives within 18 hours, 100 percent of the time.



Percent of incident management and support actions taken that are necessary to stabilize an incident that are performed within 72 hours or by the agreed upon time (FEMA): This measure reflects FEMA's role in effectively responding to any threat or hazard, with an emphasis on saving and sustaining lives within 72 hours, or by the agreed upon time, in support of state, local, tribal and territorial governments. "Actions necessary to

stabilize an incident" are defined as those functions that must be initiated immediately following an incident in order to ensure the best outcomes for survivors. These actions include establishing joint federal/state incident objectives and interoperable communications between FEMA-supported incident sites, deploying urban search and rescue resources, rapidly activating response coordination centers, and issuing timely alerts, warnings, operations orders, and situation reports. For the past five years, incident management and support actions have been performed within 72 hours, or by the agreed upon time, 100 percent of the time.



Percent of people in imminent danger saved in the maritime environment (USCG): This is a measure of the percent of people who were in imminent danger on the oceans and other waterways and whose lives were saved by USCG search and rescue teams. The number of lives lost before and after the USCG is notified and the number of persons missing at the end of search operations are factored into this percentage. Several factors hinder successful response including untimely distress notification to the USCG, incorrect distress site location reporting, severe weather conditions at the distress site, and distance to the scene. The USCG saved more than 4,200 lives in FY 2017, which was 78.8 percent of those in danger, and is consistent with long-term results and trends. The target for this measure will likely be adjusted in FY 2018 to be ambitious but more in-line with historical results. The USCG will continue to plan, train, develop better technologies, and invest in capable assets to continue their exemplary performance in saving lives in the maritime environment.

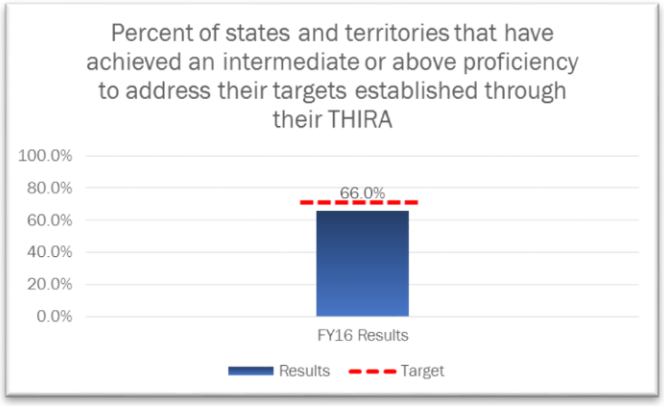
Surge Capacity Force

In the aftermath of a catastrophic event, DHS turns to its Surge Capacity Force, a cadre of federal employee heroes who help affected communities by supporting the Federal Emergency Management Agency's (FEMA) urgent response and recovery efforts. The Surge Capacity Force is made up of federal employees from every Department or Agency in the Federal Government.

The Post-Katrina Emergency Management Reform Act of 2006 (Public Law 109-295) established the Surge Capacity Force to deploy federal employees in the aftermath of a catastrophic event to help support response and recovery efforts. DHS activated the Surge Capacity Force for the first time in 2012 in support of Hurricane Sandy. More than 1,100 (non-FEMA) federal employees deployed to New York and New Jersey to supplement FEMA's substantial disaster workforce.

In the immediate aftermath of Hurricanes Harvey, Irma, and Maria, Acting Secretary of Homeland Security Elaine Duke activated the Surge Capacity Force—the second time in the Surge Capacity Force existence. Surge Capacity Force volunteers from throughout the Federal Government supported disaster survivors in Texas, Florida, Puerto Rico, and the U.S. Virgin Islands. As of September 21, 2107, more than 2,000 federal employees were deployed for these relief efforts.

Priority Goal: Enhance the Nation's ability to respond to and recover from a catastrophic disaster through whole community preparedness and partnership. By September 30, 2017, 70 percent of states and territories will achieve an intermediate or above proficiency toward meeting the targets established through their Threat and Hazard Identification and Risk Assessment (THIRA).



Performance Analysis: This measure assesses the percent of state and territorial State Preparedness Report (SPR) ratings at or above the 3.0 threshold when averaging across the planning, organization, equipment, training, and exercise elements rated by grantees for each core capability. While the target was narrowly missed in FY 2016, all indications are that the FY 2017 target will be met; however, due to Hurricanes Harvey, Irma, and Maria, FEMA is unable to provide year-end results in time for this report. The results will be available in the FY 2017-2019 Annual Performance report in early February 2018 at https://www.dhs.gov/performance-financial-reports.

Looking Forward

The Department coordinates comprehensive federal efforts to prepare for, protect against, respond to, recover from, and mitigate a terrorist attack, natural disaster or other large-scale emergency, while working with individuals, communities, the private and nonprofit sectors, faith-based organizations, and federal, state, local, tribal, and territorial partners to ensure a swift and effective recovery effort. Hurricanes Harvey, Irma, and Maria remind us all of the importance of preparedness and resilience in the face of disaster. Below are a few initiatives that advance our efforts to achieve our preparedness and resilience goals.

National Flood Insurance Program: The Department administers the National Flood Insurance Program (NFIP) to reduce the impact of flooding on private and public structures. The NFIP takes a multi-faceted approach that includes providing affordable insurance to property owners while also encouraging communities to adopt floodplain management regulations and invest in mitigation efforts; however, challenges exist in maintaining the viability of this program. To address the financial stability of the NFIP, DHS plans to support long term reauthorization of the NFIP by promoting transparency around the NFIP's revenue, expenses, risk exposure, and available risk management tools as NFIP reauthorization-related discussions progress with DHS, the Administration, and Congress. FEMA is leveraging existing investments in analytic capacity and engagements with the reinsurance industry to better understand the NFIP's risk profile and appropriate risk management strategies.

Disaster Workforce Structure: In order to be prepared for all hazards, the Department has made numerous advancements in the past decade to the disaster response workforce. The establishment of the Surge Capacity Force allows the capacity for the Department to deploy its employees in support of FEMA's existing workforce for a large-scale disasters as seen this year with Hurricanes Harvey, Irma, and Maria. The Department continues to innovate and learn from other agencies, such as developing a centralized reception, staging, onward movement, and integration process and collaborating with the Corporation for National and Community Service. FEMA has made progress, but is still far from its desired workforce structure. Moving forward, FEMA is conducting research to understand the barriers that prevent it from reaching its disaster workforce structure. Additionally, it is continuing to learn from other agencies and

will take lessons learned from Hurricanes Harvey, Irma, and Maria to address this critical need in times of crisis.

Enforce and Administer Our Immigration Laws

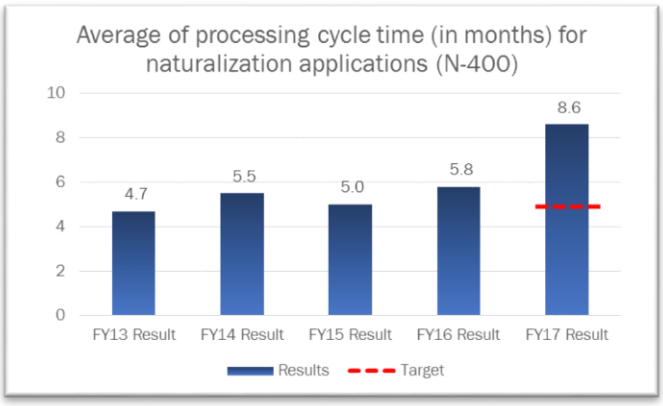
Mission 3: Enforce and Administer Our Immigration Laws

A fair and effective immigration system enriches American society, unifies families, and promotes our security. Our Nation's immigration policy plays a critical role in advancing homeland security.

Our goals for this mission are:

- Goal 3.1: Strengthen and Effectively Administer the Immigration System; and
- Goal 3.2: Prevent Unlawful Immigration.

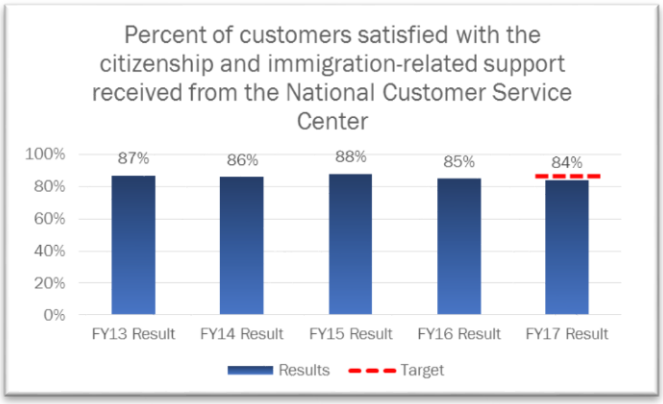
The following highlighted measures gauge our efforts to enforce and administer our immigration laws.



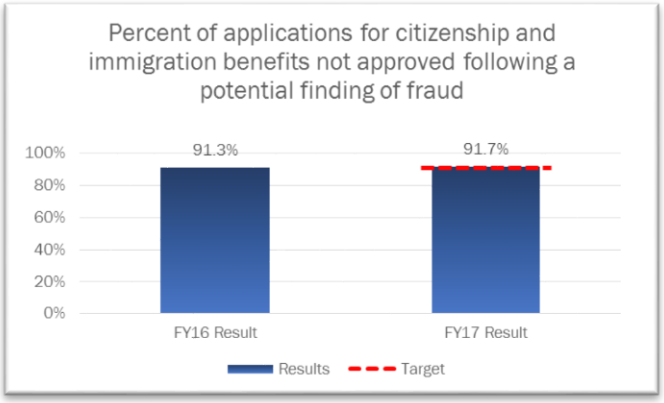
Average of processing cycle time (in months) for naturalization applications (N-400) (USCIS): This measure assesses the program's ability to meet its published processing time goals for N-400, Application for Naturalization which is filed by lawful permanent residents to attain U.S. citizenship. Naturalization applications were 26 percent higher than projected in FY 2016 and are again higher than planned in FY 2017 by 14 percent. USCIS is continuing to shift resources and prioritize workload in order to handle its case volume. Although the cycle time is above the target, USCIS has maintained the accuracy of N-400 decisions as validated through random sampling. USCIS continues to face capacity challenges which, combined with higher workload demands, will continue to negatively impact our cycle time. During FY 2018, USCIS will continue to balance workload to ensure national cycle time parity across each of its 88 field offices and leverage overtime and other scheduling options.

Percent of customers satisfied with the citizenship and immigration-related support received from the National Customer Service Center (USCIS): This measure gauges the overall rating of the immigration process and is based on the results from the following areas:

1) accuracy of information;
2) responsiveness to customer inquiries;
3) accessibility to information; and
4) customer satisfaction.



The FY 2017 result for this measure is consistent with the results for the past four years; however, there has been a slight decline the past two years which is most likely due to the fluidity in the immigration policy environment making it more difficult to satisfy customers' questions in some instances. Results are still indicative of the attention USCIS has given to the customer service approach, especially given the increased demand. USCIS is constantly listening to customer feedback and taking deliberate steps to improve the level of service provided to its customers. USCIS' customer service rating is well above the Federal Government Citizen Experience Benchmark of 78 percent as reported by American Customer Satisfaction Index in their latest report published on January 31, 2017.



Percent of applications for citizenship and immigration benefits not approved following a potential finding of fraud (USCIS): This measure reflects the Department's capacity to prevent fraud, abuse, and exploitation of the immigration system, and helps identify systemic vulnerabilities that threaten its integrity. By not approving benefits to individuals potentially attempting to commit fraud, and who were not eligible for a waiver or exemption, USCIS is actively eliminating vulnerabilities, and identifying ways to continue to deter and prevent fraud in the future. Slightly up from FY 2016 results, the initial findings of fraud were upheld 91.7 percent of the time. Initial findings of fraud are reviewed by USCIS' Fraud Detection and National Security Directorate (FDNS) before final adjudication is rendered. FDNS was created in 2004 in order to strengthen USCIS' efforts to ensure immigration benefits are not granted to individuals who pose a threat to national security or public safety, or who seek to defraud our immigration system. USCIS continues to improve communication between fraud officers and adjudicators with the assistance of improved reporting tools and investments in new technologies.

USCIS Naturalizes 15,000 New Citizens during Independence Day

On the 241st anniversary of the Declaration of Independence and the birth of the United States, 15,000 lawful permanent residents were naturalized as U.S. citizens during more than 65 naturalization ceremonies across the country. The number of new citizens naturalized on July 4, 2017 was the most in recent years. Local, state, and federal officials attended ceremonies that were held at public libraries, national parks, and museums. Teresa Nieves-Chinchilla was one of 22 people from 16 countries who were naturalized at the July Fourth naturalization ceremony in Annapolis, Maryland. Shortly before the ceremony, she had returned from a trip to her home country of Spain and in her mailbox was a long-awaited letter granting her dream—she could finally become an American citizen. Nieves-Chinchilla had been living in the U.S. for 11 years, studying space weather and solar activity at the Catholic University of America's Institute for Astrophysics and Computational Sciences, located at NASA's Goddard Space Flight Center in Greenbelt, Maryland. "This country gave me the opportunity to be a scientist, to make my life" she said.

USCIS is committed to promoting instruction and training on citizenship rights and responsibilities by offering a variety of free citizenship preparation resources for applicants, educators, and organizations that can be found online at the Citizenship Resource Center (www.uscis.gov/citizenship). Immigrant-serving organizations can register at www.uscis.gov/citizenship/organizations/civics-and-citizenship-toolkit to receive a free Civics and Citizenship Toolkit to help them develop content for classes and train staff and volunteers.

Looking Forward

The success of our Nation's immigration policy plays a critical role in advancing homeland security. The Department is focused on smart and effective enforcement of U.S. immigration laws while streamlining and facilitating the legal immigration process. Effective administration of the immigration system depends on ensuring that immigration decisions are impartial, lawful, and sound; that the immigration system is interactive and user friendly; that policy and procedural gaps are systematically identified and corrected; and that those vulnerabilities which would allow persons to exploit the system are eliminated. Below are a few initiatives that advance our efforts to achieve the Department's immigration enforcement and administration goals.

USCIS' Improvement Plans: USCIS secures America's promise as a Nation of immigrants by granting citizenship and immigration benefits, promoting awareness and understanding of citizenship, ensuring the integrity of the immigration system, and providing accurate and useful information to its customers. Over the past few years, the number of applications for benefits and benefit changes has ballooned to more than 8 million transactions per year creating a challenge to process applications in a timely fashion. The sheer volume of work has led USCIS to leverage a suite of technology tools that give customers faster and easier access to immigration information. The flagship of the newest suite of tools is *my*USCIS, an online one-stop shop for immigration information. The success of *my*USCIS will be leveraged to expanded service to continue to provide value, relevance, and reach for customers and stakeholders.

Enhancing Public Safety in the Interior of the United States: EO 13768, *Enhancing Public Safety in the Interior of the United States*, aims to effectively address those individuals who illegally enter the United States and those who overstay or otherwise violate the terms of their visas. Historically, surges of illegal immigration at the southern border with Mexico has placed a significant strain on federal resources and overwhelmed those agencies charged with border security and immigration enforcement. One of the provisions of the EO addresses this need by hiring 10,000 Immigration and Customs Enforcement Law Enforcement Officers (LEOs) and related support staff. The FY 2018 budget includes plans for the first 1,000 LEOs, and plans are in place to onboard the remaining staff over a multi-year horizon.

Mature and Strengthen Homeland Security

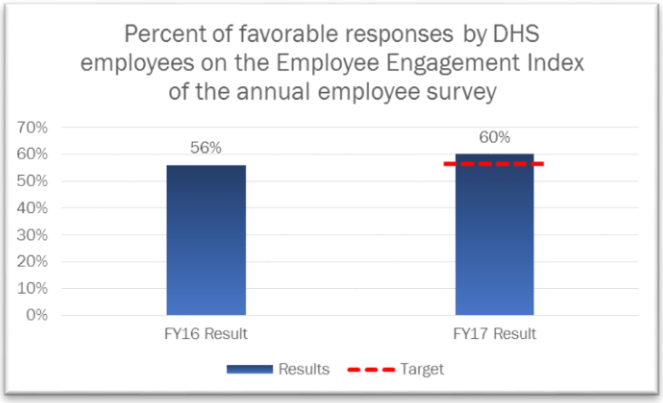
The objectives for maturing and strengthening the Department were designed to bolster key activities and functions that support the success of our strategic missions and goals. Ensuring a shared awareness and understanding of risks and threats, building partnerships, strengthening our international enterprise structure, enhancing the use of science and technology, with a strong service and management team underpin our broad efforts to ensure our front-line operators have the resources they need to fulfill the missions of the Department.

Our mature and strengthen goals are:

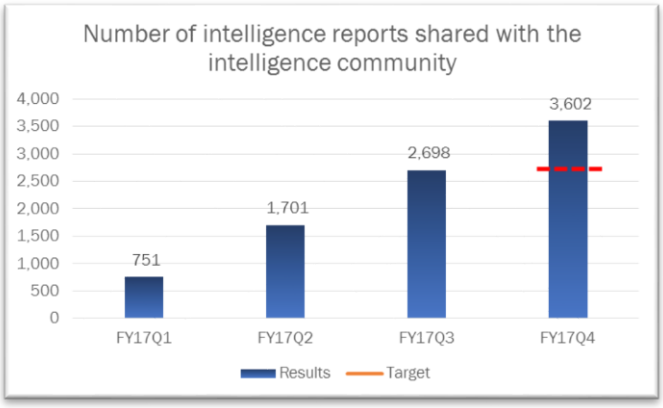
- Integrate Intelligence, Information Sharing, and Operations;
- Enhance Partnerships and Outreach;
- Strengthen the DHS International Affairs Enterprise in Support of Homeland Security Missions;

- Conduct Homeland Security Research and Development;
- Ensure Readiness of Frontline Operators and First Responders; and
- Strengthen Service Delivery and Manage DHS Resources.

Performance measures associated with the Department's Mature and Strengthen Homeland Security focus support evaluation of the operational aspects of the headquarters offices. A small number of measures aligned to this area are displayed below, and the full set can be found in the DHS Congressional Justification Overview Chapter for the Office of the Under Secretary for Management at https://www.dhs.gov/dhs-budget.

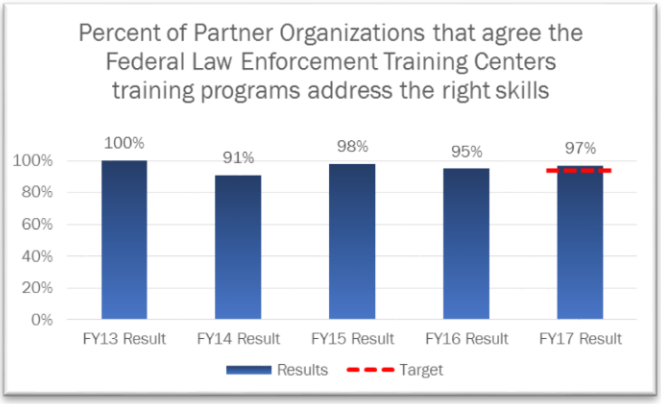


Percent of favorable responses by DHS employees on the Employee Engagement Index of the annual employee survey: This measure is based on positive response rates by DHS employees to the Employee Engagement Index (EEI) of the annual Federal Employee Viewpoint Survey (FEVS) administered by the Office of Personnel Management. The EEI is comprised of three sub-indices—Leaders Lead, Supervisors, and Intrinsic Work Experiences. Based upon the 2017 FEVS data, DHS's EEI climbed to 60 percent, a four point improvement over last year's results. This increase in EEI is the largest of any Cabinet-level agency in FY 2017. Further, DHS had the largest increase in its Global Satisfaction Index (GSI), gaining six percentage points from last year's 49 percent rating. Both USCIS and USCG have EEI scores above any of the Cabinet-level agencies, at 74 percent. Acting Secretary, Elaine Duke stated, "This progress has been no easy feat, and I am happy to see that these results reflect the tireless efforts taken throughout the Department to promote a culture of collaboration and engagement. As a Department, we have taken tremendous strides in recent years, continuously working to ensure that all employees at DHS feel supported, empowered, and equipped to successfully execute the duties and responsibilities necessary in maintaining the safety and security of the Nation."



Number of intelligence reports shared with the intelligence community: This measure reflects the DHS contribution of raw, unevaluated intelligence, to the intelligence community and the Federal Government so as to share the unique information obtained from intelligence officers in the field. In FY 2017, I&A disseminated 3,602 raw intelligence information reports, exceeding its FY 2017 goal by 34 percent. During the fiscal year, I&A was able to inform intelligence analysis, watchlisting and policy by sharing raw intelligence from a variety of DHS sources. Several key factors enabled I&A to succeed including streamlining our reporting processes and automating research techniques. These changes enhanced I&A's

ability to support our customer's needs and reduce the time it takes to identify information that has value for intelligence purposes.



Percent of Partner Organizations that agree the Federal Law Enforcement Training Centers training programs address the right skills (e.g., critical knowledge, key skills and techniques, attitudes/behaviors) needed for their officers/agents to perform their law enforcement duties (FLETC): The results of this measure provide on-going opportunities for improvements that are incorporated into FLETC's training curricula, processes, and procedures. FLETC perennially performs very well on this measure—greater than 90 percent for the past five years—as they have a very singularly focused mission to provide career-long training to law enforcement professionals to help them fulfill their responsibilities safely and proficiently. Over the past 46 years, FLETC has grown into the Nation's largest provider of law enforcement training.

Innovative Veterans Hiring Event

The recent Executive order signed on January 25, 2017 mandates the enhancement of public safety in the interior of the United States. The Secretary has the responsibility of ensuring 10,000 additional immigration officers are hired to secure the United States borders, and enforce immigration laws. In an effort to assist with achieving this goal, and increase veteran hiring numbers, the Office of the Chief Human Capital Officer worked jointly with representatives from every DHS Component to sponsor a two-day "Continue Your Service to America" veteran recruitment and hiring event. Veterans currently make up 27.9 percent of the Department's workforce. Prior to the event, the Office of the Chief Human Capital Officer, U.S. Citizenship and Immigration Services, Customs and Border Protection, U.S. Immigration and Customs Enforcement, delivered a series of veteran hiring event webinar learning sessions for veterans across the United States. The webinars assisted veterans with uploading their resumes to USAJOBS and making them searchable by federal agencies. More than 5,000 veterans participated in the webinars.

The hiring event held August 22-23, 2017 was attended by 2,570 veterans representing each branch of the military. As a result of the partnership between DHS Components for the event, over 600 veterans were interviewed, an estimated 125 tentative job offers were made, and approximately 375 candidates were moved to the next phase of the law enforcement hiring process. An innovative approach of interviewing, providing temporary job postings, and initiating the security process at the hiring event will reduce the time to hire these candidates. The hiring process generally takes four to six months to onboard an employee. Through the innovation of webinar learning sessions and an abbreviated temporary job posting and security process, DHS is able to acquire highly trained, and highly-talented veterans in an expedited manner to continue their service to America by supporting the DHS mission.

Looking Forward

Maturing and strengthening the Department and the entire homeland security enterprise—the collective efforts and shared responsibilities of federal, state, local, tribal and territorial, nongovernmental and private-sector partners, as well as individuals, families, and communities—is critical to the Department's success in carrying out its core missions and operational objectives.

Formalizing the Requirements Process: DHS's maturation and challenge includes improving numerous business practices necessary for supporting front line operations that must combat evolving threats and ensuring efficient operations. An important advancement for the Department along this journey is formalizing the requirements process. Gains in this effort come from the Department wide Joint Requirements Council (JRC) and the Radiological/Nuclear Requirements Oversight Council (RNROC). The JRC provides oversight of the DHS requirements generation process by validating capability gaps, needs, and requirements based on capability analysis. The RNROC charter is to oversee the requirements process specific to radiological/nuclear detection and nuclear forensics, vetting Component requirements, and leading to the fielding of effective solutions prior to validation by the JRC. Both efforts are advancing requirements development in DHS and will ensure efficient and effective operations into the future.

Office of the Chief Human Capital Officer: DHS continues to implement a results-oriented annual planning process to support the strategic management of human capital resources. Several key department-wide initiatives will occur in the coming year to bring the human capital community together in a unity of effort. The Department will develop an enterprise approach for co-branding DHS and Components in all human capital outreach efforts including advertising, marketing, and social media. DHS will also develop a process to automate and streamline data collection to provide leadership with real-time information to evaluate the return on investment achieved related to hiring initiatives. Furthermore, the Department is creating career pathing with online resources, assessment tools, and skill-building opportunities for the 1800 job series occupations (Inspection, Investigation, Enforcement, and Compliance), Human Resources occupations (201 job series), and other select Management lines of business occupations. Lastly, DHS will leverage existing Component programs to develop a department-wide Resilience and Family Readiness Program to support families when front-line employees need to be deployed to other geographic locations.

Financial Stewardship: DHS is expending resources to raise the baseline of our security posture, necessitating the continued evolution of the business processes and systems supporting mission delivery. With the magnitude and scope of threats continuing to grow and change every day, DHS is further maturing our resource agility and efficiency. Enterprise risk management (ERM) is foundational to delivering on the DHS mission and objectives, and integrated into each phase of the planning to execution processes. A critical aspect of the Department's integrated ERM approach is the continued maturation of a robust internal control program, ensuring taxpayer funds are expended as efficiently and effectively as possible while preventing and detecting fraud, waste and abuse. Using a risk based approach and the U.S. Government Accountability Office (GAO) criteria for standards for internal control, DHS assessed its internal control maturity by Component and key deficiency category. This Internal Control Maturity Model baseline served as the Department's starting point to measure substantial progress in addressing weaknesses and sustaining a strong control environment. The Department's comprehensive enterprise approach to remediation are driving and sustaining continuous progress, as evidenced by the ability to downgrade the Property material weakness this fiscal year. DHS will continue demonstrating strong financial stewardship, executing the multi-year strategy to remediate our two remaining material weaknesses in Financial Reporting and Information Technology controls and achieve a clean Internal Control over Financial Reporting opinion.

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.

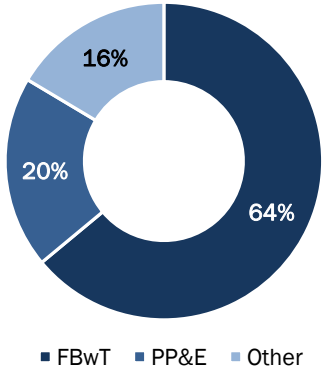
Financial Position ($ in millions)	FY 2017	FY 2016	$ Change	% Change
Fund Balance with Treasury	$ 71,466	$ 58,997	$ 12,469	21%▲
Property, Plant, and Equipment	21,887	21,220	667	3%▲
Other Assets	18,358	17,413	945	5%▲
Total Assets	**111,711**	**97,630**	**14,081**	14%▲
Federal Employee and Veterans' Benefits	58,715	58,028	687	1%▲
Debt	30,440	23,017	7,423	32%▲
Accounts Payable	4,278	3,868	410	11%▲
Deferred Revenue and Advances	5,799	3,795	2,004	53%▲
Insurance Liabilities	12,331	3,196	9,135	>100%▲
Accrued Payroll	2,276	2,114	162	8%▲
Other Liabilities	7,654	7,492	162	2%▲
Total Liabilities	**121,493**	**101,510**	**19,983**	20%▲
Total Net Position	(9,782)	(3,880)	(5,902)	<-100%▼
Total Liabilities and Net Position	**$ 111,711**	**$ 97,630**	**$ 14,081**	14%▲

Results of Operations ($ in millions)	FY 2017	FY 2016	$ Change	% Change
Gross Cost	$ 80,683	$ 69,404	$ 11,279	16%▲
Less: Revenue Earned	(13,786)	(14,499)	713	-5%▼
Net Cost Before Gains and Losses on Assumption Changes	66,897	54,905	11,992	22%▲
Gains and Losses on Assumption Changes	(494)	234	(728)	<-100%▼
Total Net Cost	**$ 66,403**	**$ 55,139**	**$ 11,264**	20%▲

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.

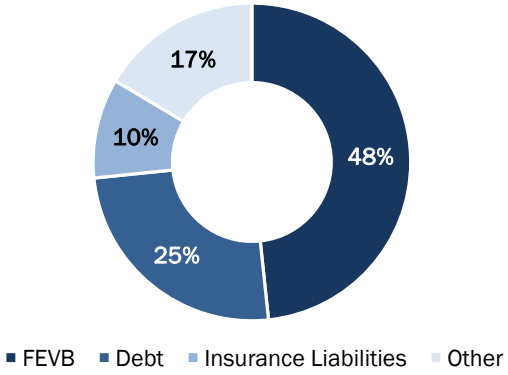
Other Assets includes items such as investments, accounts receivable, cash and other monetary assets, taxes, duties and trade receivables, direct loans, and inventory and related property.

As of September 30, 2017, the Department had $111.7 billion in assets, representing a $14.1 billion increase from FY 2016. The majority of this change is due to the increase in FEMA's FBwT to support disaster relief efforts for the significant hurricanes that struck the United States this past year.

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 NFIP and Disaster Assistance Direct Loan Program. Given the current premium rate structure, FEMA will not be able to pay its debt from the premium revenue alone;

therefore, legislation will need to be enacted to provide funding to repay the Treasury. 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, 2017, the Department reported approximately $121.5 billion in total liabilities. Total liabilities increased by approximately $20 billion in FY 2017. FEMA's disaster response costs and related increases in FEMA's debt to Treasury along with projected future flood claims drives most of this increase in liabilities.

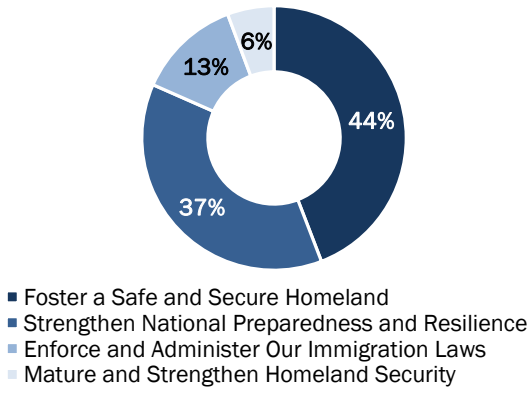
Net Position

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 $(9.8) billion because of significant expenses related to NFIP, as well as pension liabilities for USCG and USSS, which are funded for the current year only. Total net position decreased approximately $6 billion from FY 2016, in large part because of the cost associated with hurricane relief efforts.

Results of Operations

The Department operates under one unified mission: *With honor and integrity, we will safeguard the American people, our homeland, and our values*. The FY 2014-2018 Strategic Plan further details the Department's missions and focus area, which are grouped into four major missions in the Statement of Net Cost and related footnotes to allow the reader of the Statement of Net Cost to clearly see how resources are spent towards the common goal of a safe, secure, and resilient Nation.

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 increased by approximately $11 billion in FY 2017. DHS incurred a significantly larger gross cost this year to support response and recovery efforts related to the recent hurricanes.



During FY 2017, the Department earned approximately $13.8 billion in exchange revenue.

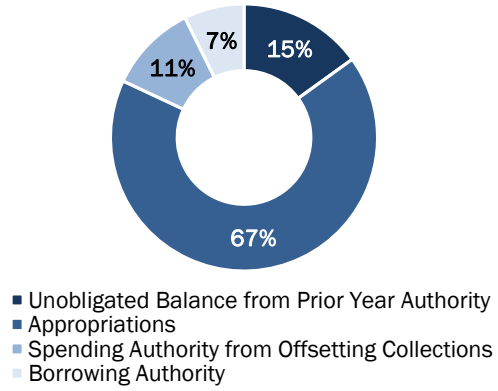
Exchange revenue arises from transactions in which the Department and the other party receive value and that are directly related to departmental operations. The Department also collects non-exchange duties, taxes, and fee revenue on behalf of the Federal Government. This non-exchange revenue is presented 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 2017	FY 2016	$ Change	% Change
Unobligated Balance from Prior Year Authority	$ 15,341	$ 18,113	$ (2,772)	-15%▼
Appropriations	68,224	58,644	9,580	16%▲
Spending Authority from Offsetting Collections	10,971	11,355	(384)	-3%▼
Borrowing Authority	7,427	1	7,426	>100%▲
Total Budgetary Authority	**$ 101,963**	**$ 88,113**	**$ 13,850**	16%▲

The Department's budgetary resources were approximately $102 billion for FY 2017. The authority was derived from $15.4 billion in authority carried forward from FY 2016, appropriations of $68.2 billion, $11 billion in collections, and $7.4 billion in borrowing authority. Budgetary resources increased approximately $14 billion from FY 2016. FEMA received a supplemental appropriation to respond to the significant disasters at the end of the fiscal year. Additionally, FEMA borrowed $7.4 billion in FY 2017 to pay insurance claims against the NFIP. Both of these served to increase the Department's budget authority significantly in FY 2017.



Of the total budget authority available, the Department incurred a total of $81.9 billion in obligations from salaries and benefits, purchase orders placed, contracts awarded, or similar transactions.

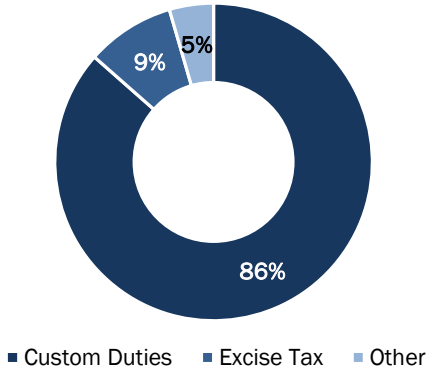
Custodial Activities

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 2017	FY 2016	$ Change	% Change
Cash Collections	$ 34,835	$ 35,142	$ (307)	-1%▼
Excise Tax	3,631	3,430	201	6%▲
Other	1,810	1,684	126	7%▲
Total Cash Collections	**$ 40,276**	**$ 40,256**	**$ 20**	0%▲

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.

Custom duties collected by CBP account for 86 percent of total cash collections. The remaining 14 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, and Debt Collection Improvement Act of 1996, see the Other Information section.

Secretary's Assurance Statement

November 14, 2017

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 financial 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, 2017 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, with the exception of the following two areas: 1) Financial Reporting and 2) Information Technology Controls and Systems Functionality, where 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 material weakness 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.

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,

Elaine C. Duke
Acting Secretary of Homeland Security

Management Assurances

DHS management is responsible for establishing, maintaining, and assessing internal control 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 Department of Homeland Security 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.

In FY 2014, GAO revised the Green Book effective beginning FY 2016 and for the Federal Managers' Financial Integrity Act reports covering that year. The Green Book provides managers the criteria for an effective internal control system, organized around internal control components, principles, and attributes. In FY 2016, the OMB revised Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. The revisions emphasize the integration of risk management and internal controls within existing business practices across an Agency. Updates to the Circular were effective in FY 2016, with the implementation of enterprise risk management requirements effective in FY 2017. Circular A-123, Appendix A, *Internal Control over Financial Reporting*, remains in effect.

Federal Managers' Financial Integrity Act, Section 2

Since Circular No. A-123 became effective 2006, DHS has worked extensively to establish, maintain, and assess internal controls. The Department has made considerable improvements in internal controls over operations, reporting, and compliance through the extensive work of staff and management at Headquarters and in the Components.

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. Management performs an analysis on the pervasiveness and materiality over any identified deficiencies to determine their impact. Based on the results of these assessments, the Secretary provides assurances over the Department's internal controls in the annual assurance statement. Any deficiency identified as a material weakness within internal control over financial reporting is defined as a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. To identify material weaknesses and non-compliance, management used the following criteria:

- Significant enough to report outside the Agency as a material weakness;
- Impacts the operating effectiveness of Entity-Level Controls;
- Impairs fulfillment of essential operations or mission;
- Deprives the public of needed services;
- Significantly weakens established safeguards against waste, loss, unauthorized use or misappropriation of funds, property, other assets, or conflicts of interest;
- Substantial non-compliance with laws and regulations; and

- Financial management systems conformance to government-wide systems requirements.

The Department instituted an Accountability Structure, which includes a Senior Management Council (SMC), the Risk Management and Assurance (RM&A) Division, and a Senior Assessment Team (SAT). The SMC approves the level of assurances for the Secretary's consideration and is comprised of the Department's Under Secretary for Management, Chief Financial Officer, Chief Readiness Support Officer, Chief Human Capital Officer, Chief Information Officer, Chief Information Security Officer, Chief Security Officer, and Chief Procurement Officer.

The RM&A Division seeks to integrate and coordinate internal control assessments with other internal control related activities and incorporates results from all of the Department's lines of business to address cross-cutting internal control issues. Finally, the SAT, led by the Chief Financial Officer and overseen by RM&A, is comprised of senior-level financial managers assigned to carry out and direct Component-level internal control over financial reporting assessments.

Component Senior Leadership provided assurance statements to the SAT that serve as the primary basis for the Secretary's assurance statements. These assurance statements are also based on information gathered from various sources including management-initiated internal control assessments, program reviews, and evaluations. In addition, these statements consider the results of reviews, audits, inspections, and investigations performed by the Department's Office of Inspector General (OIG) and GAO.

Department of Homeland Security Financial Accountability Act

Pursuant to the DHS FAA, the Department must obtain an opinion over internal control over financial reporting. Using GAO Standards for Internal Control and Circular A-123 as criteria, the Department has demonstrated continued progress in reducing its financial material weaknesses and maintaining progress over sustained processes through routine internal control testing. This robust find, fix, test and assert assessment strategy will support sustainment of the financial statement opinion and achievement of an opinion over internal control over financial reporting in the near future.

In FY 2017, the Department reduced the severity of property, plant and equipment to a significant deficiency due to hard work and demonstrated progress evidenced through the USCG and NPPD remediation and sustained efforts by the remaining components. This reduces the Department's number of material weaknesses from three to two, where 1) financial reporting and 2) IT Controls and System Functionality material weaknesses will remain. The Department remains dedicated to fully remediating financial reporting and IT system security and functionality weaknesses. A summary of corrective actions are provided in the tables below.

Table 1: Internal Control over Financial Reporting Corrective Actions

Material Weakness	Component	Year Identified	Target Correction Date
	USCG, NPPD, FEMA, USSS, and CBP	FY 2003	FY 2018
Financial Reporting	USCG, NPPD, FEMA, USSS, and CBP experienced challenges with deficiencies in multiple financial management areas. These issues may include a combination of budgetary accounting, trading partner reconciliations, journal entries, third party service monitoring, and lack of compensating controls to mitigate system limitations.		
Corrective Actions	The DHS CFO will continue to support Components in implementing corrective actions to establish effective financial reporting control activities based on component contribution to the weakness area and risk. One of the primary financial reporting condition is due to a lack of integrated financial systems at the USCG. The Department and USCG will continue to focus on implementing and executing interim manual compensating measures, while pursuing system enhancements. In addition, the Department will continue to prioritize remediation efforts based on risk and components will implement targeted corrective actions to resolve the overall Department financial reporting conditions.		
Material Weakness	**Component**	**Year Identified**	**Target Correction Date**
	All DHS Components	FY 2003	FY 2019
IT Controls and System Functionality	The Department internal control assessment identified IT Controls and System Functionality 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 FFMIA.		
Corrective Actions	The DHS CFO and CIO 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. Remediation efforts will occur across the Department with a risk-based approach to correcting root-cause weaknesses across all CFO designated systems.		

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, the material weakness 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 material weakness 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 2: FFMIA Non-compliance Corrective Actions

Non-Compliance	Component	Year Identified	Target Correction Date
	All DHS Components	FY 2003	FY 2019
FFMIA Non-compliance	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.		
Corrective Actions	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.		

Digital Accountability and Transparency Act of 2014

In addition to performing an analysis of the Department's compliance with FMFIA, FFMIA, DHS FAA, and applicable laws and regulations, management also considered its compliance with recently enacted laws. On May 9, 2014, the President signed the Digital Accountability and Transparency Act of 2014 (DATA Act) into law. By May of 2017 the law required the DHS to comply with the requirements outlined in the Act in accordance with guidance received from the Treasury and OMB. DHS will be required to report obligations by appropriation, program, object class, and award. This effort required enterprise-wide coordination and collaboration to modify business processes and systems to ensure full compliance. In FY 2016 the Department developed the initial technical solution and conducted two pilots successfully demonstrating the ability to link financial and award data. In August 2016, DHS submitted the DHS Implementation Plan Update to OMB as required. In April 2017, DHS successfully certified and submitted its first quarterly spending data for posting on USASpending.gov. In FY 2017, DHS continued to produce, test, and validate data improving the quality to ensure timely and accurate data reporting to meet and comply with the DATA Act requirements.

Federal Information Security Modernization Act of 2014 (FISMA)

FISMA provides a framework for ensuring effectiveness of security controls over information resources that support federal operations and assets, and provides a statutory definition for information security.

The Office of Inspector General (OIG) conducts an annual assessment of the DHS information security program in accordance with FISMA to determine whether DHS's information security program is adequate, effective, and complies with FISMA requirements. Per the FY 2016 OIG FISMA audit report, *"Evaluation of DHS' Information Security Program for Fiscal Year 2016,"* the OIG identified four recommendations for the Department to improve Federal information security. As a result of corrective actions taken prior to June 2017, the OIG has closed three of the recommendations from the FY 2016 FISMA audit. The final OIG recommendation has been noted as resolved but will remain open pending receipt of DHS provided evidence.

The FY 2017 OIG FISMA audit is pending completion at the time of this report's issuance. As such, the audit recommendations and Management's response to the recommendations will be provided when made available.

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 and with internal control standards. As such, the DHS CFO oversees and coordinates all financial system modernization efforts.

DHS has established a Joint Program Management Office (JPMO) to oversee Financial Systems Modernization (FSM) program management, priorities, risk, and 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 potential 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.

As a federal shared service provider, the Department of the Interior (DOI), Interior Business Center (IBC) implemented financial management system solution for DNDO at the IBC data center in FY 2016 and additional development was continuing to eventually migrate TSA and USCG onto the new solution when fully developed to meet their requirements. In March 2017, it was determined that DHS would transition the DNDO, TSA, and USCG FSM initiatives out of the DOI IBC. DHS has made a significant investment in the current financial management solution and is migrating this solution to an alternative hosting environment to complete integration and implementation. This system solution delivers a standardized baseline for DNDO, TSA, and USCG, with increased functionality and integration for DNDO. DHS is leveraging the lessons learned from this shared services implementation, reducing risk in future migrations through deliberative approaches to resource management, business process re-engineering, risk management, change management, and scheduling rigor and oversight.

In addition, USSS is on track to move to the next version of their current accounting software, Oracle Federal Financials, expected to be complete in FY 2018. Other FSM efforts are in the early stages, including FEMA's financial system, flood insurance, and grants management modernization.

Performance Accountability

Based on our internal controls evaluations, the performance information reported for the Department in our performance and accountability reports are complete and reliable, except those noted in our Annual Performance Report. The Department's performance and accountability reports for this and previous years are available on our public website: http://www.dhs.gov/performance-accountability.