15 YEARS

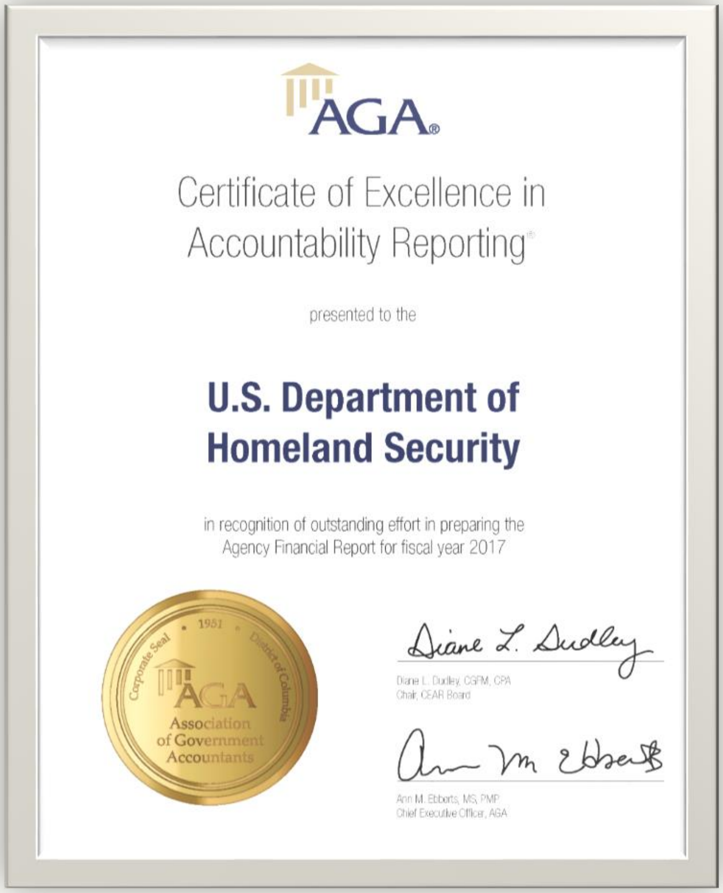
SAFEGUARDING AMERICA

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

FY 2018 AGENCY FINANCIAL REPORT

DEPARTMENT OF HOMELAND SECURITY

Certificate of Excellence in Accountability Reporting



AGA®

Certificate of Excellence in Accountability Reporting®

presented to the

U.S. Department of Homeland Security

in recognition of outstanding effort in preparing the Agency Financial Report for fiscal year 2017

Corporate Seal · 1951 · District of Columbia

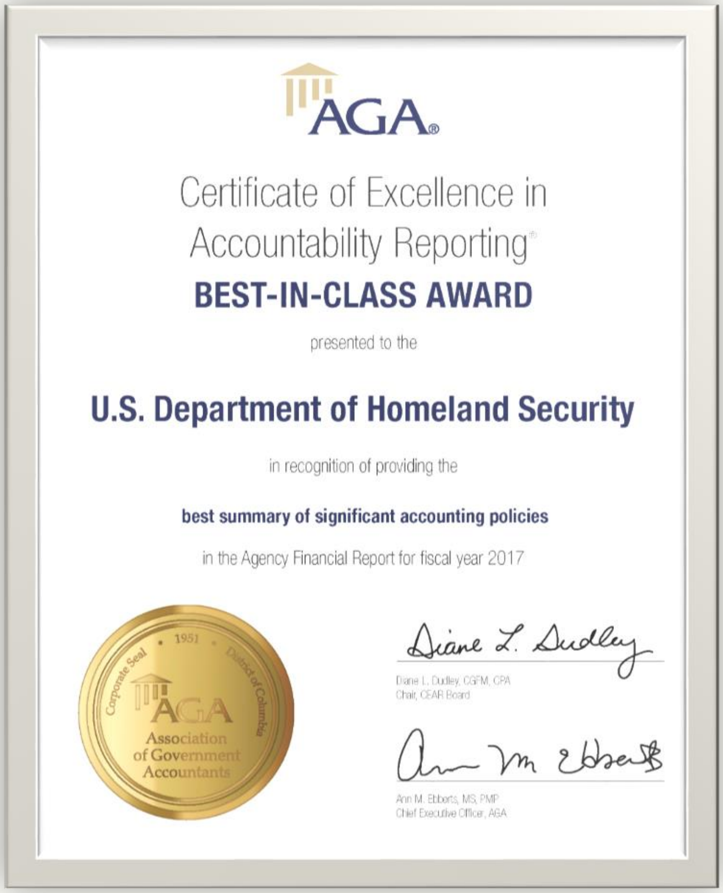
AGA

Association of Government Accountants

Diane L. Dudley

Diane L. Dudley, CGFM, CPA
Chair, CEAR Board

Ann M. Ebberts, MS, PMP
Chief Executive Officer, AGA



AGA®

Certificate of Excellence in Accountability Reporting®

BEST-IN-CLASS AWARD

presented to the

U.S. Department of Homeland Security

in recognition of providing the

best summary of significant accounting policies

in the Agency Financial Report for fiscal year 2017

Corporate Seal · 1951 · District of Columbia

AGA

Association of Government Accountants

Diane L. Dudley

Diane L. Dudley, CGFM, CPA
Chair, CEAR Board

Ann M. Ebberts, MS, PMP
Chief Executive Officer, AGA

In May 2018, DHS received its fifth consecutive Certificate of Excellence in Accountability Reporting (CEAR) from the Association of Government Accountants (AGA) for its FY 2017 Agency Financial Report, along with a best-in-class award for *Best Summary of Significant Accounting Policies*. 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) 2018 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 2018, the Department's Performance and Accountability Reports consist of the following three reports:

- DHS Agency Financial Report | Publication date: November 15, 2018.
- 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, 2019.

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

Message from the Secretary

November 14, 2018

I am pleased to present the Department of Homeland Security's (DHS) Agency Financial Report for Fiscal Year (FY) 2018. This report provides an assessment of the Department's detailed financial status and demonstrates how the resources entrusted to us were used to support our homeland security mission.

Fifteen years ago this year, DHS opened its doors for the first time, combining the efforts of 22 legacy agencies into a single department with a common mission: to protect our country from the many threats we face. These fifteen years have not been without challenge, and we learned that we must instill a culture of relentless resilience. As a department and a nation, we must focus not only on bouncing back from incidents, but on bouncing forward, adapting and innovating even while under attack, and coming back stronger to stare down the next challenge more decisively than before.

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

- Leaning in against today's threats while zooming out to prepare for those on the horizon;
- Being adaptive to keep pace with our adversaries;
- Identifying and confronting systemic risk;
- Preparing at the citizen level;
- Building redundancy and resilience into everything; and
- Raising the baseline of our security across the board—and across the world.

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

One of those challenges was to show that the Department's financial statements are accurate and transparent. For FY 2018, DHS received a clean audit opinion on its financial statements for the **sixth 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. With remaining internal control weaknesses in Financial Reporting and Information Technology Controls and Financial System Functionality, DHS is executing a multi-year strategy and plan to achieve an unmodified internal control audit opinion.

The partnerships we built since the Department was formed will be the foundation we use to continue our success. Our collaboration with other federal agencies will strengthen business processes and standards across the government. Coordination with our auditors and oversight organizations will encourage on-going improvements. We will continue to demonstrate our dedication to our mission to Congress and the American taxpayers by becoming a better, more resilient organization.

I look forward to what we will accomplish in the next fifteen years and far into the future.

Sincerely,

Kirstjen Nielsen
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.

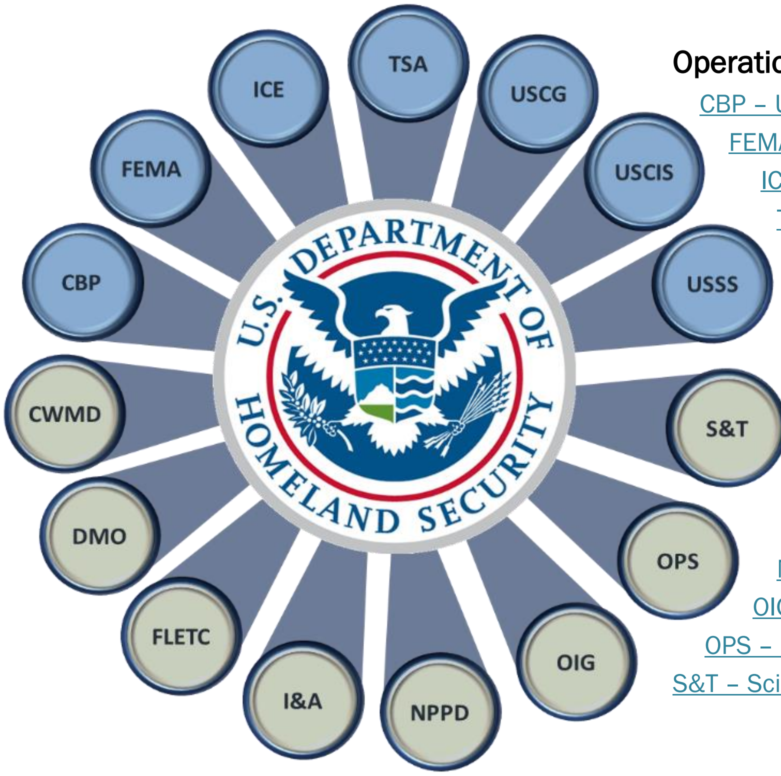
The ***Financial Overview*** section provides a summary of DHS’s financial data explaining the major sources and uses of funds and provides a quick look at our Balance Sheet, Statement of Net Cost, Statement of Changes in Net Position, Statement of Budgetary Resources, and Statement of Custodial Activities.

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[1], 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

- CWMD – Countering Weapons of Mass Destruction Office
- DMO – Departmental Management and Operations
- FLETC – Federal Law Enforcement Training Centers
- I&A – Office of Intelligence and Analysis
- NPPD – National Protection and Programs Directorate
- OIG – Office of Inspector General
- OPS – Office of Operations Coordination
- S&T – Science and Technology Directorate

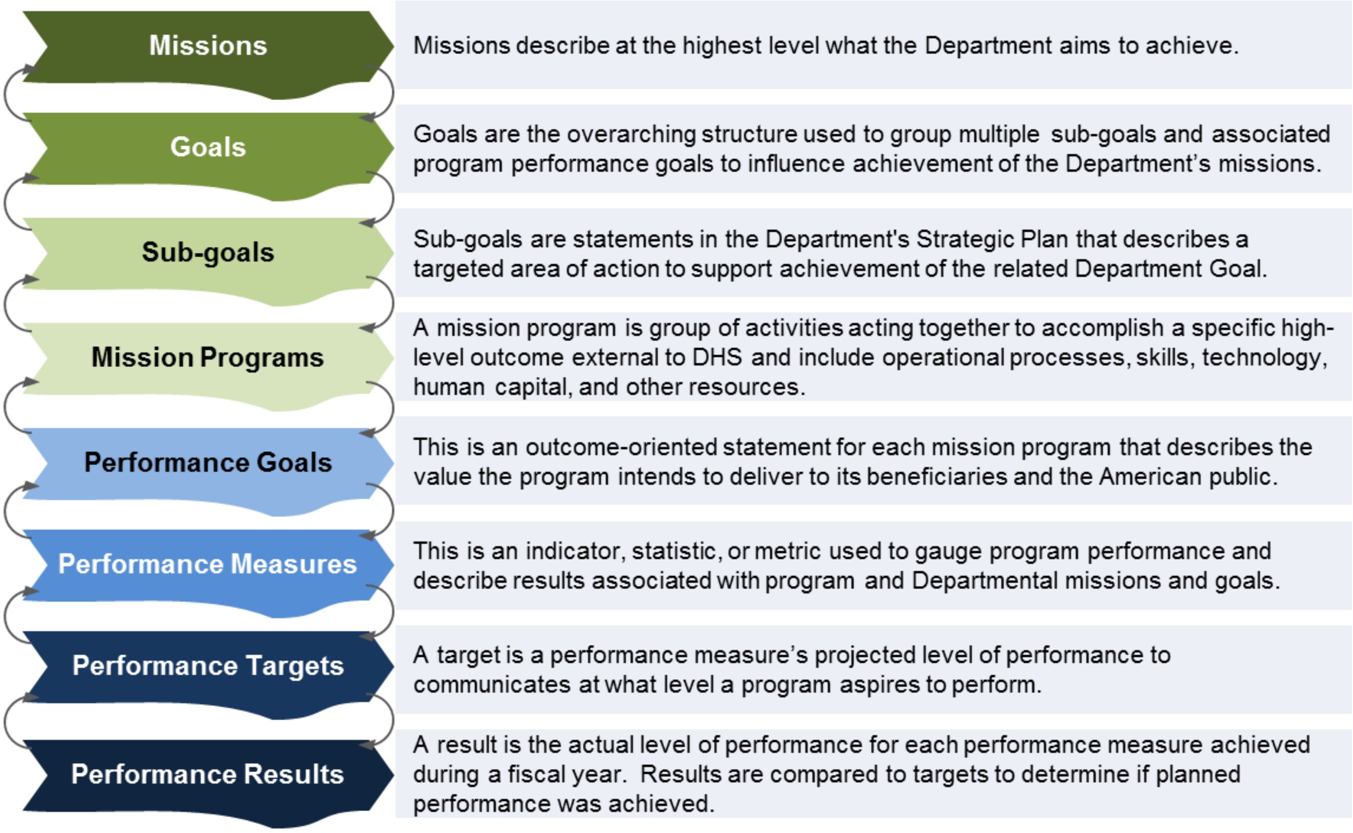
Figure 1: DHS Operational and Support Components

[1] The Countering Weapons of Mass Destruction (CWMD) Office was created in December 2017 to elevate and streamline DHS efforts to prevent terrorists and other national security threat actors from using harmful agents, such as chemical, biological, radiological, and nuclear material and devices, to harm Americans and U.S. interests. The CWMD Office consolidates the Domestic Nuclear Detection Office (DNDO), a majority of the Office of Health Affairs (OHA), and elements of the Office of Strategy, Plans, & Policy and the Office of Operations Coordination.

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 2018-2020 Annual Performance Report with the FY 2020 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.



Missions – Missions describe at the highest level what the Department aims to achieve.

Goals – Goals are the overarching structure used to group multiple sub-goals and associated program performance goals to influence achievement of the Department's missions.

Sub-goals – Sub-goals are statements in the Department's Strategic Plan that describes a targeted area of action to support achievement of the related Department Goal.

Mission Programs – A mission program is group of activities acting together to accomplish a specific high-level outcome external to DHS and include operational processes, skills, technology, human capital, and other resources.

Performance Goals – This is an outcome-oriented statement for each mission program that describes the value the program intends to deliver to its beneficiaries and the American public.

Performance Measures – This is an indicator, statistic, or metric used to gauge program performance and describe results associated with program and Departmental missions and goals.

Performance Targets – A target is a performance measure's projected level of performance to communicates at what level a program aspires to perform.

Performance Results – A result is the actual level of performance for each performance measure achieved during a fiscal year. Results are compared to targets to determine if planned performance was achieved.

Figure 2: DHS Performance Framework

Mission 1: Prevent Terrorism and Enhance Security

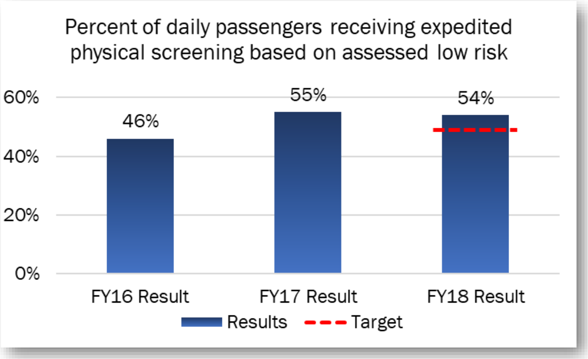
Preventing a terrorist attack in the United States remains the cornerstone of homeland security. Our vision is a secure and resilient Nation that effectively prevents terrorism in ways that preserve our freedom and prosperity. The focus for this mission is to prevent terrorist attacks, protect against the unauthorized acquisition/use of chemical, biological, radiological, and nuclear materials/capabilities, and reduce risk to the nation's critical infrastructure, key leaders, and events.

Improved Intelligence Sharing with Modest Resources

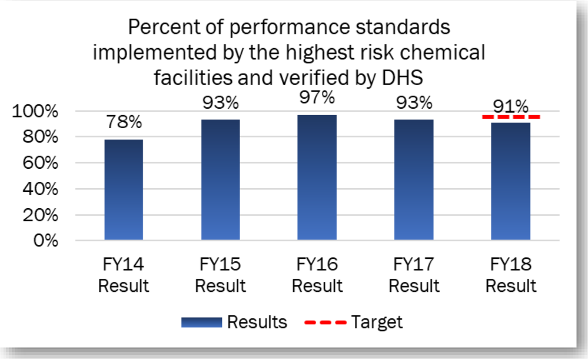
With two new positions within the Aviation Domain Intelligence Integration and Analysis Cell (ADIAC), TSA is improving their intelligence-driven operations and positively impacting TSA's information-sharing/partnering strategic objectives.

TSA's Intelligence & Analysis (I&A)-led ADIAC team formed a new TSA institution relevant to aviation private sector partners with the development of a full-time aviation industry-government threat intelligence sharing capability that has materially enhanced partner sharing and collaboration. ADIAC industry members are noticing the increased aviation threat domain awareness since ADIAC began formally accepting members in late 2017. As of this publication, there are 147 individual participants from 45 industry member organizations and 15 agencies who have been granted full membership by the joint Aviation Government and Aviation Security Coordinating Councils. The ADIAC hosts daily collaborative forums to provide value-added analytic input to stakeholders. TSA's commitment to two-way government-industry threat intelligence and information sharing has provided a trusted partnering forum that contributes directly to the TSA strategic priorities. The growing number of full members and participation in the recurring ADIAC "Industry Day" clearly demonstrate the relevance and value provided by this TSA team, providing evidence that even small fiscal outlays can make a big impact with stakeholders.

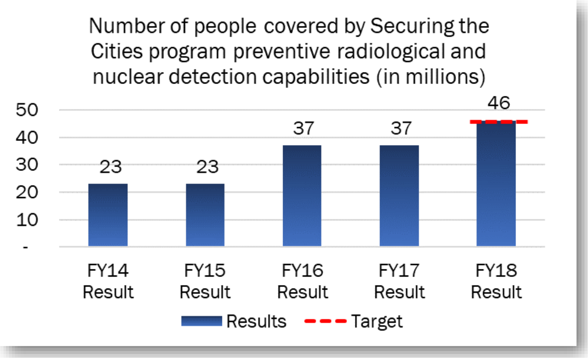
The following highlighted measures gauge our efforts to prevent terrorism and enhance security. Up to five years of data is presented if available.



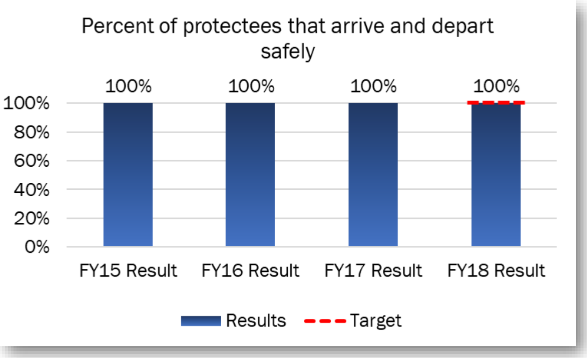
Percent of daily passengers receiving expedited physical screening based on assessed low risk (TSA): This measure gauges the percent of daily passengers who received expedited physical screening because they meet low risk protocols or have been otherwise assessed at the checkpoint as low-risk. TSA Pre√® incorporates modified screening protocols for eligible participants who have enrolled in the TSA Pre√® program as well as other known populations such as known crew members, active duty service members, and other trusted populations. In an effort to strengthen aviation security while enhancing the passenger experience, TSA is focusing on multi-layered, risk-based, intelligence-driven security procedures and enhancing its use of technology in order to focus its resources on the unknown traveler. In FY 2018, TSA achieved 54 percent expedited physical screening based on assessed low risk, exceeding the 50 percent target.



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. In FY 2018, DHS delivered guidance and requirements to the highest risk chemical facilities, prompting these facilities to include 4,028 security improvements in their security plans to satisfy the risk-based performance standards, of which 3,685 security measures have been implemented for a 91 percent result for the year. This result is primarily affected by the DHS roll-out of the Chemical Security Assessment Tool (CSAT) 2.0 system in FY 2017 which significantly increased the number of Chemical facilities required to comply with these standards. In order to improve performance, DHS will continue to prioritize the authorization, inspection, and approval of the highest risk facilities and expects to complete these in a timely fashion. As the facility count stabilizes in FY 2019, DHS expects a higher percentage of risk-based performance standards will be implemented.



Number of people covered by Securing the Cities program preventive radiological and nuclear detection capabilities (in millions) (CWMD): The Securing the Cities (STC) program provides financial assistance to state, local, and tribal organizations to develop a robust regional radiological/nuclear detection program. For the STC program to count the population as covered by a robust radiological/nuclear detection capability, the region must demonstrate that 10% or more of its standing law enforcement are trained and equipped to conduct primary screening and patrolling as part of their daily routine duties and there are equipped and trained personnel to conduct secondary screening and alarm adjudication. In addition, the region must conduct at least one multi-jurisdictional exercise a year and allow the exchange of information among regional partners and with federal agencies, and mutually assist each other in performing the radiological/nuclear detection mission. If the measure is met, the entire population from the statistical area is counted as covered. In FY 2018, the program met its target of covering 46 million people by adding the National Capital Region. Trends in this measure occur in step increases due to the nature of equipping an entire region with these capabilities.



Percent of protectees that arrive and depart safely (USSS): This measure gauges the percent of travel stops where the U.S Secret Service (USSS) protectees arrive and depart safely. The performance target is always 100 percent. Using advanced countermeasures, USSS executes security operations that deter, minimize, and decisively respond to identified threats and vulnerabilities. The protective environment is enhanced by specialized resources within the USSS, including: the Airspace Security Branch; the Counter Sniper Team; the Emergency Response Team; the Counter Surveillance Unit; the Counter Assault Team; the Hazardous Agent Mitigation and Medical Emergency Response Team; and the Magnetometer Operations Unit. Other specialized resources also serve to provide protection from threats, including chemical, biological, radiological, and nuclear materials and explosive devices. USSS has maintained a 100 percent performance record for the past four years.

Security at the Historic Singapore Summit

The USSS secured the historic bi-lateral meeting in June 2018 between President Donald J. Trump and Chairman Kim Jung-un (DPRK). The meeting took place in the Republic of Singapore and required extensive planning and coordination to ensure the safety of both delegations. The successful completion and execution of the meeting was the result of the meticulously planned efforts by the USSS, host country personnel, DOD and other federal agencies, and security personnel from the DPRK.

USSS event coordinators were involved in direct negotiations with both the Singapore government and the DPRK staff and security to oversee the development of a comprehensive operational security and safety plan that thoroughly addressed the current threat environment and vulnerabilities posed in today's world. This included conducting multiple daily meetings and walkthroughs of the event venue, as well as participating in scenario-based training to ensure all entities were well-versed in the proposed responses in the event of an emergency. In addition, the USSS, through continued involvement and successful engagement, was able to alleviate DPRK's initial apprehension regarding security and ensure the overall success of the visit.

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 at all levels of the public and private sectors, and around the world, 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 National Explosives Detection Canine Team Program: Canine teams are a key component in a balanced counter-terrorism program and are proven and reliable resources in the detection of explosives offering unique capabilities throughout diverse operating environments. TSA procures, trains, and deploys both TSA-led passenger screening canines (PSC) and explosive detection canines (EDC) led by state and local law enforcement agencies to secure our Nation's transportation systems through effective explosives detection, visible deterrence, and timely, mobile response to support aviation, mass transit, and maritime sectors. TSA plans to continue to strategically expand the use of canines to address gaps in the security posture.

USSS Human Capital Planning and Budget Implications: As USSS continues to hire personnel in accordance with their Human Capital Plan, meeting their target two years in a row, they will continue to experience resourcing challenges as an increasingly larger portion of their budget is devoted to hiring and maintenance of agency staffing. USSS is moving forward with improvements in human capital modeling capabilities to manage the diverse operations and surge capacity needed for special events and for those years where campaign support is required. In addition, USSS will increase analytic capability and capacity to support the balancing of operational and maintenance cost as resource allocations are determined.

Federal Protective Service: The Federal Protective Service (FPS) is a law enforcement and security agency with a long history of protecting U.S. Government facilities and safeguarding the millions of employees, contractors, and visitors who pass through them every day. Its history dates back to 1790 when six "night watchmen" were hired to protect government buildings in the newly designated nation's capital that became Washington, D.C. FPS is a fee funded operation with contributions from the agencies using FPS services. As the locations and mobility of the workforce change, and the landscape of the facilities being used is fluctuating, FPS is faced with funding uncertainties that are driving proposed future changes in how to fund FPS. As such, FPS is investing in modeling and analytic capabilities to provide rigor in future budget scenarios so they can have the appropriate resources they need to accomplish their role in protecting federal facilities.

Countering Weapons of Mass Destruction: The Countering Weapons of Mass Destruction (CWMD) Office was created in December 2017 to elevate and streamline DHS efforts to prevent terrorists and other national security threat actors from using harmful agents, such as chemical, biological, radiological, and nuclear material and devices, to harm Americans and U.S. interests. The CWMD Office consolidates the Domestic Nuclear Detection Office (DNDO), a majority of the Office of Health Affairs (OHA), and elements of the Office of Strategy, Plans, & Policy and the Office of Operations Coordination. Moving forward, CWMD will finalize and integrate the multiple systems and processes to realize the full benefit of this merger.

Mission 2: Secure and Manage Our Borders

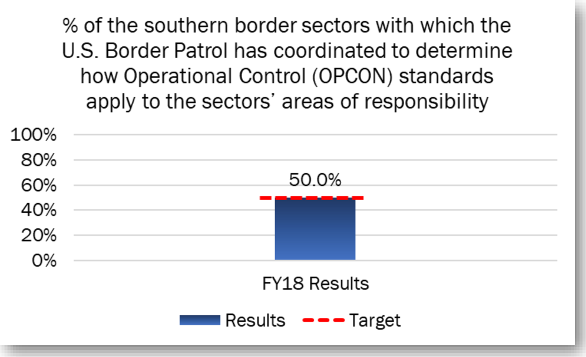
DHS secures the Nation's air, land, and sea borders to prevent illegal activity while facilitating lawful travel and trade. The focus for this mission is to secure the U.S. air, land, and sea borders and approaches, safeguard and expedite lawful trade and travel, and disrupt and dismantle Transnational Criminal Organizations and other illicit actors.

Border Wall Construction

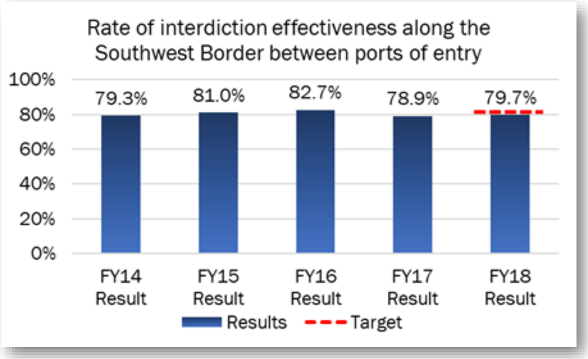
On January 25, 2017, the President issued Executive Order 13767 which directed DHS to "construct a physical wall." The impedance and denial capability that the border wall provides has been an operational requirement for the Border Patrol for many years. The border wall is part of an integrated system that will deter and prevent illegal entries, a requirement all along the Southwest border. The FY 2017 enacted budget included $341 million to construct approximately 40 miles of replacement wall and close approximately 35 gaps in existing barrier with gates. CBP received its FY 2017 funding in late-May 2017 and immediately started planning for the new infrastructure. In partnership with the U.S. Army Corps of Engineers, the first contract for design and construction was awarded for approximately two miles of primary border wall in Calexico, California in November 2017 and construction started in February 2018. As of September 30, 2018, approximately 29 of the 40 miles of replacement border wall were completed. Two of the four wall replacement projects have been completed to include approximately 20 miles of wall in Santa Teresa, New Mexico and approximately two miles in Calexico. The remaining projects are well underway to include construction of approximately 14 miles in San Diego, California (estimated for completion in May 2019) and four miles in El Paso, Texas (estimated for completion in April 2019). Construction of the first of the Rio Grande Valley gates is estimated to commence in November 2018. Concurrently, CBP is also planning and executing the FY 2018 program funded at approximately $1.375 billion as well as the FY 2019 President's budget request of $1.6 billion.

The following highlighted measures gauge our efforts to secure and manage our borders. Up to five years of data is presented if available.

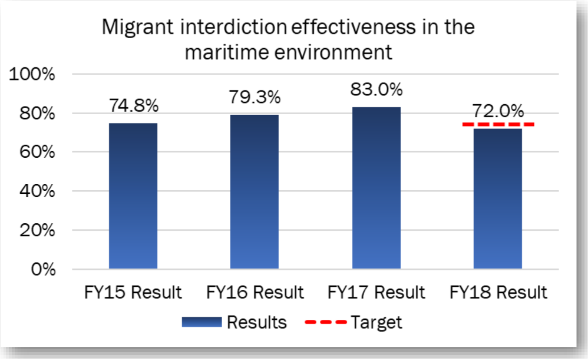
Percent of the southern border sectors with which the U.S. Border Patrol has coordinated to determine how Operational Control (OPCON) standards apply to the sectors' areas of responsibility (CBP)



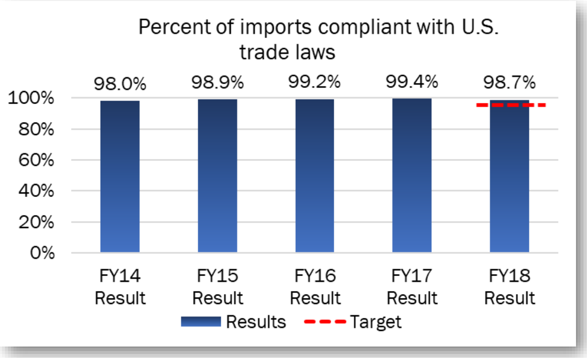
As an FY18-19 Agency Priority Goal, the Department is working to improve security along the southwest border of the U.S. between ports of entry. Implementation of the OPCON framework will enable U.S. Border Patrol's ability to impede or deny illegal border crossings, maintain situational awareness, and apply the appropriate, time-bound, law-enforcement response between the ports of entry as its contribution to DHS's overall border-security mission. Preliminary groundwork was conducted in FY 2018 to facilitate rapid deployment of the OPCON framework in FY 2019. The second half of the progress for this measure will occur in FY 2019, when U.S. Border Patrol will coordinate with each southern border sector on how the OPCON framework will apply to their area of responsibility. U.S. Border Patrol's Planning Division will travel to each of the southern border sectors to brief personnel on the measures in the OPCON framework and foster understanding about its purpose. For full reporting information on this priority goal, please visit Performance.gov or go directly to this link: https://www.performance.gov/homeland_security/APG_dhs_1.html.



Rate of interdiction effectiveness along the Southwest Border between ports of entry (CBP): 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. In FY 2018, this measure achieved 79.7 percent which is below target and slightly up compared to last year's result. A combination of increased situational awareness and a shortfall of staff to respond to this information influences the interdiction rate effectiveness. Border Patrol staffing was slightly below the 19,758 funding level. The National Guard deployment, Operation Guardian Support, has served to improve situational awareness with surveillance technology and maintenance functions, and given the Border Patrol flexibility to re-task and reprioritize response capabilities. Looking forward, the U.S. Border Patrol will continue to advocate for the necessary levels of personnel, surveillance technology and infrastructure, such as wall and access roads, required to be optimally successful in detecting and interdicting illicit cross-border activity in the overall pursuit of Operational Control.



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 U.S. Coast Guard (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 FY 2018, the USCG achieved a 72.0 percent migrant interdiction effectiveness which is significantly down from last year. The result is due to changes in the collection of reported immigrant data within the intelligence community. The new procedures are more reliable; however, these changes have resulted in an increase in the number of reported flow while the interdictions did not increase in proportion to historical trends.



Percent of imports compliant with U.S. trade laws (CBP): Ensuring that all imports are compliant and free from 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 2018, 98.7 percent of imports were found to be compliant with U.S. trade laws, meeting this year's target. This year's successful outcome is consistent with previous results. The small percent of non-compliance included misclassification of flat-rolled steel from Canada and undervaluation of Chinese knitted blouses. Various enforcement methods such as audits, targeting, and random sampling will continue to be incorporated.

An Unlikely Success: Sea Cucumbers

Related to the Department's goals to Safeguard and Expedite Lawful Trade and Travel and to Disrupt and Dismantle Transnational Criminal Organizations and Other Illicit Actors, U.S. Immigration and Customs Enforcement (ICE) in coordination with National Oceanic and Atmospheric Administration Office of Law Enforcement, and the U.S. Fish and Wildlife Service Office of Law Enforcement investigated a Sea Cucumber smuggling operation that resulted in a successful prosecution.

On April 11, 2018, a father and son pleaded guilty to charges related to their smuggling illegally harvested Sea Cucumbers worth over $17 million into the United States and selling the Chinese delicacy and folk medicine ingredient on Asian markets. Ramon Torres Mayorquin pleaded guilty to Importation Contrary to Law and his son, David Mayorquin, pleaded guilty to violating the Lacey Act. Their company, Blessing Seafood, Inc. of Tucson, pleaded guilty to conspiring to export merchandise contrary to law. David Mayorquin, on behalf of Blessings, contacted suppliers of Sea Cucumbers in Mexico and agreed to purchase approximately $13 million worth, knowing they had been illegally harvested. Ramon Mayorquin received the shipments from poachers off the Yucatan Peninsula and created invoices to be submitted to U.S. Customs officials, which falsely stated the value of the product. The company then illegally exported the product from the U.S. without filing the proper export declaration with the U.S. Fish and Wildlife Service. As part of the scheme, they made payments to bank accounts held under false names to conceal the illegal sales, and they also made payments to Mexican officials to ensure that they did not interfere.

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.

Border Security Operations - Operational Control Framework: The Border Security Operations program charged with securing America's Southwest, Northern, and certain Coastal borders. As mentioned above, an Agency Priority Goal is being implemented to improve security along the southwest border between ports of entry using the Operational Control (OPCON) framework to: 1) impede or deny illegal border crossings; 2) maintain situational awareness; and 3) apply the appropriate, time-bound, law-enforcement response between the ports of entry. Implementation of the OPCON framework will help to identify and fill capability gaps along the southwest border and result in field sectors developing operation plans based on their unique terrain, threats, flow, and resources to indicate, and record steps taken to achieve OPCON and show progress in the overall border security along the southwest border. Once OPCON is deployed along the southern border, U.S. Border Patrol plans to expand the OPCON framework to the Northern Border and Coastal sectors.

U.S. Coast Guard Recapitalization: As the Nation's maritime first responder, the U.S. Coast Guard ensures the safety, security, and stewardship of the Nation's waters by protecting those on the sea, protecting the Nation against threats delivered by sea, and protecting the sea itself. To meet the challenges of the dynamic maritime environment, the U.S. Coast Guard executes a layered, security-in-depth concept of operations, built upon a multidimensional framework of authorities, capabilities, competencies, and partnerships to apply its core operational concept of Prevention--Response. To that end, recent additions to the U.S. Coast Guard Cutter fleet have seen significant improvements in effectiveness. Examples include an increase in cocaine interdiction with the new National Security Cutter achieving 200 percent greater effectiveness than legacy cutters in kilogram interdiction per operation hour. Moving forward, the U.S. Coast Guard has an aggressive capital improvement plan to modernize the air and maritime fleet. Key elements of the plan include the 11th National Security Cutter expected in FY 2019, obtaining the first Polar Security Cutter expected to be delivered in 2023, and operating the C-27J fleet.

Transnational Criminal Organizations: U.S. Immigration and Customs Enforcement (ICE) recognizes that transnational criminals and organizations represent a significant threat to public safety and economic security throughout the United States. ICE's focus on prioritizing efforts to disrupt and dismantle Transnational Criminal Organizations (TCO) has seen a better than 20 percent success rate in the recent past. Moving forward, a comprehensive strategy and framework for the integration of all Component information and assets will enable decisions to position the Department to target TCOs in a manner to fully disrupt operations and dismantle their networks. This holistic approach to combating TCOs will make our Nation safer while maximizing the impact of the resources.

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. The focus for this mission is to strengthen and effectively administer the immigration system and prevent unlawful immigration.

Buy American, Hire American
Protecting the Interests of U.S. Workers

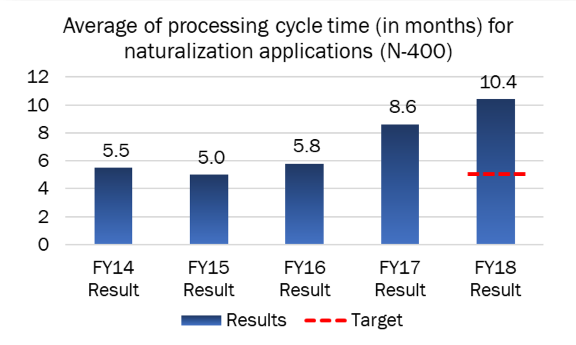
USCIS Targets H-1B Visa Fraud and Abuse

Protecting American workers by combating fraud and abuse in our employment-based immigration programs is a priority for U.S. Citizenship and Immigration Services (USCIS). Through 2018, USCIS continued its targeted approach to further detect and deter H-1B visa fraud and abuse by focusing on:

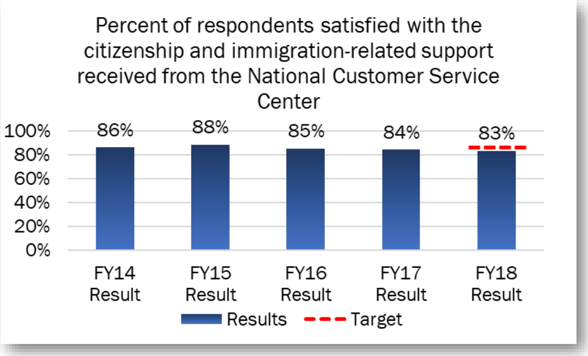
- Cases where USCIS cannot validate the employer's basic business information through commercially available data, which may be an indicator that the employer is an illegitimate organization;
- H-1B-dependent employers (those who have a high ratio of H-1B workers as compared to U.S. workers); and
- Employers petitioning for H-1B workers who work off-site at another company or organization's location.

USCIS uses targeted site visits to focus resources where fraud and abuse of the H-1B program may be more likely to occur. Additionally, the site visits help to determine whether H-1B dependent employers are evading their obligation to make a good faith effort to recruit U.S. workers. These site visits are essential to identifying employers who are abusing the system. Since the program began in FY 2017, USCIS has conducted 585 H-1B targeted site visits, of which 40 percent resulted in a finding of fraud.

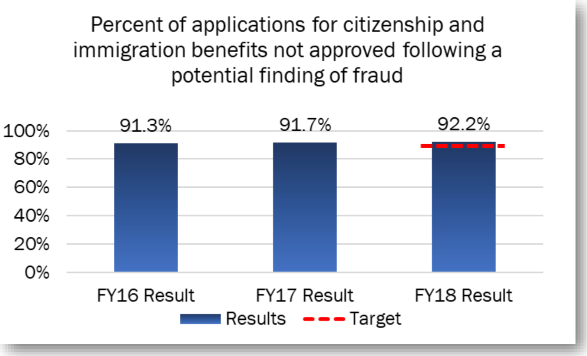
The following highlighted measures gauge our efforts to enforce and administer our immigration laws. Up to five years of data is presented if available.



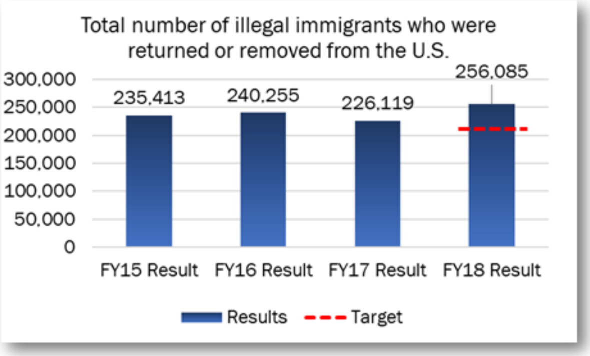
Average of processing cycle time (in months) for naturalization applications (N-400) (USCIS): This measure assesses the program's ability to meet its published processing time goals for N-400, Application for Naturalization which is filed by foreign nationals to attain U.S. citizenship. Naturalization applications have been higher than projected over the past three years which has contributed to the increased backlog and time to adjudicate. USCIS is continuing to shift resources and prioritize workload in order to handle its case volume. FY 2018 cycle time was 10.4 months, significantly above the target; however, 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. USCIS is developing a 6-year plan to rebalance the workforce and improve efficiency to effectively address cycle times and backlog while ensuring cycle time parity across each of its 88 field offices.



Percent of respondents satisfied with the citizenship and immigration-related support received from the U.S. Citizenship and Immigration Services Contact 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 applicant inquiries; 3) accessibility to information; and 4) applicant satisfaction. The FY 2018 result of 83 percent for this measure is consistent with historical results; however, there has been a slight decline the past four years. USCIS' service-rating is well above the Citizen satisfaction with U.S. Federal Government services of 69.7 percent as reported by the American Customer Satisfaction Index in their latest report. The most recent decrease in respondent satisfaction percentage can primarily be attributed to a transition of vendors for Tier 1 support that occurred during the fourth quarter of FY 2018. With the contract transition and system training completed, along with improved quality of information at Tier 1, USCIS expects respondent satisfaction scores to improve in FY 2019.



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. This measure has shown improvement year-over-year since its inception. Initial findings of fraud were upheld 92.2 percent of the time. Initial findings of fraud are reviewed by USCIS' Fraud Detection and National Security Directorate (FDNS) before final adjudication is rendered. USCIS continues to improve communication between fraud officers and adjudicators with the assistance of improved reporting tools and investments in new technologies.



Total number of illegal immigrants who were returned or removed from the U.S. (ICE): This measure describes the total number of illegal immigrants returned and/or removed from the United States by ICE Enforcement and Removal Operations (ERO). This measure includes both immigrants who have entered the country illegally, but do not already have a prior criminal conviction, along with those who have had a prior criminal conviction—providing a complete picture of all the returns and removals accomplished by the program to ensure illegal immigrants do not remain in the United States. ICE exceeded this year's target by nearly 22 percent and is a 13 percent increase over FY 2017. The largest improvement was an increase of interior removals, removing 95,357, which is a 17 percent increase over 2017 and a 46 percent increase over FY 2016.

Enforcement and Removal Operations (ERO)

ERO enforces the Nation's immigration laws in a fair and effective manner. It identifies and apprehends removable aliens, detains these individuals when necessary and removes illegal aliens from the United States. In FY 2018, the following are two high-profile cases successfully executed by ERO.

In February 2018, the ICE ERO Los Angeles Field Office contacted the Pacific Enforcement Response Center (PERC) requesting social media analytical support in preparation for Operation KEEP SAFE 1. PERC analysts conducted open source and social media analysis and provided information on 25 fugitive aliens, resulting in a total of 21 arrests.

On December 27, 2017, ICE ERO, in coordination with Salvadoran law enforcement authorities, successfully removed Leandro Cruz to El Salvador. Cruz was the 100th arrest, through the SAFE program, who was extradited to the El Salvador Policia Nacional and who was also listed on their 100 Most Wanted fugitives list. Cruz had been convicted and sentenced in Massachusetts for assault and battery as an MS-13 Gang member.

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 administers the nation's lawful immigration system, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting Americans, securing the homeland, and honoring our values. Similar to previous years, the number of applications for benefits and benefit changes continues to increase and is now more than 8 million transactions per year creating a challenge to process applications in a timely fashion. The good news is that the United States is still a beacon to the world; however, our resources to process the requests are limited. USCIS will be taking the following steps to address some of the significant challenges identified during the FY18 Strategic Review: 1) Using a six-year forecasting model, increase the number of adjudications officers in the near term, and achieving sustained officer productivity over the six-year period to manage increasing workloads; 2) Finalize infrastructure improvements that will support improved efficiencies; 3) Address the Immigration Examinations Fee Account fee schedule to fund increased staffing; 4) Deploy Refugee Affairs Division staff to border sites for credible and reasonable fear cases; and 5) Develop target processing times to meet planned throughput.

Immigration Enforcement - Enhancing Public Safety in the Interior of the United States: Enhancing public safety in the interior of the United States is another key element to the Department's immigration enforcement mandate. ICE's Enforcement and Removal Operations removes aliens from the U.S. who are subject to a final order of removal issued by an immigration court or following an administrative removability review. ERO facilitates the processing of illegal aliens through the immigration court system and coordinates their departure from the U.S. Progress has been made over the past two years with interior apprehensions and removals increasing. Local law enforcement participation in the 287(g) program is increasing and administrative arrests are also increasing. Moving forward, ICE will continue to prioritize efforts to maximize the discharge of who are subject to a final order of removal. To accomplish this, ICE will continue its efforts to staff and retain key officer and support staff consistent with EO 13768, Enhancing Public Safety in the Interior of the United States.

Mission 4: Safeguard and Secure Cyberspace

Our economic vitality and national security depend on a vast array of interdependent and critical cyber networks, 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. The focus for this mission is to strengthen the security and resilience of critical infrastructure against cyber-attacks and other hazards, secure the federal civilian government information technology enterprise, advance cyber law enforcement, incident response, and reporting capabilities, and strengthen the cyber ecosystem.

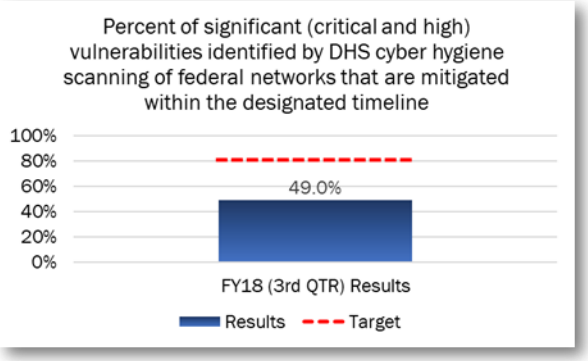
National Level Campaigns Address Nation State Cyber Threats

The National Protection and Programs Directorate's (NPPD) National Cybersecurity and Communications Integration Center (NCCIC) participated in interagency National Level Campaigns addressing cyber-activity and threats from four nation states during 2018.

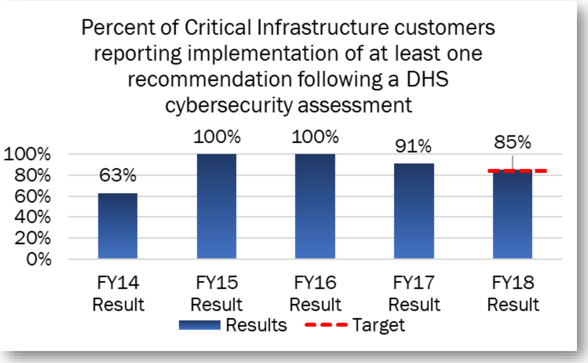
- NPPD contributed to the development and execution of National Security Council campaign operations for each nation state, bringing NCCIC capabilities and expertise to counter the cyber-activity and mitigate the threats.
- The NCCIC coordinated with and provided advance notification of upcoming products to United States corporations, Information Sharing and Analysis Centers, and international partners.
- In coordination with the Federal Bureau of Investigation (FBI), NPPD's NCCIC published multiple joint Technical Alerts and Malware Analysis Reports that publicly attributed the malicious cyber activity to specific nation states. These products provided threat actors' tactics, techniques, and procedures and indicators of compromise which enabled cyber defenders world-wide to identify and mitigate the malicious activity.

From the whole-of-government perspective, these activities improved DHS's ability to collaborate and address challenging issues associated with cyber threats. Cyber defenders in the United States took actions which improved our national security posture while cyber defenders' actions world-wide countered our adversary's activities and abilities to conduct malicious cyber-activity undetected.

The following highlighted measures gauge our efforts to safeguard and secure cyberspace. Up to five years of data is presented if available.

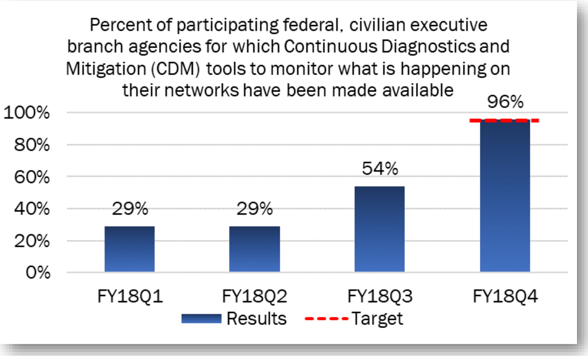


Percent of significant (critical and high) vulnerabilities identified by DHS cyber hygiene scanning of federal networks that are mitigated within the designated timeline (NPPD)
As an FY18-19 Agency Priority Goal, the Department seeks to strengthen the defense of the federal network through the increased dissemination of cyber threat and vulnerability information in near real time to federal agencies. Continuous scanning, intrusion prevention, and vulnerability assessments allow DHS to provide agencies with the necessary tools and information to take timely and appropriate risk-based actions to defend their networks. Agencies continue to work to increase their capacity to address the most serious vulnerabilities identified by the enhanced visibility from Cyber Hygiene Scanning; however, results (as of 3rd quarter)[2] of 49 percent are significantly below the target. Federal Agencies continue to expand and improve their capabilities to identify and mitigate vulnerabilities on their networks, and results are expected to improve over the life of the APG. DHS continues to work with agencies, by issuing or updating direction and guidance when appropriate, to support mitigation actions. For full reporting information on this priority goal please visit Performance.gov or go directly to this link: https://www.performance.gov/homeland_security/APG_dhs_2.html.

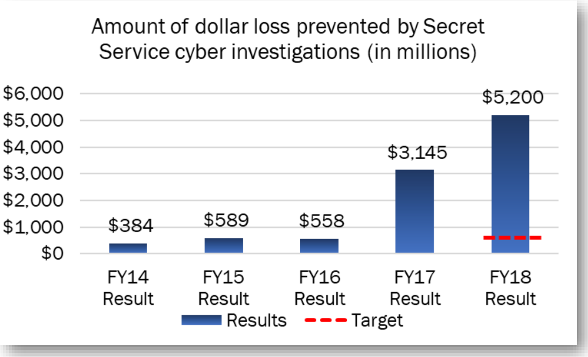


Percent of Critical Infrastructure customers reporting implementation of at least one recommendation following a DHS cybersecurity assessment (NPPD): This measure demonstrates the percent of assessed asset owners and operators of critical infrastructure that are not only developing a better understanding of their cybersecurity posture, but are also taking action to improve that posture. In FY 2018, 85 percent of organizations who received an assessment also implemented at least one cybersecurity enhancement. While the result is down from last year's, the program met the target. 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.

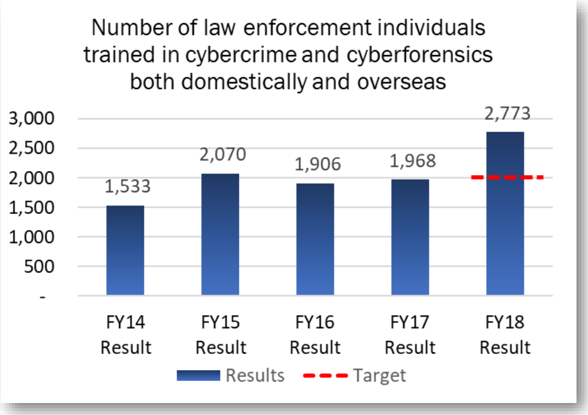
[2] 4th quarter data for this measure is not available at this time due to an issue with a reevaluation of a vulnerability rating in Quarter 4, which has been mitigated, and the results are being reviewed and updated. 4th quarter data for this measure will be available in the FY 2018-2020 Annual Performance Report published in February 2019 and will also be available on Performance.gov.



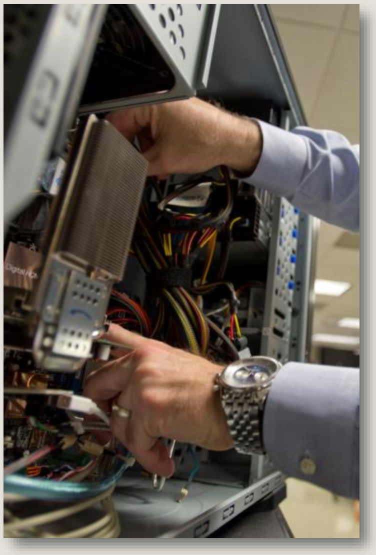
Percent of participating federal, civilian executive branch agencies for which Continuous Diagnostics and Mitigation (CDM) tools to monitor what is happening on their networks have been made available (NPPD): This measure assesses the extent to which DHS has contractually made CDM tools available to participating federal civilian executive branch agencies to monitor events on their networks. Once DHS has made the tools available through contract award, agencies must still take action to deploy and operate CDM on their networks. By making CDM tools available to agencies, they will be able to more effectively manage coordinated threats to their network. As of the end of FY 2018, 96 percent of civilian executive branch agencies had received CDM tools and were available for deployment. Significant progress and momentum for the deployment of this critical tool has been accomplished.



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. The USSS closed two very large cases in the first quarter of FY 2018 which greatly impacted the results of the measure (one relating to tax fraud and the other a significant network intrusion into a major retailer). This year's result of $5.2 billion is the largest reported for this measure, greatly exceeding the target of $650 million. The year-to-year results for this performance measure are highly variable based upon the cases closed in a particular reporting period.



Number of law enforcement individuals trained in cybercrime and cyberforensics both domestically and overseas (USSS): This measure represents the efforts of the USSS to strengthen our partners' ability, both domestically and overseas, to fight cybercrime. Today's high-tech environment presents new challenges to law enforcement and the justice system as cyber-criminals exploit computers, mobile devices, and the Internet to threaten our banking, financial, and critical infrastructures. Digital technology is used to commit any and every type of crime. Therefore, it is imperative to address the changes in technology by providing training on cyber-investigative techniques and by sharing current expertise. The USSS has trained a total of 2,773 law enforcement individuals both internal to the Service and externally. The majority of external law enforcement partners are trained at the National Computer Forensics Institute's (NCFI) innovative facility. The total number individuals trained measure is directly tied to the NCFI appropriation and these numbers will continue to increase and decrease in proportion to that budget. In FY 2018, NCFI trained 43% more people than in FY 2017 which explains the dramatic increase between fiscal years (budget increased from $13.9 Mil to $18.8 Mil).



Cashed Out Investigation – Cybercrime and an Old-Fashioned Gambling Scam

In July, 2018, the Cleveland Field Office coordinated a large scale operation entitled "Cashed Out." The Internal Revenue Service (IRS), U.S. Food & Drug Administration – Office of Criminal Investigations, and the Ohio Casino Control Commission initiated an investigation into numerous illegal gambling businesses in the Northern District of Ohio. The businesses in question were suspected of using illegal gambling slot machines, laundering illegal monetary proceeds, and evading federal taxes. A total of 33 search warrants were successfully executed (16 with USSS lead and 17 with IRS lead with USSS assistance). This expansive operation required the use of an HSI TFO and their K9 partner at 7 different locations, 10 Secret Service Investigative Analysts to process evidence, and multiple ECSAP agents to analyze electronic devices seized for successful case prosecution.

The main subject of the investigation was arrested and multiple items were seized including more than $1 million in US dollars (€373 EUR, £9,255 English Pounds, and other foreign currencies), approximately 100 pounds in silver bars and collectible coins, with various electronic devices (servers, hard drives, mobile phones, and tablets).

Looking Forward

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.

Information Security: As DHS has moved forward in implementing the CDM program, there are some systemic issues that are driving risk to full implementation. With the goal of federal agencies being able to mitigate 80% of significant (critical and high) vulnerabilities identified through DHS scanning of their networks, there is a need to have strong and persistent Information Technology governance structures across the Federal Government. Federal Chief Information Security Officers, and the institutional knowledge they bring, provide the pathway to success; however, they are often constrained by internal governance issues and lack of knowledge transfer in a high-turnover field. NPPD supports the implementation of a formalized federal cybersecurity governance structure to direct the full implementation of NPPD Cybersecurity programs and directives to improve threat information sharing, by increased visibility into risks to federal networks, establish a standardized approach for developing guidance, technical assistance, and awareness materials.

Election Infrastructure Security: In recent years, American citizens have become increasingly uneasy concerning potential threats to the Nation's election infrastructure. Cyber-intrusions to voting machines and voter registration systems diminish the overall public confidence that elected officials need to perform their public duties and undermine the integrity of the Nation's democratic process. If left unaddressed, system vulnerabilities will continue to threaten the stability of our Nation's democratic system. In January 2017, following confirmation of the September 2016 election system hacks, the Secretary of the Department of Homeland Security designated election systems as critical infrastructure (CI). This designation is given to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." To begin the process of mitigating this risk, NPPD published the *Election Infrastructure Security Resource Guide.* DHS has also built formal, trusted relationships with election officials from all 50 states, over 1,300 local jurisdictions, and a range of private sector partners; prioritized delivery of no-cost cybersecurity services and the sharing of actionable information to election officials and network security stakeholders; and deployed sensors to state and local election networks that help detect intrusions by malicious actors, quadrupling the number of sensors deployed since 2016. However, there is more to be accomplished. Moving forward, NPPD will continue to expand election infrastructure stakeholder engagement and provide needed resources and support to ensure our election processes and infrastructure are secure from cyber threats.

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. The focus for this mission is to enhance national preparedness, mitigate hazards and vulnerabilities, ensure effective emergency response, and enable rapid recovery.

PREPTalks
GW
MODERNIZING PUBLIC WARNING MESSAGING
Dennis S. Mileti, Professor Emeritus
University of Colorado Boulder
January 2018

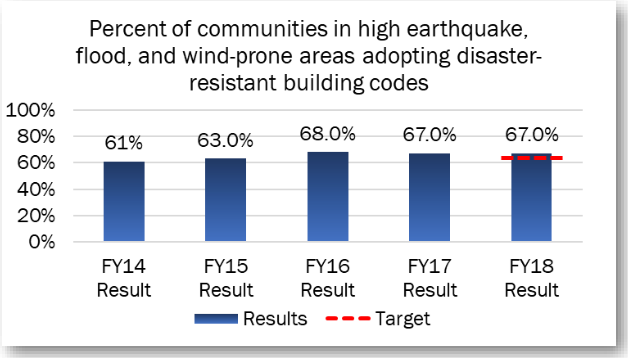
PrepTalks – New Perspectives for Emergency Managers

PrepTalks is a video series that spreads new ideas, sparks conversation, and promotes innovative leadership for the issues confronting emergency managers now and over the next 20 years. The first PrepTalk was released on February 13, 2018, and since that time, the 10 PrepTalk videos have more than 25,000 unique viewers on the PrepTalks webpage and YouTube.

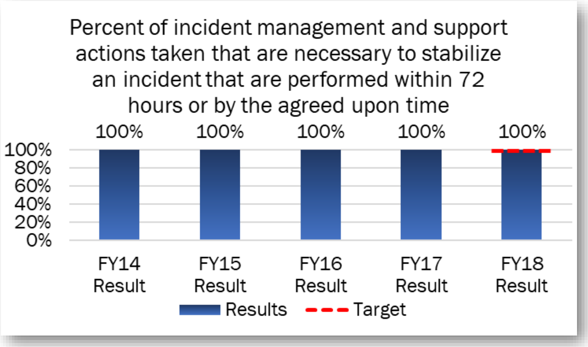
FEMA initiated a partnership to create PrepTalks with the nation's major emergency management organizations, including the International Association of Emergency Managers, National Emergency Management Association, Naval Postgraduate School Center for Homeland Defense and Security, and the National Homeland Security Consortium. Together, we attract nationally recognized experts to record high quality video presentations for the emergency management community and the public to use anytime for free.

PrepTalks benefit the nation by providing presentations from nationally recognized experts, often available only at conferences or closed-door meetings, to the entire emergency management community. PrepTalks include new views on traditional topics like, public warning and pandemic preparedness. They also promote important less traditional topics like financial literacy, social capital, and school safety. The videos are accompanied by recorded question and answer sessions and a discussion guide to help viewers put the PrepTalk knowledge into practice.

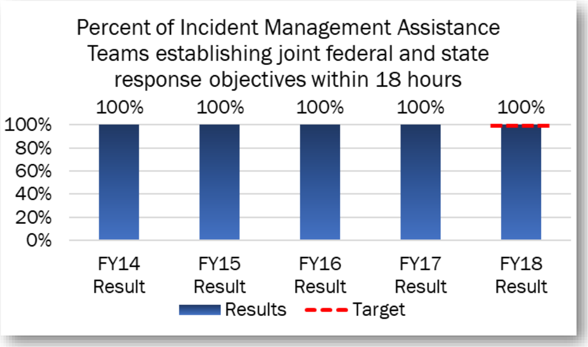
The following highlighted measures gauge our efforts to strengthen national preparedness, resilience, and our response to disasters. Up to five years of data is presented if available.



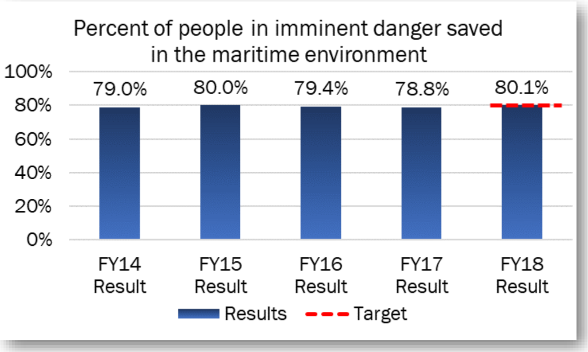
Percent of communities in high earthquake, flood, and wind-prone areas adopting disaster-resistant building codes (FEMA): This measure assesses the number of communities adopting building codes containing provisions that adequately address earthquake, flood, and wind hazards. FEMA works with code adoption and enforcement organizations to support community implementation of disaster resistant building codes, defined as being in compliance with the National Flood Insurance Program regulations, equivalent to the National Earthquake Hazards Reduction Program recommended provisions, and in compliance with the provisions of the International Codes as designated by the International Codes Council. FEMA also works with the Insurance Services Office Building Code Effectiveness Grading Schedule data to track the number of high-risk communities subject to flood, wind, earthquake, and combined perils that adopted disaster resistant building codes. FEMA continues to make progress on this measure through training, education, and outreach to communities and businesses, as evidenced by the fiscal year 2018 result of 67 percent slightly exceeding the target.



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): FEMA's response role is to effectively respond to any disaster, threat, or hazard, with a focus on saving/sustaining lives, and to support state, local, tribal, and territorial governments. This measure evaluates FEMA's ability to perform critical response actions to stabilize an incident within the first 72 hours. These actions must be initiated immediately after an incident to ensure the best outcomes for survivors. In fiscal year 2018, FEMA responded to concurrent incidents across several regions, states, and territories, and performed 100% of critical actions during each incident. FEMA issued emergency alerts with federal and state partners and the Incident Management Assistance Teams established joint federal/state incident objectives to coordinate federal response capabilities. Also, FEMA deployed urban search and rescue resources and deployed Mobile Emergency Response Support to establish interoperable communications within required timeframes. Understanding substantial impacts to the transportation, communications, energy, and health/medical infrastructure sectors during Hurricanes Harvey, Irma and Maria, FEMA deployed all available restoration capabilities to ensure the establishment of air/sea bridges, route clearance, emergency power and communications, and other enabling efforts to deliver life-saving and life-sustaining commodities.



Percent of Incident Management Assistance Teams establishing joint federal and state response objectives within 18 hours (FEMA): FEMA's Incident Management Assistance Teams (IMATs) provide a forward federal presence to facilitate the management of the national response to catastrophic incidents. Their mission is to: rapidly deploy to an incident; identify ways federal assistance could be used to best support the response and recovery efforts; and work with partners across jurisdictions to support the affected state or territory. This performance measure evaluates the IMATs' ability to deploy to an incident and establish initial joint federal and state response objectives within 18 hours of a request from a state or jurisdiction. In fiscal year 2018, FEMA's IMATs deployed to events in American Samoa, California, Florida, Hawaii, Maine, North Carolina, Puerto Rico, South Carolina, Texas, and the US Virgin Islands and met the target of this key performance measure.



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 3,900 lives in FY 2018, which was 78.0 percent of those in danger, and is consistent with long-term results and trends, although slightly missing their target. The USCG continues to plan, train, develop better technologies, and invest in capable assets to continue their exemplary performance in saving lives in the maritime environment.

FY 2018 U.S. Coast Guard Recovery Efforts for Hurricanes Harvey, Irma, and Maria

Recovery efforts continue in response to Hurricanes Harvey, Irma, and Maria and required a complex approach to managing the catastrophic impacts of several major hurricane landfalls in Texas, Florida, U.S. Virgin Islands, and Puerto Rico. The Nationally Declared Disasters were allocated $156 million for pollution response. The Coast Guard led the response and directed response teams in the affected areas to conduct rapid oil and hazardous material assessments after the storms and provided direct federal assistance to Texas, Florida, Puerto Rico, and the U.S. Virgin Islands. Using the Federal On-Scene Coordinator authority to mitigate hazards, the Coast Guard consulted with federal, state, local, tribal, and territorial governments to ensure sensitive environmental, cultural, and historical sites, as well as endangered species were protected. 4,215 vessels and related pollutants were removed from the environment over the course of eight months.

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. DHS works with individuals, communities, the private and nonprofit sectors, faith-based organizations, and federal, state, local, tribal, and territorial partners to ensure swift and effective recovery efforts after such emergencies. Hurricanes and forest fires over the past two years remind us all of the importance of preparedness and resilience in the face of disaster. Below are a couple initiatives that advance our efforts to achieve our preparedness and resilience goals.

Grants Management Modernization: Preparedness and other grant programs support our citizens and first responders to ensure that we work together as a nation to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards. These grants support capacity development and sustainment at the state, local, tribal, and territorial levels and in our Nation's highest-risk transit systems, ports, and along our borders. In 2015, FEMA began an initiative to transform the way the agency administers grants. The Grants Management Modernization (GMM) acquisition aims to streamline grants management across the agency's 40-plus grant programs through a user-centered, business-driven approach. GMM's modernized grants management solution will establish a single grants management information technology (IT) platform for FEMA's grants operations, and where possible, a common grants management life cycle and unified business processes across the Agency. This ongoing agile development effort will improve the efficiency and effectiveness of FEMA's grant operations and enhancing FEMA's mission performance.

Improving the National Flood Insurance Program: The National Flood Insurance Program (NFIP) Pivot Program is a system to replace and modernize the aging legacy system used to process insurance transactions. Pivot will be capable of processing millions of transactions in real-time, uploading claim documents, automating NFIP processes, and securely storing and disseminating critical information. The new system is following an agile development approach and expects to be fully operational, ahead of schedule, in 2020.

Catastrophic Disaster Preparedness: The Preparedness program works to ready the Nation for disasters of all kinds. Preparedness includes the management and administrative support functions associated with training and national exercise programs. Major hurricanes and fires have recently underscored the need to improve the nation's overall preparedness posture. To that end, FEMA is preparing the Nation for catastrophic disasters, including multiple concurrent disasters, by:

- Establishing FEMA Integration Teams with participating state governments, to help local emergency responders coordinate planning, tailor assistance, and facilitate FEMA assistance when disasters strike.
- Improving logistics delivery within, and especially beyond, the 48 contiguous states.
- Improving capabilities of state, local, tribal, and territorial via the National Qualification System provides a nationwide approach to ensure that responders are prepared to work together during all threats and hazards, regardless of the incidents cause or size. This is a federally-supported, state-managed, locally-executed approach.
- Significantly increasing the number of households with flood insurance to reduce the risk and impact of flooding on private structures.

- Increasing the financial preparedness of the public through partnerships and materials, including the Emergency Financial First Aid Kit.
- Building a culture of preparedness by connecting individuals, organizations, and communities with research and tools to build and sustain capabilities to prepare for any disaster or emergency.

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. The focus for this mission is to 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.

Android Team Awareness Kit (ATAK)

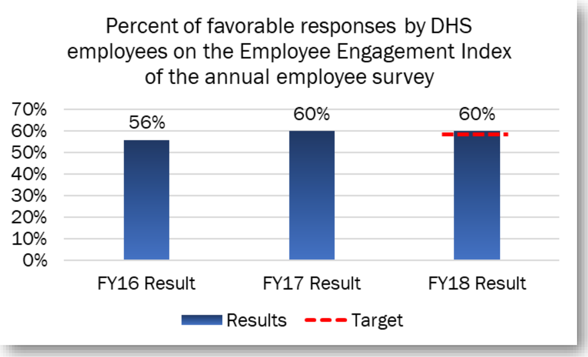
The DHS Science and Technology Directorate (S&T) deployed the Android Team Awareness Kit (ATAK) to support the complex communication and coordination needs of the multi-jurisdictional responders. A government-off-the-shelf app for Android smartphone, ATAK is available to all government agencies for free. The app uses GPS and maps to give the user a real-time situational awareness capabilities.

In 2018, S&T has deployed ATAK to support public safety through several multi-agency coordinated and cooperative operations in which all DHS Component and Homeland Security Enterprise participants benefited from improved situational awareness. These events included Super Bowl LII, the NBA All-Star game, U.S. Border Patrol's San Diego, California Sector field experiment, and a marijuana-growing sting operation. At each of these events, ATAK was successfully utilized to improve situational awareness through capabilities such as full-motion video dissemination, blue force tracking of law enforcement agents, and other geographic information. This information was available to various mobile and fixed operations centers, as well as operators in the field via mobile devices with the ATAK application. ATAK technology enables personnel from multiple agencies to track response assets, identify hazards, locate people needing rescue, coordinate interagency response, and share video feeds of operations while also maintaining tactical awareness of weather, critical infrastructure, and other important information. In FY 2018, the FLETC PO Liaison Officer worked with federal POs on more than 900 questions and issues, ranging from simple inquiries about FLETC procedures to complex matters that impact the full enterprise.

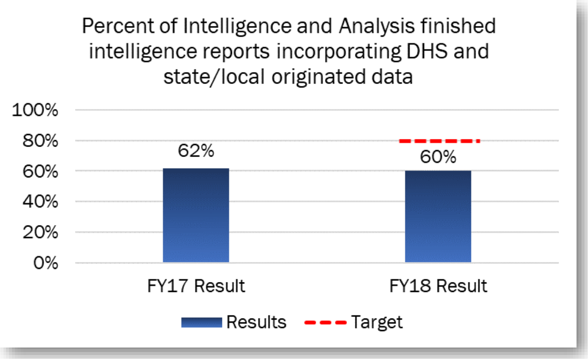
> **ATAK is like having the connectivity of a command center at your fingertips.**
>
> Statement by Homeland Security Intelligence (HSI) Special Agent/Special Response Team (SRT) member.

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

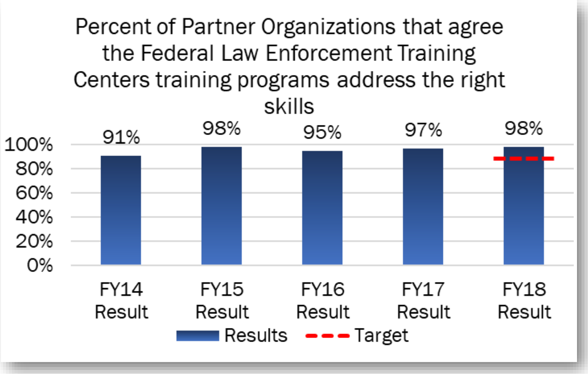
Secretary for Management at https://www.dhs.gov/dhs-budget. Up to five years of data is presented if available.



Percent of favorable responses by DHS employees on the Employee Engagement Index of the annual employee survey (MGMT): 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 2018 FEVS data, the percent of favorable responses on EEI held stable at 60% positive in 2018, slightly above the 58% target.



Percent of Intelligence and Analysis finished intelligence reports incorporating DHS and state/local originated data (I&A): This measure gauges the impact that DHS provides to the intelligence community by disseminating, in finished intelligence reports, information harnessing DHS and state, local, tribal, and territorial data that is unique. In FY 2018, 60 percent of the disseminated intelligence produced by the Office of Intelligence & Analysis (I&A) incorporated information originating from DHS collected intelligence or information directly attributable to state and local governments. While I&A did not meet its annual target, it demonstrates I&A's commitment to using DHS and state and local information in its disseminated intelligence. The results also indicate that DHS and state and local information remains relevant to I&A's analysis when communicating its assessments to its customers nationwide. I&A evaluates its collection requirements for relevancy to intelligence priorities and I&A field officers continue to seek out sources of information that can provide relevant intelligence.



Percent of Partner Organizations that agree the Federal Law Enforcement Training Centers (FLETC) 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): FLETC is the Nation's largest provider of law enforcement training. As such, FLETC bears responsibility to ensure its training meets the needs of more than 90 federal Partner Organizations and thousands of state, local, tribal, and international law enforcement officers and agents operating in the dynamic environment of the law enforcement profession. This measure gauges FLETC's success in anticipating, developing, and delivering the most current, relevant, and accurate law enforcement training possible to produce agents and officers proficient in the techniques required to perform their law enforcement duties in their operating environments. The FY 2018 results are in line with historical performance and significantly above the target of 90 percent.

FLETC Partner Organization Liaison Officer

FLETC, through strategic partnerships, prepares the federal law enforcement community to safeguard the American people, our homeland, and our values. Effective partnerships are critical to FLETC's ability to meet this mission, and to realize its vision to be America's enterprise resource for federal law enforcement training.

During FY 2018, FLETC fully implemented an effort to integrate partner relations into a single point-of-contact charged with ensuring its federal Partner Organizations (POs) have access to the information they need to achieve their training goals in support of their operational missions. Through this focused approach, the PO Liaison Officer facilitated improvement to communication mechanisms through efforts such as enhancing the FLETC PO website and orientation program, facilitating monthly meetings among PO and FLETC leadership, and instituting monthly open-dialogue sessions among small groups of partners to share information and discuss topics of mutual interest. In FY 2018, the FLETC PO Liaison Officer worked with federal POs on more than 900 questions and issues, ranging from simple inquiries about FLETC procedures to complex matters that impact the full enterprise.

<u>Looking Forward</u>

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.

Financial Stewardship: DHS is expending resources to improve our planning, programming, budgeting, and execution systems to develop the One Number System. Through our One Number System, which is currently in development, the Department will have clear line-of-sight from proposed changes to budget line items, the decision processes used to adjudicate those changes, and then the information on how those funds were expended. In addition, our financial system modernization (FSM) efforts are moving forward which will continue demonstrating strong financial stewardship, while executing a multi-year strategy to remediate our remaining material weaknesses in Financial Reporting and Information Technology controls and achieve a clean Internal Control over Financial Reporting opinion. Couple these improvements with our robust internal control program, we are ensuring taxpayer funds are expended as efficiently and effectively as possible while preventing and detecting fraud, waste and abuse. We will continue to work toward a more mature process and are addressing known gaps based on our approach to continually seek for a better solution.

Organizational Changes: DHS continues to look for opportunities to improve organizational effectiveness. Based on recent studies two major transformations are underway and will continue into the next fiscal year. The first is the CWMD effort that was previously discussed in Mission 1. The second major organizational change is occurring within the Science and Technology (S&T) Directorate to become more agile in tackling customer requests and change the way the organization responds to requests from years to days/weeks. As the research and development (R&D) arm of the DHS[3], S&T focuses on providing the tools, technologies, and knowledge products the nation's Homeland Security Enterprise needs today and tomorrow. That means S&T constantly works to bridge industry and end-user communities around the nation. S&T's R&D focus areas cover DHS's core mission areas and use our network of industry, national laboratory, and other partners seek solutions for capability gaps and define topics for future research.

Procurement Innovation: DHS established the Procurement Innovation Lab (PIL) in 2015, focused on creating a procurement culture that takes smart risks to ensure timely delivery to the important mission needs across the Department. By testing innovative techniques through actual DHS procurements and then sharing the lessons learned and best practices across the acquisition workforce, the PIL framework promotes a continuous cycle of iteration and improvement. The PIL supports strategic acquisitions for the Department, such as Grants Management Modernization and Financial Systems Modernization. To date, over 8,300 members of the acquisition workforce have participated in PIL webinars or PIL Boot Camps (one-day immersive training workshops), evidence of a growing grassroots community of procurement innovators developing across the Department. DHS is committed to maturing this nascent culture change in order to deliver exceptional results for the DHS mission and serve as a model for the Federal acquisition community.

[3] CWMD conducts R&D for Departmental radiological and nuclear detection capabilities.

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.

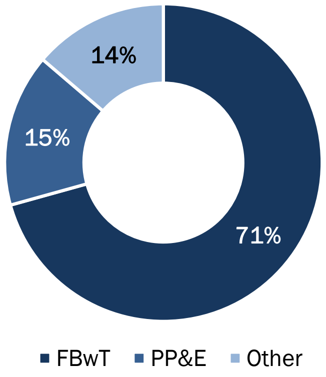
The Balance Sheet presents the resources owned or managed by the Department that have future economic benefits (assets) and the amounts owed by DHS that will require future payments (liabilities). The difference between the Department's assets and liabilities is the residual amount retained by DHS (net position) that is available for future programs and capital investments.

Financial Position ($ in millions)	FY 2018	FY 2017	$ Change	% Change
Fund Balance with Treasury	$ 105,095	$ 71,466	$ 33,629	47%▲
Property, Plant, and Equipment	23,146	21,887	1,259	6%▲
Other Assets	20,445	18,358	2,087	11%▲
Total Assets	**148,686**	**111,711**	36,975	33%▲
Federal Employee and Veterans' Benefits	61,864	58,715	3,149	5%▲
Debt	20,541	30,440	(9,899)	-33%▼
Accounts Payable	4,440	4,278	162	4%▲
Deferred Revenue and Advances	4,737	5,799	(1,062)	-18%▼
Insurance Liabilities	1,658	12,331	(10,673)	-87%▼
Accrued Payroll	2,432	2,276	156	7%▲
Other Liabilities	10,218	7,654	2,564	33%▲
Total Liabilities	**105,890**	**121,493**	**(15,603)**	-13%▼
Total Net Position	42,796	(9,782)	52,578	<-100%▼
Total Liabilities and Net Position	**$ 148,686**	**$ 111,711**	**$ 36,975**	33%▲

Results of Operations ($ in millions)	FY 2018	FY 2017	$ Change	% Change
Gross Cost	$ 82,051	$ 80,683	$ 1,368	2%▲
Less: Revenue Earned	(16,373)	(13,786)	(2,587)	19%▲
Net Cost Before Gains and Losses on Assumption Changes	65,678	66,897	(1,219)	-2%▼
Gains and Losses on Assumption Changes	1,143	(494)	1,637	<-100%▼
Total Net Cost	**$ 66,821**	**$ 66,403**	**$ 418**	1%▲

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.

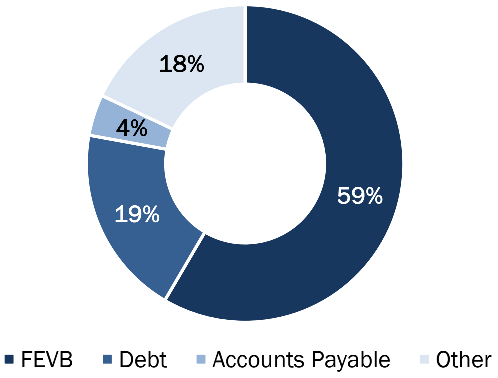
Property, Plant, and Equipment (PP&E) is the second largest asset, and include buildings and facilities, vessels, aircraft, construction in progress, and other equipment. In acquiring these assets, the Department either spent resources or incurred a liability to make payment at a future date; however, 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, 2018, the Department had $148.7 billion in assets, representing a $37 billion increase from FY 2017. The majority of this change is due to the increase in FEMA's and USCG's FBwT to support disaster relief efforts for the significant hurricanes that struck the United States and its territories in FY 2017 and the state of California wildfires in FY 2018, as well as CBP receiving increased appropriations for border security.

Liabilities – What We Owe

Liabilities are the amounts owed to the public or other federal agencies for goods and services provided but not yet paid for; to DHS employees for wages and future benefits; and for other liabilities.



The Department's largest liability is for *Federal Employee and Veterans' Benefits (FEVB).* The Department owes these amounts to current and past civilian and military personnel for pension and other post-employment benefits. The liability also includes medical costs for approved workers' compensation cases. For more information, see Note 16 in the Financial Information section. This liability is not covered by current budgetary resources, and the Department will use future appropriations to cover these liabilities (see Note 14 in the Financial Information section).

Debt is the second largest liability, and results from Treasury loans and related interest payable to fund FEMA's National Flood Insurance Program (NFIP) and Disaster Assistance Direct Loan Program. Given the current premium rate structure, FEMA will not be able to generate sufficient resources from premiums to pay its debt; therefore, legislation will need to be enacted to provide funding to repay the Treasury or cancel the debt. This is discussed further in Note 15 in the Financial Information section.

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

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

As of September 30, 2018, the Department reported $105.9 billion in total liabilities. Total liabilities decreased by $15.6 billion in FY 2018. A reduced estimated insurance liability for disaster relief efforts for the significant hurricanes in FY 2018 drives most of this decrease in liabilities.

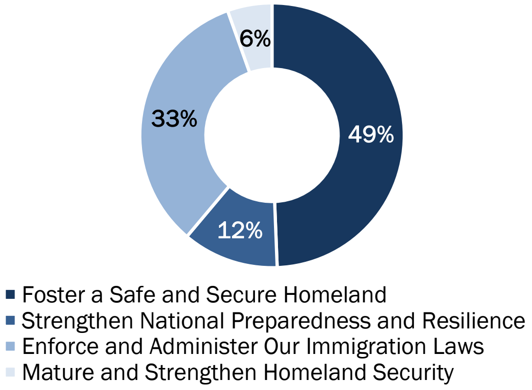
Net Position

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 $42.8 billion. Total net position increased approximately $53 billion from FY 2017, in large part because of supplemental appropriations received for the Disaster Relief Fund (DRF) for relief efforts in response to Hurricanes Harvey, Irma, and Maria in FY 2017 and wildfires in FY 2018, as well as debt relief for NFIP.

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 was $65.6 billion in FY 2018. DHS recognized increased revenue this year because of revenue earned from Immigration Examination fees and NFIP reinsurance.



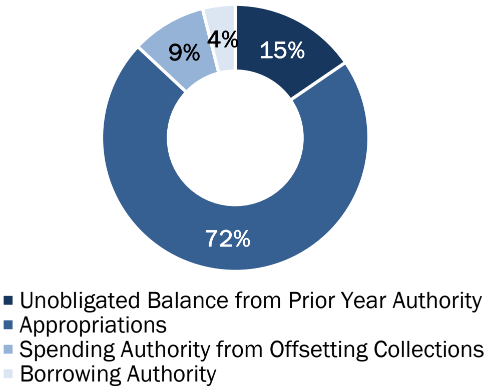
During FY 2018, the Department earned approximately $16.4 billion in exchange revenue. Exchange revenue arises from transactions in which the Department and the other party receive value and that are directly related to departmental operations. The Department also collects non-exchange duties, taxes, 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 2018	FY 2017	$ Change	% Change
Unobligated Balance from Prior Year Authority	$ 23,900	$ 15,341	$ 8,559	56%▲
Appropriations	110,725	68,224	42,501	62%▲
Spending Authority from Offsetting Collections	14,038	10,971	3,067	28%▲
Borrowing Authority	6,110	7,427	(1,317)	-18%▼
Total Budgetary Authority	**$ 154,773**	**$ 101,963**	**$ 52,810**	52%▲

The Department's budgetary resources were approximately $154.8 billion for FY 2018. The authority was derived from $23.9 billion in authority carried forward from FY 2017, appropriations of $110.7 billion, $14 billion in collections, and $6 billion in borrowing authority. Budgetary resources increased approximately $53 billion from FY 2017. Supplemental appropriations received for the Disaster Relief Fund (DRF) for relief efforts in response to Hurricanes Harvey, Irma, and Maria in late FY 2017 and wildfires in early FY 2018, as well as Congressionally approved debt relief for NFIP served to increase the Department's budget authority significantly in FY 2018.



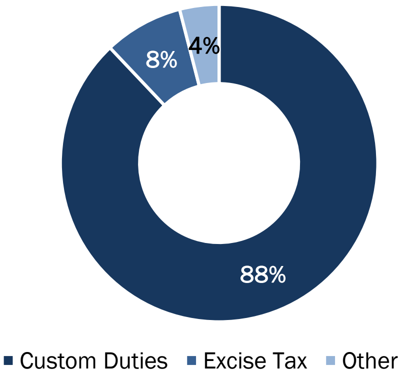
Of the total budget authority available, the Department incurred a total of $108 billion in obligations from salaries and benefits, purchase orders placed, contracts awarded, or similar transactions.

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 2018	FY 2017	$ Change	% Change
Cash Collections	$ 41,584	$ 34,835	$ 6,749	19%▲
Excise Tax	3,809	3,631	178	5%▲
Other	1,892	1,810	82	5%▲
Total Cash Collections	**$ 47,285**	**$ 40,276**	**$ 7,009**	17%▲

Custodial activity includes the revenue collected by the Department on behalf of others, and the disposition of that revenue to the recipient entities. Non-exchange revenue is either retained by the Department to further its mission or transferred to Treasury's general fund and other federal agencies. The Department's total cash collections is $47.3 billion. Total cash collections increased approximately $7 billion from FY 2017. Increased collections are related to several duty increases enacted by Executive Orders and/or as a result of United States Trade Representative investigations, including but not limited to, Steel and Aluminum imports and various products imported from China.



Custom duties collected by CBP account for 88 percent of total cash collections. The remaining 12 percent is comprised of excise taxes, user fees, and various other fees.

Other Key Regulatory Requirements

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

Secretary's Assurance Statement

November 14, 2018

The Department of Homeland Security management team is responsible for meeting the objectives of the Federal Managers' Financial Integrity Act of 1982 (FMFIA) by managing risks and maintaining effective internal control over three internal control objectives: effectiveness and efficiency of operations; reliability of reporting; and compliance with applicable laws and regulations. The Department conducted its assessment of risk and internal control in accordance with the Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. Based on the results of the assessment, the Department can provide reasonable assurance that internal control over operations, reporting, and compliance were operating effectively as of September 30, 2018 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 weaknesses related to Information Technology (IT) Controls and Systems Functionality stated above affects the Department's ability to fully comply with the Federal Financial Management Improvement Act of 1996 (FFMIA) financial management system requirements, and therefore the Department is also reporting a noncompliance with FFMIA.

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,

Kirstjen Nielsen
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.

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 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-compliances in internal control over operations, 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 2018, the Department continued to make progress in remediating material weaknesses in the areas of: 1) Financial Reporting and 2) IT Controls and System Functionality. Refer to Table 1: Internal Control over Financial Reporting Corrective Actions for details.

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

Area of Material Weakness	Component	Year Identified	Target Correction Date
	USCG, USSS, CBP, and FEMA	FY 2003	FY 2019
Financial Reporting	USCG, USSS, CBP, and FEMA experienced challenges with deficiencies in multiple financial management areas. These issues may include a combination of trading partner reconciliations, journal entries, third party service monitoring, non-routine transactions, 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. In FY 2018, the Department and USCG focused on implementing and executing manual compensating measures. USCG completed its root cause analysis resulting in additional and refined remediation strategy. USCG will increase monitoring and oversight over the implementation of the actuarial liability checklist review. USCG plans to complete its remediation by Q2 of FY 2019. In addition, the Department continues to pursue system modernization. USSS remediation strategy will be focused on properly resourcing financial operations who are adequately trained on key financial management procedures and internal controls, fully remediating property as well as fully implementing its processes and controls that changed its control environment due to the Oracle update in FY 2018. Management will be adding additional resources to the actuarial liability process at USSS to increase oversight. CBP remediation will be targeted on remaining corrective action milestones related to journal entries, third party service provider monitoring, and seized asset disclosures. To ensure non-routine transactions are handled properly (such as the FEMA transaction), DHS will review its Technical Accounting Issue Resolution process and include additional levels of management review based on the materiality of the transaction. 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.		
Area of Material Weakness	Component	Year Identified	Target Correction Date
	All DHS Components	FY 2003	FY 2020
IT Controls and System Functionality	The Department internal control assessment identified IT Controls and System Functionality as an area of 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	In FY 2018, DHS continued to implement the find, fix, and test strategy using a risk-based approach which allowed Components to focus on high impact systems further prioritized by FISCAM families. The focus was to test and find issues in systems that have not been fully assessed, while fixing prior and current year identified issues. Through this effort, DHS is postured to make significant progress in FY 2019 and downgrade the material weaknesses in FY 2020, evidenced by test of design and effectiveness.		

Federal Financial Management Improvement Act (FFMIA)

The Federal Financial Management Improvement Act of 1996 (FFMIA) requires that Federal agencies' financial management systems provide reliable financial data that complies with Federal financial management system requirements, applicable Federal accounting standards, and the U.S. Government Standard General Ledger (USSGL) at the transaction level.

OMB Circular A-123, Appendix D, Compliance with the Federal Financial Management Improvement Act of 1996, provides guidance the Department used in determining compliance with FFMIA. OMB's Appendix D provides a revised compliance model that entails a risk-and outcome-based approach to assess FFMIA compliance. The Department considered results of OIG and GAO audit reports, annual financial statement audits, the Department's annual Federal Information Security Modernization Act Report, and other relevant information. The Department's assessment also relies upon evaluations and assurances under the Federal Managers' Financial Integrity Act of 1982 (FMFIA), including assessments performed to meet the requirements of OMB Circular A-123 Appendix A. When applicable, particular importance is given to any reported material weakness and material non-conformance identified during these internal control assessments.

Based on the results of our overall assessment, the material weaknesses related to financial reporting and 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 weaknesses through significant compensating controls while undergoing system improvement efforts. The outcome of system improvement efforts will efficiently enable the Department to comply with government-wide requirements and reduce manual compensating controls. Refer to Table 1: Internal Control over Financial Reporting Corrective Actions for corrective actions to comply with FFMIA.

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. In April 2017, DHS successfully certified and submitted its first quarterly spending data for posting on USASpending.gov. In FY 2018, DHS continued to provide required quarterly submission by the due date and improved the match rate to 95.8% of dollars as of third quarter. This outpaces the benchmark established by DHS in its first fiscal year reporting (91.3% matching dollars). In addition, each Component was required to complete test of design and effectiveness over data consolidation and validation process. Based on the results of the assessment, management provides reasonable assurance that controls over the data consolidation and validation process is operating effectively. In FY 2019, DHS will implement its Data Quality Plan and will also implement a risk assessment process that enables DHS to identify and test high risk data elements, on a sample basis, to support the accuracy and validity at the data element transaction level.

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 2017 OIG FISMA audit report, *"Evaluation of DHS' Information Security Program for Fiscal Year 2017,"* the OIG identified five recommendations for the Department to improve Federal information security. As a result of corrective actions taken prior to June 2017, the OIG has closed four of the recommendations from the FY 2017 FISMA audit. The final OIG recommendation has been noted as resolved but will remain open pending receipt of DHS provided evidence.

The FY 2018 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 systems 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 made a significant investment in the financial management solution and migrated this solution to an alternative hosting environment in August 2018 to complete integration and implementation. This system solution delivers a standardized baseline for CWMD, TSA, and USCG, with increased functionality and integration for CWMD. In October 2018, TSA and USCG resumed implementation efforts while CWMD uses the current solution. DHS is leveraging the lessons learned from this shared services implementation, reducing risk in future migrations through deliberative approaches to program management, resource management, business process standardization, risk management, change management, and scheduling rigor and oversight.

In addition, USSS completed the move to the next version of their current accounting software, Oracle Federal Financials in FY 2018. Other FSM efforts in early stages, include 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.