Homeland Security

Agency Financial Report

Fiscal Year 2016

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

▶ We are DHS

About this Report

The *Department of Homeland Security* (DHS) *Agency Financial Report for Fiscal Year* (FY*) 2016* 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 2016, the Department is using the alternative approach—as identified in the Office of Management and Budget's Circular A-136—to produce its Performance and Accountability Reports, which consists of the following three reports:

- ***DHS Agency Financial Report***: Delivery date: November 15, 2016.
- ***DHS Annual Performance Report***: Delivery date: The *DHS Annual Performance Report* is submitted with the Department's Congressional Budget Justification.
- ***DHS Summary of Performance and Financial Information:*** Delivery date: February 15, 2017.

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

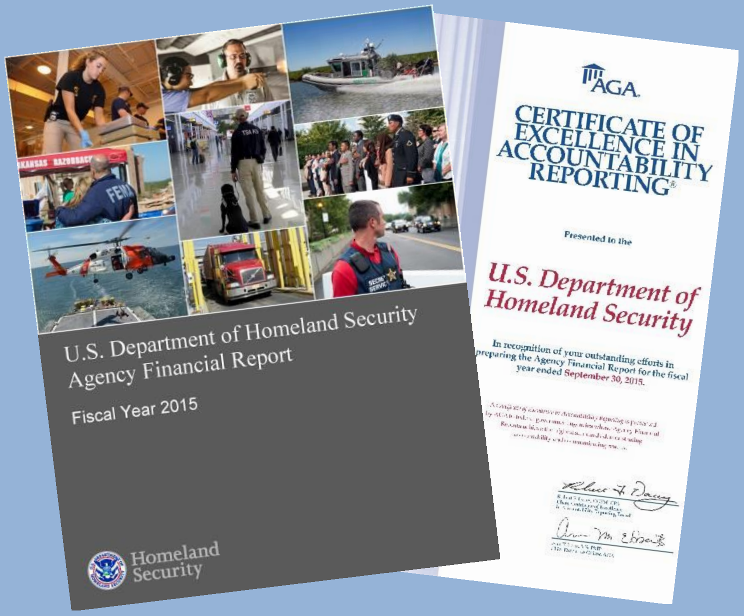
For more information, contact:

Department of Homeland Security
Office of the Chief Financial Officer
Office of Financial Management
245 Murray Lane, SW
Mailstop 200
Washington, DC 20528

Information may also be requested by sending an email to par@hq.dhs.gov.

Certificate of Excellence in Accountability Reporting

In May 2016, DHS received its third consecutive Certificate of Excellence in Accountability Reporting (CEAR) from the Association of Government Accountants (AGA) for its FY 2015 Agency Financial Report. The CEAR Program was established by the AGA, in conjunction with the Chief Financial Officers Council and the Office of Management and Budget, to further performance and accountability reporting.



U.S. Department of Homeland Security
Agency Financial Report
Fiscal Year 2015

Homeland
Security

AGA

CERTIFICATE OF EXCELLENCE IN ACCOUNTABILITY REPORTING®

Presented to the

U.S. Department of Homeland Security

In recognition of your outstanding efforts in preparing the Agency Financial Report for the fiscal year ended September 30, 2015.

[illegible]

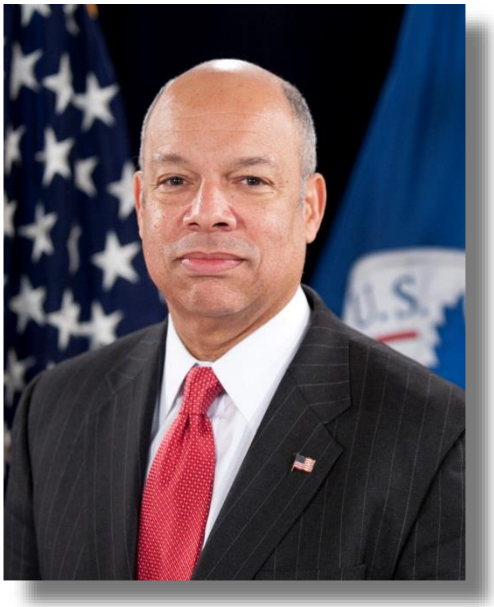
Visit Our Website
www.dhs.gov

Agency Financial Report

Fiscal Year 2016

Table of Contents

Message from the Secretary



November 14, 2016

I am pleased to present the Department of Homeland Security's (DHS) Agency Financial Report for Fiscal Year (FY) 2016. This report provides an assessment of the Department's detailed financial information and demonstrates how the resources entrusted to us were used to support our primary mission areas. This report also outlines our major goals and priorities. It illustrates our efforts to expand employee engagement and our commitment to strengthening Departmental Unity of Effort through improved processes and structure.

The new DHS mission statement we established this year serves as a capstone to our Unity of Effort initiative—"With honor and integrity, we will safeguard the American people, our homeland, and our values." This statement reflects the views and beliefs of our employees and was inspired by their comments.

As we work to fulfill this mission we must stay true to the core values of our nation including personal privacy, the freedom to travel, and the celebration of diversity among all our citizens no matter their race, gender, or nationality. While safeguarding our people and our homeland, we cannot isolate ourselves from the rest of the world. We must embrace and celebrate our differences while providing a secure and stable nation for all people.

An efficient, collaborative management system is key to the homeland security mission. Through the Unity of Effort initiative, we continually ensure that our programming, budgeting, and expenditures across the Department are mission-driven, cohesive, and transparent. We work together, across Components, to evaluate how our spending and programs can make the greatest impact toward achieving our mission.

We have strengthened our approach to the budget by focusing Department-wide on our mission needs. With the support of Congress, in FY 2017 we will fully implement a Common Appropriation Structure, which provides a simple, consistent structure across Components.

We have transformed our approach to acquisition by establishing the DHS-wide Joint Requirements Council to evaluate our Component's needs on the front-end of an acquisition. Additionally, all DHS major acquisition programs have approved life cycle cost estimates to help improve the Department's ability to deliver needed capability on time and on budget to secure our Nation.

In addition to strengthening our business processes, we have focused on improving employee morale over the past two years. It takes time to turn a workforce of more than 240,000 people in a different direction. I am pleased that after six straight years of decline, employee engagement at DHS went up three whole percentage points this year. We will continue to work to improve our engagement with employees and make DHS a workplace of choice.

Through our improved interaction and employee outreach, we are making advances toward operating together as a Department. As we continue to grow and mature as a Department, we remain keenly focused on the Department's five key mission areas: preventing terrorism and enhancing security; securing and managing our borders; enforcing and administering our immigration laws; safeguarding and securing cyberspace; and strengthening national preparedness and resilience.

Prevent Terrorism and Enhance Security

Preventing terrorist attacks on the homeland is the cornerstone of the Department's mission. Events over the past year in Brussels, Paris, San Bernardino, Orlando, and elsewhere are tragic reminders of the threats we face each day in our country and across the world. DHS's first priority remains protecting our nation from terrorist attacks. We are in a new phase of the global terrorist threat, requiring a new type of response. We have moved from a world of terrorist-directed attacks to a world of terrorist-inspired or enabled attacks where the terrorist may have never come face to face with a single member of a terrorist organization and self-radicalizes, inspired by something on the internet.

To combat these threats, our government and our coalition partners continue to take the fight militarily to terrorist organizations overseas. We have intensified our work with state and local law enforcement to share intelligence and information with Joint Terrorism Task Forces, fusion centers, local police chiefs, and sheriffs. Given the nature of the evolving terrorist threat, building bridges to diverse communities, particularly American Muslim communities, is also now a homeland security imperative.

Secure and Manage Our Borders

The Department has committed historic levels of front line personnel, technology, and infrastructure to border security in order to reduce the flow of illegal immigrants and illicit contraband while fostering legal trade and travel. Over the last 15 years, the number of apprehensions by the Border Patrol on our southwest border—an indicator of total attempts to illegally cross the border—has declined significantly. In FY 2016, total apprehensions by the Border Patrol on our Southwest Border, between ports of entry, numbered 408,870. This represents an increase over FY 2015, but was lower than FY 2014 and FY 2013, and a fraction of the number of apprehensions routinely observed from the 1980s through 2008.

Enforce and Administer Our Immigration Laws

Immigration is essential to our identity as a nation of immigrants. We continue to more sharply focus our enforcement resources on the identification and removal of public safety threats, criminal aliens, and other high-priority individuals. Our overarching goal is to enforce our immigration laws in a way that promotes public safety, national security, and border security.

Safeguard and Secure Cyberspace

Along with counterterrorism, cybersecurity remains a cornerstone of our Department's mission. Cyber threats are increasing in their frequency, scale, sophistication, and severity. This impacts everyone, both in the public and private sectors, across the country, and around the globe. Following the attacks on the Office of Personnel Management system last year, the Department launched an aggressive timetable for improving federal civilian cybersecurity through two principal systems. The first, EINSTEIN 3A, automatically blocks potential cyber intrusions on our federal systems and has already blocked over a million potential cyber threats. The second, Continuous Diagnostics and Mitigation (CDM), helps federal agencies detect and prioritize vulnerabilities inside their networks. In FY 2016, the Department provided CDM to 100 percent of the federal civilian government. Work must continue to streamline and strengthen existing functions within the Department to ensure we are prepared for the growing cyber threat and the potential for large scale attack.

Strengthen National Preparedness and Resilience

No matter the time of day or location on a map, a disaster can strike and overwhelm any of our Nation's communities. Flooding in Louisiana just a few months ago devastated the area. Working with other federal agencies, DHS opened 26 Disaster Recovery Centers, provided 63,000 families with housing assistance, and conducted over 114,000 home inspections. The Department is building a ready and resilient Nation by bolstering our preparedness and disaster response information sharing and collaboration.

Management Assurances and Performance Measurement

In FY 2016, the Department obtained its fourth consecutive unmodified audit opinion on all its financial statements. Because of robust policies and strong cooperation among management and all Components, I am able to provide reasonable assurance that the Department's financial information is complete and reliable. In addition, the Department continues to address internal control weaknesses, moving closer to our goal of achieving an unmodified internal control audit opinion. The Department is able to provide reasonable assurance that its internal controls over financial reporting are effective, with the exception of the three remaining material weaknesses identified in my Assurance Statement.

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

The Department's work to develop and implement the Common Appropriations Structure and our efforts to engage and involve staff at all levels show our continued commitment to improvement. We will continue to meet our challenges head-on, with a sense of urgency and purpose that the American people expect and that our mission requires. Thank you for your collaboration.

Sincerely,

Jeh Charles Johnson

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, its missions and goals, and provides an overview of our front-line 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, Statement of Custodial Activities, Stewardship Assets and Investments, and Limitations of Financial Statements.

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.

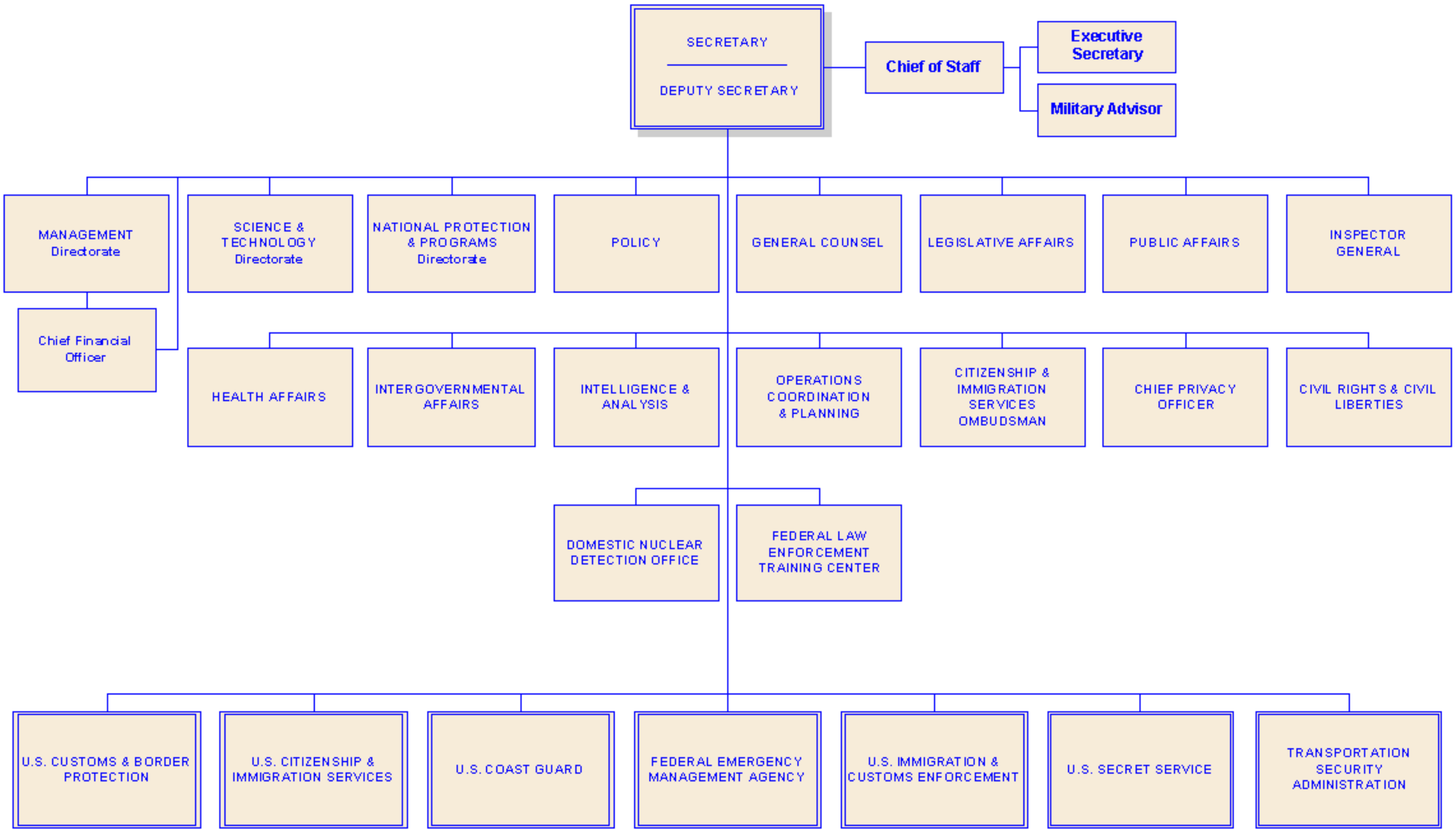
Overview

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, but our goal is clear—keep America safe.

Our Organization

DHS's operational Components lead the Department's front-line activities to protect our Nation. The enabling DHS Components provide resources, analysis, equipment, research, policy development, and support to ensure the front-line 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.

DHS Organizational Chart


SECRETARY
DEPUTY SECRETARY
Chief of Staff
Executive Secretary
Military Advisor
MANAGEMENT Directorate
Chief Financial Officer
SCIENCE & TECHNOLOGY Directorate
NATIONAL PROTECTION & PROGRAMS Directorate
POLICY
GENERAL COUNSEL
LEGISLATIVE AFFAIRS
PUBLIC AFFAIRS
INSPECTOR GENERAL
HEALTH AFFAIRS
INTERGOVERNMENTAL AFFAIRS
INTELLIGENCE & ANALYSIS
OPERATIONS COORDINATION & PLANNING
CITIZENSHIP & IMMIGRATION SERVICES OMBUDSMAN
CHIEF PRIVACY OFFICER
CIVIL RIGHTS & CIVIL LIBERTIES
DOMESTIC NUCLEAR DETECTION OFFICE
FEDERAL LAW ENFORCEMENT TRAINING CENTER
U.S. CUSTOMS & BORDER PROTECTION
U.S. CITIZENSHIP & IMMIGRATION SERVICES
U.S. COAST GUARD
FEDERAL EMERGENCY MANAGEMENT AGENCY
U.S. IMMIGRATION & CUSTOMS ENFORCEMENT
U.S. SECRET SERVICE
TRANSPORTATION SECURITY ADMINISTRATION

Our Components

The following is a description of the major Components that make up the Department of Homeland Security. Components listed below are those for which Congress appropriates funds through the budget process, whereas the Components in the financial reporting section are those tracked in the Treasury Information Executive Repository system presented in Note 1.A in the Financial Section. Click on the Component name for more information on their website. Operational Components are presented in the order they appear on the bottom of the organizational chart. The enabling Components are listed in alphabetical order.

Operational Components

U.S. Customs and Border Protection (CBP) is one of the Department of Homeland Security's largest and most complex Components, with a priority mission of keeping terrorists and their weapons out of the U.S. It also has a responsibility for securing and facilitating trade and travel while enforcing hundreds of U.S. regulations, including immigration and drug laws.

U.S. Citizenship and Immigration Services (USCIS) secures America's promise as a nation of immigrants by providing accurate and useful information to our customers, granting immigration and citizenship benefits, promoting an awareness and understanding of citizenship, and ensuring the integrity of our immigration system.

U.S. Coast Guard (USCG) is one of the five armed forces of the United States and the only military organization within the Department of Homeland Security. The Coast Guard protects the maritime economy and the environment, defends our maritime borders, and saves those in peril.

Federal Emergency Management Agency (FEMA) supports our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

U.S. Immigration and Customs Enforcement (ICE) promotes homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.

U.S. Secret Service (USSS) safeguards the Nation's financial infrastructure and payment systems to preserve the integrity of the economy, and protects national leaders, visiting heads of state and government, designated sites, and National Special Security Events.

Transportation Security Administration (TSA) protects the Nation's transportation systems to ensure freedom of movement for people and commerce.

Enabling Components

Analysis and Operations includes the Office of Intelligence and Analysis (I&A) and the Office of Operations Coordination (OPS). I&A equips the Homeland Security Enterprise with the timely intelligence and information it needs to keep the homeland safe, secure, and resilient. OPS is responsible for monitoring the security of the United States on a daily basis and coordinating activities within the Department and with governors, Homeland Security Advisors, law enforcement partners, and critical infrastructure operators in all 50 states and more than 50 major urban areas nationwide.

Departmental Management and Operations (DMO) provides support to the Secretary and Deputy Secretary in the overall leadership, direction, and management to the Department and all of its Components, ensuring the delivery of effective and efficient business and management services. DMO is responsible for budget, appropriations, expenditure of funds, accounting and finance; procurement; human resources and personnel; information technology systems; facilities, property, equipment, and other material resources; and identification and tracking of performance measurements relating to the responsibilities of the Department.

Domestic Nuclear Detection Office (DNDO) works to prevent nuclear terrorism by continuously improving capabilities to deter, detect, respond to, and attribute attacks, in coordination with domestic and international partners.

Federal Law Enforcement Training Centers (FLETC) provide career-long training to law enforcement professionals to help them fulfill their responsibilities safely and proficiently.

National Protection and Programs Directorate (NPPD) advances the Department's risk-reduction mission. Reducing risk requires an integrated approach that encompasses both physical and virtual threats and their associated human elements.

Office of Health Affairs (OHA) provides medical, public health, and scientific expertise in support of the DHS mission to prepare for, respond to, and recover from all threats.

Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (Pub. L. 107-296) by an amendment to the Inspector General Act of 1978. OIG has a dual reporting responsibility to the Secretary of DHS and to Congress. OIG serves as an independent and objective audit, inspection, and investigative body to promote economy, effectiveness, and efficiency in DHS programs and operations, and to prevent and detect fraud, waste, and abuse.

Science and Technology Directorate (S&T) is the primary research and development arm of the Department. It provides federal, state, and local officials with the technology and capabilities to protect the homeland.

Our Strategic Framework

Performance and financial information in this report is organized around the missions and goals identified in the Department's FY 2014-2018 Strategic Plan. The FY 2014-2018 Strategic Plan continues the Department's efforts to prioritize front-line operations while maximizing effectiveness and efficiency. The missions, goals, and our mature and strengthen goals of the Department are provided below.

Mission 1: Prevent Terrorism and Enhance Security

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

Mission 2: Secure and Manage Our Borders

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

Mission 3: Enforce and Administer Our Immigration Laws

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

Mission 4: Safeguard and Secure Cyberspace

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

Mission 5: Strengthen National Preparedness and Resilience

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

Mature and Strengthen Homeland Security

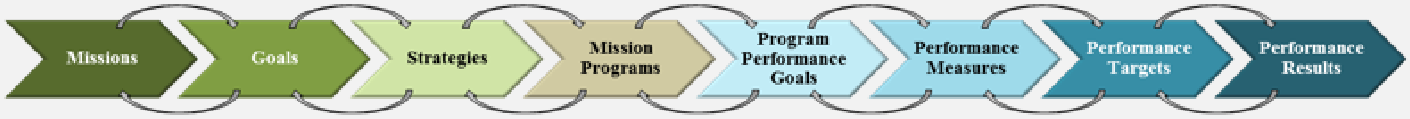
- Goal 1: Integrate Intelligence, Information Sharing, and Operations
- Goal 2: Enhance Partnerships and Outreach
- Goal 3: Strengthen the DHS International Affairs Enterprise in Support of Homeland Security Missions
- Goal 4: Conduct Homeland Security Research and Development
- Goal 5: Ensure Readiness of Frontline Operators and First Responders
- Goal 6: Strengthen Service Delivery and Manage DHS Resources

Performance Overview

The Performance Overview provides a summary of each homeland security mission, selected accomplishments, key performance measures, 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 2016-2018 Annual Performance Report with the FY 2018 Congressional Budget and can be accessed at: http://www.dhs.gov/performance-accountability.

Performance Management in DHS

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. In the following section, we describe our performance management framework and how this gets implemented. A subset of results is made available in this section of the Agency Financial Report. For the full set of measures the Department uses to gauge the delivery of results aligned to our strategy, see the DHS Annual Performance Report.



Missions:	Describes at the highest level what the Department aims to achieve.
Goals:	A goal is a statement of aim or purpose included in the Department's Strategic Plan to achieve the mission. Goals are the overarching structure used to group multiple strategies and associated program performance goals to influence achievement of the Department's missions.
Strategies:	A strategy is a statement in the Department's Strategic Plan that describes a targeted area of action to support achievement of the related Department goal.
Mission Programs:	Organized set of activities acting together to accomplish specific high-level outcomes external to an organization. Mission programs are the operational processes, skills, technology, human capital, and other resources leveraged to achieve program performance goals and the Department's missions and goals.
Program 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. Program performance goals are understood in terms of their associated performance measures and performance targets, which express the tangible objective against which actual achievement can be compared.
Performance Measures:	This is an indicator, statistic, or metric used to gauge program performance and assess progress in meeting the program performance goal, and in turn the missions, goals, and strategies of the Department.
Performance Targets:	A target is the projected level of performance for each performance measure during a fiscal year. A target is a measureable characteristic that 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.

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. Achieving this vision requires us to focus on the core goals of preventing terrorist attacks, preventing and protecting against the unauthorized acquisition or use of chemical, biological, radiological, and nuclear materials and capabilities; and reducing risk to the Nation's most critical infrastructure, key leaders, and events.

Our goals for this mission are:

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

Demonstrating Innovative Solutions

In FY 2016, the Transportation Security Administration (TSA) established the Innovation Task Force (ITF) to conduct field demonstrations of emerging capabilities. Through data and information sharing, partnering with stakeholders across the aviation sector, and fostering a platform for innovation, ITF aims to promote rapid development of new solutions and to refine requirements and processes. The goal of the ITF is to enhance TSA's ability to respond to an evolving terrorist threat and a dynamic screening environment.

The ITF established Hartsfield-Jackson Atlanta International Airport (ATL) as an innovation site and demonstrated Automated Screening Lanes (ASLs) in partnership with Delta Air Lines. The ASLs demonstration (which included automated bin returns, multiple divestiture stations, and enhanced bin tracking and data capabilities) was recognized by partner airlines, vendors, and travelers for its expediency, and for reducing wait times and improving the passenger experience. Senator Tom Carper commented, "This partnership between Delta and TSA's Innovation Task Force in Atlanta could—and should—serve as a model for other airports across the country as one of many smart solutions that could make flights more secure while also making the screening process less of a burden for passengers, airlines, and airports."

Success at ATL has encouraged expansion of ITF to target airports around the country for additional demonstrations and next-generation solutions. As TSA Administrator Peter Neffenger recognized, "[ITF] already succeeded in that they are thinking differently. It's an example of how we're changing the way we think as a system."

The following highlighted measures gauge our efforts to prevent terrorism and enhance security. Explanations of results, trend analysis, and corrective actions are provided for each measure as appropriate.

Percent of international air enplanements vetted against the terrorist watch list through Secure Flight (TSA)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
100%	100%	100%	100%	100%	100%

TSA has maintained a 100 percent vetting of international travelers against the terrorist watch list for the past five years. The Secure Flight program is a risk-based passenger prescreening system that enhances security by assessing passengers' potential risk before they arrive at the airport by matching their names against trusted traveler lists and watchlists. This serves to prevent individuals on the No Fly List from boarding an aircraft and to identify individuals for enhanced screening. After matching passenger information against government watch lists, Secure Flight transmits the matching results back to airlines before they can issue passenger boarding passes.

Percent of daily passengers receiving expedited physical screening based on assessed low risk (TSA)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
---	---	---	---	50%	46.3%

This measure was introduced to gauge 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 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 risk-based, intelligence-driven security procedures and enhancing its use of technology in order to focus its resources on the unknown traveler. In FY 2016, TSA achieved 46.3 percent, missing expectations for the first year of this measure. At the start of the fiscal year, TSA removed certain groups receiving expedited screening based on a reassessment of the risk analysis. This safety decision impacted the program's ability to reach its target. TSA is currently investigating ways to continue to grow the TSA Pre✓® enrolled population.

Percent of containerized cargo conveyances that pass through radiation portal monitors at sea ports of entry (DNDO)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
FOUO	FOUO	FOUO	FOUO	FOUO	FOUO

This measure gauges the amount of containerized cargo scanned by radiation portal monitors deployed to the Nation's sea ports of entry. Radiation portal monitors are acquired, installed, and maintained by DNDO and are used by CBP in day-to-day operations to scan incoming cargo to detect and identify dangerous nuclear and radiological sources. Although the actual results are For

Official Use Only (FOUO), this measure continues to perform at a high level, attaining its target for this fiscal year and the previous four years.

Percent of performance standards implemented by the highest risk chemical facilities and verified by DHS (NPPD)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
---	46%	78%	93%	95%	97%

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. Since the CFATS program was created, the Department has engaged with industry to identify and regulate high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with the possession of chemicals of interest. This measure reports the percent of risk based performance standards that are approved and implemented within site security plans or alternative security programs for Tier 1 and Tier 2 facilities that are compliant with the CFATS regulation. By the end of FY 2016, DHS delivered guidance and requirements to the highest risk chemical facilities, prompting these owners and operators to include 7,591 specific security improvements in their security plans in order to satisfy the risk-based performance standards, meeting the target and improving over the previous year.

Security compliance rate for high-risk maritime facilities (USCG)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
98.7%	99.3%	99.3%	99.6%	100%	97.6%

The Maritime Transportation Security Act of 2002 (MTSA) requires vessels and port facilities to conduct vulnerability assessments and develop security plans that may include passenger, vehicle and baggage screening procedures; security patrols; establishing restricted areas; personnel identification procedures; access control measures; and/or installation of surveillance equipment. MTSA facilities are a high risk subset of the national waterfront facility population given the nature of their activities and/or the products they handle which pose a greater risk for significant loss of life, environmental damage, or economic disruption if attacked. The USCG completes one scheduled and one unscheduled inspection on each facility annually and had a 97.6 percent compliance rate in FY 2016, slightly down from previous years. Facilities which have problems are given a notice of violation and/or civil penalty.

Percent of protectees that arrive and depart safely (USSS)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
---	---	---	100%	100%	100%

This measure achieved 100 percent in FY 2016 and it is expected USSS will continue this level of excellence in the future as they have set their targets to always be 100 percent for their protective mission. This measure was introduced in FY 2015 to better assess USSS protection activities by gauging the percent of travel stops where USSS protectees arrive and depart safely.

Percent of National Special Security Events that were successfully completed (USSS)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
100%	100%	100%	100%	100%	100%

This measure is a percent of the total number of National Special Security Events (NSSE) completed in a Fiscal Year where once the event commenced, a security incident(s) inside a USSS protected venue did not preclude the event's agenda from proceeding to its scheduled conclusion. These events require a tremendous amount of preplanning and coordination with numerous federal, state, and local jurisdictions. USSS has attained 100 percent for the past five years.

2016 Republican and Democratic National Conventions

The 2016 Republican National Convention (RNC) and Democratic National Convention (DNC) were the 53rd and 54th events of national significance (since September 1998) to be designated NSSEs. The USSS was the lead federal agency for operational security planning and implementation for both the 2016 RNC and DNC. The USSS initiated operational security planning for these events nearly 12 months prior to the conventions, and the successful completion of these NSSEs was the result of the coordinated efforts of a myriad of federal, state and local agencies, including other Components of DHS.

USSS RNC and DNC event coordinators invited major stakeholders to be members of an executive steering committee in each city to oversee the development of a custom operational security plan for each convention. In addition, the event coordinators recruited subject matter experts, representing more than 50 law enforcement, public safety, and military entities, to be members of nearly two-dozen subcommittees. The subcommittees were responsible for developing various aspects of these event security plans, from airspace security and crowd management to transportation security and tactical coordination, from intelligence/counterterrorism and critical infrastructure protection to explosive device response and interagency communication. Extensive and realistic multi-agency tabletop exercises, joint tactical and other practical exercises took place weeks prior to the conventions to ensure that operational security plans would work as intended. All of this preparation led to the successful completion of these vital NSSEs.

Looking Forward

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

TSA Embracing Covert Testing to Identify Gaps

DHS continues to heed lessons learned from the Office of Inspector General covert testing in the summer of 2015, and remains dedicated to security effectiveness during an unprecedentedly busy travel year. Numerous plans and programs are helping to alleviate long lines while ensuring the safety of the flying public. Future plans focus on the professionalization of Transportation Security Officers (TSOs) which includes transitioning more of the front line workforce from part-time to full-time, increasing the number of TSOs to reduce wait times and allow for a surge capability, and providing standardized professional training and development. TSA will also leverage and expand their canine teams to provide more security throughout the transportation sector, including passenger screening. The Department will also be coordinating on next generation technology for passenger and baggage screening via Integrated Product Teams (IPTs) and the Innovation Task Force by conducting field demonstrations of emerging capabilities. IPTs will closely coordinate front line operations and emerging threats to ensure TSA has cutting edge technology to reduce wait times while effectively identifying threats.

Expanding Intelligence and Information Sharing to Increase Domain Awareness

The Department continues to integrate the DHS Intelligence Enterprise (IE) and increase the flow of intelligence and information across the IE, through the DHS Data Framework, and with its federal, state, local, tribal, and territorial partners to support the Department's diverse missions and detect threats to the homeland. The IE is developing comprehensive training programs and analytic tools, which will enhance the Department's intelligence picture and collection capabilities. To support the Department's screening and vetting missions, the IE is increasing access to open source social media platforms to compare unclassified data with classified data and leveraging all available sources to identify bad actors. Moving forward, the Department and its Components are developing robust counterintelligence programs to counter threats from foreign intelligence entities and insider threats. All of this should empower the Department to leverage risk-based approaches and provide an efficient and effective way to prevent terrorist attacks.

Chemical, Biological, Radiological, and Nuclear (CBRN) Mitigation Efforts

DHS engages with international, federal, state, local, territorial, tribal, and private sector partners to counter CBRN threats. Efforts include working on sector-specific facility security planning, training, exercises, guidance documents, and developing technology solutions collaboratively to increase capabilities to mitigate CBRN threats. DHS efforts are coordinated at multiple levels—within DHS and with our many partners and stakeholder—to ensure effective solutions are applied to mitigate risk, improve current capabilities, and leverage new technologies and tools to ensure the safety and security of the United States. Moving forward, this work will then be integrated with the planning for the international Global Nuclear Detection Architecture to include: integrating interagency efforts to develop and acquire radiological and nuclear detection technologies; evaluating detector performance; ensuring effective response to detection alarms; and conducting transformational research and development for radiological and nuclear detection and forensics technologies.

Protecting the Nation's Critical Infrastructure, Key Leadership, and Events

USSS continues to make progress on implementing recommendations from the Protective Mission Panel and House Oversight and Government Reform Committee in three key areas: personnel and training; technology, perimeter security and operations; and leadership. Through Operational

Mission Support initiatives, USSS has acquired and implemented advanced protective countermeasures to improve security operations and protection at the White House Complex, the Vice President's Residence, and temporary sites. These improvements include protection from emerging explosive, chemical, biological, radiological, and cyber threats and investing in the modernization and support of mission-critical IT systems and infrastructure for protective and investigative mission operations. USSS will continue in the coming year to work towards achieving its staffing goals by pursuing retention initiatives to reduce its annual attrition and following aggressive hiring and training plans.

Mission 2: Secure and Manage Our Borders

A safe and secure homeland requires that we secure our air, land, and sea borders and disrupt and dismantle transnational criminal and terrorist organizations while facilitating lawful travel and trade.

Our goals for this mission are:

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

Another Cross-border Drug Tunnel Dismantled

Federal officials seized a cross-border tunnel on the morning of March 23, 2016 following a lengthy multi-agency investigation that resulted in six arrests and the confiscation of more than a ton of marijuana. The tunnel—more than 400 yards in length— stretches from the former El Sarape Restaurant, now a coffee shop, in Mexicali, Mexico, to a two-bedroom Calexico residence located at 902 E. Third Street, about 300 yards north of the international border. In the front room of the residence, agents found a hole concealed in the floor about three feet in diameter with an opening that descends several feet beneath the foundation.

This is the first operational tunnel discovered in Calexico in nearly a decade. According to federal investigators, it also represents the first time drug traffickers are known to have purchased property and constructed a house for the sole purpose of concealing the exit of a subterranean drug tunnel. The search warrant affidavit and charging documents allege the traffickers scouted properties in the area and selected the Third Street parcel in a residential section of Calexico. The sale of the property for $240,000 was finalized by the defendants in April 2015.

"This significant cross-border drug seizure and tunnel discovery is an excellent example of the integrated efforts taking place daily across multiple law enforcement agencies to protect America by providing secure borders," said El Centro Sector Chief Patrol Agent Rodney S. Scott. "This tunnel discovery is further proof that America's investment in border security is paying off. As we continue to improve border security, criminal organizations are forced to resort to tunneling and other complicated and costly smuggling methods, which increases their exposure to detection by law enforcement."

Rate of interdiction effectiveness along the Southwest Border between ports of entry (CBP)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
---	---	79.28%	81.01%	81%	82.67%

This measure reports the percent of detected illegal entrants who were apprehended or turned back after illegally entering the United States between the ports of entry on the southwest border. The Border Patrol achieves this desired strategic outcome by maximizing the apprehension of detected illegal entrants or confirming that illegal entrants return to the country from which they entered; and by minimizing the number of persons who evade apprehension. In FY 2016, this measure achieved 82.67 percent, which is roughly a 1.5 percent increase from FY 2015. It should be noted that resources are deployed to those areas deemed to be the highest risk and as undocumented aliens are turning themselves in, the interdiction effectiveness rate is able to reflect a higher capability to respond than our resources might otherwise allow.

Migrant interdiction effectiveness in the maritime environment (USCG)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
---	---	---	74.8%	74%	79.3%

This measure reports the percent of detected undocumented migrants of all nationalities who were interdicted by the USCG and partners via maritime routes. Thousands of people try to enter this country illegally every year using maritime routes. USCG conducts patrols and coordinates with other federal agencies and foreign countries to interdict undocumented migrants at sea, denying them entry via maritime routes to the United States, its territories and possessions. Interdicting migrants at sea means they can be quickly returned to their countries of origin without the costly processes required if they successfully enter the United States. In its second year of reporting, the USCG achieved 79.3 percent migrant interdiction effectiveness, up significantly from FY 2015. This increase is due primarily to the deployment of additional USCG assets, including a medium endurance cutter, in order to respond to a 64.5 percent increase in Cuban migrant flow across the South Florida Straits over the same time period last year. Cuban migrants made up 71.3 percent of the total known maritime migrant flow in last quarter of FY 2016.

Percent of inbound cargo identified by CBP as potentially high-risk that is assessed or scanned prior to departure or at arrival at a U.S. port of entry (CBP)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
98.00%	98.00%	99.22%	99.76%	100%	99.28%

This measure gauges the percent of international cargo coming to the United States via air, land, and sea identified as potentially high-risk, using the Automated Targeting System, that is assessed or scanned prior to loading or at arrival at a U.S. port of entry. Assessing, resolving, and when necessary scanning potentially high-risk cargo prior to loading or at arrival at ports of entry improves the safety of the U.S. public and minimizes the impact to the trade community through the effective use of risk-focused targeting. The results did not achieve the aspirational goal of 100 percent, and are slightly down from last year due to a change in the targeting methodology. The CBP Office of Field Operations will continue to work diligently to improve targeting algorithms within the Automated Targeting System as well as improvements to procedures, logistics, and scheduling with shippers and carriers.

Percent of imports compliant with U.S. trade laws (CBP)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
96.46%	97.66%	97.99%	98.89%	97.5%	99.18%

This measure reports the percent of imports that are compliant with U.S. trade laws including customs revenue laws. Ensuring that all imports are compliant and free of major discrepancies allows for lawful trade into the United States. 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. In FY 2016, 99.18 percent of imports were found to be compliant with U.S. trade laws. Results continue to improve and are at a five-year high.

ICE Makes 84 Arrests in PA, DE, and WV during Targeted Operation

In May 2016, Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations concluded a week-long enforcement operation targeting criminal aliens and other immigration violators.[1] During the operation, part of a larger agency effort prioritizing the arrest and removal of convicted criminal aliens as well as other illegally present enforcement priorities, Officers arrested 84 individuals in Pennsylvania, Delaware, and West Virginia. The arrested targets, all of whom fell under enforcement priorities set forth in DHS Secretary Johnson's 2014 memorandum, possessed convictions for corruption of a minor, robbery, felony fraud, and cocaine and heroin possession, among other crimes.

Prioritized enforcement efforts allow ICE to focus its resources on the most egregious offenders, including convicted criminals and public-safety threats to the community.

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. Thus, border security cannot begin simply at our borders. Below are a few initiatives that advance our efforts to secure and manage our borders.

[1] See ICE Newsroom, "ICE Arrests 84 in PA, DE, WV during operation targeting criminal aliens," https://www.ice.gov/news/releases/ice-arrests-84-pa-de-wv-during-operation-targeting-criminal-aliens

Joint Task Force (JTF) Implementation

On November 20, 2014, Secretary Johnson directed the creation of the Southern Border and Approaches Campaign—a unified approach to improve how the Department protects the homeland across our southern borders. The campaign will harness and more effectively coordinate the assets and personnel of CBP, ICE, the USCG, and other resources of the Department. The intent of this campaign is better coordination in enforcement and interdiction across land, sea, and air; to degrade transnational criminal organizations; and to do these things while still facilitating the flow of lawful trade, travel, and commerce across our borders. Moving forward, the Department will continue to engage the joint task force approach. This consists of: 1) JTF-East, which is responsible for our southeast maritime approaches; 2) JTF-West, which is responsible for our southwest land border; and 3) JTF-Investigations, which supports the work of the other two task forces and focuses on investigations throughout the Nation and with our foreign partners.

Biometrics Exit Program

Included in the *Intelligence Reform and Terrorism Prevention Act of 2004*, Congress directed DHS to enhance security of the U.S. border and immigration system through the development of a Biometric Air Entry and Exit System. The biometric entry system is in place and the 2016 Consolidated Appropriations Act authorized DHS to collect up to $1 billion over a period of up to 10 years through USCIS fees for the implementation of a biometric exit program across all modes of travel. The collection of these funds began in 2016 and is expected to be about $115 million per year until the $1 billion is collected in 2024. CBP is developing and deploying a biometric exit system where traveler identities are biometrically-verified upon exit from the United States at air, sea, and land ports of entry. There are four Biometric Pilots in place at ports of entry around the country that incorporate multiple modes of biometric verification to include fingerprints, iris scan, and new facial comparison scans. Current CBP estimates indicate that $1 billion in fees will cover the initial solution investment and deployment to the top 20 gateway airports. Additional funding will be necessary to fully cover the salaries and expenses associated with full deployment and sustainment beyond 2024. CBP expects to begin implementing a biometric air exit solution at airports by the end of fiscal year 2018. Planning for the sea and land Ports of Entry are underway and expected to be initiated in fiscal year 2020; however funding requirements and solutions are still being developed.

Trade Enforcement Act Implementation

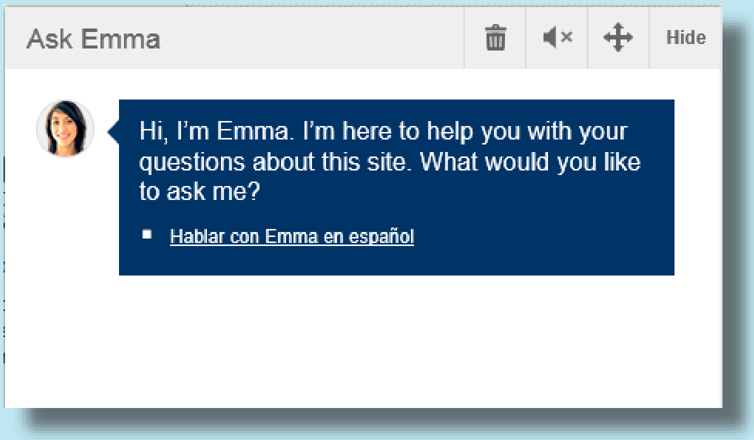
With the signing of the Trade Facilitation and Trade Enforcement ACT (TFTEA) on February 24, 2016, Congress and the Administration sent a clear signal that security through U.S. economic competitiveness and enforcement of our trade laws and regulations is one of the country's highest priorities. TFTEA is one of the most significant pieces of trade legislation for CBP in over a generation and includes major changes to trade enforcement, particularly in the area of anti-dumping. An advantage of the Act for CBP is that it provides opportunities for greater facilitation of lawful trade, such as the modernization of the drawback process for duty refunds. The Act also authorizes funding for the single window portal known as the Automated Commercial Environment (ACE) system which will be the primary system through which the trade community will report imports and exports and the government will determine admissibility.

Mission 3: Enforce and Administer Our Immigration Laws

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

Our goals for this mission are:

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



Hi, I'm Emma. I'm here to help you with your questions about this site. What would you like to ask me?

- Hablar con Emma en español

USCIS Uses Technology to Level the Playing Field for Immigrants

U.S. Citizenship and Immigration Services is leveraging technology to create multi-channel tools that give customers faster and easier access to immigration information, when and where they need it.

The flagship of the new suite of tools is *myUSCIS*, an online one-stop shop for immigration information. It includes an Explore My Options tool, civics practice test, citizenship class locator, and Find a Doctor, all of which are accessible from any mobile device, anytime, anywhere. *myUSCIS* saw nearly 3 million sessions in its first year.

myUSCIS is joined by Emma, an interactive tool that helps customers get answers to their immigration questions in plain English or Spanish. In just over 6 months, Emma responded to more than 2.7 million inquiries from more than 730,000 visitors. Ninety percent of English-speaking individuals and 85 percent of Spanish-speaking individuals were successful when using Emma to answer their questions.

USCIS is garnering a reputation as a leader in digital services for fundamentally transforming how it serves a multifaceted, mobile, and sometimes vulnerable, customer base. Public and private agencies have validated USCIS' latest innovations with several prestigious awards and recognition.

Average of processing cycle time (in months) for naturalization applications (N-400) (USCIS)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
4.6	4.7	5.5	5.0	≤ 5.0	5.8

The N-400, Application for Naturalization, is filed by an individual applying to become a U.S. citizen. Naturalization applications were 26 percent higher than projected in FY 2016 resulting in a 5.8 month average cycle time. Results are consistent with prior year results when application volume is taken into account. USCIS will continue to focus on quality, employee training, workload shifting, technology enhancements, and supervisory engagement to increase the efficiency of case processing.

Percent of customers satisfied with the citizenship and immigration-related support received from the National Customer Service Center (USCIS)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
93%	87%	86%	88%	85%	85%

This measure gauges the overall rating of the immigration process and is based on the results from the following areas: 1) accuracy of information; 2) responsiveness to customer inquiries; 3) accessibility to information; and 4) customer satisfaction. The FY 2016 result for this measure, 85 percent, is consistent with the results for the past four years and is indicative of the attention USCIS has given to the customer service approach. In addition, these results continue to exceed industry customer satisfaction averages. Throughout the year, USCIS has met the target by constantly listening to customer feedback and taking deliberate steps to improve the level of service provided to its customers.

Percent of applications for citizenship and immigration benefits not approved following a potential finding of fraud (USCIS)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
---	---	---	---	90%	91.3%

This measure reflects the Department's capacity to prevent fraud, abuse, and exploitation of the immigration system, and address 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 is the first year this measure is reporting results and exceeded expectations achieving, 91.3 percent.

Percent of detention facilities found in compliance with the national detention standards by receiving an acceptable inspection rating (ICE)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
97%	100%	100%	100%	100%	100%

ICE's Enforcement and Removal Operations (ERO) manages and oversees the Nation's civil immigration detention system. ICE detainees placed in ERO custody represent virtually every country in the world, various security classifications, both genders, and medical conditions ranging from healthy to terminally ill. Through an aggressive inspections program, ICE ensures its facilities follow ICE's National Detention Standards. While not all facilities may be found to be at standard on the initial assessment, ICE works with those facilities to ensure any shortfalls are addressed to meet the 100 percent compliance rate. ERO's Detention Standards Compliance Unit ensures that detainees in ICE custody reside in safe, secure, and humane environments and under appropriate conditions of confinement. For the fourth straight year, detention facilities found in compliance was 100 percent.

Special High Risk Charter (SHRC) Missions

ICE's Air Operations (IAO) Division, in conjunction with the Removal Management Division (RMD), has the duty and responsibility to plan and conduct SHRC flights to repatriate alien nationals who have "Failed to Comply" with their removal order, or those that cannot be removed by normal commercial air transportation to Europe, Central Asia, the Pacific Rim, Africa, and the Middle East.

IAO conducted 27 SHRC flights in FY 2016 resulting in more than 250 removals of people to dozens of countries, which includes flights to 16 new countries due to continuing efforts to repatriate individuals. This level of activity shattered previous year's SHRC removals.

In order to achieve greater success in FY 2016, IAO focused on improving its efficiency and effectiveness in the planning and execution of SHRC missions. Specifically, IAO focused on increasing its overall communication with all stakeholders which led to an increase in productivity in planning and completing SHRC missions. As a direct result of implementing newly identified operational efficiencies and creating an environment fostering a collaborative approach, FY 2016 SHRC missions have been completed with minimal issues.

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. Enforcement efforts must prioritize the identification and removal of dangerous foreign nationals who threaten our national security or the safety of our communities and must include safe and humane detention conditions and respect for due process and civil rights, as accorded by law. Below are a few initiatives that advance our efforts to achieve the Department's immigration enforcement and administration goals.

U.S. Citizenship and Immigration Services' Improvement Plans

USCIS secures America's promise as a nation of immigrants by granting citizenship and immigration benefits, promoting awareness and understanding of citizenship, ensuring the integrity of the immigration system, and providing accurate and useful information to its customers. On an average day, USCIS: completes 24,000 applications for various immigration benefits; welcomes 3,200 new citizens; answers 44,000 phone calls to our toll-free customer service line; serves 9,500 customers at 84 local offices; fingerprints and photographs 15,000 applicants at 136 application support centers; conducts 148,000 national security background checks; and processes 2,040 petitions filed by employers to bring workers to the United States. USCIS recently leveraged a suite of technology tools that give customers faster and easier access to immigration information. The flagship of the new suite of tools is *myUSCIS*, an online one-stop shop for immigration information. To improve the customer experience moving forward, USCIS will make enhancements to these tools that expand the value, relevance, and reach for customers and stakeholders.

Priority Enforcement Program (PEP)

DHS's Priority Enforcement Program (PEP) enables DHS to work with state and local law enforcement to take custody of individuals who pose a danger to public safety before those individuals are released into our communities. ICE works in more than 4,300 federal, state, and local prisons and jails throughout the country. Under PEP, ICE will seek the transfer of a removable individual when that individual has been convicted of an offense listed under the DHS civil immigration enforcement priorities, has intentionally participated in an organized criminal gang to further the illegal activity of the gang, or poses a danger to national security. PEP begins at the state and local level when an individual is arrested and booked by a law enforcement officer for a criminal violation. PEP relies on the fingerprint-based biometric data submitted during the book-in process to determine whether the individual is a priority for removal. While biometric interoperability makes PEP more efficient, effective, and accurate, it only provides awareness of a criminal's arrest. ICE officers are still required to interview the identified individual. To ensure PEP's success, DHS continues to engage in significant outreach to external stakeholders and law enforcement partners to educate them about PEP and how PEP differs from the previous program known as Secure Communities. A number of cities and counties that previously did not work with ICE are now doing so under PEP. In particular, the following large U.S. counties are participating in PEP: Los Angeles and San Diego Counties in California, Hillsborough and Pinellas Counties in Florida, and Baltimore County in Maryland.

Mission 4: Safeguard and Secure Cyberspace

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

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

Cyber Storm V: National Cyber Exercise

In March 2016, more than 1,100 people from more than 60 organizations across the country and worldwide participated in Cyber Storm V, the Nation's most extensive cybersecurity exercise which was conducted over three days.

Hosted by the Department of Homeland Security, participants ranging from across government, critical infrastructure, and the private sector were presented with a scenario. New participants included the public health sector and the retail sector. This scenario required participants to exercise their training, policies, processes, and procedures for identifying and responding to a multi-sector cyberattack targeting critical infrastructure. The Cyber Storm V scenario created an environment that promoted cooperation and information sharing across the United States government, states, the private sector, and international partners.

Percent of intelligence reports rated "satisfactory" or higher in customer feedback that enable customers to manage risks to cyberspace (I&A)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
88%	94%	94%	93%	94%	84%

The ability of federal, state, local, tribal, territorial, and private sector partners to share accurate information quickly is essential to the Nation's security and resilience. In today's interconnected world, every second can make a difference in either preventing an incident or responding to an event that affects the Nation. This measure assesses how well the Department provides actionable intelligence to our partners to manage risks to cyberspace. In FY 2016, I&A achieved an 84 percent rating, down from previous years. I&A consistently monitors customer satisfaction with all analytical products including those related to cybersecurity issues. Managers and analysts are regularly provided the feedback with the intent of ensuring all analytic products are responsive to our customer needs. I&A is evaluating changes to organizational processes and tools.

Percent of organizations that have implemented at least one cybersecurity enhancement after receiving a cybersecurity vulnerability assessment or survey (NPPD)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
---	100%	63%	100%	100%	100%

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 2016, 100 percent of organizations who received an assessment also implemented at least one cybersecurity enhancement. This year's results represent an excellent commitment by the asset owners and operators and is the third year out of the last four to achieve a 100 percent rating.

Percent of traffic monitored for cyber intrusions at civilian Federal Executive Branch agencies (NPPD)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
73.0%	82.4%	88.5%	94.3%	95%	98.7%

This measure assesses DHS's scope of coverage for potential malicious cyber-activity across participating civilian Federal Government agencies.[2] Federal Executive Branch network monitoring uses EINSTEIN network flow and intrusion detection system sensors which are deployed to trusted Internet connection locations at agencies or Internet service providers. These sensors capture network flow information and provide alerts when signatures, indicative of malicious activity, are triggered by inbound or outbound traffic. The Federal Government's situational awareness of

[2] Defined as Chief Financial Officers (CFO) Act agencies (other than the Department of Defense) as well as non-CFO Act agencies that are Trusted Internet Connection Access Provider agencies.

malicious activity across its systems will increase as more networks are monitored. In FY 2016, 98.7 percent of the Federal Executive Branch agencies network traffic was monitored for cyber-intrusions. There has been steady improvement in results since FY 2012.

Percent of known malicious cyber traffic prevented from causing harm at federal agencies (NPPD)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
---	---	100%	100%	100%	100%

This measure gages the ability of the Department of Homeland Security to defend federal civilian agency networks from cyber threats by assessing the percent of known malicious activity that is mitigated on federal agencies' networks through an active defense capability known as EINSTEIN 3 Accelerated. This is achieved by actively defending against malicious activity through detection and prevention, and applying countermeasures if needed for protection. DHS has met the FY 2016 annual target; however, results may fall below 100 percent in future fiscal years as the program expands the number of indicators and countermeasures used.

Amount of dollar loss prevented by Secret Service cyber investigations (in millions) (USSS)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
---	$1,119	$384	$589	$575[3]	$558

The USSS maintains Electronic Crimes Task Forces, which focus on identifying and locating international cybercriminals connected to cyber intrusions, bank fraud, data breaches, and other computer-related crimes. This measure reflects USSS's efforts to reduce cyber-related financial losses to the public. In FY 2016, $558 million in losses were prevented by USSS cyber-investigations. This year's target was not met as many financial and cybercrime cases are very large in scope and take a long time to investigate, and many agents were diverted to support campaign protection. USSS will improve performance by addressing staffing shortfalls, assignments, and training.

Number of law enforcement individuals trained in cybercrime and cyberforensics both domestically and overseas (USSS)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
---	1,517	1,533	2,070	1,800[4]	1,906

The specialized technical training the USSS provides in cybercrime and cyberforensics is conducted both domestically and overseas in an effort to strengthen our ability to fight cybercrime. The training serves to substantially enhance law enforcement efforts to suppress the continually

[3] FY 2016 target reflects USSS allocation of personnel to support campaign protection.
[4] FY 2016 target reflects USSS allocation of personnel to support campaign protection.

evolving and increasing number of electronic crime cases affecting communities nationwide, as well as improve and strengthen the prosecution and adjudication of those cases. The FY 2016 target was met; however, due to USSS's allocation of personnel to support campaign protection the result was slightly down from FY 2015.

Percent of planned cyber security products and services transitioned to government, commercial and open sources (S&T)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
---	89%	93%	60%	73%	73%

S&T's Cyber Security Division's (CSD) mission is to contribute to enhancing the security and resilience of the Nation's critical information infrastructure and the Internet through research and development. This measure reflects the percent of identified and completed planned transitions of cybersecurity products and/or services (e.g., technologies, tools, capabilities, standards, and knowledge products) within S&T's CSD projects to government, commercial or open sources. In FY 2016, S&T met their goal with results up from FY 2015, completing eight out of 11 planned transitions. These included the transition of: a new vehicle forensics hardware and software to support law enforcement; new technology to streamline and improve secure information sharing between DHS and its partners; an open source module development for law enforcement forensics; integration of Sonatype "application health checker" into the Software Assurance Marketplace to ensure quality of open source software; and Active-defense Resilient Mission-Oriented Cloud platform software, data sets, analyses and documentation to defend against vulnerabilities and threats in distributed and cloud computing infrastructures. CSD also released an Insider Threat Study for DHS Office of Security and a DHS Cumulative Technical Report for DHS S&T. Completing these planned transitions means cybersecurity research and development have resulted in deployable security solutions.

Major Cybercriminal Extradited From Czech Republic

Evgeny Tarasovich Levitskyy, of Nikolaev, Ukraine, was arraigned on August 5, 2016 on federal charges of conspiracy to commit bank fraud, bank fraud, conspiracy to commit wire fraud, and wire fraud.

In 2008, an American credit card processor, RBS WorldPay, was hacked in one of the most sophisticated and organized computer fraud attacks ever conducted. A team of hackers compromised the data encryption used to protect customer data on payroll debit cards and raised the account limits on compromised accounts to amounts exceeding $1,000,000. The hackers then provided a network of cashers with 44 counterfeit payroll debit cards, which were used to withdraw more than $9 million from over 2,100 ATMs in at least 280 cities worldwide, including cities in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan, and Canada. The $9 million loss occurred within a span of less than 12 hours.

This joint investigation by the U.S. Secret Service and the Federal Bureau of Investigation led to the charging of 14 individuals involved in the hack and cash out crimes. This includes the alleged frontrunner, Evgeny Tarasovich Levitskyy, who was extradited from the Czech Republic to face federal charges of conspiracy to commit bank fraud, bank fraud, conspiracy to commit wire fraud, and wire fraud. Michael Breslin, Special Agent in Charge of the United States Secret Service's Criminal Investigative Division, stated: “Based on our longstanding role in transnational cyber investigations and network intrusions, the U.S. Secret Service worked in conjunction with our law enforcement partners to provide critical evidence to further this investigation. Our partnerships in law enforcement, the private sector, and academia are our greatest resources in combatting these sophisticated and complex crimes and today's arraignment is proof that our strong commitment endures across all borders.”

Looking Forward

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyberthreat hazards. Sophisticated cyber-actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes are now being perpetrated through cyberspace, including banking and financial fraud, intellectual property violations, child exploitation, and other crimes, all of which have substantial human and economic consequences.

Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world; the linkages between cyberspace and physical systems; and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. A growing concern is the cyberthreat to critical infrastructure, which is increasingly subject to sophisticated cyber-intrusions that pose new risks. 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.

National Cybersecurity Protection System

The mission of DHS's Network Security Deployment (NSD) division is to improve cybersecurity to federal departments, agencies, and partners by developing the technologies and establishing the services needed to fulfill the Department's cybersecurity mission. To meet that mission need, NSD designs, develops, deploys, and sustains the National Cybersecurity Protection System (NCPS), which provides intrusion detection, advanced analytics, information sharing, and intrusion prevention capabilities that combat and mitigate cyberthreats to the federal executive branch information and networks. These capabilities provide a technological foundation that enables DHS to secure and defend the federal civilian government's information technology infrastructure against advanced cyber threats. NCPS advances DHS's responsibilities as delineated in the Comprehensive National Cybersecurity Initiative. Moving forward, DHS has identified an Agency Priority goal to support this effort to fully deploy by the end of calendar year 2016. See https://www.performance.gov/content/improve-federal-network-security?view=public for more information.

Continuous Diagnostics and Mitigation

DHS's Continuous Diagnostics and Mitigation (CDM) program is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides federal departments and agencies with capabilities and tools that identify what is on your network, who is on your network, and what is happening on your network. These tool provide a risk-based view of threats and enable cybersecurity personnel to mitigate the most significant problems first. As part of the Department's Cyber Agency Priority Goal, our plan is to have these tools delivered in a phased approach with the third phase being 97 percent complete, through contract award, by the end of FY 2017.

Combating Cybercrime

Today's world is more interconnected than ever before. Yet, for all its advantages, increased connectivity brings increased risk of theft, fraud, and abuse. As Americans become more reliant on modern technology, we also become more vulnerable to cyberattacks such as corporate security breaches, spear phishing, and social media fraud. Complementary cybersecurity and law enforcement capabilities are critical to safeguarding and securing cyberspace. Law enforcement performs an essential role in achieving our Nation's cybersecurity objectives by investigating a wide range of cybercrimes and apprehending and prosecuting those responsible. Now and moving forward, DHS works with other federal agencies to conduct high-impact criminal investigations to disrupt and defeat cybercriminals, prioritize the recruitment and training of technical experts, develop standardized methods, and broadly share cyber-response best practices and tools. Criminal investigators and network security experts with deep understanding of the technologies malicious actors are using and the specific vulnerabilities they are targeting work to effectively respond to and investigate cyber incidents.

Mission 5: Strengthen National Preparedness and Resilience

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

Our goals for this mission are:

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

Rescue Efforts with Our International Partners

During the deadliest disaster on record in Nepal, working as part of a small team airlifted into the remote village of Singati, members of Virginia Urban Search & Rescue (US&R) Task Force One, and California US&R Task Force 2, treated scores of civilians injured in a catastrophic earthquake. Both task forces are members of FEMA's National US&R Response System, and they were deployed to Nepal under their concurrent agreement with the United States Agency for International Development, Office of Foreign Disaster Assistance. In the midst of their medical efforts, they received reports of people trapped inside a collapsed structure. Team members raced to a caved-in building to look for signs of life. After significant effort within a very unstable building they found a boy who was sadly killed in the quake. They then worked tirelessly to save the life of a Nepalese woman who was trapped between collapsed floors. The crew's rescue efforts were complicated not only by the instability of the structure on a steep hillside, but also repeated aftershocks that triggered landslides. Given the high altitude and the limits of what could be brought in by aircraft, they worked with a limited number of basic rescue tools. Task force members leveraged their experience with the FEMA US&R tactical operational procedures and the System Readiness Assessment Program to effect this complicated dramatic rescue.

On August 18, 2016, in recognition of their heroic actions following the devastating Nepal Earthquake, task force members from both teams were honored with the prestigious Ben Franklin Award for Valor from the International Association of Fire Chiefs (IAFC). Presented annually, the Ben Franklin Award for Valor is the IAFC's most prestigious award. This award honors a firefighter for his or her expert training, professional service, and dedication to duty displayed in saving a human life.

Percent of communities in high earthquake, flood, and wind-prone areas adopting disaster-resistant building codes (FEMA)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
56%	57%	61%	63%	62%	68%

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 have adopted disaster resistant building codes over time. Progress continues to be made due to training, education, outreach, and adoption of building codes by both communities and businesses as evidenced by the FY 2016 results of 68 percent, up from FY 2015.

Percent of states and territories with a Threat and Hazard Identification and Risk Assessment (THIRA) that meets current DHS guidance (FEMA)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
---	86%	71%	77%	100%	86%

The National Preparedness Goal is, "A secure and resilient Nation 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 THIRA is a four step common risk assessment process that helps the whole community—including individuals, businesses, faith-based organizations, nonprofit groups, schools and academia and all levels of government—understand its risks and estimate capability requirements. FEMA has set the target for this measure to be 100 percent in light of its importance to the "whole community." In FY 2016, 86 percent of states and territories have developed a THIRA that meets all 4 steps of the current DHS guidance. FEMA provides technical assistance to help jurisdictions improve their THIRA by improving their targets developed for each core capability in the National Preparedness Goal and understanding their resource needs to meet their target. FEMA will continue to provide technical assistance in FY 2017, as jurisdictions specifically identified challenges with THIRA Step 3 (describing impacts and desired outcomes and establishing capability targets and target statements) and Step 4 (applying the results of the THIRA by estimating resources required to meet capability targets), as well as Whole Community Engagement.

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)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
---	100%	100%	100%	100%	100%

Actions necessary to stabilize an incident are defined as those functions that must be initiated immediately following an incident in order to ensure the best outcomes for survivors. These actions include establishing joint federal/state incident objectives and interoperable communications between FEMA-supported incident sites, deploying urban search and rescue resources, rapidly activating response coordination centers, and issuing timely alerts, warnings, operations orders, and situation reports. This measure reflects FEMA's role in effectively responding to any threat or hazard, with an emphasis on saving and sustaining lives within 72 hours, in support of state, local, tribal, and territorial governments. All response incident management and support actions initiated in FY 2016 met required timeframes and requirements for Incident Management Assistance Teams, Urban Search and Rescue, Mobile Emergency Response Support, National Response Coordination Center, FEMA Operations Center, and National Watch Center resources. FEMA has met this target four consecutive years.

Percent of people in imminent danger saved in the maritime environment (USCG)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
77.3%	79.0%	79.0%	80.0%	100%	79.3%

Minimizing the loss of life by rendering aid to persons in distress involves multi-mission stations, cutters, aircraft, and boats linked by communications networks. Search and Rescue (SAR) is one of the USCG's oldest missions. To meet this responsibility, the USCG maintains SAR facilities on the East, West, and Gulf coasts; in Alaska, Hawaii, Guam, and Puerto Rico; and on the Great Lakes and inland U.S. waterways. 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 5,204 lives in FY 2016, which was 79.3 percent of those in danger, and is consistent with long-term results and trends. The USCG will continue to plan, train, develop better technologies, and invest in capable assets to continue their exemplary performance in saving lives in the maritime environment.

Percent of recovery services through Individual Assistance delivered to disaster survivors gauging the quality of program services, supporting infrastructure, and customer satisfaction following a disaster (FEMA)

FY12 Result	FY13 Result	FY14 Result	FY15 Result	FY16 Target	FY16 Result
---	94.5%	91.5%	96.9%	94%	95.3%

Recovery assistance helps individuals and communities affected by disasters and emergencies return to normal quickly and efficiently. This measure is based upon three categories: program services; supporting infrastructure; and customer satisfaction. Sub-elements within these three categories include: providing temporary housing assistance and case management; having available grant management and internet and telephone registration systems; ensuring call centers respond quickly and business staff are in place; and delivering these services to enhance customer satisfaction of those receiving individual assistance from FEMA following a disaster. In FY 2016, FEMA met their target achieving a 95.3 percent rating of services provided to disaster survivors through the Individual Assistance Program and is slightly down from FY 2015. While the results of this measure have fluctuated, it has remained above 90 percent for the past four years. The Individual Assistance Program will incorporate after action report findings from 2016 disaster efforts to influence strategic decisions, performance framework development, and process improvements.

Mass Rescue Operation at Sea

On August 17th, 2016, USCG Sector San Juan received a distress call from cruise ship CARIBBEAN FANTASY. The cruise ship, carrying more than 500 passengers and crew onboard, experienced an engine room fire that quickly spread throughout the vessel. Sector San Juan immediately activated its Mass Rescue Operations (MRO) plan, launching USCG assets and coordinating with various federal and local agencies to assist. All 500+ passengers and crew evacuated into life rafts and were safely transported to shore by responding government, commercial, and private vessels.

The outstanding coordination and response of involved agencies is a result of the combined efforts of maritime stakeholders to ensure proper measures are in place for such an event. MRO incidents are challenging and complex, requiring extensive planning and preparation for optimal response. USCG works nation-wide with industry stakeholders, and other federal, state, and local agencies to establish and exercise regional MRO plans to ensure seamless response and multi-agency coordination should real-world incidents like this occur.

Looking Forward

The Department coordinates comprehensive federal efforts to prepare for, protect against, respond to, recover from, and mitigate a terrorist attack, natural disaster or other large-scale emergency, while working with individuals, communities, the private and nonprofit sectors, faith-based organizations, and federal, state, local, tribal, and territorial partners to ensure a swift and effective recovery effort. The Department's efforts to build a ready and resilient Nation include fostering a whole community approach to emergency management nationally; building the Nation's capacity to stabilize and recover from a catastrophic event; bolstering information sharing and building unity of effort and common strategic understanding among the emergency management team; building plans and providing training to our homeland security partners; and promoting preparedness within the private sector. Below are a few initiatives that advance our efforts to achieve our preparedness and resilience goals.

National Incident Management System (NIMS)

As part of its efforts to engage and support the Whole Community in all aspects of emergency management, the Department has established a standardized approach to guide all levels of government, nongovernmental organizations, and the private sector in working together to seamlessly manage incidents. Key tenets of NIMS include: a common operating picture to enable entities to make consistent and informed decision; interoperability to facilitate communication and sharing across agencies and jurisdictions; consistent resource management which provides coordination and standardization for incident response resources; and the incident command system which is a standardized management system for integrating equipment, personnel, procedures, and more. Moving forward, NIMS will increase the focus on resource typing and mutual aid, including the development of mutual aid networks that could operate in a modular approach similar to modern wildfire response. In addition, it will enhance information management processes including social media integration and geographical information systems.

National Flood Insurance Program

The Department administers the National Flood Insurance Program (NFIP) to reduce the impact of flooding on private and public structures. The NFIP takes a multi-faceted approach that includes providing affordable insurance to property owners while also encouraging communities to adopt floodplain management regulations and invest in mitigation efforts. Moving forward, FEMA is developing options to address affordability challenges certain policyholders may face as the program moves towards charging full-risk policy premiums. Congress is expected to use the options to inform reauthorization of the NFIP. The Administration and Congress will need to balance affordability for policy holders and the fiscal solvency of the fund. Also, the NFIP is employing recent technological advancements to enhance flood risk mapping and understand the impacts of land-use and climate change.

Interoperability

The ability to seamlessly coordinate and communicate among all stakeholders is a key aspect of the National Response Framework and a direct consequence of incidents starting and ending at the local level. In order to allow all these stakeholders to respond effectively, the concept of interoperability is applied to the many resources and processes that FEMA supports and manages. Interoperability typically refers to communications such as wireless radio systems and language and communications protocols, but can also include other aspects of response such as the resource typing, training, and qualification of response personnel. For example, resource typing definitions establish a common language and defines a resource's (for equipment, teams, and units) minimum capabilities. NIMS resource typing definitions serve as the common language for the mobilization of resources. Moving forward, FEMA is investing in grants and exercises to practice and identify best practices for interoperability across all levels of government.

Disaster Workforce Structure

In order to be prepared for all hazards, the Department has made numerous advancements in the past decade to the disaster response workforce. The establishment of the Surge Capacity Force allows the capacity for the Department to deploy its employees in support of FEMA's existing workforce for a large-scale disaster such as Hurricane Sandy. The Department continues to innovate and learn from other agencies, such as developing a centralized reception, staging, onward movement, and integration process and collaborating with the Corporation for National and Community Service. However, FEMA is still at only 54 percent of its desired workforce structure. Moving forward, FEMA is conducting research to understand the barriers that prevent it from reaching its disaster workforce structure. Additionally, it is continuing to learn from other agencies such as Department of Defense's Time Phased Force Deployment Data.

Public Assistance

Resiliency and recovery from disasters is an essential piece of the Department's mission. FEMA's Public Assistance program plays a vital role in supporting state, local, and tribal governments with recovery by providing grants to remove debris and repair public infrastructure such as roads, schools, and hospitals. In certain cases, the program also encourages communities to not just rebuild to the previous structure but to build to stronger and smarter standards. Currently, FEMA covers 75 percent of the cost of rebuilding in most cases, but that share can go higher for large disasters. Moving forward, FEMA is currently exploring the possibility of a policy that could potentially recognize and reward states with strong and timely state and local adoption and enforcement of building codes; give additional credit to states using independent ratings of code governance based on the rating received; give additional recognition for required above-model code standards for appropriate hazards; give states credit for resilience/mitigation programs; Agency programs can use these FEMA assessments in program decision-making.

Mature and Strengthen Homeland Security

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

Our mature and strengthen goals are:

- Integrate Intelligence, Information Sharing, and Operations;
- Enhance Partnerships and Outreach;
- Strengthen the DHS International Affairs Enterprise in Support of Homeland Security Missions;
- Conduct Homeland Security Research and Development;
- Ensure Readiness of Frontline Operators and First Responders; and
- Strengthen Service Delivery and Manage DHS Resources.

S&T's First Responder Group Exercise on Electronic Jamming Threats

DHS's Science and Technology (S&T) Directorate hosted a five-day, multi-agency operational exercise, from July 11-16, 2016, at the White Sands Missile Range in New Mexico to assess the impact of electronic jamming threats on first responder communications systems and mission response. The DHS S&T First Responder Electronic Jamming Exercise was a true unity of effort, with participants from DHS Components, which included ICE, CBP, USCG, and FEMA, as well as first responders from more than 40 federal, state, and local agencies, including Harris County, Texas, Office of Homeland Security and Emergency Management, and the Los Angeles County, California, Sheriff's Department.

During the exercise, responder organizations conducted emergency response scenarios while deliberate electronic jamming disabled some of their communications and navigation equipment. Responders worked to mitigate the effect of the jamming while observers collected information on their performance and mission response.

Results of the exercise are currently being analyzed to identify vulnerabilities in our Nation's responder communications networks and determine solutions; design electronic jamming mitigation technologies; identify gaps in first responder training; and provide recommendations to close them; inform policy on resilient and redundant communications requirements; and improve the ability of first responders to execute their missions in an electronic jamming environment. A final report will outline results, lessons learned, training recommendations, and mitigation strategies for first responders.

Looking Forward

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

Joint Requirements Council (JRC)

The JRC is designed to strengthen the Department's analytically-based strategic decision-making and maximize unity of effort by managing the requirements generation process, aligning requirement activities, and maturing processes to inform prioritized investment recommendations to the DHS leadership. A Component-driven and Component-led executive forum, the JRC's goal is to validate operational requirements to support capabilities aligned with strategic priorities. The JRC's goal is also to identify areas where DHS can reduce unnecessary duplication, overlap, and redundancy and prioritize capability options to improve the effectiveness and efficiency of operations. The JRC is piloting two ground-breaking DHS initiatives: 1) an annual Joint Assessment of Requirements (JAR) founded on cost-informed, feasibility and traceability criteria to prioritize emerging and existing program requirements; and 2) an annual Capability Gap Analysis (CGA) to provide senior leadership a comprehensive view of DHS's prioritized capability gaps to inform capability solution development and Research and Development investments. Future JRC plans include: 1) transitioning from establishing its structure and processes to maturing and strengthening execution and senior leader recommendations; 2) updating the JRC's strategic plan and strengthening the framework to focus on the JRC's efforts and measuring its success; 3) maturing its communication plan to inform JRC's strategy, tactics, goals and target audiences; 4) assessing the current portfolio team construct to ensure alignment with DHS priorities; 5) maturing the JAR process through 2018 and CGA process through 2019 with recommendations to inform DHS leadership investment decisions; 6) implementing the Joint Requirement Integration and Management System Knowledge Management Decision Support tool to record and track capability requirements documents during reviews, and provide a document repository; and 7) developing a requirements certification program.

Workforce Management Transformation

The Department began the development of the Workforce Management Transformation project in January 2015. The long-term objective of this effort is to have uniform processes and coordinated systems in place for managing and analyzing workforce resources. This includes: documenting and managing actual personnel levels; documenting and managing authorized personnel levels constrained by available funding; accurately pricing personnel costs to support budget formulation and out-year planning scenarios; personnel requirements modeling; and assessment of workforce gaps to inform and support leadership decision making, planning and budget formulation. Over the last year, the project team completed extensive research into the various workforce management and analysis offices/staffs of the Departments of Education, Interior, Energy, Transportation, Treasury, State, Defense, and Justice. This study reviewed their modeling approach and coverage, office structure, span of control, responsibilities, budget, and staffing to help delineate DHS's program scope. The team also developed guidance documents to define the responsibilities and objectives of a Manpower and Organization program office to be established in 2017, collected data for a Human Resource Information Technology system gap analysis requirements identification for a proposed position documentation system, and developed multiple documents to facilitate implementation of workforce management throughout the Department. Future goals include:

completion of permanent staffing of a Manpower and Organization Office within the Office of the Chief Human Capital Officer by end of FY 2018; the development a position documentation system for fielding in FY 2019; and the promulgation of consistent policy throughout the Department to manage manpower modeling and analysis, as well as the effective management of personnel authorizations and positions.

Financial Stewardship

In FY 2015, DHS continued to make substantive progress across the Components in its Financial Systems Modernization (FSM) initiative. FLETC completed a technical refresh of their accounting and budgeting system in the first quarter. USCG, TSA, and DNDO completed a global configuration phase with the Department of the Interior's Interior Business Center (DOI IBC), a federal shared service provider, in the second quarter. This phase determined the common baseline for the three Components on the DOI IBC financial management shared service. Following the global configuration phase, DNDO completed the implementation phase and went live on the financial solution in the first quarter of FY 2016. Moving forward, TSA and USCG implementations are scheduled in subsequent years. In addition, USCIS, S&T, NPPD, and the Management Directorate completed Phase I of the discovery phase with a federal shared service provider for financial management system services.

DHS Employs Innovative Approach to Critical Cybersecurity Workforce Requirement

One of the Secretary's primary goals for 2016 was to increase the Department's cybercapacity. In order to achieve this critical objective, in May of this year, the Chief Human Capital Officer, Chief Information Officer, and Chief Security Officer Councils jointly worked with representatives from every DHS Component to sponsor a DHS-wide Cyber and Technology Job Fair, which took place July 27-28. The Department identified more than 300 positions as mission critical hires across the department and posted announcements on USAJOBS, resulting in the receipt of more than 14,000 applications. A cross-department team designed the hiring event to provide an opportunity for both scheduled and walk-in candidates to be interviewed, and if selected, receive a tentative job offer and initiate the security clearance process prior to leaving the job fair.

As a result of this extensive collaboration across DHS, 326 well-qualified candidates have received tentative job offers. Typically, the federal hiring process takes four to six months from the time a hiring manager interviews a candidate until they actually come onboard. However, due to the innovative approach of initiating the security clearance process at the job fair, within the first 30 days following the hiring event, 103 candidates cleared security and 22 candidates began work. Acquiring the talent to fill these critical positions in such a streamlined manner has a significant impact on increasing the cybercapabilities within DHS, during a time when cyberthreats to our Nation are continuing to evolve and grow.

Priority Goals

Agency Priority Goals

In the FY 2016 Budget, the Obama Administration defined Agency Priority Goals (APG) which represent areas in which the Administration has identified opportunities to significantly improve near-term performance. The Department's FY 2016-2017 APGs are a set of focused initiatives that support the Agency's longer-term strategic framework. The goal statement for each of the Department's APGs is provided below. For more extensive information on our APGs, visit the public web site designed to make this information readily accessible to the public at: www.performance.gov.

Agency Priority Goal 1: Combatting Transnational Criminal Organizations** **(Aligns to Mission 2)

Goal Statement: Decrease the ability of targeted transnational criminal organizations to conduct illicit activities impacting the southern border and approaches region of the United States. By September 30, 2017, actions by the DHS Joint Task Forces via synchronized component operations will result in the disruption and/or dismantlement of 15 percent of targeted transnational criminal organizations.

Agency Priority Goal 2: Enhance Federal Network Security** **(Aligns to Mission 4)

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

Agency Priority Goal 3: Enhance Disaster Preparedness and Response** **(Aligns to Mission 5)

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

Cross-Agency Priority Goals

Cross-Agency Priority (CAP) goals were established and are being led by the Administration with participation from the relevant federal agencies to address cross-cutting issues of importance to government stakeholders. Fifteen CAP goals were announced in the 2015 budget, comprised of seven mission-oriented and eight management-focused goals with a four-year time horizon.

Each of the CAP goals has goal leads, co-leads, and collaboration from other federal agencies. They are in various stages of implementing their project plans. For more information on both the mission and management CAP goals, see www.performance.gov for the latest information.

Financial Overview

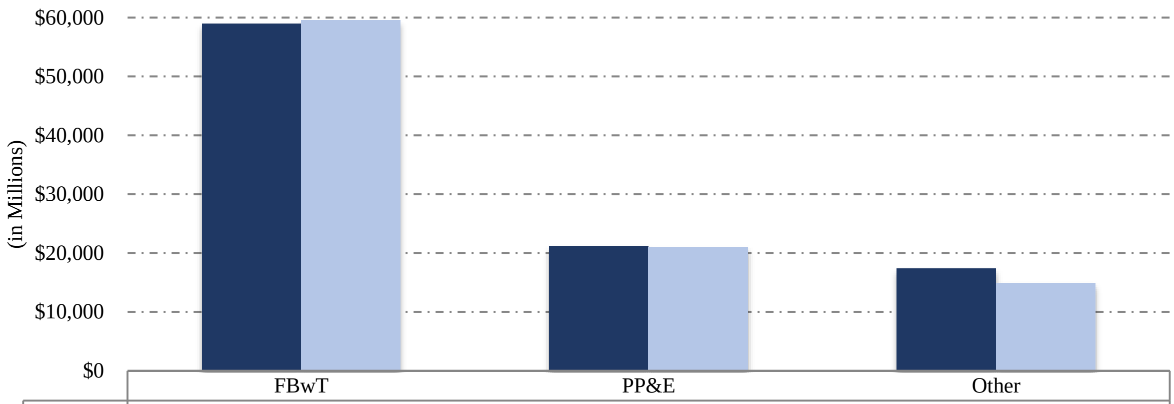
The Department's budgetary resources were approximately $88.1 billion for FY 2016. The budget represents our plan for efficiently and effectively achieving the strategic objectives set forth by Secretary Johnson to carry out our mission and to ensure that the Department manages its operations within the appropriated amounts using budgetary controls. 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. These financial statements provide the results of our operations and financial position, including long-term commitments and obligations. Budgetary accounting principles require recognition of the obligation of funds according to legal requirements, which in many cases occurs prior to the occurrence of a 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, and are reported in the Statement of Budgetary Resources. 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. KPMG LLP performed the audit of the Department's principal financial statements.

Balance Sheet

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.

Assets – What We Own and Manage

Total Assets



	FBwT	PP&E	Other
■ FY 2016	$58,997	$21,220	$17,413
■ FY 2015	$59,553	$21,067	$14,939

Assets represent amounts owned or managed by the Department that can be used to accomplish its mission. As of September 30, 2016, the Department had $97.6 billion in assets, representing a

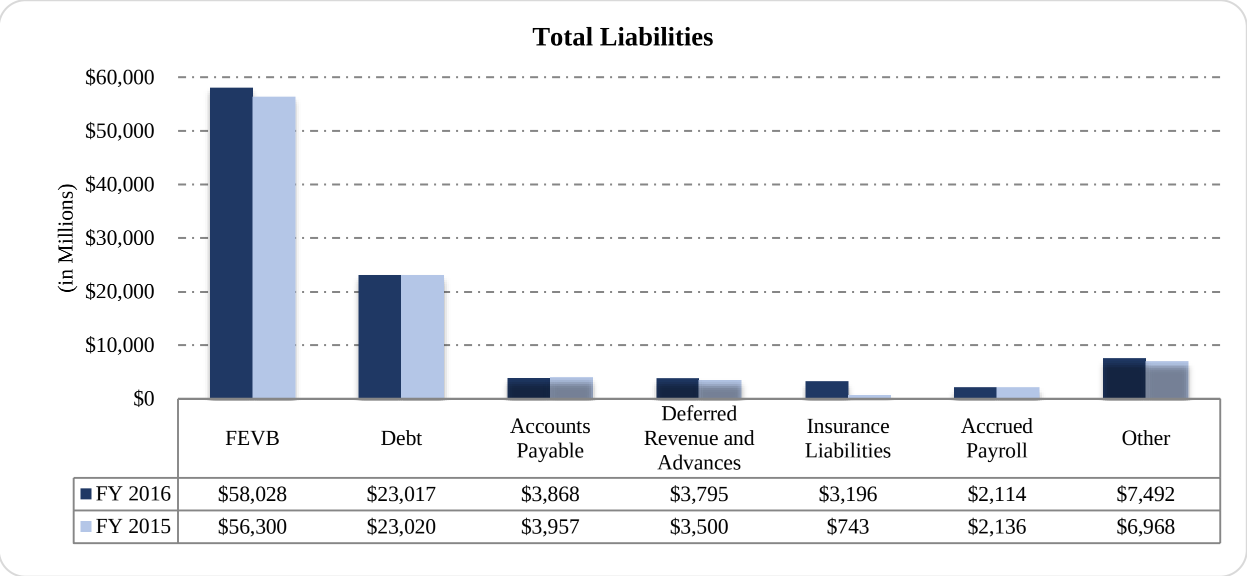
$2 billion increase from FY 2015. The increase is primarily due to accounts receivable due from British Petroleum for the Deepwater Horizon oil spill pursuant to the Consent Decree approved in April 2016. Additionally, FEMA investments for the National Flood Insurance Reserve Fund also increased, providing FEMA authority to draw upon the Treasury to make future payments related to flood claims.

Fund Balance with Treasury (FBwT), the Department's largest asset, comprises 60 percent of the total assets. FBwT balances are primarily 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, comprising 22 percent of total assets. The major items in this category 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. PP&E is recorded at cost, and depreciated over the estimated useful life of the asset. PP&E is presented net of accumulated depreciation.

Other Assets represents 18 percent of total assets, and includes investments, accounts receivable, cash and other monetary assets, taxes, duties and trade receivables, direct loans, inventory and related property, and other.

Liabilities – What We Owe



Total Liabilities

	FEVB	Debt	Accounts Payable	Deferred Revenue and Advances	Insurance Liabilities	Accrued Payroll	Other
■ FY 2016	$58,028	$23,017	$3,868	$3,795	$3,196	$2,114	$7,492
■ FY 2015	$56,300	$23,020	$3,957	$3,500	$743	$2,136	$6,968

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. As of September 30, 2016, the Department reported approximately $101.5 billion in total liabilities. Total liabilities increased by approximately $4.9 billion in FY 2016; mainly due to the disaster relief that FEMA provided in response to significant flooding that impacted the southern region of the United States. Liabilities also grew based on amounts owed to current and former

DHS employees, most specifically related to participant growth and changes in actuarial assumptions for USCG post-employment medical and retirement benefits.

The Department's largest liability is for *Federal Employee and Veterans' Benefits*, representing 57 percent of total liabilities. 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 and an estimate for incurred but not yet reported workers' compensation costs. 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 represents 23 percent of total liabilities, and results from Department of Treasury (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 pay its debt from the premium revenue alone; therefore, legislation will need to be enacted to provide funding to repay the Bureau of the Fiscal Service. This is discussed further in Note 15 in the Financial Information section.

Accounts payable, representing 4 percent of total liabilities, includes amounts owed to other federal agencies and the public for goods and services received by the Department.

Deferred revenue and advances represents amounts received by the Department for goods or services that have not been fully rendered, which are 4 percent of total liabilities.

Insurance Liabilities consist of NFIP claim activity, and represents 3 percent of total liabilities.

Accrued payroll includes unpaid wages and benefits for current DHS employees, and represents 2 percent of total liabilities.

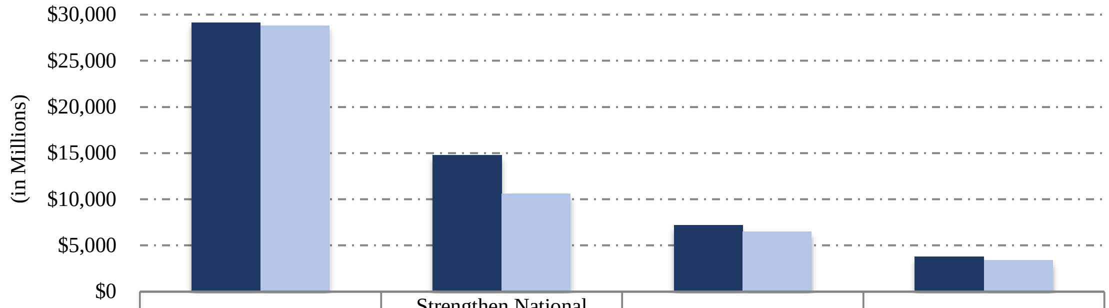
Other liabilities, comprising 7 percent of the Department's liabilities, includes amounts due to the Treasury's general fund, environmental liabilities, refunds and drawbacks, and other.

Statement of Net Cost

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.

Net Cost of Operations Before Gains and Losses



	Foster a Safe and Secure Homeland	Strengthen National Preparedness and Resilience	Enforce and Administer Our Immigration Laws	Mature and Strengthen Homeland Security
■ FY 2016	$29,152	$14,751	$7,210	$3,792
■ FY 2015	$28,821	$10,593	$6,501	$3,366

Foster a Safe and Secure Homeland, includes strategic plan missions 1, *Prevent Terrorism and Enhance Security;* 2, *Secure and Manage Our Borders;* and 4, and *Safeguard and Secure Cyberspace.* This major mission involves the security and prevention aspects of the DHS strategic plan, representing 53 percent of the Department's net cost. *Strengthen National Preparedness and Resilience* is mission 5 of the strategic plan and represents 27 percent of total net costs. *Enforce and Administer Our Immigration Laws* is mission 3 of the strategic plan and represents 13 percent of total net costs. *Mature and Strengthen Homeland Security* is the focus area of the DHS strategic plan and represents 7 percent of the Department's net cost. Note 23 in the Financial Information section shows costs by responsibility segment aligned to the major missions.

The Department's net cost of operations before gains and losses increased by approximately $5.6 billion in FY 2016; primarily due to recovery efforts related to flooding from severe storms in Oklahoma, Texas, Mississippi, and Louisiana.

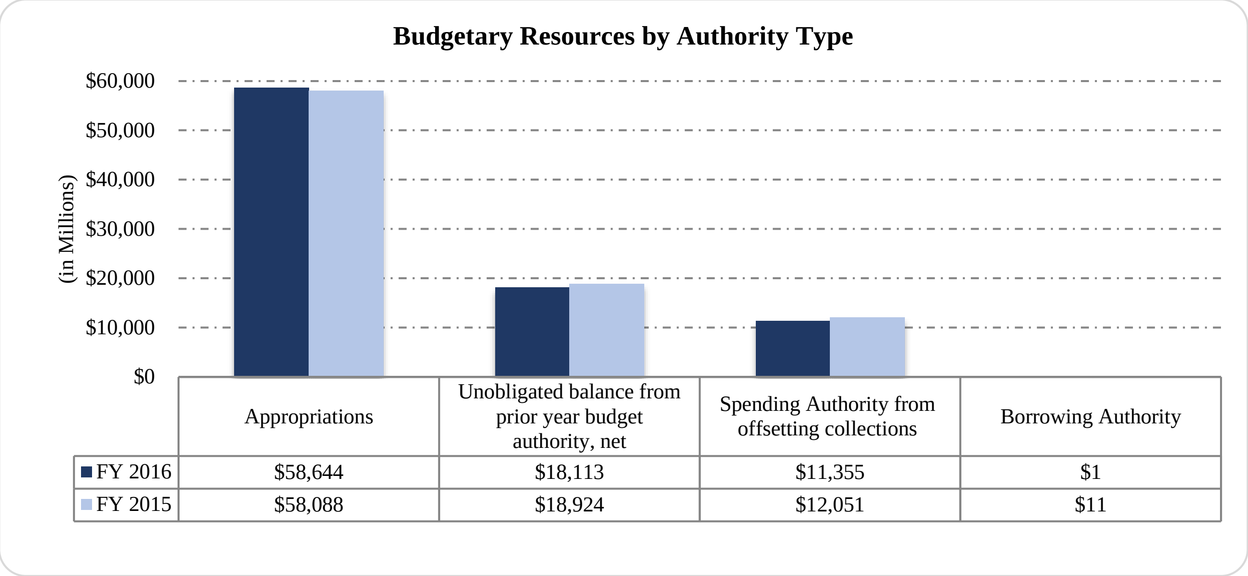
During FY 2016, the Department earned approximately $14.5 billion in exchange revenue. Exchange revenue arises from transactions in which the Department and the other party receive value and that are directly related to departmental operations. The Department also collects non-exchange duties, taxes, 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.

Statement of Changes in 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 above as well as transfers to other agencies decrease net position. Total net position is $(3.9) billion. The Department's net position is negative because of significant expenses related to NFIP, as well as pension liabilities for USCG and USSS—the Department receives funding for these liabilities for the current year only. Total net position decreased by approximately $2.8 billion from FY 2015. The decrease in net position is primarily the result of additional costs in FY 2016 related to FEMA disaster relief.

Statement of Budgetary Resources

This statement provides information on the status of the approximately $88.1 billion in budgetary resources available to the Department during FY 2016.



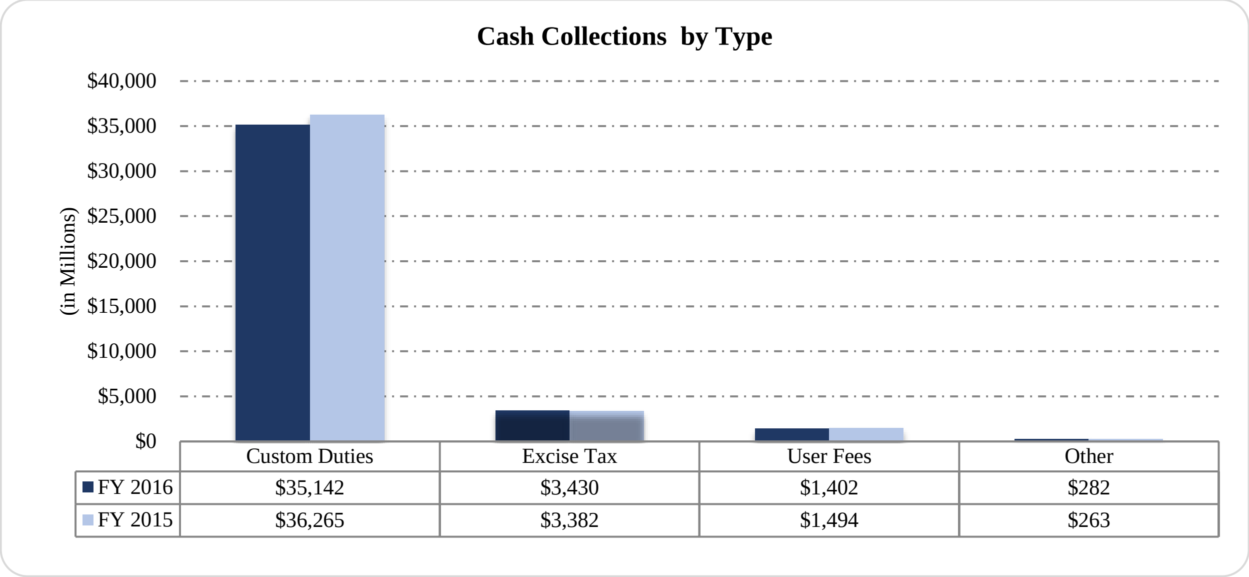
	Appropriations	Unobligated balance from prior year budget authority, net	Spending Authority from offsetting collections	Borrowing Authority
■ FY 2016	$58,644	$18,113	$11,355	$1
■ FY 2015	$58,088	$18,924	$12,051	$11

The authority was derived from appropriations of $58.6 billion, $18.1 billion in authority carried forward from FY 2015, and $11.4 billion in collections. Budgetary resources decreased approximately $1 billion from FY 2015 primarily as a result of the Department's focused efforts to improve spending efficiency, resulting in the continued decrease of unobligated budgetary resources at both the beginning and end of the fiscal year.

As of September 30, 2016, $13.5 billion of the $88.1 billion was not yet obligated. The $13.5 billion represents $10.3 billion in apportioned funds available for future use, and $3.2 billion in unapportioned and expired funds. Of the total budget authority available, the Department incurred a total of $74.6 billion in obligations from salaries and benefits, purchase orders placed, contracts awarded, or similar transactions. These obligations will require payments during the same or future period.

Statement of Custodial Activities

This statement presents 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.



Cash Collections by Type

	Custom Duties	Excise Tax	User Fees	Other
■ FY 2016	$35,142	$3,430	$1,402	$282
■ FY 2015	$36,265	$3,382	$1,494	$263

Custom duties collected by CBP account for 87 percent of total cash collections. The remaining 13 percent is comprised of excise taxes, user fees, and various other fees. An example of non-exchange revenue for the Department includes user fees that CBP collects on behalf of the Federal Government. These fees are considered non-exchange because they are a result of the Federal Government's sovereign powers rather than as a result of providing goods or services for a fee. Total cash collections decreased by approximately $1.1 billion in FY 2016 because of a lower volume of imports than in prior years.

Stewardship Assets and Investments

The Department's stewardship assets are maintained by the USCG, CBP, USCIS, TSA, FEMA, S&T, USSS, and FLETC. These heritage assets primarily consist of documents, historical artifacts, immigration and naturalization files, artwork, buildings, and structures. A heritage asset is any personal property that is retained by DHS because of its historic, cultural, educational, or artistic value as opposed to its current usefulness to carrying out the mission of the Department.

When a heritage asset is predominantly used for general government operations, the heritage asset is considered a multi-use heritage asset. The USCG has over 100 memorials, recreational areas, and other historical areas designated as multi-use heritage assets. CBP has four historical buildings and structures located in Puerto Rico, and FEMA has one training facility that is used by the Emergency Management Institute and the U.S. Fire Administration's National Fire Academy for training in Emmitsburg, Maryland.

Stewardship investments are substantial investments made by the Federal Government for the benefit of the Nation. When incurred, stewardship investments are treated as expenses in calculating net cost, but they are separately reported as Required Supplementary Stewardship Information to highlight the extent of investments that are made for long-term benefits. Included are investments in research and development, human capital, and non-federal physical property.

Limitations of Financial Statements

The principal financial statements have been prepared to report the financial position and results of operations of the Department, pursuant to the requirements of Title 31, United States Code, Section 3515(b) relating to financial statements of federal agencies. While the statements have been prepared from the books and records of the entity in accordance with generally accepted accounting principles for federal agencies and the formats prescribed by OMB, the 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.

Other Key Regulatory Requirements

See the Other Information section for Prompt Payment Act, Debt Collection Improvement Act of 1996, and Biennial User Charges Reviews information.

Management Assurances

The Federal Managers' Financial Integrity Act, Federal Financial Management Improvement Act, Department of Homeland Security Financial Accountability Act, and Digital Accountability and Transparency Act of 2014

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 USC 3512, Sections 2 and 4) and the Federal Financial Management Improvement Act of 1996 (Pub. L. 104-208), as prescribed by the U.S. Government Accountability Office (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, the 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 Office of Management and Budget (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 are effective for FY 2016 with the implementation of enterprise risk management requirements effective in FY 2017. Circular A-123, Appendix A, Internal Control over Financial Reporting remain in effect. 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 control over operations, reporting, and compliance through the extensive work of staff and management at Headquarters and in the Components. In FY 2016, the USCG demonstrated significant progress in correcting previously identified internal control deficiencies over its real property. The Department remains dedicated to fully remediating operating and financial reporting controls conditions, which supports the sustainment of its financial statement opinion and achievement of an opinion over internal control over financial reporting in the near future.

In FY 2013, the Department achieved a major milestone when it received its first unmodified opinion on all its financial statements and provided a second-consecutive modified assurance over financial reporting controls. The Department's sustained these significant achievements in FY 2014 and FY 2015. In FY 2015, the Department reduced the four remaining material weaknesses to three by remediating Budgetary Accounting to a significant deficiency and achieved an unmodified opinion on all its financial statements. Although the Department has work to do, DHS is poised and focused on building off of its FY 2016 successes in USCG real property and improving financial management and information technology in order to remediate the remaining material weaknesses in Financial Reporting, Property, Plant, and Equipment, and Information Technology.

In accordance with Circular A-123, DHS performs assessments over the effectiveness of its internal controls. The results of these assessments provide management with an understanding of the effectiveness and efficiency of programmatic operations, reliability of financial reporting, and compliance with laws and regulations. Management performs an analysis on the pervasiveness and materiality over any identified deficiencies to determine their impact. Based on the results of these assessments, the Secretary provides assurances over the Department's internal controls in the annual assurance statement.

Any deficiency identified as a material weakness within internal control over financial reporting is defined as a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. To identify material weaknesses and non-compliance, management used the following criteria:

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

DHS 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 DHS lines of business to address crosscutting 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 DHS OIG and GAO.

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

Secretary's Assurance Statement

November 14, 2016

The Department of Homeland Security is committed to a culture of integrity, accountability, fiscal responsibility, and transparency. The Department's management team is responsible for establishing and maintaining effective internal control over the three internal control objectives: effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations.

In accordance with the Federal Managers' Financial Integrity Act of 1982 (FMFIA) and the Department of Homeland Security Financial Accountability Act, I directed an evaluation of internal control at the Department in effect during the Fiscal Year (FY) ending September 30, 2016. This evaluation was conducted in accordance with the GAO Green Book and Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. The Department provides reasonable assurance that the objectives of FMFIA, Section 2 over internal control over operations have been achieved.

The Department has completed its FY 2016 evaluation of internal control over financial reporting, which includes safeguarding of assets and compliance with applicable laws and regulations, in accordance with OMB Circular A-123, Appendix A, and Departmental requirements. The Department provides reasonable assurance that our internal control over financial reporting was operating effectively as of September 30, 2016, with the exception of the three business areas: 1) Financial Reporting; 2) Property, Plant, and Equipment; and 3) Information Technology Controls and Systems Functionality, where material weaknesses have been identified and remediation is in process, as further described in the Other Information Section. In addition, DHS financial management systems do not fully conform to the objectives of FMFIA, Section 4, and the Federal Financial Management Improvement Act of 1996 (FFMIA).

The Department will continue its efforts to strengthen DHS-wide internal control systems and demonstrate their effectiveness through routine evaluation of business processes. Through sound and repeatable financial management practices, we will provide unmodified assurance and achieve a clean audit opinion on internal control over financial reporting, as required by law and regulation.

In addition to our commitment to maturing DHS's internal control ecosystem, the Department is executing incremental Component-level financial system modernization projects. The DHS financial systems modernization concept streamlines and adjusts its IT financial portfolio so that the DHS Chief Financial Officer and Components have the flexibility to meet their mission and the changing demands for financial visibility and accountability. DHS is leveraging the lessons learned from this shared services implementation, reducing risk in future migrations through deliberative approaches to resource management, business process re-engineering, change management, and scheduling rigor and oversight. In FY 2016, the Department migrated the DHS Domestic Nuclear Detection Office to a shared service provider, achieving a significant system modernization milestone. Financial system modernization will deliver functionality that enables full compliance with FMFIA, Section 4 and FFMIA.

As evidenced by our fourth consecutive unmodified opinion on the Department's financial statements, the Department remains committed to financial stewardship by providing accurate, complete, and timely information to stakeholders for mission critical decisions. We remain focused on implementing sustainable internal control practices to eliminate the remaining material weaknesses and achieve an unmodified audit opinion on internal control over financial reporting.

We will continue our pledge that taxpayer dollars are managed with integrity, diligence, and accuracy, and that the systems and processes used for all aspects of financial management demonstrate the highest level of accountability and transparency.

Sincerely,

Jeh Charles Johnson

Federal Financial Management Improvement Act

The Federal Financial Management Improvement Act of 1996 (FFMIA) requires federal agencies to implement and maintain financial management systems that comply substantially with:

- Federal financial management system requirements;
- Applicable federal accounting standards; and
- The U.S. Standard General Ledger at the transaction level.

In assessing compliance with FFMIA, the Department uses OMB guidance and considers the results of the OIG's annual financial statement audits and Federal Information Security Modernization Act (FISMA) compliance reviews. As reported in the Secretary's Management Assurance Statements, significant system improvement efforts are in progress to modernize, certify, and accredit all financial management systems to conform to government-wide requirements.

Financial Management Systems

Pursuant to the Chief Financial Officers Act of 1990, the DHS Chief Financial Officer (CFO) is responsible for developing and maintaining agency accounting and financial management systems to ensure systems comply with applicable accounting principles, standards, and requirements and with internal control standards. As such, the DHS CFO oversees and coordinates all financial system modernization efforts.

The Department adopted a decentralized strategy and will modernize individual Component financial systems, as needed. This incremental approach is consistent with OMB guidance and will allow the Department to leverage existing shared service providers' proven systems and processes in concert with DHS-wide policy and standards for implementations, instead of making costly investments in new systems. The Department is working to ensure programs are planned and executed to meet reporting requirements, minimize costs for financial operations, improve compliance with financial management standards such as FFMIA, and make certain that financial management systems have internal controls in place to support the DHS mission.

In FY 2016, the Department achieved a major system modernization milestone when DNDO migrated to the DOI IBC solution. DHS is leveraging the lessons learned from this shared services implementation, reducing risk in future migrations through deliberative approaches to resource management, business process re-engineering, change management, and scheduling rigor and oversight. In FY 2017, the Department will continue its efforts towards modernizing financial systems across the Department. Components within DHS are at different milestones in their modernization timeline, for example components like ICE and their serviced components are early in discovery, and TSA and USCG are in various planning phases. FEMA has also entered the very early stages of their planned future modernization.

Through the FSM initiative, the Department is working to improve existing financial systems to better meet FFMIA requirements. Components considering a shared service provider for their financial management system modernization will consult OMB A-123, Appendix D for the minimum requirements an external provider must demonstrate including FFMIA requirements.

Federal Information Security Modernization Act of 2014

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 FY 2015 FISMA report, OIG-16-08, Revised, Evaluation of DHS' Information Security Program for Fiscal Year 2015, cited six open recommendations. The Office of the Chief Information Security Officer (OCISO) implemented several corrective actions to close the recommendations from OIG-16-08. These actions included improving OCISO's recently established process of facilitating quarterly meetings between the Deputy Under Secretary of Management, DHS CIO and CISO, and Component Executive Leadership. The quarterly discussions focused on a Component's status in achieving FISMA compliance targets and explaining lags in progress and planned actions to meet agreed upon targets timely. DHS launched a formal IT Weakness Remediation project. This project included working with the Components to develop effective weakness remediation plans, improving status reporting, and providing bi-weekly progress of plans of action and milestones. The Department also implemented additional database checks to ensure that the data used to generate the DHS FISMA monthly scorecards is consistent with the data in Component feeder systems. To further accomplish this, OCISO verifies the data with the Components prior to finalizing the monthly scorecard. In April 2016, the Office of Inspector General's evaluation of corrective actions taken on OIG-16-08 reported that four of the six recommendations issued were closed.

The Office of Inspector General's FY 2016 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.