Annual Performance Report

Fiscal Years 2017-2019

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

▶ We are DHS

About this Report

The U.S. Department of Homeland Security Annual Performance Report for Fiscal Years (FY) 2017-2019 presents the Department's performance measures and applicable results, provides the planned performance targets for FY 2018 and FY 2019, and includes information on the Department's Strategic Review and our Agency Priority Goals. Additionally, this report presents information on the Department's reform agenda (in compliance with Executive Order 13781), regulatory reform, the Human Capital Operating Plan, and a summary of our performance challenges and high-risk areas identified by the DHS Office of the Inspector General and the Government Accountability Office. The report is consolidated to incorporate our annual performance plan and annual performance report.

For FY 2017-2019, 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 | Publication date: November 15, 2017.
- DHS Annual Performance Report | Publication date: February 5, 2018
- DHS Report to our Citizens (Summary of Performance and Financial Information) | Publication date: February 2018.

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

Contact Information

For more information, contact:

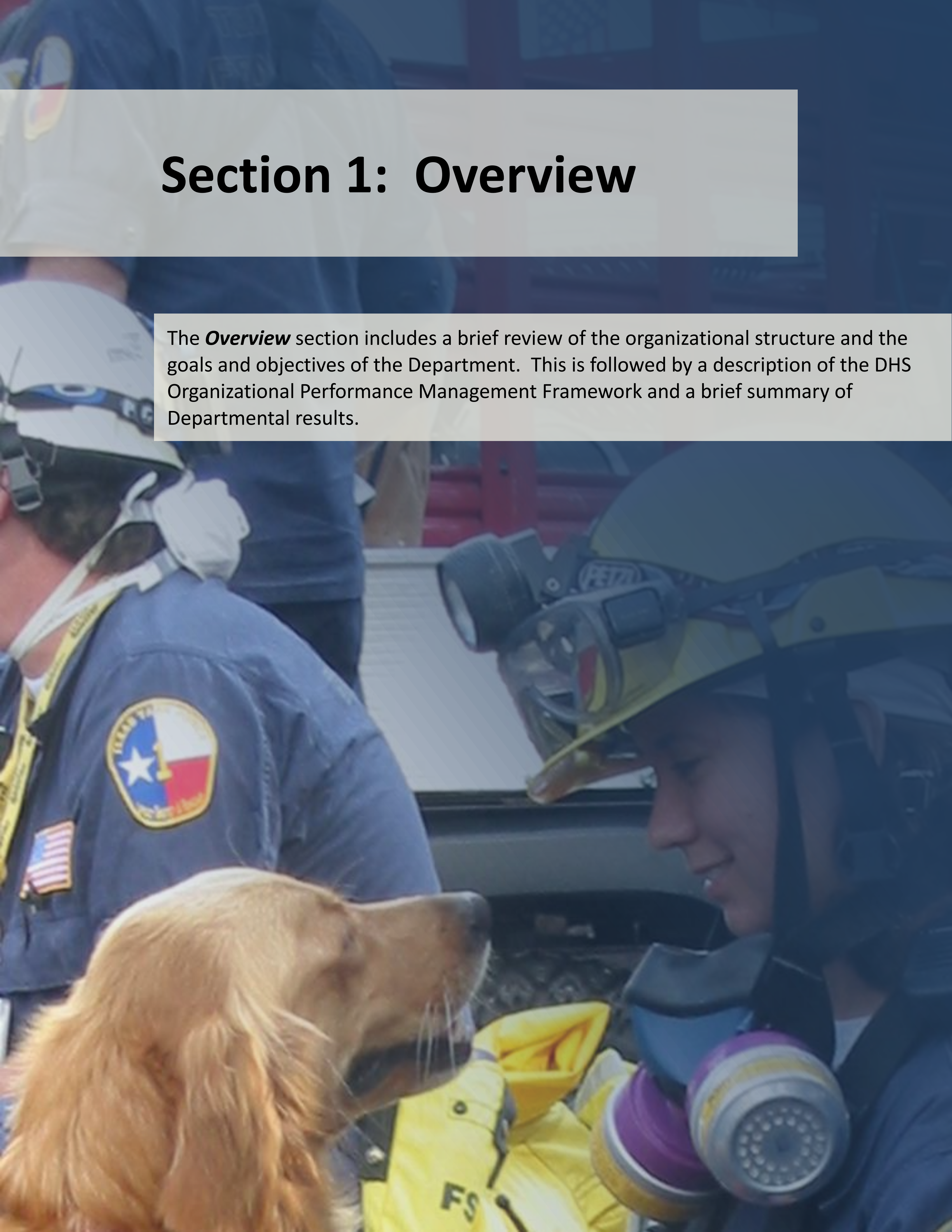
Department of Homeland Security
Office of the Chief Financial Officer
Office of Program Analysis and Evaluation
245 Murray Lane, SW
Mailstop 200
Washington, DC 20528

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

Table of Contents

Section 1: Overview

The ***Overview*** section includes a brief review of the organizational structure and the goals and objectives of the Department. This is followed by a description of the DHS Organizational Performance Management Framework and a brief summary of Departmental results.

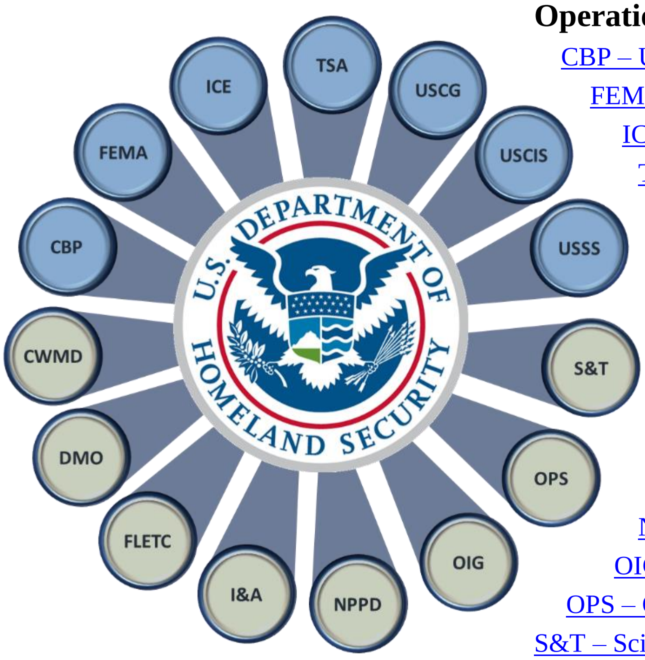


Introduction

The Department of Homeland Security (DHS) is always seeking ways to communicate the value we provide to stakeholders. This report provides a picture of our performance results for FY 2017, along with those planned for FY 2018-2019, aligned to our organizational structure. It satisfies the requirement to publish the Department's FY 2017-2019 Annual Performance Report and Annual Performance Plan. DHS uses our strategic set of measures contained in this report as a means to communicate our progress and the value we provide to our stakeholders. Additional performance measure information is also provided in the Overview chapter of each Component's Congressional Budget Justification, which contains both our strategic and management measures. This report may also be found on our public web site at Performance & Financial Reports, and the Component Congressional Justification chapters are located at DHS Budget.

Organization

DHS's operational Components lead the Department's frontline activities to protect our Nation (shaded in blue). The remaining DHS Components (shaded in light green) provide resources, analysis, equipment, research, policy development, and support to ensure the frontline organizations have the tools and resources to accomplish the DHS mission. For the most up to date information on the Department's structure, visit our web site at http://www.dhs.gov/organization.



Operational Components

CBP – U.S. Customs and Border Protection

FEMA – Federal Emergency Management Agency

ICE – U.S. Immigration and Customs Enforcement

TSA – Transportation Security Administration

USCG – U.S. Coast Guard

USCIS – U.S. Citizenship and Immigration Services

USSS – U.S. Secret Service

Support Components

CWMD – Countering Weapons of Mass Destruction Office

DMO – Departmental Management and Operations

FLETC – Federal Law Enforcement Training Centers

I&A – Office of Intelligence and Analysis

NPPD – National Protection and Programs Directorate

OIG – Office of Inspector General

OPS – Office of Operations Coordination

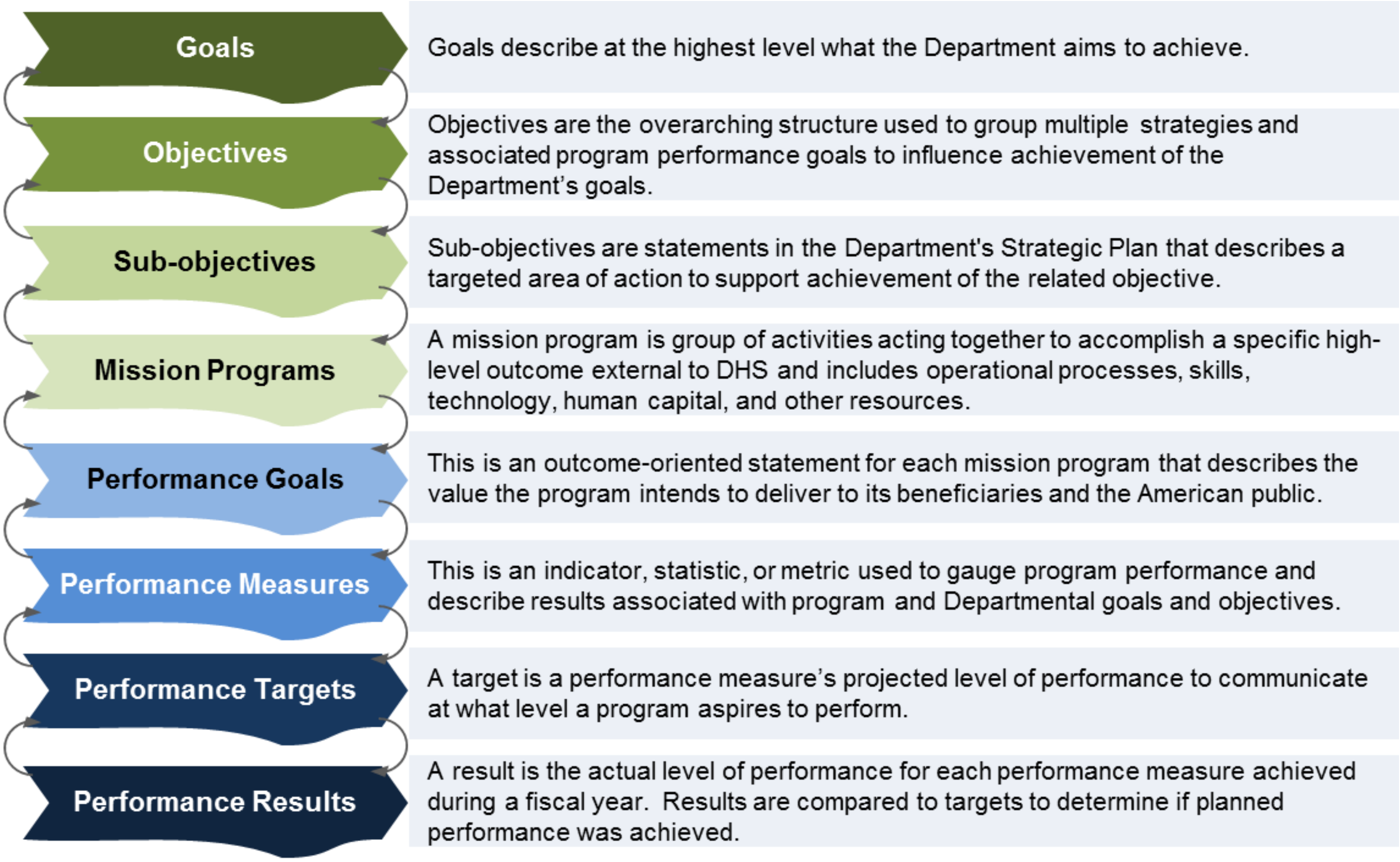
S&T – Science and Technology Directorate

Figure 1: DHS Operational and Support Components

How Our Measures Align to Strategy

The figure below shows the linkage between the Department's strategic structure, the Department's mission programs, and the measures we use to gauge performance. This approach to measurement ensures that DHS can assess the achievement of our goals and our progress in achieving Unity of Effort across the organization.

Due to the timing and movement of key DHS leadership positions during this transition year, we are presenting this year's Annual Performance Report aligned to our Components. We will resume presentation of our performance results and plan aligned to the agency strategic structure in the FY 2018 – 2020 Annual Performance Report.



Goals describe at the highest level what the Department aims to achieve.

Objectives are the overarching structure used to group multiple strategies and associated program performance goals to influence achievement of the Department's goals.

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

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

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.

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

A target is a performance measure's projected level of performance to communicate at what level a program aspires to perform.

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

Figure 2: DHS Performance Cascade

DHS Organizational Performance Management Framework

DHS has a performance framework that drives performance management and enables the implementation of performance initiatives. As depicted in the following graphic, DHS leverages our Performance Community to implement key initiatives driven by the original Government Performance and Results Act (GPRA), and signify the enduring foundation of DHS's framework. The Agency Priority Goals, Performance Review, and the Strategic Review are the newer initiatives introduced by the GPRA Modernization Act (GPRAMA).

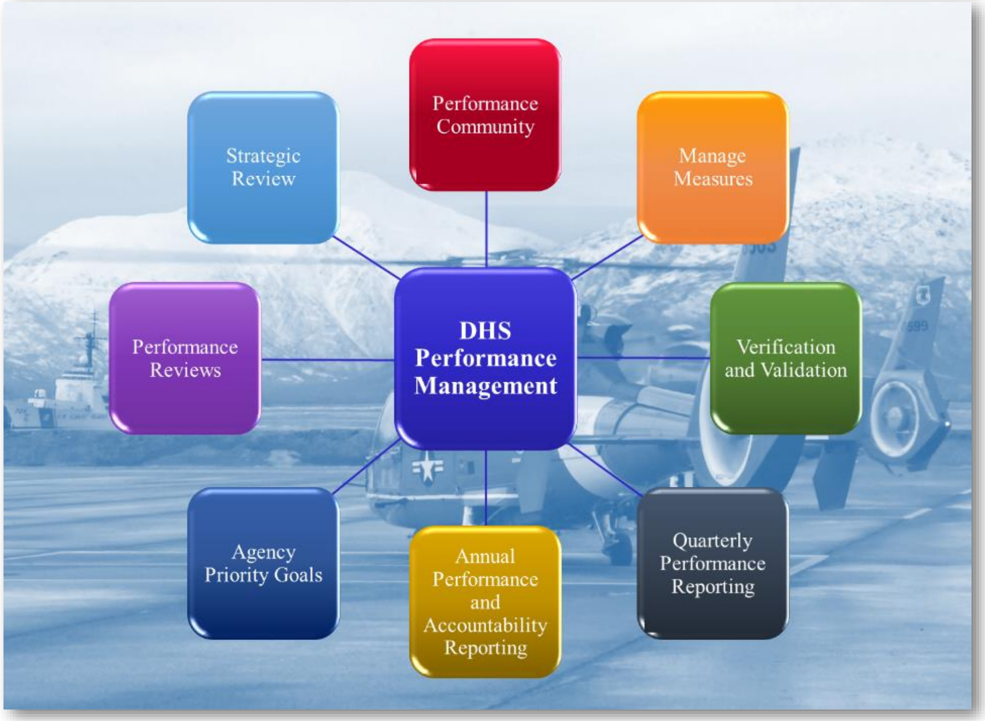

Performance Community
Strategic Review
Manage Measures
Performance Reviews
DHS Performance Management
Verification and Validation
Agency Priority Goals
Annual Performance and Accountability Reporting
Quarterly Performance Reporting

Figure 3: DHS Performance Management Framework

Performance Community

The DHS performance community is led by the Chief Operating Officer (COO), the Performance Improvement Officer (PIO), the Deputy PIO (DPIO), and the Assistant Director for Performance Management, all who are supported by performance analysts in the Office of Program Analysis and Evaluation (PA&E) located under the DHS Chief Financial Officer (CFO). In DHS, the COO and PIO are involved in managing performance through a variety of venues. The performance community also includes Component PIOs and Agency Priority Goal (APG) Leads—the senior leaders driving performance management efforts in their respective Components—interacting with senior DHS leadership on performance management issues. Component performance analysts are the performance measurement experts within their Component who communicate key guidance to program managers, provide advice on measure development concepts, collect and review quarterly and year-end data, coordinate with Component leadership on communicating results internally, and are the primary points of contact within Components on GPRAMA initiatives.

At the headquarters level, leadership and performance analysts in CFO/PA&E manage GPRAMA performance initiatives for the Department under the direction of the COO and PIO, along with guidance provided by the CFO. CFO/PA&E performance analysts are the liaison among internal and external stakeholders on performance matters, managing implementation of the framework outlined above, and ensuring the Department meets its GPRAMA responsibilities. CFO/PA&E brings together this community, shown in the diagram below, to drive performance initiatives.

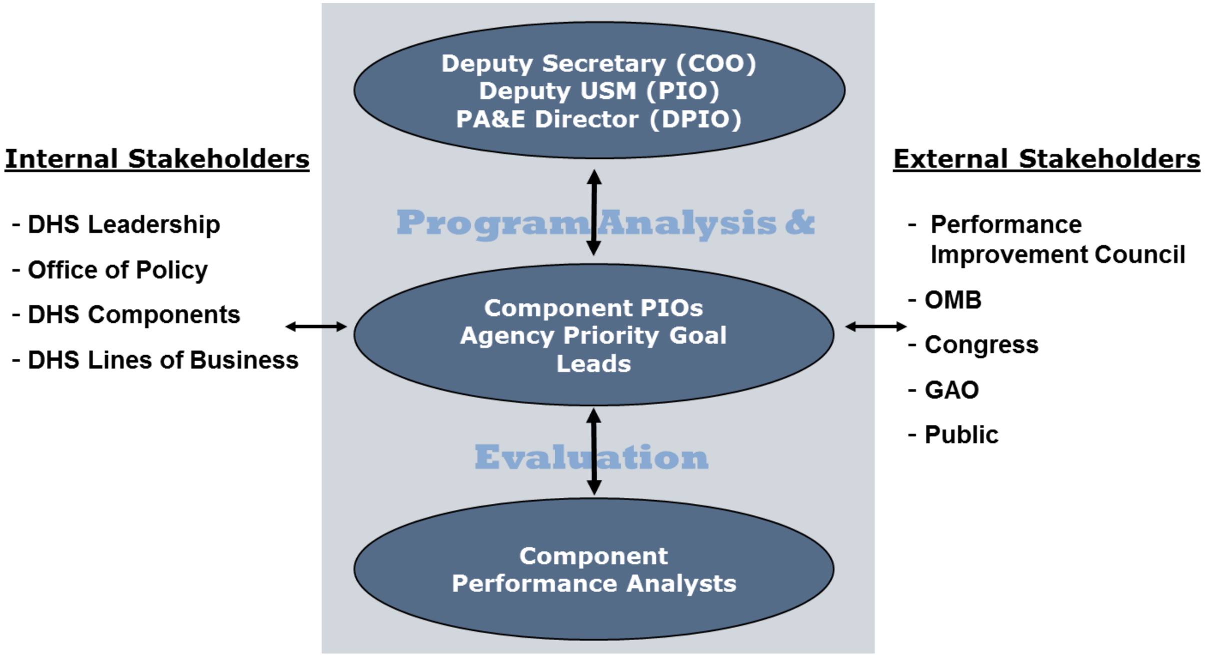


Figure 4: DHS Organizational Performance Community

Managing our Measures

With the support of leadership, CFO/PA&E initiates the annual measure improvement process to enhance our set of publicly reported measures to more effectively convey the results delivered to advance the department's strategy. Improvement ideas are derived from several sources:

- Feedback provided by senior leadership to mature our ability to describe the value delivered by DHS;
- Suggestions from the Office of Management and Budget (OMB) to achieve greater visibility into program performance and connection to program resources;
- Recommendations from other external stakeholders such as the Government Accountability Office (GAO) and Congress;
- Suggestions from CFO/PA&E performance analysts working to fill gaps and improve quality; and
- Component leadership and program managers wishing to continually implement measures that are meaningful to their business operations.

While this is a very iterative process, it generally follows the timing described in the next figure. The process begins in the fall where we concurrently implement the new measures in the agency performance plan, along with holding discussions regarding gaps and areas for improvement for the following fiscal year. In collaboration with Component programs and CFO/PA&E performance analysts, new measures concepts are developed. These concepts are then reviewed by Component leadership and submitted to DHS by June 30th. Headquarters performance analysts working in concert with leadership approve changes, which are then submitted to OMB for their review and approval. The results of this process constitute our publicly reported measures associated with our performance budget deliverables, namely our strategic and management set of measures, which are then published in the Department's APR and the Overview Chapters of the Congressional Justification.

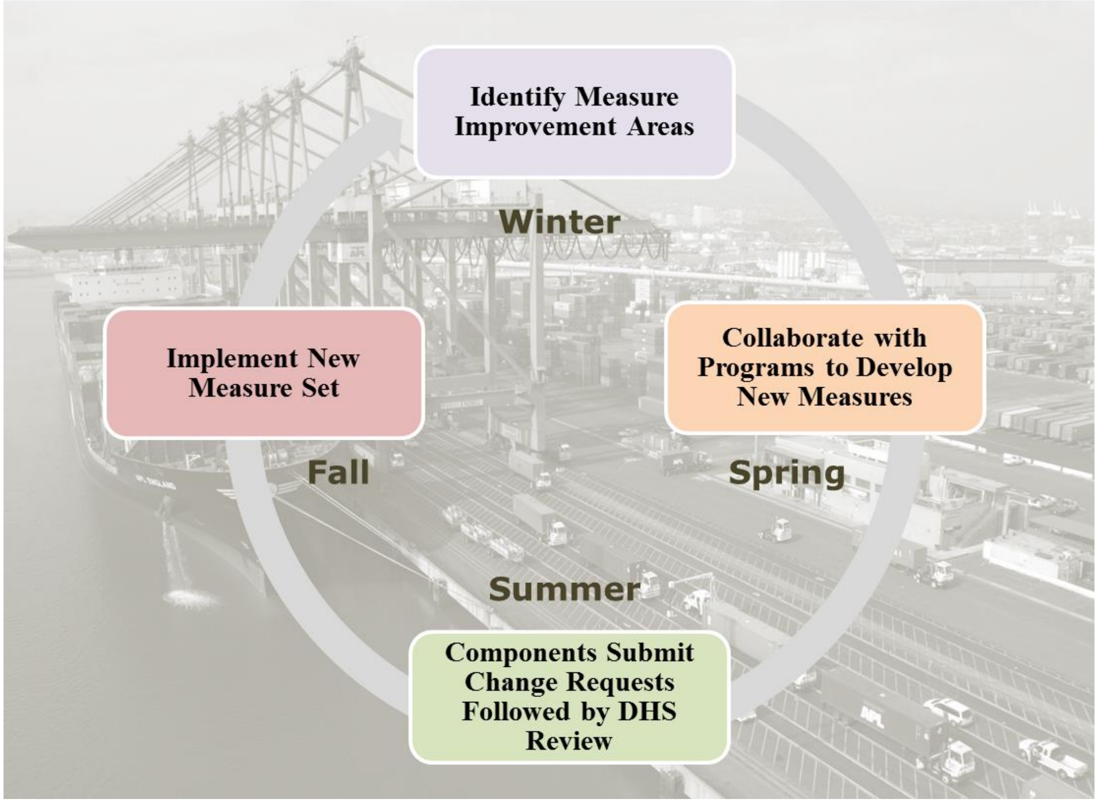

Identify Measure Improvement Areas
Winter
Collaborate with Programs to Develop New Measures
Spring
Summer
Components Submit Change Requests Followed by DHS Review
Fall
Implement New Measure Set

Figure 5: DHS Annual Measure Improvement Process

Performance Data Verification and Validation

The Department recognizes the importance of collecting complete, accurate, and reliable performance data since this helps determine progress toward achieving program and Department goals. Performance data are considered reliable if transactions and other data that support reported performance measures are properly recorded, processed, and summarized to permit the preparation of performance information in accordance with criteria stated by management. OMB Circular A-136, Financial Reporting Requirements, OMB Circular A-11, and the Reports Consolidation Act of 2000 (P.L. No. 106-531) further delineate this responsibility by requiring agencies to ensure completeness and reliability of the performance data they report by putting management assurance procedures in place.

DHS has implemented a multi-pronged approach to effectively mitigate risks and reinforce processes that enhance the Department's ability to report complete and reliable data for GPRAMA performance measure reporting. This approach consists of: 1) an annual change control process that uses a tool called the Performance Measure Definition Form (PMDF); 2) a central information technology repository for performance measure information; 3) a Performance Measure Checklist for Completeness and Reliability; and 4) annual assessments of the completeness and reliability of a sample of our performance measures by an independent review team.

Annual Change Control Process and the PMDF

CFO/PA&E has used a continuous improvement process as a means to mature the breadth and scope of our publicly reported set of measures. This process employs a tool known as the PMDF that provides a structured format to operationally describe every measure we publicly report in our performance deliverables. The PMDF provides instructions on completing all data fields and includes elements such as the measure name, description, scope of data included and excluded, where the data is collected and stored, a summary of the data collection and computation process, and what processes exist to double-check the accuracy of the data to ensure reliability. These data fields on the form reflect GAO's recommended elements regarding data quality.[1] The PMDF is used as a change management tool to propose and review new measures, make changes to existing measures, and to retire measures we want to remove from our strategic and management measure sets. This information is maintained in a Department central data repository, discussed next, and is published annually as Appendix A to our Annual Performance Report.

Central Information Technology (IT) Repository for Performance Measure Information

All of DHS's approved measures are maintained in the *FYHSP System*, which is a Department-wide IT system accessible to all relevant parties in DHS. The system is a modular database which allows for the management of the Department's performance plan and the capturing of performance results on a quarterly basis. The *FYHSP System* stores all historical information about each measure including specific details regarding: scope; data source; data collection methodology; and explanation of data reliability check. The data in the system are then used as the source for all quarterly and annual Performance and Accountability Reporting. Finally, the performance data in the *FYHSP System* are used to populate the Department's business intelligence tools to provide real-time information.

Performance Measure Checklist for Completeness and Reliability

The Performance Measure Checklist for Completeness and Reliability is a means for Component PIOs to attest to the quality of the information they are providing in our performance and accountability reports. Using the *Checklist*, Components self-evaluate key controls over GPRAMA performance measure planning and reporting actions at the end of each fiscal year. Components describe their control activities and provide a rating regarding their level of compliance and actions taken for each key control. Components also factor the results of any internal or independent measure assessments into their rating. The *Checklist* supports the Component Head assurance statements attesting to the completeness and reliability of performance data. Individual Component Head assurance statements serve as the primary basis for the assertion whether or not the Department has effective controls over financial and performance reporting.

Independent Assessment of the Completeness and Reliability of Performance Measure Data

CFO/PA&E conducts an assessment of performance measure data for completeness and reliability on a subset of its performance measures annually using an independent review team. This independent review team assesses selected Component GPRAMA measures using the methodology prescribed in the *DHS Performance Measure Verification and Validation Handbook*, documents its findings, makes recommendations for improvement, and may perform a subsequent follow-up review to observe the implementation of recommendations.

[1] Managing for Results: Greater Transparency Needed in Public Reporting Quality of Performance Information for Selected Agencies' Priority Goals (GAO-15-788). GAO cited DHS's thoroughness in collecting and reporting this information in their review of the quality of performance information in their report.

Corrective actions are required for performance measures that rate low on the scoring factors. The Handbook is made available to all Components to encourage the development and maturation of internal data verification and validation capabilities, increase transparency, and facilitate the review process. The results obtained from the independent assessments are also used to support Component leadership assertions over the reliability of their performance information reported in the Performance Measure Checklist and Component Head Assurance Statement.

Management Assurance Process for GPRAMA Performance Measure Information

The Management Assurance Process requires all Component Heads in DHS to assert that performance measure data reported in the Department's Performance and Accountability Reports are complete and reliable. If a measure is considered unreliable, the Component is directed to report the measure on the Performance Measure Checklist for Completeness and Reliability along with the corrective actions the Component is taking to correct the measure's reliability.

The DHS Office of Risk Management and Assurance, within the Office of the CFO, oversees the management of internal controls and the compilation of many sources of information to consolidate into the Component Head and the Agency Assurance Statements. The Agency Financial Report contains statements in the Management Assurance section attesting to the completeness and reliability of performance measure information in our Performance and Accountability Reports and that any unreliable measures and corrective actions are specifically reported in the Annual Performance Report.

Based on the process described above, all performance information is deemed complete and reliable except for the following measure(s): *Percent of incidents detected by the U.S. Computer Emergency Readiness Team for which targeted agencies are notified within 30 minutes*.

This measure has had data collection issues during FY 2017 that could not be corrected to produce a reliable result. The issue was that analysts were inconsistently time stamping incident tickets that start the clock on how long the U.S. CERT team has to notify the affected agency. The analysts were supposed to timestamp the ticket with the time that it was determined that the event is an incident. Analysts were time stamping the tickets using various criteria and the program could not go back and fix the accuracy of the data. The program has taken corrective actions and reliable data will be available in FY 2018.

Quarterly Performance Reporting

Quarterly reporting of the Department's strategic and management measures is provided by the various Components, reviewed by DHS Headquarters staff, and entered into our centralized IT system known as the FYHSP System which is maintained by CFO/PA&E. This information is then packaged and presented to DHS leadership and made available to internal managers as desired to support their on-going program management activities.

Performance and Accountability Reporting

The Department follows the Office of Management and Budget Circular A-136 and A-11 guidance to produce the following reports:

- DHS Agency Financial Report;
- DHS Annual Performance Report; and
- DHS Summary of Performance and Financial Information.

Combined, these reports comprise our annual performance and accountability reporting requirements. When published, all three reports are located on our public website at Performance & Financial Reports.

Agency Priority Goals

Agency Priority Goals (APGs) are one of the tenets of GPRAMA and provide opportunities for leadership to significantly drive improvement in near-term performance. APGs are defined for a two-year implementation period and the timeline is directed by OMB. DHS has historically had several APGs focusing on key leadership priorities linked to our strategic plan goals. More detailed information on the DHS APGs is presented in Section 3: Other Information.

Performance Reviews

DHS has implemented the Performance Review initiative of GPRAMA as a means for senior leadership to be engaged in the management of efforts to deliver performance results relevant to stakeholders. This process starts with the APG Goal Leads providing quarterly progress updates and measure results with explanations. These results are then examined and discussed by Department Headquarters Staff prior to reporting results to OMB for presentation on performance.gov.

Strategic Reviews

DHS conducted its fourth annual Strategic Review for the sixteen strategic goals in the DHS FY 2014-2018 Strategic Plan. For each strategic goal, teams were assembled to assess progress in the implementation of our strategic goals and propose goal progress ratings. A Headquarters team conducted a cross cutting review of the teams' assessments and made recommendations to leadership regarding goal progress ratings. Discussions among senior leaders finalized the Department's progress ratings for FY 2017. For a list of our goals that rated Noteworthy or were a Focus Area see Section 3: Other Information.

Departmental Summary of Results

A review of the results at the close of FY 2017 demonstrates that 63 percent of the Department's strategic measures met their targets as shown in the table on the next page. Upon further review, 72 percent of measures sustained or improved performance from FY 2016. The FY 2018-2019 performance plan includes a total of 99 measures, representing 7 measures that were retired from our previous performance plan and the introduction of 9 new measures.

This year's overall results are consistent with historical results. The following chart shows that the measures meeting their target on an annual basis varied between 63 to 68 percent from FY 2011 through FY 2017. Likewise, the percent of measures that maintained or improved over the prior year ranged from 70 to 78 percent. These results are consistent with programs that set ambitious and challenging performance targets as directed by OMB.

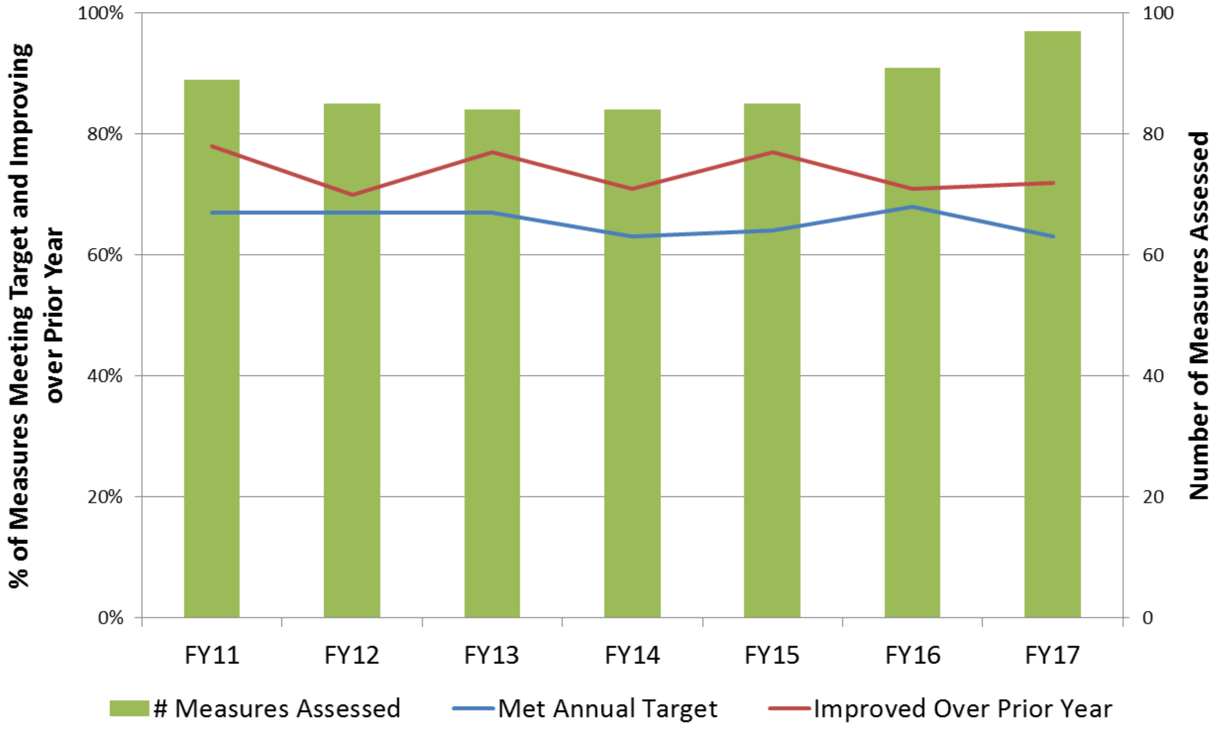
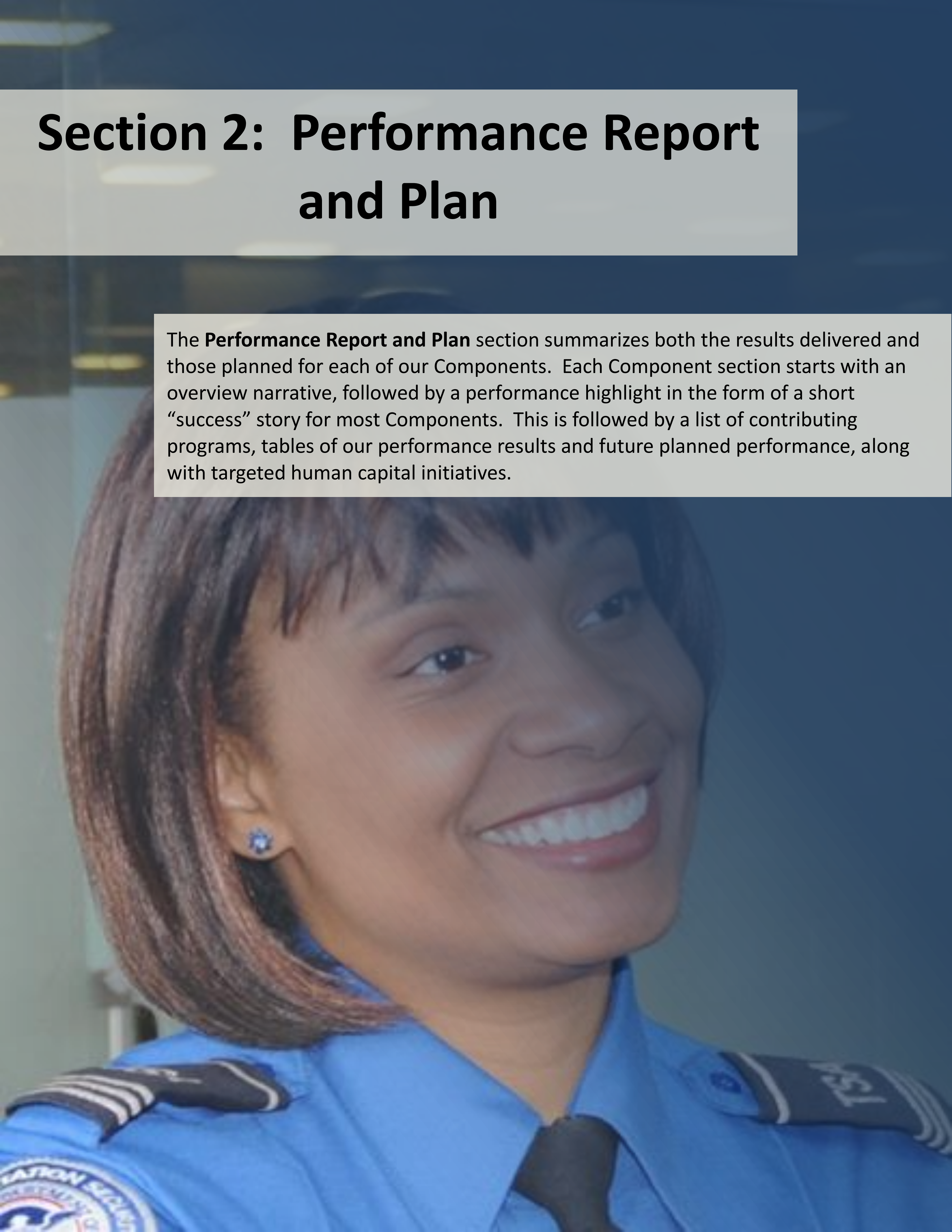


Figure 6: Percent of Measures Meeting Target and Improving over Prior Year

Section 2: Performance Report and Plan

The **Performance Report and Plan** section summarizes both the results delivered and those planned for each of our Components. Each Component section starts with an overview narrative, followed by a performance highlight in the form of a short "success" story for most Components. This is followed by a list of contributing programs, tables of our performance results and future planned performance, along with targeted human capital initiatives.



DHS Performance by Component

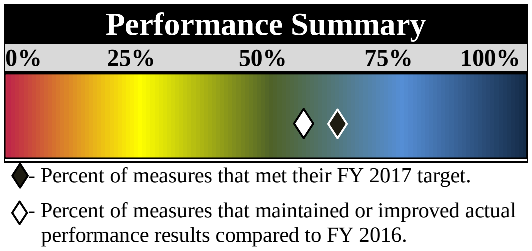
The DHS Performance by Component section of this report presents information for each Component within the Department that has strategic measures. Each Component begins with an overview to include performance, process, and challenges and risks. Next, a short "success" story from FY 2017 is provided and is followed by a list of contributing mission programs and a description of what they deliver. The final section for each Component is the Performance *Results and Plan* information, presenting measure results and future planned performance. For the performance measures, prior fiscal year results are presented for trend analysis. For those measures that did not meet their current year targets, explanations with corrective action are provided. In addition, changes to measure names and targets from the previous year's report are identified. To continually improve our set of performance measures, new measures are introduced and measures are retired each year and are identified, if applicable, in the measure tables.

Customs and Border Protection

Overview

U.S. Customs and Border Protection's (CBP) priority mission is securing the U.S. border and keeping terrorists and their weapons out of the U.S. It also is responsible for securing and facilitating trade and travel while enforcing hundreds of U.S. regulations, including immigration and drug laws.

In FY 2017, there were 11 strategic performance measures used to assess CBP's efforts. In FY 2017, 64 percent of the measures met their target and 56 percent maintained or improved actual results compared to FY 2016.



Progress: Lawful trade and travel are critically important to the health of our Nation's economy and vitality of our society. This is made clear by the steady increase in both business and tourist travelers who chose to visit the United States, and by the continued increases in the volume of imports and exports. With trade and travel projected to continue to grow, DHS and its partners must work to secure and expedite the increasing flows of people and goods to keep our Nation safe and prosperous.

Centers of Excellence and Expertise continue to increase uniformity of practices across ports of entry, facilitate the timely resolution of trade compliance issues nationwide, and further strengthen critical agency knowledge on key industry practices. DHS continued to expand the Customs-Trade Partnership Against Terrorism (C-TPAT), improving the security of private companies' supply chains against terrorism while focusing on better resource management. DHS managed the screening of nearly 400 million people entering the U.S. by implementing the improved use of innovative timesaving technologies and processes such as Global

CBP is deploying new technologies to verify travelers' identities – both when they arrive and when they leave the United States.

Entry, Pedestrian Ready Lanes, and a redesigned I-94 web portal, all of which resulted in reduced traveler wait times.

DHS continues to impact U.S. border security through targeting, screening, and apprehensions with situational awareness improvements along the Southwest Border. CBP maintained interdiction rates along the land border and CBP's Air and Marine Operations Center has sustained results in cross border conventional aircraft incursions. The U.S. Border Patrol initiated the Northern Border Coordination Center to act in a collaborative capacity with sectors and stakeholders to address information sharing on current and emerging threats. DHS conducted outreach and expanded its international footprint in Mexico and Central America by providing resources and personnel to train, advise, and assist partners to improve U.S. security.

Challenges and Risks: The U.S. border consists of 1,933 miles of southern border and 3,987 miles of northern border to secure. It is a dynamic environment where the means and tactics used by transnational criminal organizations and others to illegally cross and transport people, drugs, and illegal items is always shifting. Recent policy shifts have impacted some of the recent increased flows of illegal immigrants, along with laying out new priorities related to impedance and denial methods in terms of physical barriers and goals for operational control and interdiction success.

DHS is working to meet requirements outlined *Executive Order (EO) 13767: Border Security and Immigration Enforcement Improvements*. DHS is implementing an Agency Priority Goal for FY 2018-2019 that will advance our ability to gain and maintain operational control of, and ultimately secure, the border. See the *Introduction of FY18-19 APGs* section for more information on this effort and associated performance measures.

At Ports of Entry, smugglers continue to use a variety of tactics and techniques for concealing drugs and humans, making detection harder. In addition, the use of counterfeit documents appears to have been replaced by migrants presenting as impostors with otherwise lawful documents.

Human Capital Strategies

The large challenge facing CBP in the implementation of *EO 13767* is the increased staffing goals for Border Patrol agents. DHS has not recently been able to meet our current hiring authority for agents due to a variety of factors. In addition, retention of agents is a challenge due to the demanding nature of the job and the remote physical locations where these staff are required to live.

In response to the directive to hire an additional 5,000 Border Patrol Agents, CBP's Human Resource Management (HRM) office has developed a multi-year hiring plan to meet the new staffing requirement for Border Patrol. Of the 5,000 planned agent increase, the first surge is planned for 500 agents in FY 2018 and is in addition to the normal attrition hiring conducted by CBP HRM. This initial hiring surge will lay the foundation for increasing operational control in certain key areas along the border. The goal is to increase and maintain a Border Patrol Agent workforce to gain and maintain operational control of the border.

CBP's HRM office has developed a 4-step plan to achieve success which includes:
1) expanding authorities to do direct hires, improve qualification standards, and achieve background investigation reciprocity;
2) improving business processes to achieve 65 percent reduction in time-to-hire; 3) enhancing recruitment through more effective digital and TV campaigns as well as targeted sponsorships; and increasing mobility and incentives to improve retention.

Revenue Collection and Revenue Gap

Revenue collection is one of CBP's most important and oldest functions, and has recently been re-designated as a Priority Trade Issue (PTI) for the agency, per the Trade Facilitation and Trade Enforcement Act of 2015, signed into law in February 2016. The Revenue PTI focuses on enforcing trade laws, facilitating legitimate trade, and collecting lawfully owed duties and fees.

The Revenue National Targeting and Analysis Group (NTAG), located in Chicago, Illinois, provides a national strategic perspective on trade through risk analysis and multidisciplinary trade strategies. It develops and applies risk management techniques to support trade security and trade compliance. The NTAG targets and identifies concerns that place revenue at risk through a variety of methods, including: 1) Analyzing import data to identify revenue risk; 2) Monitoring the effectiveness of targeting programs; 3) Investigating referrals received through a number of channels such as the e-Allegations system; and 4) Ensuring proper controls and oversight of the drawback process.

Since CPB is the 2nd largest collector of revenue for the U.S. Treasury, even a small improvement in collections has an enormous impact as was seen in 2017. As of September 30, 2017, the current estimate of CBP's overall under-collections improved by more than $300 million dollars from FY 2016. CBP thoroughly scrutinizes revenue collection because of illicit attempts to evade duties and fees, which defraud the U.S. Government and undermine lawful business.

The Revenue PTI supports CBP's mission by: 1) facilitating the movement of legitimate trade by enabling fair and lawful trade and travel, segmenting risk, and focusing actions in the post-entry environment; 2) improving U.S. economic competitiveness by enforcing trade laws while regulating and ensuring proper revenue collection; 3) pursuing revenue collection through a risk-based approach to identify and address violators and their circumvention schemes; and 4) promoting mechanisms, both traditional and innovative, to address revenue risks, while also improving trade intelligence and collaboration with partners.

Mission Programs

The mission programs that deliver performance results for this objective are:

- **Border Security Operations:** The Border Security Operations program is charged with securing America's Southwest, Northern, and Coastal borders in coordination with the U.S. Coast Guard. Through the coordinated use of the Department's operational capabilities and assets of the U.S. Border Patrol and Air and Marine Operations, Customs and Border Protection improves operational effectiveness by working across the Department to prevent terrorists and terrorist weapons, illegal aliens, smugglers, narcotics, and other contraband from moving across the U.S. border.
- **Trade and Travel Operations:** Managed by the Office of Field Operations and the Office of Trade, the Trade and Travel Operations program allows the Department to better intercept potential threats at the ports before they can cause harm while expediting legal trade and travel. The program includes a multi-layered system of people, technology, intelligence, risk information, targeting, international cooperation, and expanded shipper and traveler vetting that provides greater flexibility and capacity to accomplish these functions prior to arrival at the U.S. border.

Performance Results and Plan

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Trade and Travel								
Amount of smuggled outbound currency seized at the ports of entry (in millions) (CBP)								
$31.9	$36.9	$37.7	$37.6	$28.9	$30.0	$39.0	$30.0	$30.0
Number of smuggled outbound weapons seized at the ports of entry (CBP)								
---	731	411	505	661	400	421	400	400
Percent of cargo by value imported to the U.S. by participants in CBP trade partnership programs (CBP)								
54.7%	55.2%	53.9%	52.2%	53.0%	53.0%	53.1%	53.0%	53.0%
Percent of import revenue successfully collected (CBP)								
98.88%	98.73%	99.56%	98.61%	99.06%	100%	99.05%[1]	100%	100%
Percent of imports compliant with U.S. trade laws (CBP)								
96.46%	97.66%	97.99%	98.89%	99.18%	97.5%	99.38%	97.5%	97.5%
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)								
98%	98%	99.22%	99.76%	99.28%	100%	99.50%[2]	100%	100%

[1] – Customs and Border Protection deploys a multi-pronged approach to trade facilitation and enforcement: informed compliance; stakeholder engagement; and structured summary targeting to manage the $2.4 trillion in imports which enter the U.S. The small percent of under collections is due to misclassifications associated with commercial trucks from Canada, water heater parts from Malaysia, ceiling fans from China, and nonwoven laminated fabrics from China; false preferential Free Trade Agreement claims from South Korea and Canada North American Free Trade Agreement; and finally Anti-Dumping / Counter-vailing Duties evasion on paper products and rubber tires from China. Various enforcement methods such as audits, targeting, and statistical random sampling will be incorporated to bridge the revenue gap. As part of its formal Trade Compliance Measurement process, the Office of Trade will provide the significant revenue discrepancies to the relevant National Targeting and Analysis Groups (NTAG) for analysis and operation or targeting formulation. The NTAGS will in turn work with the Centers of Excellence and Expertise to mitigate the trade risk through additional enforcement actions and trade outreach efforts.

[2] – This measure gauges the overall percent of inbound cargo identified as potentially high risk by the Automated Targeting System (ATS) in the sea, air, and land environments that is reviewed, scanned, or otherwise examined prior to loading or at arrival at a US port of entry. Significant methodology revisions to the inbound targeting algorithms for vessel and air modes to improve targeting effectiveness began in FY 2016 and were fully implemented by May 2017. Borderstat data extraction routines were not updated to reflect the new targeting methodology in ATS until after the changes were tested and made permanent, and final ATS targeting report updates were completed in August 2017. The net effect was a slight decrease in examinations for air mode and a larger decrease for vessel mode during this transition. To improve measure results, the CBP Office of Field Operations will continue to work with the Targeting & Analysis Systems Program Directorate to resolve status tracking problems and information processing errors and with shippers and carriers to rectify logistical and scheduling issues.

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Border Operations								
Percent of detected conventional aircraft incursions resolved along all borders of the United States (CBP)								
96.0%	99.3%	98.8%	99.3%	99.7%	98.5%	97.9%[1]	98.5%	98.5%
Percent of people apprehended multiple times along the southwest border (CBP)								
---	16%	14%	14%	12.3%	≤ 17%	10.5%	≤ 17%	≤ 17%
Percent of recurring border surveillance implemented in remote low risk areas between ports of entry (CBP)								
---	---	---	---	---	70.0%	90.4%	93.0%[2]	96.0%

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Percent of time the U.S. Border Patrol meets its goal of responding to potential illegal activity in remote, low-risk areas (CBP)								
---	---	---	---	---	95.0%	96.4%	96.0%	97.0%
Rate of interdiction effectiveness along the Southwest Border between ports of entry (CBP)								
---	---	79.3%	81.0%	82.7%	81.0%	78.9%[3]	81.0%	81.0%

1 – In FY 2017 there were 188 of 192 border incursions that were resolved for an overall success rate of 97.9 percent. The Air and Marine Operations Center was unable to resolve four border incursion suspect tracks due to poor radar in the area where three aircraft were visually reported crossing the border, and one where there were no law enforcement assets to respond.

2 – FY 2018 target previously published as 80.0% in the FY 16-18 Annual Performance Report. Component updated targets to reflect prior year results and future expectations.

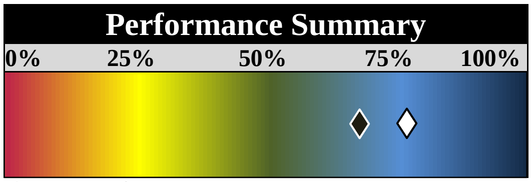
3 – This measure reports the percent of detected entrants who were apprehended, or turned back after illegally entering the United States between the ports of entry on the southwest border. The Border Patrol achieves this result by maximizing the apprehension of detected illegal entrants or confirming that illegal entrants return to the country from which they entered; and by minimizing the number of persons who evade apprehension. In FY 2017, this measure achieved 78.9 percent which is a decrease from FY 2016. Concurrently, border detection technology has increased, yielding greater situational awareness of illegal entrants who previously would have gone undetected, however agent staffing shortages reduce the ability to respond.

Federal Emergency Management Agency

Overview

The 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.

In FY 2017, there were 16 strategic performance measures used to assess FEMA's performance. In FY 2017, 69 percent of the measures met their target and 77 percent maintained or improved actual results compared to FY 2016.



◆- Percent of measures that met their FY 2017 target.

◇- Percent of measures that maintained or improved actual performance results compared to FY 2016.

Progress: The Department continues to make strides in decreasing risk and mitigating hazards. FEMA's efforts have led to increases in: the percent of communities in high earthquake, flood, and wind-prone areas that adopted disaster-resistant building codes; the percent of the population where Risk MAP has been deployed, enabling communities to take mitigation action to reduce risk; and the percent of U.S. population (excluding territories) covered by planned mitigation strategies.

DHS continues to build capabilities that enhance national preparedness by implementing the National Preparedness System. One of the key factors of the national preparedness system is the Threat and Hazard Identification and Risk Assessment (THIRA), which 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. More than half of states and territories have reported increases in average capability ratings.

Challenges: The Cascadia Rising exercise found that the emergency management community lacked the capacity to respond to the unique complexities of a truly catastrophic disaster and there remain gaps in catastrophic planning across the whole community. For example, many jurisdictions had not synchronized their plans with those of partner agencies, leading to gaps and duplication of effort. Challenges also exist in encouraging preparedness actions to be taken by historically underserved populations. There continue to be gaps in state and public preparedness; however, it is the responsibility of states to invest in their own capability and capacity needs. While State Preparedness Reports demonstrate a gradual increase, most jurisdictions' core capabilities are still significantly below their target.

While performance targets have been met in mitigating hazards and vulnerabilities, the debt owed by the National Flood Insurance Program (NFIP) is one barrier to the financial stability of the program. Additional barriers include policyholders not paying full risk rates including rates to cover catastrophic events. The Administration proposed reforms to address these barriers. In addition, DHS faces a challenge of increasing populations becoming vulnerable to natural and manmade disasters as critical infrastructure becomes more outdated. For instance, levees and dams are aging, and 40 percent are assessed as high risk, leaving unmitigated risk that can result in loss of life, property, and economic loss.

Human Capital Strategies

FEMA is working to address shortfalls in the incident workforce. The incident workforce has had an on-going problem in hiring, retention, and training and qualification. FEMA has begun a review of its force structure, and is configuring a two-pronged approach to address the problem. First is making sure that there is a steady pipeline of new incident workforce personnel. Second is making sure the training program aligns with the hiring tempo to ensure personnel are qualified and can be deployed.

Surge Capacity Force

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

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

In the immediate aftermath of Hurricanes Harvey, Irma, and Maria, Acting Secretary of Homeland Security Elaine Duke activated the Surge Capacity Force—the second time in the Surge Capacity Force existence. Surge Capacity Force volunteers from throughout the Federal Government supported disaster survivors in Texas, Florida, Puerto Rico, and the U.S. Virgin Islands. As of January 4, 2018, more than 4,000 federal employees were deployed for these relief efforts through the Surge Capacity Force.

Mission Programs

The mission programs that deliver performance results for FEMA are:

- **Disaster Relief Fund:** The Disaster Relief Fund is used to fund eligible response and recovery efforts associated with major domestic emergencies that overwhelm state and tribal resources pursuant to the Robert T. Stafford Disaster Relief and Emergency Assistance Act, P.L. 93-288, as amended. Through this fund, FEMA can authorize federal disaster support activities as well as eligible state, tribal, territorial, and local actions.
- **Education, Training, and Exercises:** The Education, Training, and Exercises program is comprised of the National Exercise Program and the National Training and Education Division, which includes the Emergency Management Institute, the Center for Domestic Preparedness, and the U.S. Fire Administration. These entities provide emergency management, response and recovery training, and exercise coordination to improve the knowledge, skills, and abilities of federal, state, local, tribal, and territorial emergency management personnel.
- **Grants:** FEMA's Grants program leads the Federal Government's financial assistance to state and local jurisdictions and regional authorities as they prepare, respond to, and recover from all hazards. The program provides grants to enhance jurisdictions' resiliency to man-made and other major disasters and to enhance their homeland security strategies.
- **Mitigation:** The Mitigation program works to strengthen mitigation nationwide to reduce the Nation’s vulnerability to natural disasters or other emergencies, and to facilitate adoption and enforcement of up-to-date design and construction practices through state and local building codes. The program supports activities that result in sound risk management decisions by individuals, the private-sector, and public-sector entities by conducting three core activities: risk analysis, risk reduction, and insurance against flood risk.
- **National Flood Insurance Fund:** The National Flood Insurance Fund aims to reduce the impact of flooding on public and privately-owned property by mapping areas of flood risk, providing flood insurance, encouraging communities to adopt and enforce sound floodplain management regulations, and paying claims.
- **Preparedness and Protection:** The Preparedness program works to prepare the Nation for disasters of all kinds. Preparedness includes the management and administrative support functions associated with training and national exercise programs.
- **Regional Operations:** The Regional Operations program includes the leadership, management, and mission support functions of the ten FEMA regions across the Nation. The program works with communities to reduce the impact of natural disasters; prepare families and individuals for all possible hazards; and support state, local, and tribal partners with technical assistance and grants for projects that aim to reduce risks, improve public safety, and protect the environment.
- **Response and Recovery:** The Response and Recovery program coordinates the core federal response capabilities used to save lives, and protect critical infrastructure in communities throughout the Nation that have been overwhelmed by the impact of a major disaster or an emergency.

Performance Results and Plan

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Man-made or Natural Incident Preparedness								
Percent of adults that took a preparedness action at their workplace, school, home or other community location in the past year (FEMA)								
---	---	---	---	---	90%	91%	92%	94%
Percent of federal agencies ready to initialize continuity of essential functions and services in the event of a catastrophic disaster (FEMA)								
---	---	---	96.6%	99.0%	97.0%	97.2%	98.5%	100%
Percent of states and territories that have achieved an intermediate or above proficiency to address their targets established through their THIRA (FEMA)								
---	---	---	---	66%	70%	70%	70%	70%
Percent of states and territories with a Threat and Hazard Identification and Risk Assessment (THIRA) that meets current DHS guidance (FEMA)								
---	86%	71%	77%	86%	100%	86%[1]	100%	100%
Percent of the U.S. population directly covered by FEMA connected radio transmission stations (FEMA)								
85%	90%	90%	90%	90%	90%	90%	90%	90%
Percent of time the Integrated Public Alert and Warning System (IPAWS) infrastructure is operating and available for use by federal, state, and local officials for the dissemination of emergency alerts (FEMA)								
---	---	---	---	99.8%	99.9%	99.9%	99.9%	99.9%

1 – In support of the National Preparedness System component "Identifying and Assessing Risk," FEMA annually determines the number of states and territories with approved risk assessments. Jurisdictions that receive preparedness grant funding from FEMA must use the Threat and Hazard Identification and Risk Assessment (THIRA) to annually identify and assess risk and establish capability targets based upon the risks they face. This information helps jurisdictions make programmatic decisions to build and sustain, plan for, and validate capabilities. Each year, FEMA analyzes state, territory, urban area, and tribal THIRA and State Preparedness Report (SPR) submissions using a checklist to evaluate if jurisdictions' THIRA submissions comply with DHS guidance per the Comprehensive Preparedness Guide 201 Second Edition: Threat and Hazard Identification and Risk Assessment Guide. In FY 2017, 48 out of 56 states and territories completed a THIRA that meets all steps of the current DHS guidance. States and territories had the most difficulty in meeting the following two areas in DHS guidance: developing capability targets consistent with the core capability definitions in the National Preparedness Goal, and including at least one estimated impact and desired outcome for each of the core capabilities. In the fourth quarter of Fiscal Year 2017, FEMA's National Preparedness Assessment Division and Regional Offices hosted three technical assistance workshops in Philadelphia, Chicago, and Seattle to help states, territories, tribes, and urban areas improve their 2017 THIRA and SPR submissions. During these workshops, FEMA representatives led discussions, presentations, and activities to help enhance the quality of THIRA inputs, including threats and hazards of concern, context descriptions, capability targets, desired outcomes, estimated impacts, and resource requirements. FEMA will continue to work with all states to improve their THIRA capabilities.

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Man-Made or Natural Incident Investments								
Benefit to cost ratio of the hazard mitigation grants (FEMA)								
---	---	---	---	1.6	1.4	1.6	1.5	1.6
Percent of communities in high earthquake, flood, and wind-prone areas adopting disaster-resistant building codes (FEMA)								
56%	57%	61%	63%	68%	63%	67%	64%	65%
Percent of U.S. population (excluding territories) covered by planned mitigation strategies (FEMA)								
71.0%	76.7%	79.6%	80.8%	81.0%	79.0%	82.1%	85.0%[1]	85.0%

1 – FY 2018 target previously published as 79.0% in the FY 16-18 Annual Performance Report was revised to better reflect expected performance.

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Man-Made or Natural Incident Response								
Operational readiness rating of FEMA's specialized incident workforce cadres (FEMA)								
---	---	---	---	61%	74%	60%[1]	80%	80%
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)								
---	100%	100%	100%	100%	100%	100%	100%	100%
Percent of Incident Management Assistance Teams establishing joint federal and state response objectives within 18 hours (FEMA)								
---	100%	100%	100%	100%	100%	100%	100%	100%
Percent of incident management planned workforce currently on board (FEMA)								
---	---	---	---	---	76%	71%[2]	80%	80%
Percent of shipments for required life-sustaining commodities (meals, water, tarps, plastic sheeting, cots, blankets, and generators) and key initial response resources delivered by the agreed upon date (FEMA)								
---	---	---	---	99.0%	95.0%	N/A[3]	95.0%	95.0%
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)								
---	94.5%	91.5%	96.9%	95.3%	95.0%	95.4%	95.0%[4]	96.0%
Percent of recovery services through Public Assistance delivered to communities gauging the quality of program services, supporting infrastructure, and customer satisfaction following a disaster (FEMA)								
---	86.2%	90.9%	92.0%	90.0%	93.0%	91.0%[5]	93.0%	93.0%

1 – FEMA focused on efforts to improve operational readiness throughout FY 2017 by adding employees to its incident workforce in order to increase overall force strength, and by qualifying employees in their position. FEMA qualified 257 employees, bringing the total qualified to 6,267, and increased the total number of employees completing all classroom training requirements by 268. FEMA anticipates the percentage of qualified personnel should improve in the coming months as employees gain experience during current deployments. In FY 2018, FEMA will work to continue increasing and qualifying the incident workforce, and will refine those targets as necessary. FEMA has begun review of its IM Force Structure, which will provide FEMA a better understanding of required staffing needs to support disaster operations. FEMA will also continue efforts to align performed tasks with training objectives, revise required courses, and correlate training materials more closely with FEMA Qualification System Core Competencies. This will be done in an effort to decrease the average time to qualification to ensure that qualification rates will be able to keep better pace with staffing and maintain a ready workforce.

2 – In Q4, FEMA increased its overall force strength to 11,601 (789 new hires), though overall availability remains low given the high deployment activity. FEMA has begun a review of its force structure, which will provide a better understanding of FEMA's required staffing needs. FEMA will also continue efforts to align performed tasks with training objectives, revise required courses, and correlate training materials more closely with FEMA.

3 – This measure was unable to report data in time for publication due to the ongoing response and recovery efforts in support of Hurricanes Harvey, Irma, and Maria. Results will be made available in next year's Annual Performance Report.

4 – FY 2018 target previously published as 96% in the FY 16-18 Annual Performance Report was adjusted to be more in-line with historical results and expected future performance.

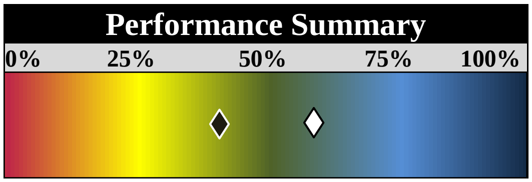
5 – FEMA continued to roll out its updated Public Assistance program delivery roles, processes, and tools, what FEMA refers to as an updated delivery model, by adding eleven disasters in the third and fourth quarters of FY 2017. The model is designed to improve efficiency, accessibility, timeliness, accuracy, and simplicity. These efforts effect 85 percent of this composite measure. Even though FEMA did not meet its target this fiscal year, an overall increase over FY 2016 indicates continued improvement in the delivery of Public Assistance. The improvements were driven by increased customer satisfaction and increased timeliness. However, these improvements were weighed down by struggles to fill organizational positions. While demonstrating improvement on this measure, FEMA still experiences time delays in the initial delivery of Public Assistance. Specifically, only 85 percent of kickoff meetings occurred within 21 days of FEMA receiving a request for Public Assistance. To address the timeliness of initial operations, FEMA will continue to roll out its updated program delivery roles, processes and tools. While these updates place less emphasis on initial timeliness—as opposed to overall timeliness—they provide an ability to monitor performance in real-time and take quick corrective actions.

Immigration and Customs Enforcement

Overview

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. ICE was created in 2003 through a merger of the investigative and interior enforcement elements of the former U.S. Customs Service and the Immigration and Naturalization Service. ICE now has more than 20,000 employees in more than 400 offices in the United States and 46 foreign countries.

In FY 2017, there were seven strategic performance measures used to assess ICE's efforts. In FY 2017, 43 percent of the measures met their target and 60 percent maintained or improved actual results compared to FY 2016.



◆- Percent of measures that met their FY 2017 target.

◇- Percent of measures that maintained or improved actual performance results compared to FY 2016.

Progress: Transnational Criminal Organizations (TCOs) are considered the greatest high-risk criminal organizations and individuals within illicit trade, travel, and finance. The Southern Border and Approaches Campaign Strategy focused DHS efforts on enforcement and interdiction activities to degrade TCOs, while still facilitating the flow of lawful trade, travel, and commerce across our borders. ICE Homeland Security Investigations has been a key part of this effort, directing their significant criminal investigations to focus on TCOs, and to work to disrupt or dismantle these organizations.

DHS efforts continued to improve interaction with state and local law enforcement, targeting aliens who pose a danger to national security or a risk to public safety, recent illegal entrants, and illegal immigrants who are fugitives or obstruct immigration controls. Improvements were seen from the establishment of Mobile Criminal Alien Teams that assist in locating and arresting convicted criminals.

ICE also leads the Joint Task Force (JTF)-Investigations, and is part of the JTF-West and JTF-East, which continue to leverage intelligence, information sharing, coordination, and focused operational plans to disrupt and dismantle targeted TCOs.

New policy direction contained in *Executive Order (EO) 13768, Enhancing Public Safety in the Interior of the United States*, aims to drive future efforts to effectively address those individuals who illegally enter the United States and those who overstay or otherwise violate the terms of their visas.

Operation Silent Partner covertly introduces currency counters into criminal organizations through confidential informants and undercover agents to create a unique and specific targeting opportunity. In FY 2017, this operation contributed to the seizure of $3.4 million in bulk cash.

Challenges and Risks: Historically, surges of illegal immigration at the southern border with Mexico have placed a significant strain on federal resources and those agencies charged with border security and immigration enforcement. With policy shifts related to recent EOs to remove illegal immigrants, with a focus on those already residing in the interior of the country, ICE faces a challenging task that is impacted by the effectiveness of other parts of the Federal Government, specifically the Department of Justice's ability to receive and process illegal immigration cases. Additional challenges exist in maintaining and managing resource to support unaccompanied children, those with temporary protected status, and other immigration related change in laws and executive orders that have occurred over the past few years. In addition, DHS faces hurdles from cities that do not honor ICE detainers, which makes arresting interior illegal immigrants even more of a challenge.

Human Capital Strategies

One of the provisions of EO 13768 directs the hiring of 10,000 ICE Law Enforcement Officers (LEOs) and related support staff to increase capacity to support the administration's plan to strengthen immigration enforcement both in the interior and at the border. ICE has developed a multi-year year hiring plan to increase LEOs and Non-LEOs by 16,596 positions by FY 2024. The FY 2018 budget is the first year of implementation and included the first 1,000 LEOs and 606 Non-LEOs. ICE is finalizing their plans which will include Veteran hiring opportunities, unique advertising campaigns, improvements in hiring process to reduce time-to-hire, and will look to other opportunities for retention approaches. Once on board, ICE is developing training regimes to ensure rapid integration, along with specialized skills, to easily integrate with current workforce.

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

In February 2017, President Trump signed Executive Order 13773, aimed at targeting transnational criminal organizations (TCO), such as drug cartels or gangs like Mara Salvatrucha (MS -13). The Executive Order is a multifaceted approach in attacking TCOs that pose a threat to national security and/or public safety. U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), remains vigilant in disrupting and dismantling violent gang activity in collaboration with our state, local, and tribal, and foreign law enforcement partners.

ICE initiated Operation Community Shield in 2005, a cross-border effort in response to the rapid growing threat of transnational "street" gangs entering the U.S. On the night of April 11, 2017, four young men were brutally killed by members of MS-13 in a Long Island, New York (NY) park. In response to the violence, HSI NY established Operation Matador (OPMAT). OPMAT is a multi-pronged approach in which HSI NY partnered with other DHS Components to combat MS-13 in the greater New York City area. The interagency DHS approach is devised to combat the proliferation of MS-13. OPMAT is primed to disrupt and dismantle MS-13 through five key elements: intelligence gathering; actionable lead development; targeted enforcement; Criminal and Racketeer Influenced and Corrupt Organization investigation development; and community outreach to at-risk youth in the affected cities.

From May 9, 2017 to June 30, 2017, OPMAT has led to 68 arrests of known gang members, 60 of which were established as MS-13 gang members. ICE remains committed to working in a unified approach in combating gang violence and disrupting the MS-13 pipeline.

Mission Programs

The mission programs that deliver performance results for ICE are:

- **Enforcement and Removal Operations (ERO):** Enforcement and Removal Operations enforces the Nation's immigration laws by identifying and apprehending illegal immigrants, detaining those individuals pending final determination of removability, and removing them from the United States by legal processes and procedures. This program carries out its mission through a range of initiatives and activities that focus on identifying and prioritizing the removal of recent border entrants and individuals who pose a significant threat to national security or public safety, including fugitives and illegal immigrants convicted of crimes.
- **Homeland Security Investigations (HSI):** The Homeland Security Investigations (HSI) program conducts

criminal investigations to protect the United States against terrorist and other criminal organizations that threaten public safety and national security. HSI combats transnational criminal enterprises that seek to exploit America's legitimate trade, travel, and financial systems. This program upholds and enforces America's customs and immigration laws at and beyond our Nation's borders.

- **Office of Principal Legal Advisor (OPLA):** The Office of the Principal Legal Advisor provides legal counsel and representation, personnel training, and litigation support to ICE to ensure public safety and homeland security. This program serves as the exclusive DHS representative in removal proceedings before the Department of Justice Executive Office for Immigration Review. The Executive Office for Immigration Review is responsible for adjudicating immigration proceedings in the United States.

Performance Results and Plan

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Transnational Criminal Organizations								
Percent of significant Homeland Security Investigation cases that result in a disruption or dismantlement (ICE)								
---	---	---	---	---	15.8%	22.9%	15.8%	15.9%

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Immigration Enforcement								
Average length of stay in detention of all convicted criminal aliens prior to removal from the United States (in days) (ICE)								
31.9	33.5	37.5	40.3	43.9	≤ 44.0	48.8[1]	≤ 44.0	≤ 44.0
Number of convicted criminal illegal immigrants who were returned or were removed from the U.S. (ICE)[2]								
225,390	216,810	177,960	139,368	138,669	140,000	127,699[3]	126,000[4]	151,000
Number of enforcement-related actions against employers that violate immigration-related employment laws (ICE)								
---	4,743	2,191	1,928	1,880	1,854	1,730[5]	1,854	1,854
Percent of detention facilities found in compliance with the national detention standards by receiving a final acceptable inspection rating (ICE)								
97%	100%	100%	100%	100%	100%	100%	100%	100%
Percent of ICE removals that support current enforcement priorities (ICE)								
---	---	---	---	---	99.0%	97.3%[6]	Retired[7]	
Percent of removal orders secured by ICE attorneys that support current enforcement priorities (ICE)								
---	---	---	---	85%	85%	100%	Retired[8]	
Total number of illegal immigrants who were returned or removed from the U.S. (ICE)								
---	---	---	---	---	New Measure		210,000	238,000

1 – ICE exceeded the Criminal Average Length of Stay (ALOS) target by nearly 5 days. ALOS is affected by factors outside of ICE's control including federal court decisions, such as Rodriguez v Robbins in the 9th Circuit which mandates bond hearings for cases detained more than 180 days. The surge in early FY 2017 saw an influx of individuals from Guatemala, Honduras, and El Salvador – as such, there were relatively fewer Mexicans and therefore a higher ALOS across the population in detention. The increase from FY 2016 to FY 2017 was also affected by the decrease in CBP apprehensions of criminals. Detention stays associated with CBP turnovers are typically shorter than those associated with ICE or

other agency arrests; this then increases the ALOS across the population as well. To improve performance, ICE has increased joint efforts with the Department of State to address timing and straightforward return processing.

2 – Measure name changed from "*Number of convicted criminal aliens removed per fiscal year*" to make transparent the scope of the measure.

3 – This measure includes removals from the U.S. under any type of removal order, as well as voluntary returns of immigration violators to their country of origin, for those individuals with a criminal record. In FY 2017, ICE removed or returned 10,970 fewer criminal illegal immigrants than FY 2016. While 3,500 more detainers were issued in FY 2017 compared to FY 2016, noncompliant jurisdictions continue to disrupt the removal of criminal aliens by declining over 8,000 detainers, more than double the FY 2016 total. Decreasing CBP apprehensions at the border have also contributed to a decrease in the number of criminal removals. While fewer criminal illegal immigrants were removed or returned, ICE's recent enforcement efforts have led to a 12 percent increase in the arrests of criminal illegal immigrants from FY 2016. To improve performance, ICE will continue with current interior enforcement efforts and joint efforts with the Department of State.

4 – FY 2018 target previously published as 140,000 in the FY 16-18 Annual Performance Report and is updated based on recent trends in immigration.

5 – In order to comply with the EOs that were released in FY 2017, HSI reassigned existing special agent personnel which impacted the results for this measure. HSI has prioritized worksite investigations for FY 2018. To ensure that HSI meets its targets, HSI is planning enforcement initiatives for FY 2018.

6, 7 – Due to Executive Order 13768 eliminating specific immigration priorities and the timing of data collection, this measure narrowly missed its target. This measure is being retired.

8 – This measure is retired due to EO 13768 eliminating specific immigration priorities.

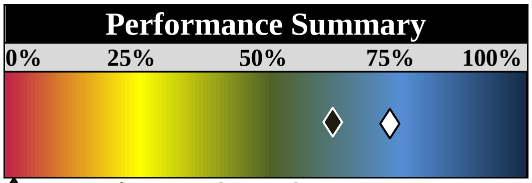
Transportation Security Administration

Overview

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

The attacks on September 11, 2001 resulted in the creation of the Transportation Security Administration, and was designed to prevent similar attacks in the future. Driven by a desire to help our nation, tens of thousands of people joined TSA and committed themselves to strengthening our transportation systems while ensuring the freedom of movement for people and commerce.

In FY 2017, there were nine strategic performance measures used to assess TSA's efforts. In FY 2017, 67 percent of the measures met their target and 75 percent maintained or improved actual results compared to FY 2016.



◆- Percent of measures that met their FY 2017 target.

◇- Percent of measures that maintained or improved actual performance results compared to FY 2016.

Progress: DHS continues to vet 100% of domestic passengers and checked baggage each day in order to ensure the safety and security of the travelling public. DHS Trusted Traveler programs enrolled more than 3 million more travelers to receive expedited screening, enabling the Department to focus on unknown and high-risk travelers and DHS has now achieved more than 5 million travelers enrolled in TSA Pre✓®. DHS security partnerships were also effectively strengthened and expanded within the Intelligence Community through the development of Priority Intelligence Requirements regarding intelligence collection and reporting. This was also accomplished with international partners through United Nations Resolution 2309 and through the creation of the Aviation Domain Intelligence Integration and Analysis Cell which enables the government to share information more effectively with the travel industry. Compliance with aviation security standards was also strengthened through the completion of international airport assessments and air carrier inspections. In Surface transportation, TSA collaborated closely with industry and government partners to identify and secure critical surface transportation assets. In support of those efforts, TSA provided industry partners with technical assistance, training, and exercises.

Challenges and Risks: Specific improvements need to be made to airport perimeter and access security, passenger rail operations, and identity vetting. DHS recognizes these challenges and is actively working to implement recommendations for enhancing risk-based security measures for all transportation modes and in identified areas. Future risks are the evolving and emerging threats as our adversaries are constantly finding and trying new ways to infiltrate and disrupt our way of life. To address these risks, the DHS Science and Technology Directorate researches new and emerging formulations of explosives and subsequently works with equipment manufacturers to develop the best possible technology to mitigate threats. Intelligence sharing is also critical to the mitigation of this risk and is done through avenues such as the National Targeting Center.

Have You Opted In?
Expedited Screening
TSA Pre✓
Dedicated TSA Pre✓ lanes
Keep your shoes, coat and belt on
Leave your laptop and liquids in your bag

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

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

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

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

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

Mission Programs

The mission programs that deliver performance results for TSA are:

- **Aviation Screening Operations:** The Aviation Screening Operations program applies intelligence-driven, risk-based, layered passenger and baggage screening procedures and technology to increase aviation security to prevent terrorism and criminal activity. The program implements processes that allow personnel at security checkpoints to focus on high-risk and unknown travelers while managing the passenger experience. The program also ensures the 100 percent screening of checked baggage for prohibited items. Other activities include training the screener workforce, vetting airline passengers, and canine operations.

- **Other Operations and Enforcement:** The Other Operations and Enforcement program encompasses security reviews, assessment, and enforcement activities in the various modes of commercial transportation. The program includes intelligence and analysis, visible intermodal prevention and response teams, domestic and international inspectors, reviews and assessments, Federal Air Marshals, deputizing airline pilots, and training crew members in self-defense. This program ensures compliance with transportation-related regulations and standards, providing credentialing services for transportation sector, and the vetting of the transportation workforce to prevent terrorism and criminal activity.

Performance Results and Plan

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Transportation Security								
Average number of days for DHS Traveler Redress Inquiry Program (TRIP) redress requests to be closed (TSA)								
93	52	62	50	44	< 55	50	< 55	< 55
Percent of air carriers operating from domestic airports in compliance with leading security indicators (TSA)								
98.1%	98.0%	98.0%	98.0%	98.0%	100%	97.7%[1]	100%	100%
Percent of attended interchanges of rail cars containing rail security sensitive materials transiting into or through high-threat urban areas (TSA)								
---	---	---	---	---	New Measure		95%	95%
Percent of daily passengers receiving expedited physical screening based on assessed low risk (TSA)								
---	---	---	---	46%	50%	55%	50%	50%
Percent of domestic cargo audits that meet screening standards (TSA)								
---	---	---	---	98%	96%	97.7%	97%	98%
Percent of foreign airports that serve as last points of departure and air carriers involved in international operations to the United States advised of necessary actions to mitigate identified vulnerabilities in order to ensure compliance with critical security measures (TSA)								
---	100%	100%	100%	100%	100%	100%	Retired	
Percent of foreign last point of departure (LPD) airports that take action to address identified vulnerabilities (TSA)								
---	---	---	---	---	New Measure		70%	70%
Percent of international cargo audits that meet screening standards (TSA)								
---	---	---	---	97%	96%	97.6%	97%	98%
Percent of overall compliance of domestic airports with established aviation security indicators (TSA)								
95.0%	94.4%	94.0%	95.0%	93.0%	100%	93.9%[2]	100%	100%
Percent of overall level of implementation of industry agreed upon Security and Emergency Management action items by mass transit and passenger rail agencies (TSA)								
39%	69%	78%	80%	71%	75%	74%[3]	77%	79%
Percent of passenger data submissions that successfully undergo Secure Flight watch list matching (TSA)								
---	---	---	---	---	100%	100%	100%	100%
Percent of TSA regulated entities inspected per fiscal year by transportation security inspectors (TSA)								
---	---	---	---	---	New Measure		90%	90%

1 – The performance results indicate the percentage of air carriers found to comply with transportation security regulations through TSA inspections. TSA aggressively works with air carriers to ensure they comply with all security requirements and takes enforcement and other actions when necessary. TSA's Office of Security Operations will work with air carriers on security deficiencies and vulnerabilities to

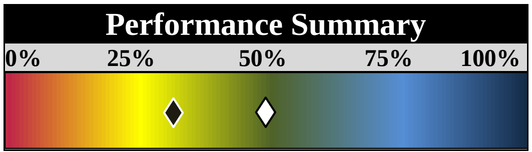
ensure that airports are 100 percent in compliance with the security rules and regulations that they follow.
2 – The performance results indicate the percentage of airports found to comply with transportation security regulations through TSA inspections. TSA aggressively works with the airports to ensure they comply with all security requirements and takes enforcement and other actions when necessary. TSA's Office of Security Operations will work with airports on security deficiencies and vulnerabilities to ensure that airports are 100 percent in compliance with the security rules and regulations that they follow.
3 – As of September 30, 2017, 39 of 53 Mass Transit Systems met the criteria as measured by Baseline Assessment for Security Enhancement (BASE) assessments, just shy of the target of 75 percent. Efforts to improve BASE scores will focus on information sharing activities to include emphasizing implementation of modal security action item best practices in those areas with low scores. TSA Surface Inspectors will provide information and recommendations for improvement, in particular highlighting the availability of TSA training and exercise resources. Transit agencies will also be encouraged to review practices in place at counterpart agencies with superior programs.

U.S. Citizenship and Immigration Services

Overview

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. USCIS is the government agency that oversees lawful immigration to the United States and is funded primarily by immigration and naturalization benefit fees charged to applicants and petitioners.

In FY 2017, there were six strategic performance measures used to assess USCIS' efforts. In FY 2017, 33 percent of the measures met their target and 50 percent maintained or improved actual results compared to FY 2016.



◆- Percent of measures that met their FY 2017 target.

◇- Percent of measures that maintained or improved actual performance results compared to FY 2016.

Progress: USCIS processes more than 8 million citizenship and immigration benefit requests annually and these continue to grow.

To promote the assimilation of lawful immigrants in American society, USCIS holds naturalization information sessions across the country. USCIS also conducts citizenship education training seminars for citizenship educators. Grants are also awarded to numerous organizations to help permanent residents prepare and apply for citizenship.

Since local communities play a critical role in welcoming and assisting immigrants, USCIS relies on state and local networks to help educate immigrants about naturalization and lawful immigration. Through these partnerships, USCIS provides information and resources to help facilitate outreach and engagement, training and technical assistance, and citizenship education for communities.

The American Council for Technology and Industry Advisory Council presented USCIS with the Igniting Innovation Award for their work with *my*USCIS, a service, available in both English and Spanish that helps individuals navigate the immigration process. The online tool provides up-to-date information about immigration benefits, resources to find citizenship preparation classes and doctors across the country, and tools to help prepare for naturalization, such as the civics practice test.

Challenges and Risks: Although more than 8 million benefit requests are processed, the amount of requests received has driven the backlog to more than one million pending cases and has increased cycle times for several form types. DHS will continue to mitigate challenges by redirecting cases to other locations with additional capacity, and shifting adjudication priorities to address high priority caseloads.

USCIS Naturalizes 15,000 New Citizens during Independence Day

On the 241st anniversary of the Declaration of Independence and the birth of the United States, 15,000 lawful permanent residents were naturalized as U.S. citizens during more than 65 naturalization ceremonies across the country. The number of new citizens naturalized on July 4, 2017 was the most in recent years. Local, state, and federal officials attended ceremonies that were held at public libraries, national parks, and museums.

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

Mission Programs

The mission programs that deliver performance results for USCIS are:

- **Employment Status Verification:** The Employment Status Verification (E-verify) program enables authorized employers to quickly and easily verify the work authorization of their newly hired employees. E-Verify is an Internet-based system that compares information from an employee's Form I-9, Employment Eligibility Verification, to data from U.S. Department of Homeland Security and Social Security Administration records to confirm employment eligibility within seconds.
- **Fraud Prevention and Detection Account:** The Fraud Prevention and Detection Account supports activities related to preventing and detecting fraud in the delivery of all immigration benefit types. The program leads efforts to identify threats to national security and public safety, detect and combat immigration benefit fraud, and remove systemic and other vulnerabilities.
- **H-1B Nonimmigrant Petitioner Account:** The H-1B Nonimmigrant Petitioner Account supports activities related to the adjudication of employment-based petitions for nonimmigrant workers seeking an H-1B visa. This program allows U.S. employers to temporarily employ foreign workers in specialty occupations.
- **Immigration Examinations Fee Account:** The Immigration Examinations Fee Account (IEFA) is the primary funding source for USCIS. Fees collected from immigration benefit applications and petitions are deposited into IEFA and are used to fund the cost of processing immigration benefit applications and associated support benefits, as well as to cover the cost of processing similar benefit requests for applicants without charge, such as refugee and asylum applicants.

Performance Results and Plan

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Immigration Benefits								
Average of processing cycle time (in months) for adjustment of status to permanent resident applications (I-485) (USCIS)								
5.1	4.7	6.0	6.4	6.9	≤ 4.0	9.3[1]	≤ 4.0	≤ 4.0
Average of processing cycle time (in months) for naturalization applications (N-400) (USCIS)								
4.6	4.7	5.5	5.0	5.8	≤ 5.0	8.6[2]	≤ 5.0	≤ 5.0
Percent of customers satisfied with the citizenship and immigration-related support received from the National Customer Service Center (USCIS)								
93%	87%	86%	88%	85%	85%	84%[3]	85%	85%
Percent of workers determined to be "Employment Authorized" after an initial mismatch (USCIS)								
0.24%	0.22%	0.19%	0.17%	0.16%	≤ 0.70%	0.15%	≤ 0.60%	≤ 0.50%
Percent of students enrolled in classes under the Citizenship and Integration Grant Program that show educational gains (USCIS)								
---	---	---	75%	75%	80%	75%[4]	80%	80%
Percent of applications for citizenship and immigration benefits not approved following a potential finding of fraud (USCIS)								
---	---	---	---	91.3%	90%	91.7%	90%	90%

1 - This measure assesses the program's ability to meet its published processing time goals for the processing of the I-485, Application to Register for Permanent Residence or Adjust Status. USCIS experienced an elevated I-485 cycle time as a result of higher than expected FY 2017 receipts (FY 2017 receipts were 16 percent higher than projected). Although the cycle time is above the target, USCIS has maintained the accuracy of I-485 decisions. USCIS continues to face capacity challenges which, combined with higher workload demands, will continue to negatively impact our cycle time. USCIS is continuing to shift resources and prioritizing workload in order to handle its case volume. During FY 2018, USCIS will continue to balance workload to ensure national cycle time parity and leverage overtime and other scheduling options.

2 - USCIS experienced an elevated N-400 cycle time as a result of higher than expected FY 2017 receipts (FY 2017 receipts were 14 percent higher than projected). USCIS is continuing to shift resources and prioritizing workload in order to handle its case volume. Although the cycle time is above the target, USCIS has maintained the accuracy of N-400 decisions. USCIS continues to face capacity challenges which, combined with higher workload demands, will continue to negatively impact our cycle time. During FY 2018, USCIS will continue to balance workload to ensure national cycle time parity across each of its 88 field offices, and leverage overtime and other scheduling options.

3 - It is likely that because Immigration Service Officers and Customer Service Representatives were unable to completely answer some callers' questions due to fluidity in the immigration policy environment, customer satisfaction dropped. We anticipate that increased content on self and live help channels will result in improvements over the next quarters.

4 - This measure reports on grant recipients’ ability to increase English knowledge necessary for students receiving services under the program to pass the naturalization test. USCIS did not meet its target since a significant percentage of enrolled students (49.8 percent) were not both pre- and post-tested. USCIS believes that the students who did not return to post-test are more likely to have achieved measurable educational gains and have a higher level of confidence in their ability to be successful in the naturalization process. In FY 2018, USCIS plans to increase its monitoring efforts and technical assistance for the grant recipients that fail to meet pre- and post-testing targets. In-person grant recipient training conducted in October of 2017 addressed student assessment and retention. Beginning in FY 2018, USCIS may consider an applicant's past performance with respect to pre and post testing before making any new award.

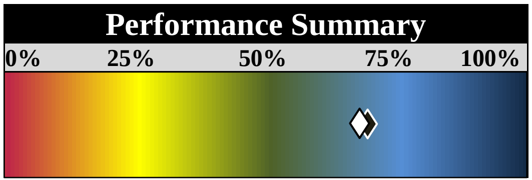
U.S. Coast Guard

Overview

U.S. Coast Guard (USCG) is one of the five designated armed services of the United States. The USCG has a distinct blend of authorities, capabilities, competencies, and partnerships that provide the President, Secretary of Homeland Security, Secretary of Defense, and other national leaders with the capabilities to lead or support a range of operations to ensure the safety, security, and stewardship in the maritime domain. The USCG has 11 statutory missions. They are:

- Ports, Waterways, and Coastal Security;
- Drug Interdiction;
- Migrant Interdiction;
- Defense Readiness;
- Other Law Enforcement
- Marine Safety;
- Search and Rescue;
- Aids to Navigation;
- Living Marine Resources;
- Marine Environmental Protection; and
- Ice Operations.

In FY 2017, there were seven strategic performance measures used to assess USCG's efforts. In FY 2017, 71 percent of the measures met their target and 71 percent maintained or improved actual results compared to FY 2016.



◆- Percent of measures that met their FY 2017 target.

◇- Percent of measures that maintained or improved actual performance results compared to FY 2016.

Progress: The USCG saved more than 4,000 lives this past year and responded to more than 19,000 search and rescue cases. In addition, the USCG played a major role in the recent response in support of Hurricanes Harvey, Irma, and Maria saving or assisting more than 11,000 victims. The USCG made significant progress in the maritime domain. Due to changes in the Cuban Parole Policy, also known as "wet foot/dry foot," migrant flow from Cuba has greatly diminished, and subsequently, USCG's migration interdiction rate improved dramatically. The decrease in Cuban migrant flow enabled USCG patrol assets to improve response and have greater interdiction success in the Florida Straits.

In January 2017, the U.S. terminated the Cuban Parole Policy (including the "Wet Foot-Dry Foot" policy), leading to a dramatic decline in undocumented Cuban maritime migration. This policy change helped reduce flow by 91% from January thru August 2017, as compared to a similar period in FY

In USCG's response role, they responded to more than 10,000 pollution incident reports and managed hundreds of cleanup projects. USCG also deployed the National Strike Force as federal coordinator in response to dozen of hazardous substance incidents. The USCG also played a major role in the recent response in support of Hurricanes Harvey, Irma, and Maria.

In other areas, the USCG made significant progress in maintaining aids to navigation despite the severe hurricanes this year. Also, significant efforts were seen in large interdictions of drugs in the maritime environment. Finally, the USCG made great strides in international engagements, fostering new and improved relationships.

Challenges and Risks: DHS must continue to mitigate narcotics smuggling by interdicting smugglers at sea, where narcotics are packaged in larger and more concentrated loads and are easier to locate. Additionally, efforts must continue to leverage intelligence with interagency partners to better target drug movements prior to reaching the United States. In addition, the USCG's aging fleet requires ongoing recapitalization to maintain effective emergency response capabilities for search and rescue and major contingency incidents.

Coast Guard Air Station Houston responds to search and rescue requests after Hurricane Harvey in Houston, Texas, Aug. 27, 2017. (U.S. Coast Guard photo by Petty Officer Third Class Johanna Strickland)

USCG Assists More Than 11,000 Hurricane Victims

During August and September, nature dealt the Nation a triple punch with Hurricanes Harvey, Irma, and Maria. Harvey made landfall on the Texas coastline on August 25, 2017 as a Category four hurricane, with winds up to 130 miles per hour and 51.9 inches of torrential rain that set records for the greatest rainfall ever recorded in the continental United States. Harvey caused extensive flooding in Houston, Port Arthur, and the Beaumont areas of Texas.

Irma followed shortly after, hitting Puerto Rico, the Virgin Islands, and Florida; leaving 75 dead in the U.S. alone, destruction exceeding $50 billion, and widespread environmental impacts. Not to be outdone, Maria struck Puerto Rico as a powerful category five storm with sustained winds in excess of 150 miles per hour. Maria had a disastrous impact on the entire island, causing extensive flooding, complete loss of the power grid, severe shortages of clean drinking water, and some $95 billion in damage, environmental, and economic impacts. At least 55 deaths are directly related to Maria, and hundreds more may have been indirectly caused by the storm.

The USCG launched one of the largest responses in its history to these three natural disasters, and saved or assisted more than 11,200 persons in extremis. Following pre-established contingency plans, USCG mobilized more than 2,900 personnel, including 200 active duty, 800 reservists, and 150 civilians. The Coast Guard committed 66 helicopters that flew more than 1,600 hours in the effort, 28 fixed wing aircraft flying more than 1,400 hours, 29 cutters, and 115 shallow water assets. USCG teams also restored significant numbers of lost and damaged aids to navigation, mitigated environmental concerns from reported oil and hazardous material releases, and resolved many other significant waterways management issues.

Mission Programs

The mission programs that deliver performance results for USCG are:

- **Maritime Law Enforcement:** The Maritime Law Enforcement program preserves America's jurisdictional rights within our maritime borders and suppresses violations of U.S. Federal law on, under, and over the seas. The Coast Guard is the lead Federal maritime law enforcement agency for enforcing national and international law on the high seas, outer continental shelf, and inward from the U.S. Exclusive Economic Zone (EEZ) to inland navigable waters, including the Great Lakes. The following statutory missions contribute to the Coast Guard's Maritime Law Enforcement program: Drug Interdiction; Migrant Interdiction; Living Marine Resources; and Other Law Enforcement.
- **Maritime Security Operations:** The Maritime Security Operations program encompasses activities required by legislative, executive, and policy mandates to detect, deter, prevent, disrupt, and recover from terrorist attacks and other criminal acts in the maritime domain. It includes the execution of antiterrorism, response, and select recovery operations. This program conducts the operational element of the Coast Guard's Ports, Waterways, and Coastal Security mission and complements the other two elements: the establishment and oversight of maritime security regimes, and maritime domain awareness.
- **Maritime Prevention:** The Maritime Prevention program mitigates the risk of human casualties and property losses, minimizes security risks, and protects the marine environment. The following

statutory missions contribute to the Coast Guard's Maritime Prevention program: Ports, Waterways, and Coastal Security (PWCS); Marine Safety; and Marine Environmental Protection.

- **Maritime Response:** The Maritime Response program mitigates the consequences of marine casualties and disastrous events. The Coast Guard minimizes loss of life, injury, and property loss by searching for and rescuing persons in distress in the maritime environment. Coast Guard preparedness efforts ensure incident response and recovery resources are fully ready and capable to minimize impact of disasters to people, the environment, and the economy. The following statutory missions contribute to the Coast Guard's Maritime Response program: Search and Rescue and Marine Environmental Protection.
- **Maritime Transportation Systems Management:** The Marine Transportation System Management program ensures a safe, secure, efficient and environmentally sound waterways system. The U.S. Coast Guard minimizes disruptions to maritime commerce by assessing and mitigating risks to safe navigation and by providing waterways restoration capabilities after extreme weather events, marine accidents, or terrorist incidents. The Coast Guard works in concert with other Federal agencies, state and local governments, marine industries, maritime associations, and the international community to optimize balanced use of the Nation's marine transportation system. The following statutory missions contribute to the Coast Guard's Marine Transportation System Management program: Aids to Navigation and Ice Operations.

Performance Results and Plan

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Waterways and Maritime Resources								
Availability of maritime navigation aids (USCG)								
98.3%	98.2%	98.2%	97.7%	97.7%	97.5%	97.5%	97.5%	97.5%
Fishing regulation compliance rate (USCG)								
98.3%	98.1%	97.5%	97.1%	96.8%	97.0%	97.1%	97%[1]	97.0%
Interdiction rate of foreign fishing vessels violating U.S. waters (USCG)								
---	---	---	---	---	New Measure		18%	18%
Number of breaches at high risk maritime facilities (USCG)								
---	---	---	---	---	New Measure		≤ 235	≤ 219
Number of detected incursions of foreign fishing vessels violating U.S. waters (USCG)								
160	189	198	224	176[2]	< 224	136	Retired	
Security compliance rate for high risk maritime facilities (USCG)								
98.7%	99.3%	99.3%	99.6%	97.6%	100%	98.0%[3]	Retired	

1 – FY 2018 target previously published as 96.5% in the FY 16-18 Annual Performance Report. The target was revised in light of recent information and historical trends.

2 – Previously published as 163, but updated once additional information was collected.

3 - This measure is a leading indicator of maritime facility security and resiliency in our Nation's ports. While performance did not fully achieve this aspirational target of 100 percent, data indicate that the overall Security Compliance Rate for High Risk Maritime Facilities remains extremely high at 98.0%. In total, only 68 of the approximately 3,400 High Risk Facilities were not in compliance. USCG will continue its efforts to achieve success in protecting our high risk maritime facilities. To that end, USCG is recommending a new measure, "Number of breaches at high risk maritime facilities" to better access risk in this area.

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Man-Made or Natural Incident Response								
Percent of people in imminent danger saved in the maritime environment (USCG)								
77.3%	79.0%	79.0%	80.0%	79.4%	100%	78.8%[1]	80%[2]	80%
Three-year average number of serious marine incidents (USCG)								
---	---	---	696	688	≤ 698	684	≤ 698	≤ 698

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

[2] – FY 2018 target previously published as 100% in the FY 16-18 Annual Performance Report. The target was adjusted to be more in-line with historical results and expected future performance. Search and Rescue targets are derived from an analytical approach described in the USCG's Addendum to their Search and Rescue manual.

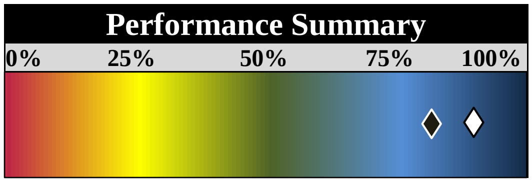
Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Border Operations								
Migrant interdiction effectiveness in the maritime environment (USCG)								
---	---	---	74.8%	79.3%	74.5%	83.0%	75.0%	75.0%

U.S. Secret Service

Overview

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. The USSS has grown from a small bureau staffed by a few operatives in 1865, to a law enforcement organization of nearly 7,000 employees worldwide. Today, the USSS fights crime on a global scale through its field offices located in the United States, Canada, Mexico, South America, Europe, Africa and Asia. The agency works closely with local, state, and federal law enforcement organizations. These entities are valued partners of the USSS, and they are integral to the agency's investigative and protective endeavors.

In FY 2017, there were 11 strategic performance measures used to assess USSS' efforts. In FY 2017, 82 percent of the measures met their target and 91 percent maintained or improved actual results compared to FY 2016.



◆- Percent of measures that met their FY 2017 target.

◇- Percent of measures that maintained or improved actual performance results compared to FY 2016.

Progress: USSS ensured the personal security of candidates of family members, along with a number of large campaign-related events during a campaign year which required significant resources to be utilized. Despite the extraordinarily high operational tempo, USSS ensured that all protected personnel arrived and departed safely 100 percent of the time for more than 7,700 stops. This achievement is particularly notable as the Presidential campaign had more than 3,500 protective stops, more than any prior campaign. More than 5 million people were screened with seizures of tens of thousands of weapons at checkpoints during campaign events and other protective stops.

Challenges and Risks: In spite of the enormous successes achieved during this assessment period, the challenge of hiring, retaining, and impacting the morale of USSS personnel remains. Long duty hours and extensive travel experienced by USSS protective personnel have resulted in work-life imbalance. Employee morale has the potential to create significant challenges in retaining current personnel. An increase in employee attrition would place a further burden on existing personnel and would thus intensify work demands and work-life balance for agents. USSS will continue to balance its resources to best meet the demands of the protective and investigative missions.

2017 Presidential Inauguration

The 2017 Presidential Inauguration was the 57th event of national significance designated a National Special Security Event (NSSE) since 1998. The USSS was the lead Federal agency for operational security planning and implementation for the event. The USSS initiated operational security planning nearly 12 months prior to the inauguration in the midst of a record campaign year that also involved multiple NSSEs including: the Democratic and Republican National Conventions, and the 71st United Nations General Assembly. The successful completion of the three-day 2017 Presidential Inauguration was the result of the coordinated efforts by numerous federal, state, and local agencies, including other components of the Department of Homeland Security.

USSS event coordinators invited major stakeholders to be members of an executive steering committee to oversee the development of a comprehensive operational security and safety plan that reflects the current threat environment and vulnerabilities posed in today’s world. 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 the 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. USSS event coordinators also coordinated extensive and realistic multi-agency tabletop exercises, joint tactical and other practical exercises to ensure that operational security plans would work as intended. All of this preparation led to a successful and safe Presidential Inauguration.

Mission Programs

The primary mission programs that deliver performance results for USSS are:

- **Protective Operations:** The Protective Operations program protects the President and Vice President and their families, former Presidents and their spouses, and other designated individuals. It also secures the White House Complex, Vice President's Residence, and other designated places. The program designs, coordinates, and implements operational security plans for designated National Special Security Events (NSSEs). In addition, the program investigates, evaluates, disseminates, and maintains information concerning known, potential, or perceived threats to protectees and NSSEs. The program is staffed by special agents, uniformed officers, and administrative, professional, and technical personnel and works closely with the military and federal, state, county, local, and international law enforcement organizations.

- **Field Operations:** The Field Operations program supports the daily operations of the domestic and international field offices. The program is staffed by special agents, uniformed officers, and administrative, professional, and technical personnel who divide their time between conducting criminal investigations of financial crimes, cybercrimes, counterfeit currency, protective intelligence, and providing protection support as needed.

Performance Results and Plan

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Protect Leaders and National Security Events								
Amount of dollar loss prevented by Secret Service cyber investigations (in millions) (USSS)								
---	$1,119	$384	$589	$558	$600	$3,145[1]	$650	$700
Financial crimes loss prevented through a criminal investigation (in billions) (USSS)								
$2.75	$4.20	$3.04	$1.47	$2.42	$1.90	$3.55	$2.10	$2.30
Number of cyber mitigation responses (USSS)								
---	---	---	---	157	250	253	390	400
Number of financial accounts recovered (in millions) (USSS)								
---	3.90	0.29	0.93	0.51	0.40	27.18	0.50	0.50
Number of law enforcement individuals trained in cybercrime and cyber forensics both domestically and overseas (USSS)								
---	1,517	1,533	2,070	1,906	1,900	1,968	2,000[2]	2,000
Percent of currency identified as counterfeit (USSS)								
0.0085%	0.0072%	0.0068%	0.0058%	0.0057%	<0.0088%	0.0093%[3]	<0.0088%	<0.0088%
Percent of National Center for Missing and Exploited Children (NCMEC) examinations requested that are conducted (USSS)								
100%	100%	100%	100%	100%	100%	100%	100%	100%
Percent of National Special Security Events that were successfully completed (USSS)								
100%	100%	100%	100%	100%	100%	100%	100%	100%
Percent of protectees that arrive and depart safely (USSS)								
100%	100%	100%	100%	100%	100%	100%	100%	100%
Percent of total protection activities that are incident-free at the White House Complex, Vice President's Residence, and other protected facilities (USSS)								
100%	100%	100%	99.7%	100%	100%	100%	100%	100%
Terabytes of data forensically analyzed for criminal investigations (USSS)								
---	4,002	4,902	6,052	3,334	7,000	5,019[4]	5,000[5]	5,100

1 – During FY 2017 Secret Service closed an investigation into a substantial network intrusion impacting a major US retailer. This case involved over 4.5 million access devices and potential fraud losses totaling well in excess of our annual performance target. This performance measure is highly volatile based upon the cases closed in a particular reporting period.

2 – Previously published as 1,600, but updated to be in line with prior results and expectations moving forward.

3 – The personnel resources demanded by the 2016 Presidential Campaign resulted in a delay in the entry of counterfeit notes and subsequent backlog. There is also an administrative staffing shortage that contributed to the backlog. The conclusion of the campaign allowed a partial shift back to investigations and the

clearing of this counterfeit note backlog. Because counterfeit statistics are credited upon entry, this resulted in a higher than expected FY 2017 result (a portion of the notes should have been credited to prior fiscal years). If there had been no delay and resulting backlog, all fiscal years would have met the expected targets. In addition, the counterfeit passed value is slightly higher in FY 2016 and FY 2017 compared to past fiscal years due to digital counterfeiting techniques. USSS will improve performance by addressing staffing shortfalls through hiring and retention. The Secret Service will continue to evaluate appropriate out-year targets for this measure as changes in technology affect counterfeit trends.

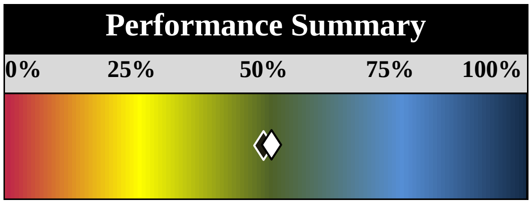
4 – The Criminal Investigations program did not meet its goal in FY 2017; however, the USSS and its partners forensically analyzed 5,019 terabytes of data, a 49 percent increase from FY 2016. While the number of terabytes analyzed has been historically increasing each fiscal year, campaign staffing and other required protective duties impacted investigations more heavily than anticipated. USSS will improve performance by addressing staffing shortfalls through hiring and retention. USSS will continue to evaluate appropriate out-year targets for this measure as changes in staffing levels and impact of campaign protection need further refinement.
5 – Previously published as 7,000, but updated to be in line with prior results and future expectations

Analysis and Operations

Overview

Analysis and Operations (A&O) 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.

In FY 2017, there were six strategic performance measures used to assess Analysis and Operations' efforts. In FY 2017, 50 percent of the measures met their target and 50 percent maintained or improved actual results compared to FY 2016.



◆- Percent of measures that met their FY 2017 target.

◇- Percent of measures that maintained or improved actual performance results compared to FY 2016.

Progress: DHS continues to impact overall security across all aspects of the Homeland Security Enterprise through effective and timely intelligence and information it needs to keep the Homeland safe, secure, and resilient. I&A is a member of the U.S. Intelligence Community (IC) and is the only IC element statutorily charged with delivering intelligence to our state, local, tribal, territorial and private sector partners, and developing intelligence from those partners for the Department and the IC.

Security is also enhanced through OPS which provides information daily to the Secretary of Homeland Security, senior leaders, and the homeland security enterprise to enable decision-making; oversees the National Operations Center (NOC); and leads the Department's Continuity of Operations and Government Programs to enable continuation of primary mission essential functions in the event of a degraded or crisis operating environment.

Challenges and Risks: DHS faces evolving threats that impact I&A's data collection methods and analytic requirements to deliver unique predictive intelligence and analysis to operators and decision-makers at all levels.

Likewise, OPS must ensure that the NOC is operationally effective, 24 hours a day, seven days a week, 365 days a year, and serves as the primary, national-level hub for situational awareness, maintains a common operating picture, and manages information fusion, information sharing, and executive communications.

Mission Programs

The mission program that delivers performance results for A&O is:

- **Analysis and Operations:** The Analysis and Operations program analyzes and shares domestic threat and hazard information through the activities of the Office of Intelligence and Analysis and the Office of Operations Coordination. These two offices work together to improve intelligence, information sharing, and coordination with stakeholders. These offices also develop protective measures and countermeasures to protect the homeland.

Performance Results and Plan

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Mission Support								
Number of intelligence reports shared with the intelligence community (I&A)								
---	---	---	---	---	2,680	3,602	2,730	2,784
Percent of Intelligence and Analysis finished intelligence reports incorporating DHS and state/local originated data (I&A)								
---	---	---	---	---	80%	62%[1]	80%	80%
Percent of intelligence reports rated "satisfactory" or higher in customer feedback that enable customers to manage risks to cyberspace (I&A)								
88%	94%	94%	93%	84%	95%	90%[2]	95%	95%
Percent of intelligence reports rated "satisfactory" or higher in customer feedback that enable customers to understand the threat (I&A)								
90%	93%	95%	95%	95%	95%	94%[3]	95%	95%
Percent of National Operations Center incident reports and situational awareness products produced and disseminated to the homeland security enterprise within targeted timeframes (OPS)								
---	---	---	---	---	90%	98%	90%	90%
Percent of risk assessments for federal security support of large public/community special events completed within the targeted time frame (OPS)								
---	---	---	---	---	98%	99.4%	98%	98%

1 – While I&A made steady progress over the fiscal year, shifting priorities, as well as changing customer intelligence requirements, limited I&A's ability to incorporate more DHS-originated information. I&A's 80 percent target is aspirational and FY 2017 data collection will serve as a baseline for future years. I&A is constantly identifying and accessing new sources of DHS information through our presence within the National Network of Fusion Centers and our efforts to modernize our Information Technology infrastructure.

2 – While this year's 95 percent target was missed, I&A remains committed to ensure our intelligence reporting addresses customer's requirements and contributes to their policy or operational decisions. I&A continues to incorporate all feedback into its regular operational performance review to improve our intelligence reporting. In FY 2018, I&A plans to refine its intelligence requirements to ensure they align with its customer's cyber information needs.

3 – I&A narrowly missed its target and continues to improve the quality of its intelligence products - both its raw and finished intelligence products. I&A continues to incorporate all feedback into our operational performance reviews to improve our intelligence reporting. No corrective actions are going to be taken as this is within I&A's acceptable range of performance.

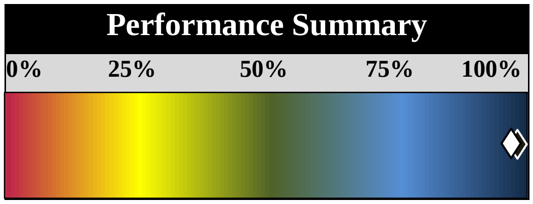
Countering Weapons of Mass Destruction Office

Overview

As of December 2017, the Department officially established the Countering Weapons of Mass Destruction (CWMD) Office in response to the current threat environment and to streamline and unify CWMD efforts. The CWMD Office will lead DHS efforts to protect Americans and U.S. interests from chemical, biological, radiological, and nuclear material and devices.

By consolidating key DHS functions into a single office with a CWMD focus, DHS can achieve greater policy coordination and strategic planning, as well as greater visibility for this critically important mission.

In FY 2017, CWMD reported on five strategic performance measures to assess its mission effectiveness. In FY 2017, 100 percent of the measures met their targets, and 100 percent maintained or improved actual results compared to FY 2016.



◆- Percent of measures that met their FY 2017 target.

◇- Percent of measures that maintained or improved actual performance results compared to FY 2016.

Progress: DHS maintains a strong operational presence, integrating multiple capabilities to better prevent, detect, locate, and interdict chemical, biological, radiological, and nuclear threats from numerous pathways. Mobile radiological and nuclear detection capability has expanded significantly, allowing it to be employed at numerous national security events. Additionally, radiological and nuclear education efforts and cooperative assessments of fielded detection capability have both increased during this period.

Progress was seen in balancing risk, cost, and schedule with respect to the acquisition of large-scale nuclear detection equipment at ports of entry. The program has worked toward being more integrated with, and responsive toward, front line operators, understanding their operational needs and the environment they operate in.

The Department has made progress in securing the Nation from biological threats working with the Science and Technology Directorate to establish requirements to enhance the BioWatch Program's technology. The Biodetection Technology Enhancement effort will seek to improve the Department's ability to protect the Nation from biological threats. In FY 2017, CWMD deployed near-term technology enhancements to improve the BioWatch Program's ongoing daily operations. CWMD also made progress on federal, state, and local coordination after a biological incident by hosting or supporting exercises that test and improve this capability among different government agencies, disciplines, and regions

Challenges and Risks: The ability to detect chemical, biological, radiological, and nuclear threats at useful distances to protect life and property, including materials obscured by shielding, packaging, or defensive measures, remains limited by existing detection equipment capabilities. The Department continues to invest in research for new equipment capabilities and concepts of operation while encouraging a layered approach in deployed partner capabilities to overcome detection challenges and reduce risks in all pathways.

CWMD will continue to coordinate with state and local governments to implement preventive and protective chemical, biological, radiological, and nuclear threats measures and reachback for federal assistance in a timely manner.

New Application Enhances Biodetection

The BioWatch Program rolled out a new mobile app to state and local partners in more than 30 jurisdictions nationwide where BioWatch operates its round-the-clock biodetection system. Established in 2003 to monitor the air for signs of bioterrorism, the BioWatch system relies, in part, on a network of field technicians, who place and retrieve filters from BioWatch air sampling units, and authorized laboratorians, who analyze the filters for indications of biological threats.

The new mobile app, known as the Sample Tracking Tool (STT), is a major step in implementing short-term technology upgrades with long-term impact. The app allows real-time tracking of samples from the field to the lab with detailed data collection about the sample's environment and weather conditions at the time it was retrieved.

DHS deployed the STT to support security for Super Bowl 51 in Houston, Texas. The STT enabled field and lab teams to more efficiently collect, process, and analyze more than 400 samples from the 40 collection units added to assess biological threats during the special security event. The STT integrates the work of field and lab technicians in a given jurisdiction as well as across jurisdictions and with federal partners. The tool improves the system's early warning capabilities by enhancing existing operations, which, in turn, enables rapid decisions to save lives in the face of a biological attack.

Mission Programs:

The mission programs that deliver performance results for CWMD are:

- **Capability and Operational Support:** The Capability and Operational Support program provides situational awareness and decision support for DHS leadership and federal partners. CWMD manages and supports the national bio-detection system, coordinates DHS biological defense activities, and supports preparedness for biological and chemical events to help communities prepare, respond, and recover. The program also supports bio-detection in more than 30 jurisdictions, including activities such as sample collection, laboratory analysis and support, consumables, reagents, and local quality checks.
- **Capability Building:** The Capability Building program funds programs and activities that provide chemical, biological, radiological, nuclear, and medical support, as well as funding readiness activities, in support of federal, state, local, tribal, territorial, and international partners and DHS operating components. CWMD pursues this by establishing, maintaining, and supporting programs and activities to defend against weapons of mass destruction, and combat bio-threats and pandemics.

Performance Results and Plan

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Weapons of Mass Destruction								
Average time (in hours) to initiate a BioWatch National Conference Call to discuss the detection of a biological agent of concern and assess the risk to public health with federal, state, and local partners (CWMD)								
---	---	---	---	---	≤ 3.0	2.0	≤ 3.0	≤ 3.0
Number of people covered by Securing the Cities program preventive radiological and nuclear (rad/nuc) detection capabilities (in millions) (CWMD)								
---	---	23.0	23.0	37.0	37.0	37.0	46.0	49.0

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Percent of cargo conveyances that pass through radiation portal monitors upon entering the nation via land border and international rail ports of entry (CWMD)								
FOUO	FOUO	FOUO	FOUO	FOUO	FOUO	FOUO[1]	FOUO	FOUO
Percent of containerized cargo conveyances that pass through radiation portal monitors at sea ports of entry (CWMD)								
FOUO	FOUO	FOUO	FOUO	FOUO	FOUO	FOUO[1]	FOUO	FOUO
Time between laboratory receipt of BioWatch detector samples to completion of screening for known biological micro-organisms of interest (in hours) (CWMD)								
---	---	---	---	---	≤ 7.0	5.0	≤ 7.0	≤ 7.0

1 – This measure met its annual target.

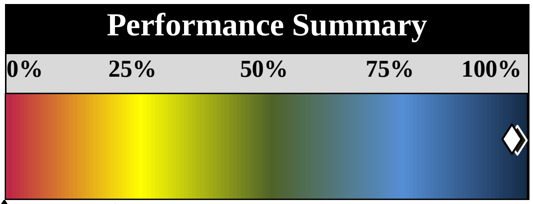
Federal Law Enforcement Training Centers

Overview

The Federal Law Enforcement Training Centers (FLETC) provides career-long training to law enforcement professionals to help them fulfill their responsibilities safely and proficiently. Over the past 47 years, FLETC has grown into the Nation's largest provider of law enforcement training. Under a collaborative training model, FLETC's federal partner organizations deliver training unique to their missions, while FLETC provides training in areas common to all law enforcement officers, such as firearms, driving, tactics, investigations, and legal training. Partner agencies realize quantitative and qualitative benefits from this model, including the efficiencies inherent in shared services, higher quality training, and improved interoperability. FLETC's mission is to train all those who protect the homeland, and therefore, its training audience also includes state, local, and tribal departments throughout the U.S. Additionally, FLETC's impact extends outside our Nation's borders through international training and capacity-building activities.

FLETC researchers and instructors conducted groundbreaking research on the effects of Electronic Stability Controls on the Precision Immobilization Technique (PIT) resulting in significant changes to FLETC curriculum, and initiating discussion in changes to law enforcement tactics nationwide.

In FY 2017, there were two strategic performance measures used to assess FLETC's efforts. In FY 2017, 100 percent of the measures met their target and 100 percent maintained or improved actual results compared to FY 2016.



◆ - Percent of measures that met their FY 2017 target.

◇ - Percent of measures that maintained or improved actual performance results compared to FY 2016.

Progress: FLETC is a perennial top performer as evidenced by their steady performance in growing and maintaining a strong network of training partners and continuing to receive top satisfaction ratings for the in-residence training conducted by FLETC.

Challenges and Risks: Moving forward, FLETC's biggest challenge will be managing the influx of new training requirements due to the planned hiring required to support the Executive Orders on Border Security, Immigration Enforcement, and Interior Enforcement.

FLETC Delivers Critical Tactical Medical Training

Approximately seven years ago, the Federal Law Enforcement Training Centers (FLETC) began to develop and implement Tactical Medical curriculum in basic and advanced training. Tactical Medical training provides law enforcement with the knowledge and skills necessary to prevent the loss of life in an austere or high threat environment, and includes training to treat life threatening injuries in an environment with limited equipment, lack of medically trained personnel, and prolonged time until evacuation. Implementation of this training was in support of the Department's direction to include tactical medical training in all basic law enforcement training for DHS law enforcement personnel and to standardize this training across DHS.

Tactical Medical training focuses on addressing the most preventable causes of death, along with concepts of self-care and buddy-care. The curriculum furthers the "Zero Loss" initiative developed by the DHS Office of Health Affairs. Officers routinely provide feedback and lessons learned on how they utilized this training to save lives and/or limit the severity of injuries. Additionally, officers have shared that the training gives them confidence in knowing they can save their own lives in situations where help may be delayed. An integral part of the training's success is the issuance of an Individual First Aid Kit to the students upon completion of the training, which provides the equipment and supplies required to utilize the learned skills, including a Special Operation Forces Tactical Tourniquet. FLETC delivered Tactical Medical training to over 3,000 officers and agents from federal, state, local, and tribal departments during FY 2017.

Mission Programs

The mission program that delivers performance results for FLETC is:

- **Law Enforcement Training:** The Law Enforcement Training program provides law enforcement training to federal, state, local, tribal, and international law enforcement agencies. The program provides training in areas common to all law enforcement officers, such as firearms, driving, tactics, investigations, and legal training. Under a collaborative training model, federal partner organizations also deliver training unique to their missions as part of this program. The program enables law enforcement stakeholders both within and outside of DHS the ability to obtain quality and cost effective training.

Performance Results and Plan

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Mission Support								
Number of Federal law enforcement training programs and/or academies accredited or re-accredited through the Federal Law Enforcement Training Accreditation process (FLETC)								
74	97	107	114	119	123	129	128	133
Percent of Partner Organizations that agree the Federal Law Enforcement Training Centers training programs address the right skills (e.g., critical knowledge, key skills and techniques, attitudes/behaviors) needed for their officers/agents to perform their law enforcement duties (FLETC)								
96%	100%	91%	98%	95%	95%	97%	90%[1]	90%

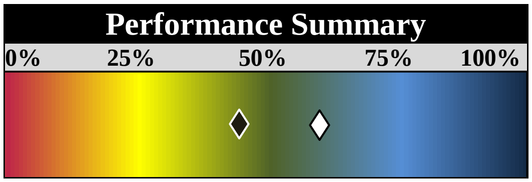
1 – FY 2018 target previously published as 95% in the FY 16-18 Annual Performance Report. The FY 2018 target is changing to meet the basic training goals associated with the Executive Orders on Border Security, Immigration Enforcement, and Interior Enforcement. These requirements will increase FLETC's throughput for the next three to seven years. Because there is a negative correlation between student throughput and student satisfaction, targets are being adjusted and will be monitored and adjusted as necessary.

National Protection and Programs Directorate

Overview

National Protection and Programs Directorate (NPPD) leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. NPPD's vision is a safe, secure, and resilient infrastructure where the American way of life can thrive.

In FY 2017, there were fifteen strategic performance measures used to assess the NPPD's efforts. In FY 2017, 47 percent of the measures met their target and 62 percent maintained or improved actual results compared to FY 2016.



◆- Percent of measures that met their FY 2017 target.

◇- Percent of measures that maintained or improved actual performance results compared to FY 2016.

Progress: DHS continues to coordinate with critical infrastructure owners and operators, and public and private sector partners, to share cyber threat information, manage risk, increase awareness of threats, and develop plans. DHS commenced sharing of cyber threat indicators with non-federal entities to enhance their capability to defend against known cyber threats. DHS also worked with critical infrastructure sectors to implement the National Institute of Standards and Technology (NIST) Cybersecurity Framework that will strengthen the resiliency and security of critical infrastructure by enabling owners and operators to follow a set of industry standards and best practices to help manage their cybersecurity risks. To engage local communities, DHS initiated the "Connect, Plan, Train, and Report" campaign to help better prepare business and their employees to proactively think about the role they play in the safety and security of their business and communities. With the completion of the contract award for the delivery, the Continuous Diagnostics and Mitigation (CDM) tools are in place to enable Federal agencies to better understand the assets and personnel that operate on their networks. The implementation of the CDM tools have resulted in agencies discovering previously unknown assets on their networks that will allow for greater awareness of vulnerabilities and more effective mitigation. To protect the government's most sensitive systems and data, DHS began assessments of agency-identified High Value Assets (HVAs) to identify vulnerabilities and weaknesses for agency remediation. The identification and prioritization of HVAs allowed DHS to focus limited resources on the most impactful assessments. Also DHS implemented an Automated Indicator Sharing (AIS) solution to allow for the distribution of cyber threat information in near real time with federal agencies. The number of cyberthreat indicators shared with federal partners has sustained at high levels over the past two years.

The CDM program has achieved increased savings (~$600M) through the consolidation of tool purchases reflecting a 70% savings compared to IT Schedule 70.

The Federal Protective Service (FPS) continues to perform a vital service of protecting more than 9,000 federal facilities nationwide. FPS is a federal law enforcement agency that provides integrated security and law enforcement services in support of federally owned and leased facilities and the people who occupy or visit them. FPS, in addition to federal facility protection, provides protective services in dozens of special events annually across the country.

Challenges and Risks: The cyberthreat to the Nation's critical infrastructure continues to grow and evolve as the increased connectivity of components of critical infrastructure and interdependencies, with their cascading impacts, expands both the attack surface and vulnerabilities for adversaries to exploit. Understanding of the complexities of both the increasing connectivity to the internet and the dependency of domestic infrastructure on foreign supply chains are still evolving. This increased exposure and interdependencies, coupled with the continued challenges in hiring and retaining an adequate cybersecurity workforce within DHS, present significant challenges.

While DHS made progress in delivering tools, assessing network security, and sharing information, significant challenges remain. In particular, senior agency leadership engagement on cybersecurity remains the critical ingredient to the successful implementation of DHS cybersecurity tools across the Federal Government. Due to the exceptionally high turnover of agency Deputy Secretaries and CIOs in a Presidential transition year, senior leadership engagement on cybersecurity will be a DHS focus moving forward. The cybersecurity workforce both within DHS and across the Federal Government also remains a concern. To implement and operate DHS-provided cybersecurity tools requires an agency cyber workforce with adequate staffing levels and specific skill sets. The lack of cybersecurity professionals in the federal workforce remains an issue in implementing and operating DHS-provided solutions.

Human Capital Strategies

DHS faces challenges when hiring for top cyber professionals. The DHS Chief Human Capital Officer (CHCO), in coordination with DHS Components and the Office of Personnel Management (OPM), is leading efforts to streamline the hiring process and create an environment of pay and flexibility that will attract and retain talent to implement the cybersecurity strategies needed to secure the .gov network. A few examples of policies being developed is the creation of a new excepted personnel system for cyber-professionals that would allow for greater flexibility in hiring, developing, and retaining top cybersecurity talent within DHS. CHCO and OPM are also working with NIST to implement the Cybersecurity Workforce Framework that clearly defines occupations and required skills within cybersecurity. The definition and classification of the current DHS cybersecurity workforce identify gaps regarding personnel and skill sets to be addressed.

Malware Impacts to the Nation’s Supply Chain

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

Mission Programs

The mission programs that deliver performance results for NPPD are:

- **Cybersecurity:** The Cybersecurity program advances computer security preparedness and the response to cyberattacks and incidents. The program includes activities to secure the federal network, respond to incidents, disseminate actionable information, and collaborate with private sector partners to secure critical infrastructure.
- **Emergency Communications:** The Emergency Communications program is responsible for advancing the Nation's interoperable emergency communications capabilities to enable first responders and government officials to continue to communicate in the event of disasters.
- **Federal Protective Service:** The Federal Protective Service protects federal facilities, their occupants, and visitors by providing law enforcement and protective security services. The program provides uniformed law enforcement and armed contract security guard presence, conducts facility security assessments, and designs countermeasures for tenant agencies in order to reduce risks to federal facilities and occupants.
- **Infrastructure Protection:** The Infrastructure Protection program leads and coordinates national programs and policies on critical infrastructure security and resilience and develops strong partnerships across government and the private sector. The program conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators and state, local, tribal, and territorial partners understand and address risks to critical infrastructure.

Performance Results and Plan

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Critical Infrastructure								
Percent of contract security force evaluations conducted at high-risk facilities resulting in no countermeasure-related deficiencies (NPPD)								
---	---	---	---	---	New Measure[1]		85%	85%
Percent of customers implementing at least one cybersecurity assessment recommendation to improve critical infrastructure and federal network security (NPPD)[2]								
---	100%	63%	100%	100%	100%	91%[3]	85%[4]	85%
Percent of facilities that are likely to integrate vulnerability assessment or survey information into security and resilience enhancements (NPPD)								
---	---	---	---	90%	80%	92%	80%	80%
Percent of Facility Security Committee Chairs (or designated officials) satisfied with the level of security provided at federal facilities (NPPD)								
---	---	---	---	---	78%	77%[5]	79%	80%
Percent of high-risk facilities that receive a facility security assessment in compliance with the Interagency Security Committee (ISC) schedule (NPPD)								
---	34%	93%	100%	96%	100%	100%	100%	100%
Percent of performance standards implemented by the highest risk chemical facilities and verified by DHS (NPPD)								
---	46%	78%	93%	97%	95%	93%[6]	95%	95%

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Critical Infrastructure								
Percent of respondents reporting that DHS critical infrastructure information will inform their decision making on risk mitigation and resilience enhancements (NPPD)								
---	---	---	---	92%	74%	95%	77%	80%

1 – This is a new measure for DHS's FY 2018 Performance Plan but has prior data: FY 2013 – 97%, FY 2014 – 97%, FY 2015 – 97%, FY 2016 – 98%, FY 2017 – 83%.

2 – Measure name changed from "*Percent of organizations that have implemented at least one cybersecurity enhancement after receiving a cybersecurity vulnerability assessment or survey*."

3 – DHS operates cyber security assessment programs focused on the private sector, industrial controls, and government sector. This measure evaluates whether these assessments result in action by the assessed organization to improve their security posture. For FY 2017, 91 percent of customers responding to 180 day feedback surveys reported implementation of significant enhancements to cybersecurity as a result of the assessments. Cyber assessments, including architecture reviews and penetration testing, are critical to preventing cyber incidents and prevention is the most cost effective tool in the cybersecurity arena. Making enhancements is at the discretion of the customer, based on their internal policies, procedures, and priorities. A study of DHS cybersecurity assessment offerings began in early 2017. The results of the study will be used to ensure the assessments included in this measure are targeted to the appropriate customers and that any recommended actions are appropriately tailored to the customer's operational maturity.

4 – FY 2018 target previously published as 100% in the FY 16-18 Annual Performance Report has been revised to be more in-line with recent results and projected performance.

5 – FPS assesses the effectiveness of protection and security services via the customer satisfaction of the Facility Security Committee Chairs, or their designated officials, it serves. The Facility Security Committee Chairperson is the representative of the primary tenant and is the primary customer of FPS Facility Security Assessments and countermeasure consultation. Understanding satisfaction enables FPS to make better informed decisions to enhance the services it provides to its tenants. FPS achieved a score of 77 percent satisfied respondents (answered satisfied or very satisfied) to the question, "Overall, what is your satisfaction level with FPS services?" FPS received responses from 1,639 respondents who auto-identified as a Facility Security Committee Chair or Designated Official. Of those respondents, 1,267 responded with a greater than neutral response. In October 2017, FPS released a new Strategic Plan. Goal 3 states that FPS will continue to strive to be the market leader of protection services and enterprise risk management. The objectives of Goal 3 include strengthening the DHS role in the Government Facility Sector (GFS) by providing innovative and unduplicated information that improves GFS protection capabilities and continuing to develop relationships with key stakeholders such as the Facility Security Committees. Using the data gathered from the Voice of the Customer survey and working through the field forces and the Facility Security Committees, FPS can better align service to customer needs

6 – This measure assesses the amount of DHS verified performance standards implemented by the highest risk chemical facilities to ensure compliance with the Chemical Facility Anti-terrorism Standards (CFATS) regulation. In FY 2017, DHS delivered guidance to the highest risk chemical facilities, prompting these owners and operators to include 21,412 performance standards in their security plans. Of the 21,412 performance standards, 19,914 have been implemented. Implementing these performance standards improves the overall security of the highest risk chemical facilities. The revised tiering methodology for determining the highest risk facilities resulted in facilities changing tier, and either dropping out of or coming into the program. The significant movement of facilities entering and leaving the program resulted in an overall decrease in the percentage. In October 2016, DHS rolled out the Chemical Security Assessment Tool (CSAT) 2.0 system, an updated online portal that helps DHS identify facilities that meet the criteria for high-risk chemical facilities. During FY 2017, the implementation of CSAT 2.0 resulted in significant movement of facilities entering and leaving the program. As a result of these updates, DHS saw an overall decrease in the percentage of performance standards implemented by the highest risk chemical facilities, particularly as more facilities were reviewed and re-tiered using the CSAT 2.0 system. DHS will continue to prioritize the implementation of performance standards across the highest risk chemical facilities.

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Federal Network Security								
Percent of annual risk and vulnerability assessments completed for twenty-three cabinet level agencies and one-third of all non-cabinet level agencies (NPPD)								
---	---	---	---	42%	60%	35%[1]	40%[2]	45%
Percent of federal, civilian executive branch personnel for whom EINSTEIN intrusion prevention system coverage has been deployed (NPPD)								
---	---	---	---	80%	100%	95%[3]	Retired[4]	
Percent of incidents detected by the U.S. Computer Emergency Readiness Team for which targeted agencies are notified within 30 minutes (NPPD)								
---	89.0%	87.2%	96.6%	97.0%	96.0%	N/A[5]	98.0%	100%
Percent of incidents detected or blocked by EINSTEIN intrusion detection and prevention systems that are attributed to Nation State activity (NPPD)								
---	---	---	---	---	New Measure		20%	21%
Percent of participating federal, civilian executive branch agencies for which Continuous Diagnostics and Mitigation (CDM) tools to monitor what is happening on their networks have been made available[6]								
---	---	---	---	---	97%	0%[7]	95%[8]	100%
Percent of respondents indicating that operational cybersecurity information products provided by DHS are helpful (NPPD)								
---	---	---	---	---	78%	92%	90%[9]	90%
Percent of significant (critical and high) vulnerabilities identified by DHS cyber hygiene scanning of federal networks that are mitigated within the designated timeline (NPPD)								
---	---	---	---	---	New Measure		80%	90%
Percent of survey respondents that were satisfied or very satisfied with the timeliness and relevance of cyber and infrastructure analysis based products (NPPD)								
---	---	---	---	93%	90%	93%	92%	94%
Percent of traffic monitored for cyber intrusions at civilian Federal Executive Branch agencies (NPPD)								
73.0%	82.4%	88.5%	94.3%	98.7%	95.0%	99.4%	Retired[10]	

1 – DHS provides an objective third-party perspective on the current cybersecurity posture of an agency's unclassified network and is required to conduct assessments for all CFO Act agencies and one-third of remaining federal agencies each year. Risk and Vulnerability Assessments (RVAs) provide cybersecurity stakeholders with commercial best practices and threat intelligence integration to help develop better decision making and risk management guidance. Due to the implementation of a new prioritization model and limited funding only 20 federal agencies received an RVA in FY 2017 out of a required 57. The prioritization for a RVA is no longer focused specifically on federal agencies but state and local agencies, as well as critical infrastructure sectors and operators are included. The prioritization is based on total time on a waitlist, a special leadership request, an incident occurring, and calculated risk to each critical infrastructure sector. DHS continues to work within available funding and is prepared to increase the number of assessments when funding is made available. The plan is to conduct three concurrent assessments which will increase the total number of assessments during the fiscal year. DHS has started coordinating with contracting agencies to have personnel on standby for further guidance with short suspense. In FY 2018, DHS will use an RVA prioritization method to determine which federal, state, local, or critical infrastructure entity will receive a RVA. Due to the increased demand and expansion of RVAs to multiple stakeholders outside of the federal sector, it is unlikely that DHS will increase the number of RVAs provided to federal agencies under current funding.

2 – FY 2018 target previously published as 80% in the FY 16-18 Annual Performance Report was adjusted to better align with past performance and expected future results.

3 – The EINSTEIN 3 Accelerated (E3A) program delivers intrusion prevention capabilities by detecting malicious traffic, and preventing it from harming agency networks. The FY 2017 result reflects an increase of approximately 525,000 federal civilian personnel protected by E3A intrusion prevention services from the FY 2016 end of year result. For FY 2017, 95 percent of the federal, civilian executive branch personnel, and 100 percent Chief Financial Officer (CFO) Act agency personnel are protected by at least one E3A countermeasure. DHS continues to work with relevant internet service providers (ISPs), and federal entities to deploy E3A at remaining Small/Micro agencies; however, these agencies have fewer Information Technology (IT) staff, and E3A competes with resources dedicated to day-to-day operations, and other cybersecurity initiatives and requirements.

4 – This measure being retired as the implementation is substantially complete. The 23 CFO Act Agencies have been covered and ongoing efforts will continue with the small and micro-agencies.

5 – The program was unable to produce results in FY 2017 due to data collection process problems. The issue was that analysts were inconsistently time stamping incident tickets that start the clock on how long the U.S. CERT team has to notify the affected agency. The analysts were supposed to timestamp the ticket with the time that it was determined that the event is an incident. Analysts were time stamping the tickets using various criteria and the program could not go back and fix the accuracy of the data. The program has taken corrective actions and reliable data will be available in FY 2018.

6 – Measure name changed from "*Percent of participating federal, civilian executive branch agencies for which Phase 3 continuous diagnostics and mitigation tools have been delivered to monitor their networks*" to more clearly reflect to a lay audience the capabilities being delivered.

7 – The Continuous Diagnostics and Mitigation (CDM) program provides federal agencies with capabilities to identify cybersecurity risks, prioritize those risks, and enable mitigation of the most significant problems first. Thus it is imperative that contracts to implement CDM on the federal network are awarded in a timely manner. Phase 3 of CDM focuses on boundary protection and event management across the security lifecycle. Due to agencies underestimating the size of their networks and the subsequent need to cover many more endpoints than originally estimated, required the program to re-allocate resources designated for Phase 3 to Phase 1. This financial restructuring, coupled with the FY 2017 Continuing Resolution, has delayed the program initiating Phase 3 acquisitions. Phase 2 contracts have been awarded and are currently being implemented by Agencies. The CDM Program Management Office has completed its re-baselining activities as directed by DHS and the program has moved forward with Phase 3 activities including completion of pre-solicitation planning and preparation activities for the first Task Order for Phase 3. That Task Order is currently in Source Selection and is expected to be awarded in Q2 FY 2018. The remaining Task Orders are being planned and expected to be awarded Q3 & Q4 FY 2018 and into FY 2019.

8 – FY 2018 target previously published as 100% in the FY 16-18 Annual Performance Report was adjusted to better align with past performance and expected future results.

9 – FY 2018 target previously published as 78% in the FY 16-18 Annual Performance Report was adjusted to better align with past performance and expected future results.

10 – This is an implementation measure for the installation of EINSTEIN 2 sensors that has nearly reached 100%. Any changes to this measure will occur as a result of micro agencies network flow go through a Trusted Internet Connection with EINSTEIN 2 sensors installed.

Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Man-Made or Natural Incident Preparedness								
Percent of States and Territories with operational communications capabilities at the highest levels relative to Threat and Hazard Identification and Risk Assessment (THIRA) preparedness targets (NPPD)								
---	---	---	---	55%	56%	55%[1]	57%	58%

1 – Emergency communications technologies are rapidly evolving, which has resulted in increased complexity for state, local, tribal, and territorial partners. To address these challenges, DHS provides training, coordination, tools, and guidance to help its partners develop their emergency communications capabilities. DHS uses the THIRA process to identify the level of operational communications capabilities available throughout the United States. THIRA data is reported by states/territories at the end of the calendar year, thus the data available for FY 2017 reporting is from calendar year 2016. DHS fell short of the target with only 55% of states and territories rating their operational communications as meeting target capability levels. By ensuring effective emergency communications across the nation, DHS helps to ensure effective emergency response, which ultimately strengthens national preparedness and resilience. DHS is working to improve operational communications by: conducting planned observations in major urban areas; focusing on data operability and land mobile radio strengths and challenges; planning for the integration of data into incident communications through the Communications Unit Working Group; piloting intensive state workshops to develop a Statewide Communications Interoperability Plan that covers all public safety communications systems to ensure information flows seamlessly; updating technical assistance offerings to address stakeholder needs and changing technology; supporting the development of a nationwide survey to collect critical data to drive the nation's emergency communication policies, programs, and funding; and working with the Department of Interior and states to sign agreements allowing non-Federal agencies to access the Federal Enforcement and Incident Response Interoperability Channels to increase interoperability.

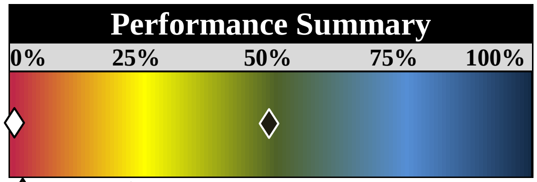
Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Man-Made or Natural Incident Response								
Percent of calls made by National Security/Emergency Preparedness users during emergency situations that DHS ensured were connected (NPPD)								
99.4%	96.8%	99.3%	99.3%	99.0%	98.0%	99.3%	98.5%	99.0%

Science and Technology Directorate

Overview

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. Technology and threats evolve rapidly in today's ever-changing environment. S&T monitors those threats and capitalizes on technological advancements at a rapid pace, developing solutions, and bridging capability gaps. S&T's mission is to deliver effective and innovative insight, methods, and solutions for the critical needs of the Homeland Security Enterprise.

In FY 2017, there were two strategic performance measures used to assess S&T's efforts. In FY 2017, 50 percent of the measures met their target and zero percent maintained or improved actual results compared to FY 2016.[2]



◆- Percent of measures that met their FY 2017 target.

◇- Percent of measures that maintained or improved actual performance results compared to FY 2016.

Progress: DHS's Research and Development activities have a critical impact on the departmental missions. The advanced technologies, knowledge products, technical analyses, laboratories, and university-based research contribute to the effectiveness and efficiency of DHS operations. From wireless emergency alert improvements to thermal sensor warning for fire safety to mitigating threats from Vehicle Improvised Explosive Devices, S&T has made significant progress improving technology and processes to make the nation safer.

Challenges and Risks:

For all research elements, the greatest challenge in the results and outcomes of research and development programs is the uncertainty of the practicality of the results that will be delivered and the ongoing funding to support the work in light of this uncertainty. The management controls and planning processes instituted in the research elements make them a strong steward for government funding; however funding fluctuations can disrupt research efforts and the potential to deliver needed capabilities to the operational elements within the Department. These fluctuations can also strain the organization's ability to retain top-level expertise and talent.

> "The explosives detection canine is the best, most versatile mobile explosive detection tool at our disposal for protecting the Homeland from the explosive threat."

[2] S&T'S performance on these two publicly reported measures is not fully indicative of the work accomplished in FY 2017. For some examples, please visit S&T's "Our Work" page for details.

S&T Testing Aims to Mitigate Threat from Vehicle IEDs

Vehicle–Borne Improvised Explosive Device (VBIED, also known as car bombs) continue to pose a real and evolving threat to even the most secure compounds. The Explosives Division (EXD) within the Homeland Security Advanced Research Projects Agency of DHS's S&T has taken measures to address this threat directly. EXD's Homemade Explosives (HME) program conducts Large–Scale VBIED testing to mitigate the threat posed by massive car bombs and to ensure such attacks do not occur in the U.S.

In March 2017, S&T EXD conducted a series of explosives tests with varying charge sizes. "Due to the wide variety of types of and materials used to make HMEs, we sometimes have to conduct controlled real-life events to discover new ways of combatting emerging trends in explosives," according to HME Deputy Program Manager Dave Hernandez. These tests, conducted at Fort Polk, Louisiana, brought together the HME preparation expertise of the U.S. Naval Surface Warfare Center's (NSWC) Indian Head facility and the live fire testing capability of the U.S. Army Corps of Engineers' Engineering, Research, and Development Center in Vicksburg, Mississippi.

The data from the Fort Polk tests show the damage that different types of HME mixes can inflict. Such information on large-scale detonations could not be accurately calculated before these tests were conducted and will facilitate the development of new mitigation techniques for larger-scale explosions.

"The information generated from this testing will aid the DoD and law enforcement communities by revealing data on the impact of a large–scale VBIED; enabling better protection for vulnerable targets," HME Program Manager Elizabeth Obregon said. "As the HME threat is constantly changing, a continued effort in this area is required in order to provide timely information to those organizations conducting analysis and acquisitions."

Mission Programs

The mission programs that deliver performance results for S&T are:

- **Acquisition and Operations Analysis:** The Acquisition and Operations Analysis programs provide expert assistance to entities across the homeland security enterprise to ensure that the transition, acquisition, and deployment of technologies and information improve the efficiency and effectiveness of operational capabilities across the homeland security enterprise. This program assists in testing and evaluation, standards development, requirements analysis, systems engineering, and supporting technology transition.
- **Laboratory Facilities:** The Laboratory Facilities program oversees and provides capabilities through our laboratories vital to the homeland security mission that provide core competencies in air transportation security, radiological detection and first responder safety, chemical agent detection, biological threat assessment, and animal diseases and food chain protection. The laboratory network enables America's best scientists and engineers to apply their expertise and develop solutions to our most dangerous threats.
- **Research, Development, and Innovation:** Research, Development, and Innovation is a portfolio of customer-focused and output-oriented research, development, and testing and evaluation programs. The program consists of specific portfolios to include: Border Security, Chemical/Biological/ Explosives Defense, Counter Terrorist, and First Responder/Disaster Resilience. These portfolios support the needs of the operational components of the Department and the first responder community to address capability gaps.

- **University Programs:** University Programs supports critical homeland security-related research and education at U.S. colleges and universities to address high-priority DHS-related issues and to enhance homeland security capabilities over the long term. University Programs includes DHS Centers of Excellence and Minority Serving Institutions, a consortium of universities generating groundbreaking ideas for new technologies and critical knowledge for the homeland security enterprise.

Performance Results and Plan

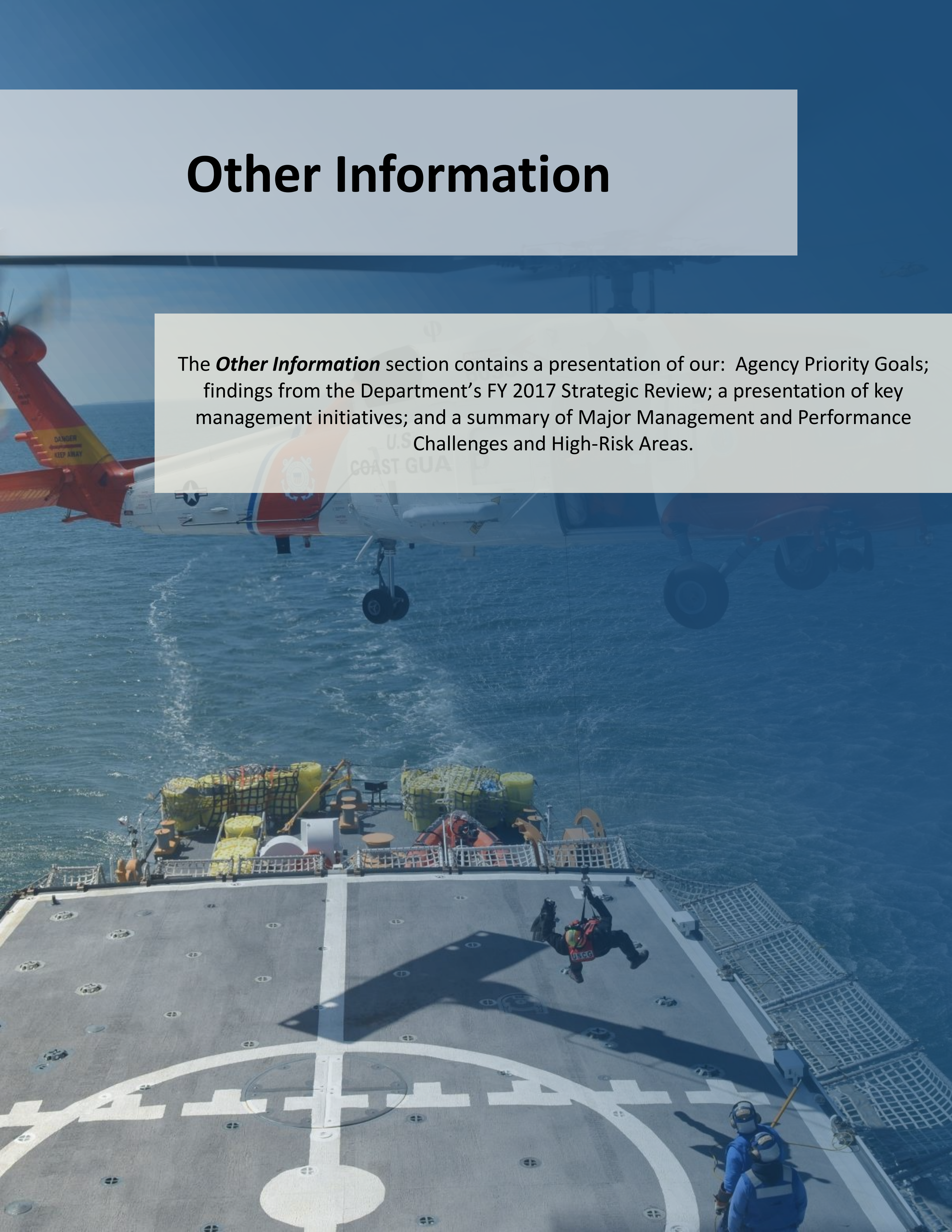
Prior Results					FY 2017		Performance Plan	
FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	Target	Result	FY 2018	FY 2019
Mission Support								
Percent of planned cybersecurity products and services transitioned to government, commercial and open sources (S&T)								
---	89%	93%	60%	73%	80%	71%[1]	80%	80%
Percent of Apex technologies or knowledge products transitioned to customers for planned improvements in the Homeland Security Enterprise[2] (S&T)								
---	---	---	82%	100%	80%	83%	80%	80%

[1] – The result of this measure consists of the Cyber Security Division (CSD) completion of planned transitions of cybersecurity products and/or services, which means cybersecurity research and development efforts have resulted in deployable security solutions. In FY 2017, CSD completed five out of seven planned transitions for the following: Transition to Practice project, Cyber Security Research Infrastructure Program, and three for Network & System Security program. The remaining two planned transitions were delayed due to contracting delays and internal policy discussions impacting program schedule. Regular technical and program management oversight will help bring leadership focus to the achievement of transitions planned for the fiscal year.

[2] – This measure tracks transitions of high priority and high value research and development projects that make up the Apex programs. A successful transition is the ownership and operation of a technology or knowledge product by a customer within the Homeland Security Enterprise. In FY 2017, S&T completed five of six planned transitions. These transitions mean high priority and high value research and development projects are being delivered to improve homeland security operations.

Other Information

The ***Other Information*** section contains a presentation of our: Agency Priority Goals; findings from the Department's FY 2017 Strategic Review; a presentation of key management initiatives; and a summary of Major Management and Performance Challenges and High-Risk Areas.



Agency Priority Goals (APG)

DHS's APGs are a set of focused initiatives that support the Agency's achievement of its strategic framework and are one of the tenets of GPRAMA. APGs are defined for a two-year implementation period which provide opportunities for leadership to significantly drive improvement in near-term performance.

This year is a transition year where the Agency closes out the current APGs and introduces new APGs for next two years. Below are two sections. The first section presents the final results and progress update for the current FY16-17 APGs. The next section presents the new FY18-19 APGs and provides the details about each.

Close out of FY16-17 APGs

Agency Priority Goal 1: Combatting Transnational Criminal Organizations

Impact and 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 (JTFs) via synchronized component operations will result in the disruption and/or dismantlement of 15 percent of targeted transnational criminal organizations.

Key Measure Final Results:

	FY17 Target	FY17 Result
Percent of transnational criminal organizations targeted by the Joint Task Forces that are disrupted or dismantled	15%	21%

The JTFs exceeded the target to disrupt or dismantle targeted transnational criminal organizations. This result was accomplished through the execution of coordinated operational plans and investigations and leveraging the joint efforts of the operational components and all the task forces.

Overview: TCOs are self-perpetuating associations of individuals who operate transnationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means. This is accomplished while protecting their activities through a pattern of corruption and/ or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms. There is no single structure under which transnational organized criminals operate; they vary from hierarchies to clans, networks, and cells, and may evolve to other structures.

TCOs are an adaptive and innovative adversary; they are known to search for new ways to leverage their business model to generate profits and engage in criminal activity - whether it be finding new smuggling routes and methods or entering into new criminal enterprises. TCOs represent a persistent threat to western hemisphere stability, economic prosperity, free trade, and security, because of their control of illicit trade, travel, and finance—by utilizing existing and/or creating new illegal pathways for smuggling throughout the Southern Border and Approaches region. This region extends from the waters off Los Angeles, California, eastward to Puerto Rico and the Virgin Islands, and southward to the North Coast of South America. The region includes approximately 2,000 miles of land border with Mexico, 3,050 miles of coastline along California, the Gulf of Mexico, and Florida, as well as the airspace spanning U.S. territorial land and waters, and international waters of the Eastern Pacific Ocean, and Caribbean Sea. The greatest criminal threat within this region is posed by TCOs in regional groups in Central and South America and the Caribbean. This threat is based on their ability to generate massive illicit profits, which they have been known to use to suborn public officials and law enforcement, and perpetuate drug-related violence and other crimes, such as kidnappings and extortion.

To more effectively combat the TCO threat, DHS established the JTFs to integrate intelligence, planning, interdiction and investigative efforts across U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the U.S. Coast Guard, and to prioritize and target threat streams operating in the Southern Border and Approaches region, as well as combat TCO activity and splinter organizations present within the U.S. and internationally. DHS will leverage both domestic and international resources and capabilities through intelligence, information sharing, and law enforcement collaboration to weaken and eliminate TCOs who pose the greatest threat to border security, while still facilitating the flow of lawful trade, travel, and commerce across our nation’s borders.

Disrupting and/or dismantling TCOs is a primary outcome of the JTFs and is a result of concentrated, unified actions taken by DHS law enforcement components to identify, target and stop some of the most dangerous and damaging criminal and smuggling operations impacting our Nation’s southern border and approaches regions. Daily actions are taken to counter and degrade threats posed by TCOs, but true disruptions and dismantlements of operations are hard won battles. Disruptions and dismantlements incapacitate threats from targeted TCOs, represent the best and most enduring successes against these criminal organizations, and demonstrate gains to border security made possible through coordinated law enforcement campaigns. Since new threats continuously present themselves, new lists are created throughout each year that targets the highest priority threats.

Progress Update: The JTFs made significant strides in achieving their performance goals during the past two years. In collaboration with its partners, JTF-East (JTF-E) developed a Regional Integrating Group (RIG) framework to achieve DHS unity of effort objectives.

JTF-E supported RIGs and pre-existing regional interagency groups to establish intelligence coordinating mechanisms and surged additional resources to support named operations in the joint operating areas (JOAs). JTF-E facilitated the establishment of Joint Intelligence and Operation Coordination Centers (JIOCCs) during FY 2017 surge operations that fused field input with investigative support to generate actionable intelligence and asset coordination. JTF-E’s efforts resulted in increased participation in JIOCCs and surge operations by the DHS Component agencies and their field units, DoD Joint Interagency Task Force South (JIATF–S), DoD Joint Task Force-North (JTF-N), National Guard Bureau, and domestic and international law enforcement partners. The joint surge operations also netted criminal arrests and drug/currency seizures.

Similarly, JTF-Investigations (JTF-I) continued to refine the Comprehensive Criminal Network Analysis and the National Case Management and Integrated Action Plans to serve as department-wide processes and standards for dismantling the top criminal networks impacting homeland security. JTF-I currently is managing ten Homeland Criminal Organization Target (HOMECORT) investigations addressing DHS priorities. The HOMECORT BOLT OVERSEIZE investigation is targeting a TCO comprised of affiliated TCOs operating in Ecuador, Colombia, Peru, and the United States. From the inception of this investigation to date as direct result of JTF-I’s efforts this HOMECORT investigation has resulted in the arrest of more than 120 suspects, representing significant impact.

JTF-West (JTF-W) used Operation CX17 as the strategic framework for operations

targeting prioritized TCOs, illicit networks, and threats to the Southwest border. The TCOs/networks targeted were involved in alien smuggling (23), drug trafficking (16), multi-commodity (6) and one weapons smuggling. JTF-W operations resulted in 283 criminal arrests,
63 administrative arrests, 14 visa cancellation/revocations, and 492 illegal alien (IA) apprehensions. During FY17, JTF-W International Engagement Section focused on consolidating existing relationships and developing new partnerships with international stakeholders. Thirty seven percent of the named operations (17 of 46) were supported by DHS international Components and foreign mission partners. In support of these 17 named operations, Southwest Border Corridors utilized existing mechanisms and personnel to exploit and expand information on JTF-W TCO priority targets.

Agency Priority Goal 2: Enhance Federal Network Security

Impact and 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.

Key Measure Final Results:

Percent of participating federal, civilian executive branch agencies for which Phase 1 and 2 continuous diagnostics and mitigation tools have been delivered to monitor their networks	FY17 Target	FY17 Result
	100%	100%

The Continuous Diagnostics and Mitigation (CDM) program provides federal agencies with capabilities to identify cybersecurity risks, prioritize those risks, and enable mitigation of the most significant problems first. Thus it is imperative that contracts to implement CDM on the federal network are awarded in a timely manner. As of the end of Q1 FY 2017, there were 69 agencies participating in Phase 1 (asset management) and 65 agencies participating in Phase 2 (user management) tools. The final award for Phase 2 tools was completed in Q1 FY 2017 and 100% of Phase 1 and Phase 2 have been delivered to participating federal, civilian executive branch agencies. This effort will continue with a follow-on APG in FY18-19.

Overview: The 2014 Quadrennial Homeland Security Review and the FY14-18 DHS Strategic Plan recognizes the continuing need to secure the federal civilian executive branch agencies' information technology networks and systems. By law, each head of a federal department or agency is primarily responsible for their agency's own cybersecurity. The Department of Homeland Security has overall responsibility for protecting federal civilian executive branch systems from cyber threats, helping agencies better defend themselves, and providing response teams to assist agencies during significant incidents. There is no one "silver bullet" for cybersecurity. The key is to install multiple layers of protection to best secure federal networks.

DHS's National Cybersecurity and Communications Integration Center (NCCIC) is the U.S. government's 24/7 hub for cybersecurity information sharing, incident response and coordination. The NCCIC shares information on cyber threats and incidents, and provides on-site assistance to victims of cyberattacks. The NCCIC is also where DHS manages the EINSTEIN system, the first basic layer of protection DHS provides at the network perimeter of each federal civilian executive branch agency. While there are three parts to the EINSTEIN set of capabilities, the focus is currently on the deployment of the third phase, known as

EINSTEIN 3 Accelerated which has the capacity to identify and block known malicious traffic.

DHS also helps federal agencies identify and fix problems inside their networks in near real-time using the Continuous Diagnostics and Mitigation program (CDM). Once fully deployed, CDM will constantly scan agency networks for vulnerabilities that bad actors could exploit if they did breach an agency's perimeter. The CDM Program consists of three phases that are currently in various stages of availability to federal civilian executive branch agencies. The first phase of CDM focuses on "What is on the Network," specifically asset management. This includes hardware and software assets, managing configuration settings, and vulnerabilities, all of which are foundational capabilities to protect systems and data. Phase 2 ("Who is on the Network") covers user account and network privilege management; and Phase 3 ("What is Happening on the Network") covers boundary protection, event management and security lifecycle management.

As of October 1, 2015, DHS has delivered the first phase of CDM to the 23 civilian Chief Financial Officer Act agencies, covering 97 percent of the federal civilian Executive Branch government. These agencies are expected to deploy these CDM tools on their networks within the fiscal year.

Information sharing is also fundamental to achieving cybersecurity. The NCCIC shares information on cyber threats, vulnerabilities, and incidents. In order to sufficiently address the rapidly evolving threats to our cyber systems, DHS and its partners must move beyond information sharing methods that are overly reliant on manual processes to be able to share cyber information in as close to real-time as possible. DHS is pursuing an aggressive schedule to deploy one of its next-generation information sharing techniques. The Department has an automated system in place to share cyber threat indicators, and DHS will extend this capability across the Federal Government and to the private sector, so that the larger community can send and receive threat indicators in near real-time.

This goal aligns with Administration cybersecurity priorities. The goal was established in coordination with OMB policies and guidance, to include the Cybersecurity Strategy and Implementation Plan, the Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements, and the Cybersecurity CAP goal.

Progress Update: *Continuous Diagnostics and Mitigation (CDM):* The CDM Program has delivered all Phase 1 tools and Phase 2 tools to all participating agencies and has met its FY 2017 target of 100%. The final Phase 2 award was delayed due to a protest and completed in Q1 FY 2017.

The CDM Program Management Office has completed its re-baselining activities as directed by the Department and had an Acquisition Decision Event 2B in Q4 FY 2017. Based on the Acquisition Decision Event 2B results, the Program Management Office has moved forward with Phase 3 activities including completion of pre-solicitation planning and preparation activities for the first Task Order (Dynamic Emerging Federal Enterprise Network Defense (DEFEND) Group B) for Phase 3. That Task Order is currently in Source Selection and is expected to be awarded in Q2 FY 2018. The remaining Task Orders (DEFEND Groups A, C, D, E, & F) are being planned and expected to be awarded Q3 & Q4 FY 2018 and into FY 2019. The General Services Administration has awarded the CDM Tools Special Item Number (CDM Tools SIN) in August 2017 and the Program is positioned to use that instrument to procure CDM vetted products for all the DEFEND Task Orders.

National Cybersecurity Protection System (NCPS): By September 30, 2017, 234 federal, civilian executive branch Departments and Agencies (D/As) entities were brought on to E3A services, representing approximately 2.079 million users, or 95% of the total user population. In FY 2017, emphasis on E3A deployments were applied to all remaining federal, civilian executive branch departments and agencies that did not apply E3A capabilities to their networks, by December 18, 2016 as required in the Federal Cybersecurity Enhancement Act of 2015.

Automated Indicator Sharing (AIS): Now that all DHS Components have the ability to share and receive cyber threat indicators in a machine-readable format, NPPD's focus is shifting to encourage increased sharing into the community. In addition, NPPD will be working with DHS Components and external agencies on how best to ingest cyber threat indicators in an automated manner.

Risk and Vulnerability Assessments (RVAs): DHS Cybersecurity Risk and Vulnerability Assessments (RVA) test an organization's ability to defend itself from malicious cyber-attacks. The RVA is a critical element in Federal cybersecurity and is a cost-effective means to prevent a cyber incident. This measure quantifies the number of unique federal agencies that received RVAs. Overall, 14 RVAs were completed across 4 agencies in Q4, raising the total to 42 RVAs provided to 20 unique federal agencies in FY2017 (35% of target agencies).

Agency Priority Goal 3: Enhance Disaster Preparedness and Response

Impact and 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.

Key Measure Final Results:

Percent of states and territories that have achieved an intermediate or above proficiency to address their targets established through their THIRA	FY17 Target	FY17 Result
	70%	70%

States and territories that receive preparedness grant funding from FEMA must use the Threat and Hazard Identification and Risk Assessment (THIRA) annually to establish capability targets based on identified risks. In the State Preparedness Report, states and territories rate themselves relative to targets they set in their THIRAs for each of the core capabilities identified in the National Preparedness Goal. Analysis of the FY 2017 submissions shows that 38 out of 54 states and territories (70%) achieved an average rating of intermediate or above proficiency across all high-priority core capabilities.

Overview: FEMA continues to allocate resources to supplement whole community investment to prepare for the greatest challenge in emergency management—a catastrophic disaster. In order to successfully respond to and recover from a catastrophic event, the whole community, including FEMA, state and local governments, and individuals that may be affected, need to build and sustain capabilities and implement the National Preparedness System to achieve the National Preparedness Goal of a secure and resilient Nation.

In order to achieve this goal, FEMA has implemented activities and programs that assist in addressing gaps in state and local planning efforts, improved the governance, coordination structures, and guidance for managing the Agency's incident workforce, and designed and delivered accessible information and tools to promote collective actions and empower grassroots problem solving.

Progress Update: In order to successfully respond to and recover from a catastrophic event, the whole community, including FEMA, state and local governments, and individuals that may be affected, need to build and sustain capabilities and implement the National Preparedness System to achieve the National Preparedness Goal of a secure and resilient Nation. To achieve this goal, FEMA implemented activities and programs that assisted in addressing gaps in state and local planning efforts, improved the governance, coordination structures, and guidance for managing FEMA's incident workforce, and designed and delivered accessible information and tools to promote collective actions and empower grassroots problem solving. Throughout the two years of this Agency Priority Goal (APG), FEMA made progress toward achieving this goal by completing the following:

- In FY 2016, FEMA provided technical assistance trainings to 90 jurisdictions with the goal of improving their FY 2017 Threat and Hazard Identification and Risk Assessment (THIRA) and State Preparedness Report (SPR) submissions. FEMA focused on assisting jurisdictions with defining the resources they need to reach their THIRA core capability targets and to include the whole community in disaster planning to increase capabilities by sharing resources with neighboring jurisdictions and leveraging resources from the non-governmental sector.
- FEMA provided national level data on state capabilities to over 26 federal agencies to help refine, develop, and implement preparedness programs and initiatives such as training and planning support. Analysis of FY 2017 submissions shows that 38 out of 54 states and territories (70%) achieved an average rating of intermediate or above proficiency across all high-priority core capabilities, an increase of one state from FY 2016 to FY 2017.
- To support whole-community planning in FY 2016 -2017, 62 of 175 (35%) National Exercise Program (NEP) exercises included private and nonprofit sector partners as a sponsor or major participant of the exercise. Some of the events were: National Association of Counties Climate Adaptation Tabletop; Building Resiliency with Diverse Communities Impact Study Tabletop; National Seminar and Tabletop Exercise for Institutions of Higher Education; and the Emergency All-Sector Response Transnational Hazards Exercise Federal Sector Senior Leadership Tabletop Exercise.
- FEMA decreased disaster administrative costs 3.5 percentage points between FY 2016 and FY 2017, and reached 70% completion of the five year goal to decrease disaster administrative costs by five percentage points. Meeting this performance goal is important to FEMA's mission because it demonstrates progress towards increasing the efficiency of disaster operations, as FEMA continues to prioritize effectively delivering its mission.
- FEMA completed a Memorandum of Agreement with the U.S. Small Business Administration (SBA) for out-of-sequence declarations, which facilitates SBA making a declaration under its own authority and providing loans to disaster survivors in instances when a state may be appealing its initial denial for a presidential declaration, allowing FEMA to directly address any potential duplication of benefits.

- FEMA implemented Phase 1 of the Continued Temporary Housing Assistance (CTHA) improvement recommendations, which consisted of developing a communication product, a procedural change, and a system modification to prevent unnecessary CTHA requests and redirect outreach for survivors who are most in need. Through this process FEMA is able to triage more efficiently CTHA requests and minimize unnecessary casework or handle-times for FEMA agents.
- FEMA produced an Individual Assistance Shared Costs Programs video to inform external emergency managers and Reservists of the programs FEMA shares costs with under the Individual Assistance, and Individuals and Households Program.

The Individuals and Households Program Unified Guidance was published to provide FEMA employees, emergency management partners, political leadership, and the public with a single, comprehensive reference containing policy statements and eligibility criteria for all forms of Individuals and Households Program assistance. This guidance replaces existing stand-alone policies and provides State, Territory, and Indian Tribal Government officials a concise reference tool to assist with the needs of disaster survivors in their jurisdiction.

Introduction of FY18-19 APGs

DHS is implementing the following APGs for FY18-19 to reflect current priorities.

Agency Priority Goal 1: Enhance Southern Border Security

Impact and Goal Statement: Improve security along the southwest border of the U.S. between ports of entry. By September 30, 2019, DHS will implement the Operational Control (OPCON) framework to 100% of southwest border sectors between ports of entry as the means to enhance security.

Key Measure:

Percent of southwest border sectors that have implemented the Operational Control framework	FY18 Target	FY19 Target
	N/A	100%

Challenge: United States Border Patrol (USBP) works in a dynamic environment with multiple and varied threats that are constantly changing and evolving. Some of these threats and challenges include illegal border crossings by individuals with potential ties to terrorism, as well as smugglers, criminals, and other unlawful individuals motivated by employment opportunities and family reunification. Other threats include illegal goods that criminal organizations attempt to move across the border, such as instruments of terrorism, narcotics, and other contraband.

The Southern Border environment consists of 1,993 miles of varied terrain including deserts, rugged mountainous areas, forests and coastal areas. The border varies not only in geography but also in the presence of transportation routes and population centers. Partnerships with local, state, federal, tribal, and international law enforcement partners across the Southwest Border also vary by location, and much of the land along the southwest border is owned by local ranchers and other private citizens. USBP needs to coordinate with these community stakeholders to facilitate southern border security.

Given the variance in threats, partnerships, community relationships, and geographic features and conditions, implementation of a strategy for improving security will require analysis and measurement of commonalities along the border, and at the same time provide allowances for the unique operating environments for each of the nine Border

Patrol sectors and for each station within the sectors.

Opportunity: USBP has the opportunity to improve southern border security and protect the Nation by articulating a framework to advance operational control of the border. This framework relies on the interconnectedness of the three pillars of OPCON: Situational Awareness, Impedance and Denial, and Law Enforcement Resolution.

OPCON is our results-based framework, which is defined as: USBP's ability to impede or deny illegal border crossings, maintain situational awareness, and apply the appropriate, time-bound, law-enforcement response between the ports of entry as its contribution to DHS's overall border-security mission.

Implementation of the OPCON framework will align our strategies, tools, and tactics across the southern border. It will also incorporate the use of intelligence and decision support tools to advance border security. Additionally, CBP will develop methods to measure and communicate the results of implementation to advance understanding of the current security on the southern border.

Once matured and deployed along with southern border, future efforts plan to expand the OPCON framework to the Northern Border and Coastal sectors, so that OPCON is the established end state for all land borders between ports of entry.

Agency Priority Goal 2: Strengthen Federal Cyber Security

Impact and Goal Statement: Strengthen the defense of the federal network through the increased dissemination of cyber threat and vulnerability information in near real time to federal agencies. By September 30, 2019, federal agencies will mitigate 90% of significant (critical and high) vulnerabilities identified through DHS scanning of their networks within the designated timeline.

Key Measure:

Percent of significant (critical and high) vulnerabilities identified by DHS cyber hygiene scanning of federal networks that are mitigated within the designated timeline	FY18 Target	FY19 Target
	80%	90%

Challenge: The cybersecurity threat to federal networks continues to grow and evolve at an alarming rate. Adversaries in cyberspace conduct attacks against federal networks in near real time and collect sensitive data and information in a matter of minutes. Data breaches at the Office of Personnel Management (OPM) and the Internal Revenue Service (IRS) has exposed the data and information of millions of Americans to criminal organizations and hostile nation states. Protecting the personally identifiable information of the American people and other sensitive information pertaining to national security is critical to the Federal government maintaining the trust and confidence of the American public.

DHS alone cannot secure the computer networks of federal agencies. The challenge moving forward will be to enable agency use of DHS provided tools and information to take action with the same speed and agility as our adversaries. Federal agencies must work in close collaboration with DHS to ensure that DHS cybersecurity programs and tools are meeting their needs and evolving alongside the threat. Leadership engagement and prioritization of cybersecurity across the Federal Government will be critical to agencies using vulnerability and threat information DHS shares with them to take timely and risk based actions regarding their network security.

While many agencies utilize DHS provided cyber security programs, participation is voluntary. The DHS cyber security programs that are measured in this agency priority goal are deployed across the vast majority of federal agencies, but some agencies either cannot or will not participate due to lack of resources or expertise to deploy, and operate the tools. All 23 non-defense CFO Act agencies utilize DHS provided cyber security programs along with many smaller to mid-sized agencies that often utilize a shared service option. For the purposes of this agency priority goal, only those agencies that participate in DHS cyber security programs are being counted in the performance measures.

Opportunity: The array of cybersecurity programs that DHS offers to agencies will enable DHS and agencies to have increased situational awareness of the cybersecurity posture of their networks. Through continuous scanning, intrusion prevention, and vulnerability assessments DHS will provide agencies with the necessary tools and information to take timely and appropriate risk based actions to defend their networks. This will allow agencies to move with comparable speed and agility as our adversaries and increase the time and cost to conduct successful attacks. To ensure the successful implementation and use of these capabilities, DHS will continue to engage with senior agency leadership and appropriate information technology and security experts to apply these programs into agency cybersecurity practices.

The deployment of Continuous Diagnostics and Mitigation (CDM) capabilities onto agency networks is a critical step towards increased situational awareness of what assets, people and events are operating on a network. CDM is designed to provide capabilities incrementally to provide agencies with increased information on the security posture of their networks to aid in risk based decision making. Initially an agency must know what hardware and software is on its network before it can take steps to defend it. The capability to monitor user access and events on a network will be implemented in the near future.

DHS has focused significant leadership attention and investment towards the deployment of cybersecurity programs to defend the federal network. The transition of technology and tools to participating agencies will continue to be a leadership priority to ensure a smooth transition from acquisition into network security operations. The implementation of these programs is now at a maturity level within Federal agencies to permit the measurement of outcomes related to agency use of the information DHS provides to take actions to secure their networks. This will enable DHS to better manage its cybersecurity programs to increase value and performance delivered to its federal customers.

Strategic Review Results

DHS conducted this fourth annual review of progress in implementing our strategic plan goals last winter and spring to coincide with the schedule directed by the Office of Management and Budget. The review used the FY 2014-2018 DHS Strategic Plan goal structure that existed at that time to assess progress. DHS determined the goal progress ratings listed below in the Headquarters Review and discussions with senior leadership. Noteworthy progress demonstrates a goal that exceeded expectations, implemented innovative strategies, and impacted stakeholders in a positive manner. Focus area goals are ones that due to a variety of factors, including external pressures not completely controlled by the Department, continued focus is needed to enhance progress in the future The goal progress findings for the FY 2017 strategic review were:

Noteworthy Progress

- Goal 2.2: Safeguard and Expedite Lawful Trade and Travel

Focus Areas

- Goal 2.1: Secure U.S. Air, Land, and Sea Borders and Approaches
- Goal 3.2: Prevent Unlawful Immigration
- 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 5.2: Mitigate Hazards and Vulnerabilities

Goal 2.1: Secure U.S. Air, Land, and Sea Borders and Approaches

This goal was focused on the Department's ability to detect and prevent the illegal entry of goods and people into the United States that pose a threat to national, economic, and public safety. Together with other federal, state, local, and tribal law enforcement officers, the Department helps maintain a secure nation. Securing the borders and approaches is an ongoing and complex task influenced by many situational and policy factors outside of the direct influence of DHS. While the Department has made progress in its ability to identify and apprehend individuals trying to illegally enter the United States or smuggle contraband across our borders, the nature of the ever-evolving threats continue to present new and complex challenges to the Department's ability to protect U.S. borders and approaches.

Achievements

DHS continues to impact U.S. border security through targeting, screening, and apprehensions with situational awareness improvements along the Southwest Border. CBP maintained interdiction rates along the land border while the U.S. Coast Guard and its partners continued to remove large quantities of cocaine in the maritime environment. CBP's Air and Marine Operations Center has sustained results in cross border conventional aircraft incursions. The U.S. Border Patrol initiated the Northern Border Coordination Center to act in a collaborative capacity with sectors and stakeholders to address information sharing on current and emerging threats. DHS conducted outreach and expanded its international footprint in Mexico and Central America by providing resources and personnel to train, advise, and assist partners to improve U.S. security.

Challenges

DHS faces evolving threats along the border and must continue to refine and execute strategies for border security, targeting illegal immigration and the flow of illegal goods. Progress on securing and managing our borders in the future will be driven by recent

Executive Orders that require extensive investment in manpower, technology, and infrastructure for implementation. The lack of strong governance in Mexico, Central America, and Cuba also contributes to the flows of migrants and narcotics across both the land and maritime borders. The changing demographics of illegal immigration requires significant resources to facilitate and appropriately care for Unaccompanied Alien Children (UAC) and family units. There is the need to facilitate better coordination within DHS to achieve unified efforts to enforce immigration laws. Sufficient manpower is also a concern as the Border Patrol is currently under its mandated agent personnel minimum (not accounting for 5,000 new agents required by Executive Order 13767).

DHS must continue to mitigate narcotics smuggling by interdicting smugglers at sea, where narcotics are packaged in larger and more concentrated loads and are easier to locate. Additionally, efforts must continue to leverage intelligence with interagency partners to better target drug movements prior to, and at, the U.S. border.

Corrective Action

During FY 2017, as a result of policy changes, illegal migrant activity along the Southern and maritime border significantly decreased; however, drug flows remained persistently high. DHS will continue to focus on staffing, infrastructure, and technology related to the implementation of the Immigration and Border Security Executive Orders. This includes enhanced recruitment efforts to meet Border Patrol hiring needs with assistance from the human resources community, adding new capabilities and infrastructure along the land and maritime border, and continuing to identify and mitigate research and development gaps (such as small dark aircraft and maritime surveillance). USCG has continued to implement its Western Hemisphere Strategy to improve border security efforts and mitigate risks. DHS efforts to increase interagency coordination will continue through the Joint Task Forces as well as a focus on building the capabilities of partner nations, especially in Central America. Efforts to publicly communicate our immigration policies will be maintained and enhanced to provide visible deterrence to those wanting to enter the United States illegally.

Goal 3.2: Prevent Unlawful Immigration

DHS is committed to providing effective immigration enforcement that focuses on the Department's resources on identifying, locating, and arresting foreign nationals who pose the largest threat to the United States. With policy shifts related to recent EOs to remove illegal immigrants, with a focus on those already residing in the interior of the country, the top priorities include threats to national security, convicted criminals, threats to public safety, and recent border crossers. DHS also focuses on reducing the drivers of unlawful immigration, creating a culture of employer compliance that deters employers from exploiting undocumented workers, strengthening partnerships with outreach efforts toward state and local law enforcement, prosecuting and removing criminals, identifying and preventing large-scale immigration fraud, enhancing efficiency in the removal process, and improving the detention system.

Achievements

DHS continued its focus on improved interaction with state and local law enforcement, targeting aliens who pose a danger to national security or a risk to public safety, recent illegal entrants, and aliens who are fugitives or obstruct immigration controls. ICE implemented innovative tactics through the establishment of Mobile Criminal Alien Teams to locate and arrest convicted criminals. While ICE continues to prioritize enforcement and work with state and local law enforcement, immigration trends continue to strain capacity demonstrated by an increase in migration from Central America and a surge in asylum and credible fear cases. The number of those individuals in ICE custody who claim credible fear has doubled. Prior year increases in the number of undocumented Cuban maritime migrants attempting illegal entry to the U.S. was thwarted with the change in the Cuban parole policy, reducing rate of Cubans trying to enter the country, enabling USCG patrol assets to improve response and have greater interdiction success in the Florida Straits.

Challenges

Despite accomplishments in removals, significant external forces continue to exert pressure on the interior enforcement mission including increased asylum and credible fear cases, insufficient numbers of asylum officers, insufficient numbers of Immigration Judges to process final removal orders, recalcitrant countries refusing to repatriate their citizens, and the necessity for a whole of government coordinated approach. Even with positive steps in collaboration, state and local laws and policies limiting cooperation pose a risk to DHS's ability to promptly identify and arrest criminal illegal immigrants. Additionally, substantial coordination is required with the Department of Justice and the State Department to address prosecution and removal of criminal illegal immigrants to their countries of origin. Furthermore, the number of credible fear claims is straining DHS detention capacity by increasing the average daily population to an all-time high.

Corrective Action

DHS is committed to effective immigration enforcement and will reduce risks by increasing resources and expanding enforcement operations, programs, and capabilities facilitating the identification, location, and arrest of all removable aliens, in accordance with EO 13768. DHS is pursuing a number of strategies to help mitigate current risks and address existing challenges, including: 1) using EO staffing authority to hire additional Law Enforcement Officers (LEOs) and non-LEOs; 2) expanding engagement opportunities with state and local jurisdictions to improve interior enforcement efforts; 3) expanding the 287(g) program to qualified law enforcement agencies; 4) continuing coordination and increase joint efforts with the Department of State (DOS) and foreign governments to reduce the number of recalcitrant countries and to ensure timely return of foreign nationals with final orders of removal; and 5) increasing collaboration with the Department of Justice to increase the number of immigration judges to reduce the backlog of pending immigration cases.

Goal 4.1: Strengthen the Security and Resilience of Critical Infrastructure against Cyber Attacks and other Hazards

DHS collaborates with federal, state, local, tribal, territorial, international, and private-sector entities to maintain near real-time situational awareness of both physical and cyber events, share information about risks that may disrupt critical infrastructure, and build capabilities to reduce those risks. DHS accomplishes this by identifying and understanding interdependencies, collaborating with stakeholders to identify and develop effective cybersecurity policies and best practices, and reducing vulnerabilities and promoting resilient critical infrastructure design. DHS has effectively incorporated cybersecurity into critical infrastructure strategic planning through initiatives such as Presidential Policy Directive-8, the National Preparedness Goal, the U.S. Coast Guard Cyber Strategy, and the Sector Specific Plans, which all reflect the impact of the cyber threat to critical infrastructure.

Achievements

DHS made progress in 2016 by continuing to coordinate with critical infrastructure owners and operators, and public and private sector partners, to share cyber threat information, manage risk, increase awareness of threats, and develop plans. DHS commenced sharing of cyber threat indicators with a total of 74 non-federal entities to share information and enhance their capability to defend against known cyber threats. DHS also worked with critical infrastructure sectors to implement the National Institute of Standards and Technology (NIST) Cybersecurity Framework that will strengthen the resiliency and security of critical infrastructure by enabling owners and operators to follow a set of industry standards and best practices to help manage their cybersecurity risks. To engage local communities, DHS initiated the "Connect, Plan, Train, and Report" campaign to help better prepare business and their employees to proactively think about the role they play in the safety and security of their business and communities. Lastly, in partnership with other federal agencies, DHS developed a joint strategy with Canada and a U.S. action plan to address North American electrical grid security and resiliency.

Challenges

The cyber threat to the Nation's critical infrastructure continues to grow and evolve as the increased connectivity of components of critical infrastructure and interdependencies, with their cascading impacts, expands both the attack surface and vulnerabilities for adversaries to exploit. Understanding of the complexities of both the increasing connectivity to the internet and the dependency of domestic infrastructure on foreign supply chains are still evolving. This increased exposure and interdependencies, coupled with the continued challenges in hiring and retaining an adequate cybersecurity workforce within DHS, present significant challenges. While DHS has made progress in sharing information and managing risk, challenges remain in measuring the outcomes of cybersecurity programs and limitations of current toolsets used to engage with domestic critical infrastructure owners and operators to manage risk and foreign dependencies. This is largely attributed to the fact that DHS conducts this capacity building within a voluntary risk management system, in collaboration with non-federal owners and operators. While it remains difficult to measure progress in the private sector, states report to DHS that cybersecurity is their lowest-rated core capability for the fifth year in a row. This rating is in spite of greater investment in longer-term, internal cybersecurity by state governments.

Corrective Action Plan

During FY 2018, DHS will develop a strategy for measuring long-term outcomes for voluntary cybersecurity and critical infrastructure security and resilience (CISR) risk management programs. The measurement strategy for the voluntary cybersecurity and CISR programs will be coordinated and finalized by the end of FY 2018. DHS will mature programs that analyze domestic infrastructure foreign dependencies and foreign investment in the United States. To address domestic infrastructure foreign dependencies, DHS will transition from an expert opinion-based prioritized list to a requirements based analytic and production approach that better clarifies critical foreign dependencies. In FY 2018, DHS will prioritize analytic efforts that will dictate what internationally-focused analysis is conducted. Lastly DHS will continue to enhance workforce planning and analysis activities to understand current and future talent needs and drive strategies to enhance recruitment, retention, and training. DHS will produce annual summary reports and provide statutorily-required data to Congress in compliance with the *Cybersecurity Workforce Assessment Act*, *Border Patrol Pay Agent Pay Reform Act of 2014*, and the *Federal Cybersecurity*

Workforce Assessment Act of 2015. In FY 2018, DHS will continue work towards developing a new cybersecurity excepted service personnel system to address some of the inflexibilities in hiring and retaining key cybersecurity personnel.

Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise

The Federal Government provides essential services and information that many Americans rely on and cybersecurity is one of the biggest threats to this capability. Not only must the government protect its own networks, it must serve as a role model to others in implementing security services. DHS plays a leading role in securing the federal civilian information technology (IT) network by coordinating government-wide cybersecurity technology purchases, equipping civilian government networks with innovative cybersecurity tools and protections, and ensuring that government-wide policies and standards are consistently and effectively implemented.

Achievements

In 2016, DHS completed the contract award for the delivery of a portion of the Continuous Diagnostics and Mitigation (CDM) tools to enable federal agencies to better understand the assets and personnel that operate on their networks. The implementation of the CDM tools have resulted in agencies discovering previously unknown assets on their networks that will allow for greater awareness of vulnerabilities and more effective mitigation. To protect the government's most sensitive systems and data, DHS began assessments of agency-identified High Value Assets (HVAs) to identify vulnerabilities and weaknesses for agency remediation. The identification and prioritization of HVAs allowed DHS to focus limited resources on the most impactful assessments. Also DHS implemented an Automated Indicator Sharing (AIS) solution to allow for the distribution of cyber threat information in near real time with federal agencies. The number of cyber threat indicators shared with federal agencies increased from 1,250 in March of 2016 to 118,251 by the end of the fiscal year.

Challenges

While DHS made progress in delivering tools, assessing network security, and sharing information, however, significant challenges remain. In particular, senior agency leadership engagement on cybersecurity remains the critical ingredient to the successful implementation of DHS cybersecurity tools across the Federal Government. The cybersecurity workforce both within DHS and across the Federal Government also remains a concern. To implement and operate DHS provided cybersecurity tools requires an agency cyber workforce with adequate staffing levels and specific skill sets. The lack of cybersecurity professionals in the federal workforce remains an issue in implementing and operating DHS provided solutions. Within DHS, staffing shortages limit the Department's ability to meet goals for conducting assessments of HVAs, deploying additional countermeasures through the EINSTEIN system to block malicious traffic, and implementing CDM tools. In spite of efforts to secure the federal network, cybersecurity remains a challenge as evidenced by over 90% of major federal agencies citing cybersecurity as a major management challenge.

Corrective Action Plan

DHS plans to complete the implementation of CDM Phase 1 and Phase 2 capabilities for the majority of federal agencies in 2018. Agencies that do not fully implement CDM during the remaining period of performance for their current contract will be responsible for completing the deployment. The delivery of CDM Phase 3 tools was delayed due to re-allocation of resources to Phase 1, however initial delivery of Phase 3 tools is expected in early 2018. The initial release of the CDM Dashboard took place in October 2017 that will allow for visibility and monitoring of vulnerabilities by DHS. To provide intrusion prevention capabilities, DHS plans on expanding agency deployment of the EINSTEIN system across remaining agency components. The expansion of the EINSTEIN system will be focused on the remaining small and micro agencies that currently do not have coverage. Progress is expected to be incremental as small and micro agencies often do not have the dedicated IT staff and resources to support EINSTEIN deployment to their respective networks. Further expansion of the AIS program is also planned in 2018 to increase the number of shared threat indicators in near real time, as well as to increase the number of agencies sharing threat indicators with DHS and other agencies. DHS will continue to expand assessments of HVAs in FY 2018, and track the mitigation of DHS identified vulnerabilities based on priority determination by the Office of Management and Budget, the National Security Council, and the White House. Finally, DHS will assist Federal Chief Information Officers and Chief Information Security Officers through the provision of governance guidance to support their agencies' adoption of the DHS provided cybersecurity programs of CDM, EINSTEIN, AIS, and HVA assessments.

Goal 5.2: Mitigate Hazards and Vulnerabilities

DHS is uniquely positioned not only to support communities during a disaster, but also to enable partners to take steps that decrease risk and mitigate future hazards before a disaster strikes. While risk cannot be completely eliminated, DHS can influence and support positive outcomes in reducing risks by: mitigating hazards and vulnerabilities through promoting public and private sector awareness and understanding of community-specific risks; reducing vulnerability through effective mitigation and disaster risk reduction measures; and preventing maritime incidents by establishing and ensuring compliance with standards and regulations.

Achievements

The Department continues to make strides in decreasing risk and mitigating hazards through the efforts of FEMA and USCG. In the maritime environment, vessel compliance and waterways management continue to be the primary means of preventing hazards and vulnerabilities. DHS completed nearly ten thousand foreign vessel exams, more than 40,000 domestic vessel inspections, and more than 10,000 facility inspections, assessing safety, security, and environmental regulatory compliance. Overall performance improved despite continued industry growth of two to three percent. FEMA efforts led to increases in: the percent of communities in high earthquake, flood, and wind-prone areas that adopted disaster-resistant building codes; the percent of the population where Risk MAP has been deployed, enabling communities to take mitigation action to reduce risk; and the percent of U.S. population (excluding territories) covered by planned mitigation strategies.

Challenges

While performance in this area is meeting expectations, the debt owed by the National Flood Insurance Plan (NFIP) is one barrier to the financial stability of the program and there is no current ability to repay. FEMA paid the U.S. Treasury almost $4B in interest since the program's inception and expects to pay nearly $500M annually in the next few years. This interest diverts funds that could grow the future event Reserve Fund. Additional barriers include policyholders not paying full risk rates including rates to cover catastrophic events. The Administration proposed reforms to address these barriers. In addition, DHS faces a challenge of increasing populations becoming vulnerable to natural and manmade disasters as critical infrastructure becomes more outdated. For instance, levees and dams are aging, and 40 percent are assessed as high risk, leaving unmitigated risk that can result in loss of life, property, and economic loss.

Additional challenges exist in the maritime industry which has been growing and becoming more complex in nature, resulting in risk to the US Coast Guard's ability to ensure the safety, security, and environmental protection of the nation's critical waterways. Not only has the amount of commercial vessel traffic increased by two to three percent annually over the last two decades, but the technical systems that maritime industry uses have become more complex. Coupled with the increasing international demand for a smaller environmental footprint, current and future workload demands may result in additional risk to mariner and passenger lives, property damage, and damage to the natural environment.

Corrective Action Plans

To address the financial Stability of the NFIP, DHS plans to support long term reauthorization of NFIP by accelerating premium increases for policyholders paying less than full risk rates, promoting transparency around the NFIP’s revenue, expenses, risk exposure, and available risk management tools as NFIP reauthorization-related discussions progress with DHS, the Administration, and Congress. Additionally, DHS purchased reinsurance for 2017 such that reinsurers will cover 26% of losses between $4B and $8B arising from a single flooding event. FEMA made an additional reinsurance purchase for 2018. FEMA is leveraging existing investments in analytic capacity and engagements with the reinsurance industry to better understand the NFIP’s risk profile and appropriate risk management strategies.

Management Initiatives

This section highlights relevant Management Initiatives related to regulatory reform, the Human Capital Operating Plan, and Reform Agenda initiatives.

Regulatory Reform

In early 2017, the President issued two Executive Orders directed at government-wide regulatory reform. *Executive Order (EO) 13771, Reducing Regulation and Controlling Regulatory Costs*, requires agencies to (1) eliminate two existing regulations for every new significant regulation that the agency wishes to issue, and (2) offset costs of new significant regulations with deregulatory cost savings. *Executive Order 13777, Enforcing the Regulatory Reform Agenda*, includes a number of requirements to institutionalize and enforce regulatory reform initiatives.

Section 4 of *EO 13777* specifies that agencies should measure their progress in performing regulatory reform tasks. Specifically, the executive order states that agencies should incorporate performance indicators into their annual performance plans; those performance indicators should measure progress toward the goals of: 1) improving implementation of regulatory reform initiatives and policies, and 2) identifying regulations for repeal, replacement, or modification. Pursuant to the above requirements, DHS has moved forward to implement this guidance.

Performance Review

On April 28, 2017, the Office of Management and Budget issued *Memorandum M-17-23*: *Guidance on Regulatory Reform Accountability under Executive Order 13777: Enforcing the Regulatory Reform Agenda.* In that Memorandum, OMB stated that, beginning with the FY 2019 Annual Performance Plan, agencies must include, at a minimum, the following five performance indicators.

1. Evaluations

Number of evaluations to identify potential EO 13771 deregulatory actions that included opportunity for public input and/or peer review	FY18 Target	FY19 Target
	3	4

Description and Data Collection Methodology: This indicator represents the number of evaluations DHS will issue in the given FY *and* for which DHS will seek public input or peer review. The evaluations are used to identify potential *EO 13771* deregulatory actions. These evaluations include proposed rules and regulatory impact analyses that publish during the FY, and exclude interim final rules, final rules, and collection of information. DHS has a centralized regulatory clearance process managed by the Office of the General Counsel (OGC). Evaluations will be tracked through the internal DHS regulatory tracking systems as well as based on publication in the Federal Register.

2. Deregulatory Actions Recommended

Number of EO 13771 deregulatory actions recommended by the Regulatory Reform Task Force to the agency head, consistent with applicable law	FY18 Target	FY19 Target
	13	14

Description and Data Collection Methodology: This indicator represents the number of *EO 13771* deregulatory actions that the Regulatory Reform Task Force recommends to the Secretary in a given fiscal year, consistent with applicable law. These *EO 13771* deregulatory actions include proposed rules, interim final rules, final rules, collections of information, and guidance documents. Through the Regulatory Reform Task Force (and data calls to the Components, if necessary), OGC will track recommendations made to the Secretary.

3. Deregulatory Actions Recommended & Issued

Number of EO 13771 deregulatory actions issued that address recommendations by the Regulatory Reform Task Force	FY18 Target	FY19 Target
	6	7

Description and Data Collection Methodology: This indicator represents the number of EO 13771 deregulatory actions that DHS issues in a given fiscal year based on recommendations that the Regulatory Reform Task Force made to the Secretary. These *EO 13771* deregulatory actions include proposed rules, interim final rules, final rules, collections of information, and guidance documents that publish in the given fiscal year. DHS has a centralized regulatory clearance process managed by OGC. All regulatory and deregulatory actions are tracked through internal DHS regulatory tracking systems as well as based on publication in the Federal Register.

4. Regulatory Actions Issued & Deregulatory Actions Issued

Number of EO 13771 regulatory actions and, separately, EO 13771 deregulatory actions issued	FY18 Target	FY19 Target
	10 / 6	12 / 7

Description and Data Collection Methodology: This indicator contains two parts.

- First, this indicator represents the number of final *EO 13771* regulatory actions that DHS publishes in the given fiscal year. These *EO 13771* regulatory actions include interim final rules and final rules, and exclude proposed rules.
- Second, this indicator represents the number of final deregulatory actions that DHS publishes in the given fiscal year. These *EO 13771* deregulatory actions include all the actions based on the recommendations of the Regulatory Reform Task Force in addition to any other actions issued by DHS during the given fiscal year. These *EO 13771* deregulatory actions include interim final rules, final rules, collections of information, and guidance documents that publish in the given fiscal year, and exclude proposed rules.

DHS has a centralized regulatory clearance process managed by OGC. All regulatory and deregulatory actions are tracked through internal DHS regulatory tracking systems as well as based on publication in the Federal Register.

5. Total Incremental Cost

Total incremental cost of all EO 13771 regulatory actions and EO 13771 deregulatory actions (including costs or cost savings carried over from previous fiscal years)	FY18 Target	FY19 Target
	$0	TBD

Description and Data Collection Methodology: This indicator represents the total incremental cost of all *EO 13771* regulatory actions and *EO 13771* deregulatory actions at the end of the fiscal year.

Current Status

DHS is committed to regulatory reform. Regulatory components throughout DHS continue to review their regulatory and related stock, analyze the impacts and costs of that stock, identify possible deregulatory actions, and draft deregulatory actions. DHS hopes to make good progress this year in identifying and issuing deregulatory actions.

In addition, DHS continues to work on a number of regulatory actions in support of additional executive order-driven initiatives. For example, the President has issued various Executive Orders related to immigration matters, including the following ones:

- EO 13767: Border Security and Immigration Enforcement Improvements;
- EO 13768: Enhancing Public Safety in the Interior of the United States;
- EO 13780: Protecting the Nation from Foreign Terrorist Entry into the United States; and
- EO 13788: Buy American and Hire American.

The regulatory actions that flow from these immigration Executive Orders are also high-priority items that require the attention and work of DHS regulatory components, especially the immigration components: USCIS; CBP; and ICE.

Finally, DHS also continues to work on regulatory action required by statutes, such as those required by the *Implementing Recommendations of the 9/11 Commission Act of 2007* and the *Sandy Recovery Improvement Act of 2013*.

Next Steps

The DHS Regulatory Reform Task Force continues its work in identifying regulations for repeal, replacement, or modification; and in implementing regulatory reform initiatives and policies consistent with the regulatory reform executive orders. As well, as discussed above, DHS regulatory components continue their work in developing and issuing regulatory and deregulatory actions.

Human Capital Operating Plan (HCOP)

The Office of the Chief Human Capital Officer (OCHCO) continued to meet the challenges of the current dynamic security and budget environments, by developing and implementing strategies to close mission-critical skills gaps cost-effectively to achieve current and future mission needs. Over the last year, DHS has taken significant steps to identify and address critical skills gaps through a results-oriented, Human Capital Operational Plan (HCOP) that identifies the Department's goals, objectives, and performance measures linked to DHS strategy. The HCOP emphasizes management integration, accountability tracking, and the use of human capital data analysis to meet DHS mission needs.

FY 2017 was the third year DHS developed and implemented an annual operational plan jointly developed by OCHCO and the Human Capital Leadership Council (consisting of Human Resources Directors in each operational Component and OCHCO executives) to support continuous performance improvement. The Department also conducted another full-year of HRstat reviews – quarterly, data-driven assessments of program performance in support of each of the four HCOP goals.

These planning and implementation efforts by the DHS human capital community along with the integration and support provided by line of business partners were key to GAO awarding DHS "Fully Addressed" ratings in four human capital outcomes in its February 2017 High Risk Report.

During the mission critical occupation (MCO) exercise in March 2016, DHS designated 75.9 percent of its combined civilian/military workforce as MCOs, and 70.1 percent as priority MCOs (PMCO) – employees who perform the Department's most critical operational missions. During the revalidation, DHS identified, for the first time, its more than 230,000 personnel as either directly performing or supporting a DHS Strategic Plan mission area. During FY 2017, for each PMCO, Components built workforce plans that documented required actions to close these skills gaps, helping the Department add more than 2,700 employees (2.3 percent) in PMCOs.

DHS is building upon its efforts to integrate human capital planning with operational planning through continued deployment of position management, manpower and organization, and data analytics initiatives, which identify current and future personnel required to perform the Department's critical and evolving responsibilities. The net result of improving position management and documentation will be to provide time-phased, location-based documentation of current and future requirements for Border Patrol Agents, Deportation Officers and Investigators, Secret Service Special Agents, and other mission critical and mission support occupations throughout the Department to inform both the financial planning and hiring processes.

DHS has strengthened its human capital information technology (IT) program by establishing a continuous portfolio analysis process as well as strategic improvement opportunity initiatives that fill gaps in the portfolio. The Human Capital Segment Architecture Blueprint update uses a three-year cycle to review and analyze the DHS human capital IT portfolio to identify capability gaps in IT solutions and addresses those gaps by setting technical and business requirements for acquisition of effective solutions. The initiatives include connecting IT systems DHS currently uses to make the systems more effective and make our workforce more efficient, as well as acquiring new automation capabilities. As a result of OCHCO's work to support the Human Capital Segment Architecture, Department-wide requirements will be more clearly defined and will provide the foundation for more efficient and effective human capital operations into the future.

Increasing Recruitment and Streamlined Personnel Hiring

Continuing to employ Department-wide and Component-specific recruitment strategies is a key element to sustain progress in skill gap closure. Components will establish updated Component Recruitment and Outreach Plans (CROPs), which include a focus on targeted recruitment for identified DHS PMCOs. Building on the mission-focused statement of requirements generated by these strategic initiatives, the Department will develop an enterprise approach for co-branding DHS and Components in all human capital outreach efforts including advertising, marketing, social media, and other human capital outreach efforts.

To supplement the CROP and provide real-time recruitment, marketing, and outreach data, OCHCO transitioned to a standardized method of collecting recruitment data. The Recruiting, Outreach, and Marketing Matrix allows DHS to track attendance, recruiting costs, target audience, and marketing focus, helping to maximize recruiting return on investment. OCHCO will develop requirements to automate and streamline this data collection method in FY 2018. In December 2016, OCHCO coordinated a Pathfinder Business Operations hiring event targeting interns and recent graduates, during which more than 100 candidates received tentative job offers. In addition, DHS hired 591 Pathways interns and recent graduates in FY 2017, an increase of 58 percent compared to FY 2016. In August 2017, the Department conducted a veteran-specific hiring event in support of the recent Executive Orders on border security and immigration enforcement. More than 2,500 veterans attended the two-day event, of which more than 250 received tentative job offers or advanced to the next step of the law enforcement hiring process. In support of the veterans hiring event, OCHCO used a new Office of Personnel Management (OPM) USAJOBS capability called "resume mining" that allowed hiring managers to search more than two million resumes. Throughout FY 2017, DHS had a strong recruiting presence at events sponsored by key law enforcement groups for women and minority law enforcement professional associations. These activities will be instrumental in helping the Department meet emerging needs for high priority missions, in particular the 5,000 Border Patrol Agents and 10,000 law enforcement officers directed by Executive Order.

DHS increased its cybersecurity workforce planning and analysis efforts to gain better insight into cybersecurity work to meet mission needs and meet statutory mandates (the Border Patrol Agency Pay Reform Act - P.L. 113-277, Cybersecurity Workforce Assessment Act - P.L. 113-246, and Federal Cybersecurity Workforce Assessment Act of

2015 - P.L. 114-113.) During FY 2017, DHS made great progress in identifying and coding cybersecurity positions and employees according to the National Initiative for Cybersecurity Education Workforce Framework, and refined processes for validating and communicating DHS-wide cybersecurity onboard and vacancy counts. DHS captured results of these efforts—including workforce gap analyses—in a comprehensive report for Congress, which we will update in future years. The Department identified approximately 10,000 federal civilian, U.S. Coast Guard military, and contractor positions with significant cybersecurity responsibilities, including approximately 6,700 federal civilian positions. As of the end of the third quarter of FY 2017, DHS has coded more than 90 percent of encumbered civilian positions to comply with direction from Congress and OPM. DHS also launched a series of news alerts to Components regarding the effective use of human capital flexibilities. The July 2016 Cyber and IT Hiring Fair led to the hiring of over 400 IT/cybersecurity professionals. Lastly, DHS continues to design a new cybersecurity personnel system using authority granted to the Secretary via P.L. No. 113-277. In FY 2017, OCHCO crafted several foundational design elements of the new personnel system and identified key policy decisions to focus on with the DHS Office of the General Counsel, Component cybersecurity and human capital staff, and OPM with whom Congress asked DHS to coordinate implementation.

Improving Personnel Training, Professional Development, and Education Opportunities

OCHCO has implemented multiple initiatives to enhance the effectiveness and return on investment in the training, professional growth, and development of its people. The DHS Leader Development Program conducted a study revealing that completion of Cornerstone (DHS-wide supervisory development requirements) is predictive of increased FEVS scores. OCHCO found that organizations whose supervisors completed more Cornerstone-required training had higher FEVS scores compared to organizations whose supervisors completed less Cornerstone-required training. Thirteen separate FEVS indices were higher when Cornerstone training completion hours were higher. The study is the first of its kind at DHS and adds original research to the federal human capital space, contributing to a business case for investing in leader development as an investment in workforce engagement, and as such, workforce performance. Study results were briefed to the Employee Engagement Executive Steering Committee as a best practice and dovetail with the Acting Secretary’s decision to introduce the DHS Leadership Year initiative.

OCHCO facilitated improved employee engagement through department-wide activities including: the launch of “DHS Leadership Year” by the Acting Secretary, designed to reinforce a culture of leadership excellence; a “listening tour’ by the Acting Secretary to hear how to most effectively support the workforce; sharing of best practices and new ideas through the Employee Engagement Steering Committee; and a continued structured, rigorous approach to Component-level employee engagement action planning. DHS’s efforts to improve employee engagement yielded a significant increase in the Federal Employee Viewpoint survey results for 2017. The Department’s response rate exceeded the government-wide rate by 3.5 percentage points and DHS’s Employee Engagement Index (EEI), composed of three sub-indices (Leaders Lead, Supervisors, and Intrinsic Work Experience) increased four percentage points, reflecting an overall upward trend in Federal Employee Viewpoint Survey (FEVS) scores across the Department. DHS’s increase in EEI was the largest of any cabinet-level agency. In addition, DHS will leverage existing Component programs to develop a Department-wide Resilience and Family Readiness Program to support families of front-line employees.

OCHCO implemented the Department's new Common Training Cost Structure, which provides a common cost structure to track mission and support training expenditures DHS-wide. OCHCO developed the first ever data visualization of classroom mission training across all components, allowing organizations DHS-wide to easily share training courses and curricula, reducing redundancies and increasing consistency in outcomes. Through the implementation of the DHS wide Mandatory Training (MT) application and review process, SLD&E successfully reviewed four MT courses ensuring criteria were met. This effort has significantly improved MT training quality and overall effectiveness, while decreasing duplicative efforts DHS-wide, saving the both employee time and financial resources. OCHCO also successfully conducted a DHS-wide internal review to evaluate the current use of learning technology and developed a DHS Learning Technology Strategy Report to support the Workforce Development Strategy.

Retain Exceptional Performers

The Joint Duty Program was launched during FY 2017 to provide the DHS workforce with opportunities to 1) enhance operations and mission execution; 2) support unity of effort; and 3) enhance leadership and professional development opportunities. The pilot began in May 2017, with the assignment of Joint Duty participants in the DHS Joint Task Force elements. Program success is leading to the continued phased expansion throughout DHS. DHS is creating career pathing with online resources, assessment tools, and skill-building opportunities for the 1800 job series occupations (Inspection, Investigation, Enforcement, and Compliance), 201 job series (Human Resources), and other occupational series within Management lines of business.

To strengthen the professionalism of the Department's HR cadre and to provide a developmental path for new HR hires, OCHCO launched the DHS HR Academy. The academy will provide a range of developmental experiences, from internships, to rotations, to classroom, and to on-line training opportunities, in foundational and specialized HR topics. OCHCO/SLDE hosted the annual DHS Education Fair, with more than 35 colleges/universities participating. More than 350 employees attended the fair and met with representatives from multiple colleges/universities to learn about their degree and certificate programs. The Education Fair also showcased the 11 OPM Alliance Schools who offer Federal Government employees, and their dependents, discounted tuition rates.

Reform Agenda

On March 13, 2017, President Trump signed Executive Order (EO), *Comprehensive Plan for Reorganizing the Executive Branch*, to improve the efficiency, effectiveness, and accountability of the executive branch. The order required all federal agencies to submit a reform plan to the Office of Management and Budget (OMB) by September 11, 2017. To address this EO, DHS immediately established the Organizational Effectiveness Working Group (OEWG), comprised of executives from all Components, HQ Directorates and Offices, and Management Lines-of-Business with the intent of developing an Agency Reform Plan.

The plan reflects the output of a 24-week analysis conducted by the OEWG, which was chartered by the DHS Deputy Secretary to develop reform proposals. Per OMB guidance, the OEWG assessed opportunities to strengthen and solidify the mission and role of DHS and improve its business processes.

The DHS proposals respond to OMB's requirement to identify areas to eliminate activities, restructure or merge, and improve organizational efficiency and effectiveness. Additionally, the DHS plan outlines the Department's efforts to improve workforce management practices as part of its long-term workforce shaping strategy.

The Department's approach was to reach out to the general public and to DHS employees and contractors to solicit ideas and concepts. The OEWG received more the 50,000 proposals and ideas from the general public. This information was used to distill ideas into select key issues at the single and cross-Component levels and also within the interagency. Evidence from such entities as the Government Accountability Office and the DHS Office of Inspector General was used to inform the issues. Courses of action are being developed with implementation to begin in 2018 and continue through completion.

Direction from the Office of Management and Budget during the November timeframe provided additional guidance for how the Department will consider near-term actions to affect the FY 2019 budget request for the Department.

The cumulative result of these efforts will be a Department that is better positioned to protect the Nation through the efficient and effective delivery of its mission programs.

Ongoing Activities

The Department undertook a number of initiatives to improve organizational effectiveness, accountability, and efficiency prior to the release of EO 13781, including the Department's Field Efficiencies Initiative, reorganization of National Protection and Programs Directorate (NPPD), and IT Infrastructure Strategy. In addition, the Department's response to the series of other Executive Orders issued in 2017 is reformative in and of itself. The Department will continue these initiatives, being careful to integrate and combine like efforts where appropriate.

Some specific examples of improvements in organizational effectiveness include:

- **Joint Base Cape Cod Utilization**: Working with the USCG and other federal partners, the Field Efficiencies Program Management Office (PMO) is increasing the utilization of owned space at Joint Base Cape Cod
- **Modular Firing Range (MFR) Strategy**: The Field Efficiencies PMO is currently developing a strategic sourcing vehicle to provide a low-cost solution for firearms qualifications using shared locations in densely populated DHS locations.
- **NPPD Reorganization**: NPPD developed a plan to enhance its operational mission by establishing the Cyber and Infrastructure Security Agency, which includes a realignment of current NPPD programs and offices.

Unity of Effort

The Department is continuing to make progress under the "Unity of Effort" initiative. This includes a commitment to a transparent and unified decision-making processes. Examples of this work includes:

- Continuing to utilize the senior leader forums which include the Senior Leaders Council (SLC) and the Deputy's Management Action Group (DMAG). These forums drive Departmental decisions in a transparent and collaborative fashion. Additionally, they enable DHS leaders to have frank, productive conversations regarding DHS areas of interest.
- The Deputy Secretary issued DHS's inaugural Strategic Planning Guidance (SPG) for Fiscal Year 2017, DHS's annual strategic planning agenda and

strategy documentation standards.

- The Department continues to develop and issue Resource Planning Guidance (RPG) and Operational Planning Guidance (OPG). The RPG outlines leadership priorities for Operational Components and DHS Headquarters offices. This document is critical to ensuing DHS leadership guidance is understood and utilized in the Department's resource allocation process. The OPG designates the Department's operational plans for the next fiscal year.
- Winter Studies, which are chartered by the RPG, are in-depth analytic efforts designed to prepare for the Department's Program and Budget Review (PBR). These efforts, which are led by a Component and Headquarters office, conduct analysis ahead of the Department's PBR to allow the DMAG to make decisions on critical homeland security areas based on analysis and data.
- Joint Task Forces (JTF) continue to maximize the use of their respective operational plans to coordinate and align activities to disrupt Transnational Criminal Organizations (TCOs). The JTF's mission requires them to leverage authorities across the JTF to maximize effectiveness.

Major Management and Performance Challenges and High-Risk Areas – Summary of Progress

DHS responds to reports on major management and performance challenges, and high-risk areas from the DHS Office of Inspector General (OIG) and the U.S. Government Accountability Office (GAO), respectively. Annually, OIG reports what is considered to be the most serious challenges facing the Department. Every two years, GAO identifies federal programs and operations that are high risk because of their greater vulnerabilities to fraud, waste, abuse, and mismanagement. GAO also includes areas needing broad-based transformations to address major economic, efficiency, or effectiveness challenges.

OIG's 2017 Major Management and Performance Challenges report focused on highlighting the underlying causes of the Department's persistent management and performance challenges, which hamper efforts to accomplish the homeland security mission efficiently and effectively. The Inspector General (IG) identified these challenges as two-fold. First, the Department leadership must commit itself to ensuring DHS operates more as a single entity rather than a collection of components. Second, the Department leadership must establish and enforce a strong internal control environment typical of a more mature organization. The IG then discussed related challenges in four broad areas:

- Challenges in Committing to Intra-component Cooperation
- Workforce Challenges
- The Challenge to Become a Learning Organization
- Challenges Transforming IT Systems

Additional details can be found in the OIG's report *Major Management and Performance Challenges Facing the Department of Homeland Security*, OIG-17-08, dated November 3, 2017, located at: https://www.oig.dhs.gov/sites/default/files/assets/2017-11/OIG-18-11-Nov17.pdf.

The Department's Management response letter to the IG's report recognized that the OIG's new approach this year in highlighting "underlying causes" of challenges provided a valuable input; however, by taking this high-level approach, the report understated a number of significant efforts during the last few years that are leading to greater unity of efforts amongst DHS Headquarters offices and operating Components. These efforts included the continued maturation of the DHS Joint Requirements process and DHS Joint Task Forces, as well as an ongoing 12-region "field efficiency" initiative that is taking a Department-wide view of all mission support activities to identify and implement colocation and consolidation opportunities to increase DHS Component operations' effectiveness and efficiency.

A full copy of the Department's response can be found in the DHS FY 2017 Agency Financial Report, located at: https://www.dhs.gov/sites/default/files/publications/dhs_agency_financial_report_fy2017_1.pdf, starting on page 205.

The most recent report, GAO *High Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others (GAO-17-317)*, can be found at: http://www.gao.gov/assets/690/682765.pdf was published on February 15, 2017. The two areas in which DHS is the lead federal agency, as well as seven government-wide areas with significant DHS equities, are listed below.

Scope	Issue Area	Year Issue First Added to GAO's High Risk List
DHS-specific	Strengthening DHS Management Functions	2003
	National Flood Insurance Program	2006
Government-wide	Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructures and Protecting the Privacy of Personally Identifiable Information	1997
	Strategic Human Capital Management	2001
	Managing Federal Real Property	2003
	Ensuring the Effective Protection of Technologies Critical to U.S. National Security Interests	2007
	Improving Federal Oversight of Food Safety	2007
	Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks	2013
	Improving the Management of IT Acquisitions and Operations	2015

DHS carries out multiple complex and highly diverse missions that range from aviation and border security, to emergency response, cybersecurity analysis, and chemical facility inspection. All are focused on securing our Nation from the many threats we face. The Department continually strives to improve the efficiency and effectiveness of all its programs and operations, however, the areas identified above merit a higher level of focus and attention. It is important to note that overcoming challenges in these areas requires long-term strategies for ensuring stable operations, sustained management attention, and resources; which the Department is providing.

The remainder of this section provides a brief summary of the Department's efforts in addressing each GAO high-risk area.

GAO High-Risk – Status Update

GAO High-Risk Area: Strengthening DHS Management Functions (DHS-specific)

Overview: In 2003, GAO designated "Implementing and Transforming DHS" as high risk, due to the significant challenges associated with transforming 22 agencies, into one cohesive department. This high risk area includes challenges related to strengthening and integrating four management areas: acquisition, information technology (IT), financial, and human capital management.

In response to this high-risk designation, DHS biannually publishes the *Integrated Strategy for High Risk Management* (Integrated Strategy) which GAO has stated "provides a path for DHS to be removed from GAO's high-risk list," if implemented and sustained (see https://www.dhs.gov/sites/default/files/publications/DHS%20Integrated%20Strategy%20for%20High-Risk%20Management%20-%20August%202016_1.pdf). In 2013, GAO acknowledged DHS's significant maturation and narrowed this high risk area from "Implementing and Transforming DHS" to "Strengthening DHS Management Functions." According to GAO, this refocusing is a reflection of "the considerable progress in transforming [DHS's] original component agencies into a single cabinet-level department."

Lead Office and Official: Office of the USM, Michelle Benecke, Executive Director for Management Integration

Progress: In September 2017, DHS published its thirteenth Integrated Strategy, which outlines DHS's progress and serves as the roadmap for removal from GAO's high-risk list. The strategy is composed of 11 initiatives with goals and metrics that correlate directly to GAO's 30 agreed-upon high risk outcomes. GAO's outcomes consist of desired end-states of maturation for several of DHS's management functions.

GAO has highlighted DHS's efforts on this high-risk issue area as a select example of an administration initiative leading to progress and listed the progress made as among the most highly-rated across the Federal Government (High Risk Series: Key Actions to Make Progress Addressing High-Risk Issues, GAO-16-480R, dated April 25, 2016). Making major strides during the past two years, the Department has:

- "Fully Addressed" or "Mostly Addressed" a total of 21 of the 30 (70 percent) GAO outcomes – 20 when GAO published its February 2017 High-Risk Series and an additional outcome reaching "Fully Addressed" status in June 2017. This is a significant improvement compared to 47 percent (14 of 30) in 2015 and 26 percent (8 of 31) in 2013.
- Fully met three of the five (60 percent) criteria for list removal (leadership commitment, a framework to monitor progress and corrective action plans), making DHS one of four agencies on the High Risk List to have met at least three of GAO's criteria; and partially met the two remaining criteria (capacity [i.e., resources] and demonstrated, sustained progress).
- Achieved a fifth consecutive unmodified (i.e., clean) audit opinion on all five financial statements in November 2017. This success is a confirmation of the Department's ongoing commitment to sound financial management practices, with its first unmodified audit opinion in December 2013. These successes led to GAO assessing the associated outcomes as "Fully Addressed."
- Received a downgrade to DHS's property, plant and equipment (PP&E) material weakness. A material weakness is a control gap that increases the risk of an error in financial data and keeps DHS from getting a clean audit opinion on internal control. In reducing the PP&E weakness, DHS demonstrates that its procedures and controls to properly and timely account for DHS-owned assets and record them into the financial system are effective and solid.
- Continued to conduct annual cycles of strategic human capital planning and implementation, demonstrating the sustainability of the GAO outcomes for human capital management.
- Made significant progress in reforming its acquisition process by implementing governance structures, updating policies and processes, standardizing and professionalizing the DHS acquisition leadership and workforce, and overseeing the Department's major acquisitions in an integrated manner.
- Developed the Cyber Maturity Model to identify gaps and prioritize funding requests, cited by the Office of Management and Budget (OMB) as a best practice and upon which Congress appropriated an additional $100 million for FY 2016-2017.

Since 2010, DHS has intensified its focus on strengthening its management foundation so that it could support higher-order initiatives. Examples include: strengthening the delegations of authority to clarify the roles between the Department and Components; elevating the role of the Program Accountability and Risk Management (PARM) function to improve the quality and oversight of acquisition programs; improving the quality and integrity of the Department's financial statements; and, using the lessons learned from the Integrated Investment Life Cycle Management pilots to implement the Unity of Effort initiative. This effort focuses on strengthening all elements of the investment process, including strategy development, planning, and joint requirements, which will ensure that the total budget is spent effectively and efficiently.

Planned Actions and Key Milestones: DHS will continue to implement the *Integrated Strategy* and other efforts that contribute to strong and efficient management functions. During FY 2018, DHS expects to accomplish the following:

- Continue addressing the outstanding GAO outcomes and sustain progress in meeting GAO's criteria for high-risk list removal.
- Obtain the fifth consecutive clean audit opinion on financial statements.
- Continue the DHS Human Capital Leadership Council practice of annually updating operational plans to support the implementation of the FY 2015-2019 Human Capital Strategic Plan.
- Continue strengthening acquisition oversight and management throughout the Department. There are five associated GAO outcomes for acquisition. DHS's goal is to be rated by GAO as having fully addressed or mostly addressed these five outcomes in the February 2019 *High-Risk Series: An Update.*
- Maintain the security of DHS's internal information technology (IT) systems and networks through continued cross-Component collaboration (for example, continued actions to improve Federal Information Security Modernization Act [FISMA] scores); and bring all 12 categories of scores into compliance.

GAO High-Risk Area: National Flood Insurance Program (DHS-specific)

Overview: The Federal Emergency Management Agency's (FEMA) National Flood Insurance Program (NFIP) is a key component of the Federal Government's efforts to limit the damage and financial impact of floods. However, it likely will not generate sufficient revenues to repay billions of dollars borrowed from the U.S. Department of the Treasury to cover claims starting with the 2005 hurricanes and catastrophic losses. The lack of sufficient revenues highlights structural weaknesses in how the program is funded. Also, GAO found weaknesses in NFIP management and operations, including financial reporting processes and internal controls, and oversight of contractors that place the program at risk. FEMA has begun to address these issues, including implementing legislation, improving contractor oversight, initiating product and policy rating redesign, obtaining reinsurance, and taking the first steps toward financial systems modernization with the NFIP Pivot Program, which replaces the NFIP's legacy mainframe solution.

In 1968, Congress created NFIP, which offers flood insurance to homeowners, renters, and business owners in participating communities. Participating communities agree to adopt and enforce ordinances that meet or exceed FEMA requirements to reduce the risk of flooding. Private sector write-your-own (WYO) insurance company partners sell NFIP policies under their own names, with claims and related expenses paid for by the Federal Government. FEMA also sells policies directly through a servicing agent.

Congress reauthorized NFIP for five more years in the *Biggert-Waters Flood Insurance Reform Act of 2012* (BW-12) which mandated certain premium rate increases to begin transitioning the program from subsidized rates to full actuarial rates reflective of risk to better ensure the fiscal soundness of the program. The *Homeowner Flood Insurance Affordability Act of 2014* (HFIAA) repealed certain parts of BW-12, including a provision phasing out grandfathered rates; set limits on premium rate increases for certain policyholders; and applied an annual surcharge to all policyholders.

Lead Office and Official: FEMA Federal Insurance and Mitigation Administration (FIMA), Roy E. Wright, Deputy Associate Administrator for Federal Insurance and Mitigation

Progress: FEMA (1) implemented premium rate increases; (2) applied new surcharges; (3) released new rates and mapping standards; and (4) is transforming the NFIP to improve the experience of NFIP policyholders.

- To advance the agency's initiative to replace the NFIP's legacy mainframe solution, the FEMA Insurance Systems Program Management Office (PMO) coordinated with FEMA's Office of the

Chief Procurement Officer and Office of the Chief Information Officer to develop the System Engineering Life Cycle and Acquisition artifacts necessary to garner approval for a DHS Acquisition Decision Memorandum (ADM) for the "Analyze/Select" Phase (ADE-2A/2B), completed in the first quarter of FY 2017. This ADM gave the PMO permission to proceed to the "Obtain" phase and begin obtaining the target solution, with Initial Operating Capability to be delivered in Q2 FY18, and Full Operating Capability to be delivered by FY20.

- FEMA published the NFIP Rate Guidance Issue in bulletins to WYO insurers in April and October 2017, allowing the mandated six months required for consultation and notice of changes impacting their IT systems and operational processing procedures.
- FEMA integrated the following requirements into its ongoing program and reporting processes:
    - Set 25 percent annual premium rate increases for businesses, mandated under BW-12, which took effect in April 2016.
    - Set the annual premium rate increases, as required by HFIAA, at an average rate between 5-15 percent per risk class, without exceeding the 18 percent cap on annual premium rate increases for any individual policy.
    - Applied a preferred risk premium rate for the first year to policies on properties that are newly mapped into a special flood hazard area, with increases of 18 percent per year until the rate reaches full risk rate.
- FEMA expedited flood insurance reform and implemented program changes through policy and by leveraging existing processes to release program updates every six months. Specifically, FEMA released mapping standards by publishing them on www.FEMA.gov in May and November 2017, allowing the mandated time required for public comment.

As NFIP integrates critical rate requirements into the program, it will refocus to longer-term initiatives, including program updates and rulemaking initiatives. During the Fall of 2016, new reports and studies provided information critical to shaping NFIP's next steps in meeting the following requirements. During FY 2017, FEMA maintained a brochure on alternative flood mitigation methods for buildings to help communities and policyholders mitigate flood risk and rates. To fulfill the requirement to clearly communicate risk of policyholders including grandfathered policyholders, NFIP insurers, working with WYO companies, are collecting current flood zone determinations to populate FEMA's HFIAA-mandated clear communication of risk to property owners. FEMA is executing this requirement through a staged implementation that began April 2016 and will allow FEMA to identify all grandfathered policies by the Spring of 2019. FEMA will continue to track and monitor progress on implementation of the concept of operations and how they relate to GAO recommendations for effectiveness.

In addition, not all policyholders pay full-risk rates nor does the program charge sufficient rates to cover catastrophic events. The 2019 budget proposal highlights the need to provide affordability assistance to certain homeowners as FEMA works to put the NFIP on a more sustainable financial footing by signaling to homeowners the true cost associated with the risk of living in a floodplain. This would be accomplished through a targeted, means-tested affordability program that offers premium assistance based on income or ability to pay, rather than location or date of construction. In its current structure, the NFIP makes rates "reasonable" by offering discounts and cross-subsidies primarily based on a building's age, map changes at a building's location, or by considering mitigation activities undertaken by the property owner or community. This legislative proposal would end this practice and establish a targeted affordability program for NFIP policyholders. Such a program would shield low-income policyholders who currently receive discounts or subsidies from substantive rate increases, while ensuring those able to pay, despite the age or location of their property, do so. Low-income policyholders would still be subject to standard annual adjustments to all rates, accounting for inflation and actuarial practices, however.

Planned Actions and Key Milestones: Major acquisition lifecycle framework milestones for FEMA's insurance system modernization activities include:

- Initial Operating Capability (IOC): The IOC includes establishing the Pivot infrastructure (hosting environment, development tools, cybersecurity, etc.), the Pivot Analytics and Reporting Tool (PART), establishing a data migration plan, delivering near-real time claims information, and establishing an appeals tracker. The PART tool was placed into production in October 2017, and the remaining functions are being released in Q2 FY 2018, on or ahead of schedule. The program is currently on track to decommission the legacy system ahead of the approved Full Operational Capability date of FY 2020.
- ADE-2A and 2B: The Acquisition Review Board (ARB) met on December 15, 2016 and the Under Secretary for Management (USM) approved the program passing ADEs 2A and 2b, and entering the "obtain" phase. These milestones involved the approval of requirements, concept of operations, life cycle costs, and AoA artifacts before proceeding to the acquisition phase.
- ADE-1: The NFIP Pivot Program also appeared at an ARB in September 2015. This milestone involved validating the mission need and capability development plan for the program, and authorizing FEMA to begin analyze/select activities.

GAO High-Risk Area: Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information (Government-wide)

Overview: Federal agencies and our Nation's critical infrastructure—such as power distribution, water supply, telecommunications, and emergency services—rely extensively on computerized information systems and electronic data to carry out their operations. Safeguarding these systems and data is essential to protecting national and economic security, as well as public health and safety. This safeguarding of federal computer systems and the systems that support critical infrastructure—referred to as cyber Critical Infrastructure Protection (CIP)—is a continuing concern. Federal information security has been on GAO's list of high risk areas since 1997. In 2003, GAO expanded this high risk area to include cyber CIP. Risks to information systems include continuing insider threats from employees and business partners, escalating and emerging threats from around the globe, the ease of obtaining and using hacking tools, the steady advance in the sophistication of attack technology, and the emergence of new and more destructive attacks. In 2015, GAO added protecting the privacy of personally identifiable information (PII) to this area.

Lead Office and Official: National Protection and Programs Directorate (NPPD) Office of Cybersecurity and Communications (CS&C), Peter Petrianni, Deputy Director, Information Management Office

Progress: DHS continues to work towards ensuring the security of federal information systems and critical infrastructure and protecting the privacy of PII. While addressing cybersecurity requires a whole-of-government approach and robust collaboration with the private sector, DHS continues to lead the Federal Government's efforts to improve civilian cybersecurity. In particular, DHS continues to advance its ability to develop and share situational awareness of cyber threats and vulnerabilities while providing a baseline of security for federal civilian agencies.

For example, DHS's National Cybersecurity Assessment and Technical Services (NCATS) team continues to increase its cyber hygiene scanning activities, which ensure that federal agencies are aware of vulnerabilities in their Internet-facing systems. As of April 30, 2017, the NCATS team detected 200,560 vulnerabilities. Under the Federal Information Security Modernization Act of 2014, DHS released its first binding operational directive (BOD) in May 2015, which requires agencies to quickly patch their most critical cyber vulnerabilities based on the results of NCATS cyber hygiene scans. Two years after the BOD's issuance, federal agencies continue to quickly patch their most critical vulnerabilities. In addition, a general reduction in time to patch non-critical vulnerabilities also followed the issuance of the BOD. It is expected that similar outcomes will result from agencies' increased visibility into their assets and vulnerabilities as CDM Phase 1 tools are installed. The Department is developing an FY 2018-2019

Agency Priority Goal, which will measure agencies' use of NCATS and CDM vulnerability assessment results to ensure quick patch management related to critical vulnerabilities.

In addition, in FY 2016, the NCATS team completed 71 Risk and Vulnerability Assessments (RVAs) for federal agencies, the majority of which focused on agency-identified high-value assets. Through April 2017, 19 RVAs had been completed for federal agencies, again with a focus on high-value assets. RVA services include, among other things, penetration testing, wireless discovery and identification, database scanning, web application scanning and testing, and social engineering. Each RVA focused on a high-value asset that also included a strategic architecture review provided by DHS's Federal Network Resilience division. Significantly, DHS currently provides agencies with actionable risk mitigation information based on cyber hygiene scans and RVAs focused on high-value assets and has already met the June 2018 deadline for this requirement.

DHS also strengthened the effectiveness of its partnerships with the private sector and other federal agencies in securing cyber critical infrastructure. For example, DHS has made efforts to provide CDM to other federal agencies. As of December 31, 2016, DHS had provided CDM Phase 1 and Phase 2 tools to 100% of participating agencies. Since then, agencies have deployed tools and their agency-level dashboards to monitor and manage their security. DHS CDM Federal Dashboard 3.0 received its authority to operate in August 2017 and became operational in October 2017. During Q1 FY 2018, DHS successfully established Information Exchanges between several Agency Dashboards and the Federal Dashboard. In FY 2018, DHS will continue to establish information exchanges until all agencies are complete. The estimated completion date for Information Exchanges is Q4 FY 2018.

DHS continues to provide EINSTEIN intrusion detection and prevention services to federal agencies. EINSTEIN 3 Accelerated (EINSTEIN 3A), which actively blocks known malicious traffic, is currently being deployed through the primary internet service providers serving the Federal Government. As of June 30, 2017, all civilian CFO Act agencies and approximately 77 small agencies were protected by at least one countermeasure, which amounts to an overall federal civilian agency coverage of 94 percent. The National Cybersecurity and Communications Integration Center (NCCIC) has improved public-private sector partnerships by improving information sharing so they can block threats before penetrating networks or otherwise detect intrusions sooner. NCCIC continued its dissemination of alerts, warnings, and bulletins through April 2017. In addition, it implemented the Automated Indicator Sharing (AIS) capability in accordance with the Cybersecurity Information Sharing Act of 2015. As of September 30, 2017, NCCIC had shared approximately 1,335,036 unique indicators through the AIS capability. As of September 30, 2017, 135 non-federal entities—including several information sharing and analysis organizations, managed security services providers and commercial threat feeds—are connected to the AIS capability and 32 federal agencies are connected. Seven organizations are actively sharing into the AIS capability, including four non-federal information sharing and analysis organizations or security providers, which share on behalf of their membership.

Furthermore, DHS delivered the National Cyber Incident Response Plan to the White House on January 18, 2017, as required by the National Cybersecurity Protection Act of 2014 and Presidential Policy Directive 41. In FY 2016, the NCCIC provided 23 onsite incident response and recovery team deployments. As of April 2017, it had provided 18 onsite deployments in FY 2017.

In the past, GAO reported that DHS's National Cybersecurity Protection System (NCPS) was partially, but not fully, meeting its stated system objectives of detecting intrusions, preventing intrusions, analyzing malicious content, and sharing information. GAO has also reported that DHS also had not developed metrics for measuring the performance of NCPS, recommending DHS take action to enhance NCPS's capabilities, among other things. As of October 2017, NCPS continues to enhance its current intrusion detection approach. More specifically, a contract has been awarded and the NCPS Program Office is proceeding into development and execution of the implementation plan to operationalize the Advanced Analytics capability. Additionally, the National Protection and Programs Directorate (NPPD), specifically the Office of Cybersecurity and Communication (CS&C), finalized a new Government Performance and Results Act Modernization Act measure against which CS&C will be reporting at the end of the first quarter of FY 2018. This measure will focus on the extent to which the NCPS intrusion detection and prevention capabilities detect or prevent nation state threat activity. The measure also is included as a supporting measure in the aforementioned Agency Priority Goal for FY2018 and FY 2019, which focuses on federal cybersecurity outcomes. Finally, CS&C and OMB continue to work on the congressional report required by the Cybersecurity Act of 2015, which will examine the effectiveness of NCPS and CDM. This report will highlight areas for improved performance measurement within the NCCIC related to how the NCPS capabilities can be used to support prevention, detection, information sharing, hunt and incident response functions.

With respect to ensuring privacy compliance and the protection of PII and other sensitive information. NPPD's Office of Privacy has conducted publicly available privacy impact assessments (PIAs) on its cybersecurity programs, which assess and mitigate any impact a system or program may have on the privacy of individuals. As discussed in PIAs, DHS has processes in place to implement data minimization to ensure data collection is limited to information that is determined to be necessary to understanding cyber threats. NPPD's Office of Privacy ensures privacy protections are built into the design of the NCCIC's technical capabilities. For example, during the implementation of the AIS capability, NPPD's Office of Privacy developed and oversaw the implementation of system requirements consistent with the privacy protections mandated by the Cybersecurity Information Sharing Act of 2015.

To further protect the Federal Government's information systems and to collaboratively protect non-federal entities, DHS will increase its EINSTEIN 3A coverage in accordance with the "Cybersecurity Act of 2015," continue supporting agencies through the procurement and deployment of CDM capabilities, and increase the volume of cyber threat indicators and defensive measures shared through the AIS capability while analyzing the relative value of those indicators. Additionally, DHS will continue to implement the requirements of Presidential Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."

DHS continues to work with NPPD to develop a comprehensive cybersecurity workforce strategy, in order to recruit and retain qualified cybersecurity professionals. Reference the preceding section on "Strategic Human Capital Management" for more information.

Planned Actions and Key Milestones: To further protect the Federal Government's information systems and to collaboratively protect non-federal entities, DHS will increase its EINSTEIN 3A coverage, in accordance with the Cybersecurity Act of 2015, continue supporting agencies through the procurement and deployment of CDM capabilities, and increase the volume of cyber threat indicators and defensive measures shared through AIS capability while analyzing the relative value of those indicators.

During FY 2018, DHS expects to make important progress in reinforcing DHS's role in protecting the Federal Government's information systems and the Nation's cybercritical infrastructures (Government-wide). Specifically, DHS plans to:

- Purchase and deliver CDM Phase 1 and 2 tools for 100 percent of the participating Federal agencies.
- Provide agencies with actionable risk mitigation information based on cyber hygiene scans and RVAs focused on high-value assets.
- Deliver a revised National Cyber Incident Response Plan to the White House, as required by the *National Cybersecurity Protection Act of 2014* and Presidential Policy Directive 41.

GAO High-Risk Area: Strategic Human Capital Management (Government-wide)

GAO Overview: Addressing national challenges requires a high-quality federal workforce able to work seamlessly with other agencies, levels of government, and across sectors. However, current budget and long-term fiscal pressures, declining levels of federal employee satisfaction, the changing nature of federal work, and a potential wave of employee retirements could produce gaps in leadership and institutional knowledge. Mission-critical skills gaps impede federal agencies from cost-effectively serving the public and achieving results. Additional efforts are needed to coordinate and sustain efforts to close critical skill gaps and better use workforce analytics to predict emerging skills gaps. DHS has taken significant steps over the last year to develop and demonstrate sustained progress in implementing a results-oriented, human capital plan that identifies departmental human capital goals, objectives, and performance measures, and is also linked to the Department's overall strategic plan.

In December 2014, Congress passed two pieces of cybersecurity workforce legislation, specifically the Border Patrol Pay Reform Act of 2014 and the Cybersecurity Workforce Assessment Act, and in December 2015, Congress passed the Federal Cybersecurity Workforce Assessment Act. The Border Patrol Pay Reform Act of 2014 granted the Secretary the authority to create a cybersecurity excepted service personnel system. This authority allows for a variety of human capital management changes, including alternative hiring procedures, alternative compensation, and the creation of a senior cyber service. The laws also required DHS to increase its cybersecurity workforce analysis and planning efforts.

Lead Office and Official: Management Directorate, Office of the Chief Human Capital Officer (OCHCO), Roland Edwards, Deputy Chief Human Capital Officer

Progress: The Human Capital Leadership Council (consisting of the Human Resources directors of each operational Component and Office of the Chief Human Capital Officer (OCHCO) executives) recently released the FY 2018 Human Capital Operational Plan (HCOP) that aligns the upcoming year's human capital priorities with the department's strategic goals and includes performance objectives for workforce planning, recruitment, and learning and development, and other areas.

In March 2016, as a result of the biennial mission critical occupation (MCO) revalidation, DHS designated 75.9% of its combined civilian/military workforce as MCOs, and 70.1% as priority MCOs (PMCO) – employees who perform the Department's most critical operational missions. During the revalidation, DHS identified all of its more than 230,000 personnel as either directly performing or supporting a DHS Strategic Plan mission area. For each PMCO, Components built workforce plans that documented actions to close these skill gaps, helping the Department add more than 2,700 employees (2.3%) in PMCOs. In early FY 2018, DHS will again guide Components through an in-depth assessment of MCOs by functions to better define personnel and capabilities dedicated to each mission area.

In December 2016, OCHCO coordinated a Pathfinder Business Operations hiring event targeting interns and recent graduates, initially filling 37% of 300 positions identified, and 591 Pathways positions by the end of FY 2017. In addition, the Department conducted a veteran-specific special hiring event to support the Presidential direction on border security and immigration enforcement. DHS first conducted twelve "DHS is Hiring" webinars in June and July 2017, attracting more than 5,000 participants online and over 3,500 participants by phone. More than 2,500 veterans attended the two-day event in August 2017, during which 528 were hired or advanced to the next step of the law enforcement hiring process. To support these recruitment initiatives, OCHCO is using a new OPM USAJOBS capability called "resume mining" that allows hiring managers to search more than 2 million resumes. More than 530 users have been trained and registered for the "resume mining" capability. Throughout FY 2017, DHS had a strong recruiting presence at events sponsored by key law enforcement groups for women and minority law enforcement professionals. These activities will be instrumental in helping the Department meet emerging high priority mission needs, in particular the 5,000 Border Patrol Agents and 10,000 Deportation Officers directed by Executive Order. To supplement the Component Recruitment Outreach Plan (CROP) and provide real-time recruitment, marketing, and outreach data, OCHCO has transitioned to a standardized data collection methodology. The Recruiting, Outreach, and Marketing Matrix allows DHS to track attendance, recruiting costs, target audience, and marketing focus, helping to maximize recruiting return on investment.

To address DHS-wide skill gaps, OCHCO has assessed the DHS two-year workforce development plan (WDP) from 2016 and provided a written assessment to GAO in October 2017. Informed by that information, OCHCO is developing the FY 2018-19 edition of the WDP. The positive impact of our leader development program on employee engagement was documented in a recent study, Leader Development Works! Measuring the Impact of DHS's Cornerstone Program on Employee Engagement

Survey Results. Results from the study determined that overall Federal Employee Viewpoint Survey scores for organizations with high Cornerstone completion rates exceeded those organizations with low completion rates by three percentage points. Additionally, the Employee Engagement Index scores were more than two percentage points higher. DHS has also made significant progress in capturing employee inputs to enhance both engagement and mission effectiveness. The Acting Secretary, CHCO, and other senior leaders throughout the Department have established a robust series of "listening tours" and town hall meetings, implemented feedback mechanisms to understand the challenges facing the workforce, and are implementing improvement ideas.

DHS has increased its cybersecurity workforce planning and analysis efforts to gain better insight into cybersecurity work to meet mission needs and statutory mandates (the Border Patrol Agency Pay Reform Act - P.L. 113-277, Cybersecurity Workforce Assessment Act - P.L. 113-246, and Federal Cybersecurity Workforce Assessment Act of 2015 -- P.L. 114-113). During FY 2017, DHS made great progress in identifying and coding cybersecurity positions and employees according to the National Initiative for Cybersecurity Education Workforce Framework, and refined processes for validating and communicating DHS-wide cybersecurity onboard and vacancy counts. DHS captured results of these efforts – including workforce gap analyses – in a comprehensive report for Congress that will be updated in future years. The Department has identified approximately 10,000 civilian, military, and contractor positions with significant cybersecurity responsibilities, including approximately 6,700 federal civilian positions, and coded more than 90% of encumbered civilian positions to comply with direction from Congress and the Office of Personnel Management (OPM). DHS also launched a series of news alerts to Components regarding the effective use of human capital flexibilities. Lastly, DHS continues to design a new cybersecurity personnel system using authority granted to the Secretary via P.L. 113-277. In FY 2017, OCHCO crafted several foundational design elements of the new personnel system and identified key policy decisions to focus on with the DHS Office of the General Counsel, Component cybersecurity and human capital staff, and OPM with whom Congress asked DHS to coordinate implementation. OCHCO is managing a set of activities, ranging from drafting policy to creating training and communication materials, related to finalizing the system and preparing DHS for launch.

Planned Actions and Key Milestones: To sustain a GAO assessment of "Fully Addressed" for implementing the Human Capital Plan and continue progressing toward a "Fully Addressed" assessment for the remaining outcomes, the Department-wide human capital community and its key stakeholders will, in FY 2018 and beyond:

- Continue to implement the HCSP through annual operational plans and data-driven performance reviews, to include continual monitoring and evaluation of the human capital dashboard
- Continue to employ Department-wide and Component-specific recruitment strategies is key to sustaining progress in skill gap closure.
- Components will update annual Component Recruitment and Outreach Plans (CROP), with a focus on targeted recruitment for PMCOs.
- Continue to apply the five-step workforce planning framework for the department's priority MCOs, which consist of 17 occupations most impactful to DHS's overall mission areas.
- DHS will also track all cyber recruitment, outreach, and marketing for all components due to the critical need across the enterprise.
- Improve visibility of program training costs and quality by implementing a DHS-wide Common Training Cost Structure, implementing enterprise training metrics, and sharing information among Components on common training offerings.
- Complete piloting and fully implement the Joint Duty Assignment Program to provide cross-Component rotational experiences to develop DHS leaders with broad departmental perspectives.
- Conduct annual recruitment planning sessions to prioritize events and ensure alignment with workforce planning and diversity analysis, to meet or exceed hiring goals.

- Continue to work through the DHS Employee Engagement Steering Committee to improve Component engagement action planning processes, share and spread best practices, and keep DHS leadership apprised of issues and challenges related to employee engagement.

GAO High-Risk Area: Managing Federal Real Property (Government-wide)

GAO Overview: The Federal Government's real property holdings are vast and diverse with a combined area of over three billion square feet (SF). Since federal real property management was placed on the high risk list in 2003, the government has given high-level attention to this issue and has made strides in real property management, but continues to face long-standing challenges. The Federal Government continues to maintain too much excess and underused property and relies too heavily on leasing in situations where ownership would be more cost efficient in the long run. The Federal Government also faces ongoing challenges in protecting its facilities.

With more than 100 million SF of building space, leases through the U.S. General Services Administration (GSA) and direct leases from the private sector account for more than half of DHS's building space. Payments on these leases accounted for 81 percent of DHS's FY 2017 operating outlays for real estate at $1.8 billion. DHS has employed several strategies to improve real property management, reduce overreliance on leasing, reduce leasing costs, and reduce excess and underused property.

The Federal Protective Service (FPS) is charged with protecting and delivering integrated law enforcement and security services to facilities owned or leased by GSA.

Lead Office and Official: Management Directorate, Office of the Chief Readiness Support Officer (OCRSO), Tom Chaleki, Deputy Chief Readiness Support Officer

Progress: DHS continued its space efficiencies and reduction efforts which aim to achieve the right facility, at the right location, at the right cost. DHS also continued efforts to reduce the real property footprint by focusing on SF reduction and cost savings to reduce dependency on leased locations and improve space utilization in both leased and owned locations. FPS provides integrated security and law enforcement services to federally owned and leased buildings, facilities, property, and other assets.

Federal Real Property Management: Through the Unity of Effort initiative, DHS is ensuring that programming, budgeting, and expenditures across the Department are mission-driven, cohesive, and transparent. In 2017, DHS strengthened its approach to the budget by focusing Department-wide on mission needs and fully implementing a Common Appropriation Structure, which provides a simple, consistent structure across components. Because some DHS components do not account separately for funding for facilities acquisition and maintenance in their Resource Allocation Plan (RAP) submissions, DHS also conducted the DHS Real Property Resource/Funding Requirements Assessment Study (Assessment Study) in FY 2017 to better link the DHS real property vision and national strategy to the budget process. The FY 2017 Assessment Study allowed DHS to compile real property funding requirements at the Departmental level, and for the first time, provide senior Department officials with visibility into real property requirements at the Departmental level. OCRSO through the Office of Program Analysis and Evaluation (PA&E) within the Office of the Chief Financial Officer (CFO) institutionalized this annual requirement in the 2019 RAP guidance linking budget requests with planned real property requirements.

The DHS real property program is focused on activities that optimize the real property inventory by providing the optimal square footage in support of the disparate mission of homeland security missions. DHS continues to reconfigure and build-out new spaces in accordance with the 2014 Workspace Standard and the DHS Real Property Efficiency Plan (RPEP) subject to available funding. The DHS Workspace Standard provides criteria for office and related spaces (conference rooms, break rooms, file rooms, etc.) not to exceed 150 SF/per person.

In 2017, DHS chartered a temporary Field Efficiencies Program Management Office (FE-PMO) to implement a unified cross component planning process and identify opportunities for consolidations along common and/or similar mission functions with compatible mission support requirements, anchor locations, or future mission needs. The FE-PMO will conduct three regional studies during FY 2017 and FY 2018, and establish integrated real property mission support plans for all major metropolitan regions with a significant concentration of DHS assets and activities by FY 2022. The regional plans will focus on increased utilization of DHS assets in support of improved efficiency.

Protection of Facilities: FPS leads efforts within a complex operating environment to protect and secure federal facilities from increasingly dangerous and unpredictable physical and cyber threats. FPS continues to develop national-level policies, operational initiatives, capabilities and programs that are grounded in the seamless integration of law enforcement, security, and intelligence activities. These efforts are instrumental for threat detection and deterrence while enhancing security and promoting facility and infrastructure resilience. For example:

- FPS is the co-lead for the Government Facilities Sector (GFS) as part of the National Infrastructure Protection Plan. As co-Sector Specific Agencies, FPS and GSA chair the sector's Government Coordinating Council (GCC).
- FPS continues to develop strategies for effecting cybersecurity in facility safety and security control systems. FPS has led the effort to incorporate cyber security controls in the recent release of the *ISC's Risk Management Process: Appendix B: Countermeasures*. FPS is currently working toward implementation of interim operating capability for the Federal Facilities Control System Strategy. Implementation of the strategy includes assessment activities, stakeholder engagement and education, and protective intelligence information sharing relevant to cyber threats (actors, incidents).
- FPS is in the process of enhancing the capabilities of its Modified Infrastructure Survey Tool *(MIST)*, FPS's facility protection tool, to incorporate the constantly changing environment. For example, in FY 17, FPS implemented a cyber-physical question set to its assessment process, a mechanism to track countermeasure implementation status, a threat module aligned with the ISCs design basis threat (DBT), a risk analysis profile, a consequence scoring algorithm, and several other features to enhance the capabilities of the organization and continue to improve upon the efficiency of the FPS protective mission.

FPS applies the national standards and strategies to develop or improve and implement operational policies and procedures across the mission areas. GAO has issued recommendations to FPS pertaining to risk assessment and the protective security officer (PSO) program. FPS's efforts have resulted in the closure of the majority of recommendations in these two areas. For the few that remain, FPS is actively working to address their closure through efforts including the following:

- FPS continues to enhance its Facility Security Assessment (FSA) Program incorporating industry best practices and updated ISC standards. Through the demonstrated success of this program, FPS has validated its position as the lead organization in the effort of federal facility protection, becoming not only a consultant to GAO on assessment related audits, but also through consultation requests from federal agencies not included in the regular FPS inventory. Through these engagements, FPS provides subject matter expertise, assessment support, mitigation strategy recommendations, and the use of MIST.
- FPS actively participates in supporting public-private partnerships through the leading of panel discussions at the ASIS international convention. Most recently, FPS led panel discussions in the Protection Trifecta—Integrating Security, Law Enforcement, and Intelligence operations and conducted presentations in Active Threat response in Federal Campus', Screening Operations, and Breaking and Entering—Lessons Learned in Penetration Testing. All presentations were very well received.

- Since the implementation of FPS' formal FSA program, FPS has conducted over 6,000 FSAs and recommended more than 22,000 countermeasures to Facility Security Committees.
- FPS has matured initiatives that cut across various aspects of the PSO program to ensure that requirements for PSOs are clearly defined, communicated, and monitored. Since the November 2015 revision of the PSO Oversight and Monitoring directive, which provided clarity on internal oversight responsibilities and processes, FPS continues to refine procedures and evaluate potential improvements to contract protective security services. FPS Contracting Officer Representatives receive in depth training on the specifics of FPS PSO directives and contract statement of work so that they are prepared to identify and address any compliance issues quickly. FPS recognizes that there are opportunities to modernize aspects of the program to include tracking time on post as well as management of the training and certification data.
- Separate from the programmatic efforts noted above, FPS has also recognized the importance of better tracking of recommendations from issuance to closure and beyond to ensure that actions being taken to address GAO recommendations align with agency goals.

  FPS conceptualized and has begun development of a Protection Center of Excellence (PCoE) to establish standardized training for security professionals across the government. FPS formed a PCoE Development Cell at the Federal Law Enforcement Training Centers (FLETC) which includes representatives from FLETC, DHS, the U.S. Department of Justice, the Federal Aviation Administration, the U.S. Department of Defense, and other ISC member agencies. FLETC and FPS have conducted a crosswalk of FLETC's current curriculum to identify related ISC competencies. Further, FLETC and FPS are soliciting FLETC partner organizations to determine if their respective agencies have a need or desire to train within the PCoE. FPS continues to assess PCoE support staff requirements.

GAO High-Risk Area: Ensuring the Effective Protection of Technologies Critical to U.S. National Security Interests (Government-wide)

Overview: In 2007, GAO designated ensuring the effective protection of technologies critical to U.S. national security interests as a high risk area because these weapons and technologies are often targets for espionage, theft, reverse engineering, and illegal export. Although the government has taken significant steps to address this issue area, it remains high risk because some programs in this area are ill-equipped to address the ongoing challenges of balancing national security concerns and economic interests.

The Federal Government must improve coordination of existing programs to identify strategic reforms that will help ensure the advancement of U.S. interests. GAO's high risk list notes the role of the U.S. Immigration and Customs Enforcement's (ICE) Export Enforcement Coordination Center (E2C2) as a potential platform for improving coordination efforts for export-control programs. E2C2 serves as a conduit between the U.S. Intelligence Community, the Information Triage Unit, and federal export enforcement agencies for the exchange of information related to potential U.S. export controls violations. E2C2 aims to deconflict potential enforcement actions among the participating export control enforcement agencies.

GAO also noted the importance of improving security cooperation and disclosure for this issue area, particularly with regard to Foreign Military Sales (FMS). U.S. Customs and Border Protection (CBP) is responsible for controlling the export of articles related to these sales.

Lead Office and Official: DHS Office of Strategy, Policy and Plans , Christa Brzozowski, Deputy Assistant Secretary for Trade and Transport Policy Office of Strategy, Policy, and Plans

Progress: To improve coordination of export-control related programs, DHS has made efforts to improve E2C2 operations. E2C2 established the Export Enforcement Intelligence Working Group (EEIWG) to draft and approve the roles and responsibilities of an export enforcement intelligence cell. In 2013, the

EEIWG drafted a white paper outlining the E2C2 Intelligence Cell's mission, its general roles and functions, and recommended tasks and a structure to facilitate enhanced coordination and intelligence sharing among E2C2 partner agencies. Recently the EEIWG mission has evolved and it is now meeting monthly with inter-agency partners to collaborate on export enforcement issues. Since September 2017, the EEIWG has meet twice and is working on coordinating multiple actions against numerous entities involved in ISIS logistical support network. Although staffing at the E2C2 remains an issue, and at this time is primarily performing deconfliction rather than intelligence analysis activities, DHS is committed to working with E2C2 partner agencies to fully staff the intelligence cell. To further improve security cooperation and disclosure, DHS has made improvements to FMS oversight. Working with E2C2 partner agencies to fully staff the intelligence cell, CBP and the Defense Security Cooperation Agency (DSCA) formed an informal working group to discuss the electronic sharing of the Letter of Offer and Acceptance (LOA) data for FMS cases. CBP and DSCA are working to automate the data exchange. The Memorandum of Understanding between the agencies has been signed by both agencies. The proposed system will strengthen the accounting of FMS exports. CBP is on track to have the system completed in early 2018.

Planned Actions and Key Milestones: To continue protecting technologies critical to national security:

- The Department of Commerce recently assigned a new Assistant Director and one part-time intelligence analyst at E2C2. It is anticipated that these additional resources can assist in the near term, although appropriate resources and interagency personnel will still be required to fully implement the EO mandates.
- E2C2 has established Export Enforcement Intelligence Working Group (EEIWG) to leverage relationships with several DOD components and foster collaboration on issues of mutual interest.
- CBP is on track to create and implement a centralized process for tracking FMS shipments and enhancing the FMS export data validation process by CY2017.
- Defense Security Cooperation Agency (DSCA) will sign the Inter Service Agreement (ISA).
- DHS approves the ISA.
- DSCA begins sharing the FMS case data in early 2018.
- CBP fully automates the FMS case data system, including the decrementation of exports against the FMS case data.

GAO High-Risk Area: Improving Federal Oversight of Food Safety (Government-wide)

Overview: In 2007, GAO added federal food safety oversight to the high risk list because of risks to the economy, public health, and safety. Several major trends create food safety challenges. First, a substantial and increasing portion of the U.S. food supply is imported. Second, consumers are eating more raw and minimally processed foods. Third, segments of the population that are particularly susceptible to foodborne illnesses, such as older adults and immune-compromised individuals, are growing. Given CBP's oversight role in food importation, DHS has a nexus to this high risk issue area. CBP is responsible for inspecting imports, including food products, plants, and live animals, for compliance with U.S. law and for assisting all federal agencies in enforcing their regulations at the border. GAO has identified areas in which CBP can improve food import oversight capabilities.

GAO has also emphasized the need to develop a government-wide performance plan for food safety. Although DHS is not among the agencies with primary food safety oversight responsibility, DHS was a member of the Food Safety Working Group which, if reconvened, could serve as a broad-based, centralized, collaborative mechanism for this and other purposes.

Lead Office and Official: CBP, Office of Field Operations, Mikel Tookes, Deputy Executive Director, Agriculture Programs and Trade Liaison

Progress: CBP has undertaken several initiatives with the U.S. Department of Agriculture (USDA) to improve federal food safety oversight. For example:

- In September 2013, the Department of Homeland Security (DHS) and USDA issued its joint 2014-2019 joint strategic plan for the Agricultural Quarantine Inspection (AQI) program and identified performance measures to monitor progress towards program goals. DHS and USDA developed performance measures for many aspects of the AQI program including interagency coordination, identification of high priority pests, and pest and animal disease training.
- In July 2014, CBP deployed a web-based canine tracking system to all canine personnel including agriculture canine handlers to enter daily activity data. The system will improve efficiency and accuracy in canine program tracking and reporting. Moreover, a working group of subject matter experts from DHS CBP deemed the data elements captured in the system as relevant to the program. Additionally, canine activity data is now reviewed and approved by supervisors monthly at CBP field offices.
- In May 2015, CBP issued a staffing model strategy and action plan - the Agriculture Resources Allocation Model Strategy and Action Plan (2015-2018). The staffing model is a workload-based management tool designed to project optimal staffing levels for CBP agriculture specialists in support of CBP decision making and budget planning and it will be the primary tool that informs staffing decisions in all environments - air, land, and sea. Moreover, CBP will be equipped to identify optimum agriculture specialist staffing numbers and continue to dialogue with USDA's Animal and Plant Health Inspection Service (APHIS) to ensure that the CBP agriculture specialist funding source is full cost recovery and the model is updated periodically.
- In July 2015, CBP conducted training for those supervisors identified as not having canine training including new incoming supervisors. As of December 2015, 26 staff attended the training. CBP will conduct future training for new supervisors and the agency plans to complete additional agriculture canine modules as part of the training curriculum.
- In March 2016, APHIS and CBP documented requirements to interface our systems to improve Agricultural Quarantine Inspection data quality including identifying needed data elements and reference codes to eliminate data errors. To achieve this interface, APHIS and CBP established working groups comprised of subject matter experts who jointly identified and clarified needed data elements, planned system connection logistics, and implemented system integration activities for the purpose of minimizing duplication of data entry, reducing data errors, improving data quality and integrity, and sharing information and analytics.

As a result of the aforementioned efforts and CBP's dedication to food safety, CBP has successfully met the intent and fully implemented of all of the CBP assigned recommendations associated with this narrative.

Planned Actions and Key Milestones: CBP will continue to report on deployment and improvement of AQI data as both agencies work toward modernization, interoperability, and automation of data systems. However, USDA must have the capability to interface with all CBP systems in order for system-to-system interoperability to be successful. CBP has completed all agriculture modules in the International Trade Data System (ITDS) and Cargo Enforcement Reporting and Tracking System (CERTS) have been completed and are awaiting USDA completion of their interface system, Agriculture Risk Management (ARM). CBP and the APHIS, Plant Protection and Quarantine, Quarantine Policy, Analysis Support Staff meet weekly to discuss the APHIS Participating Government Agencies Message Sets for CBP's Automated Commercial Environment (ACE) and the interface between the CBP systems and ARM. CBP and APHIS also meet regularly on the Border Interagency Executive Council that includes representatives from all federal agencies that have a role in importing, exporting, or border management. Additionally, CBP and APHIS meet on the International Trade Data Systems Board for the single-window development through ACE. As a result of the aforementioned efforts and CBP's dedication to food safety, CBP has successfully met the intent and fully implemented of all of the CBP assigned recommendations associated with this narrative.

GAO High-Risk Area: Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks (Government-wide)

Overview: In February 2013, GAO designated "Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks" as a government-wide high risk area. In addition to creating significant financial risks for the Federal Government, the effects of climate change could (1) threaten coastal areas with rising sea levels, (2) alter agricultural productivity, (3) affect water supplies, (4) increase the intensity and frequency of severe weather events, and (5) increase the frequency and volume of population movement and consequent goods movement. GAO found that the Federal Government is not well organized to address the fiscal exposure presented by the effects of climate change, and needs a government-wide strategic approach with strong leadership to manage related risks. GAO also found that climate change may increase the Federal Government's fiscal exposure related to federal facilities, federal insurance programs—such as FEMA's National Flood Insurance Program, and federal disaster aid—such as FEMA's Disaster Relief Fund.

The projected impacts of climate change intersect with DHS in several areas. Notably, DHS facilities may be exposed to greater risks and an increase in the cost of aid provided following a disaster.

Lead Office and Official: Office of the USM, Chip Fulghum, Deputy Under Secretary for Management and Chief Sustainability Officer

Progress: In FY 2017, DHS continued efforts to address mission related national climate resilience, as appropriate, to meet the requirements of Executive Order 13693: *Planning for Federal Sustainability in the Next Decade*. The DHS Climate Resilience Director Group led efforts to revise the DHS Climate Action Plan (CA-Plan).

DHS increased focus on the climate change/national security nexus in FY 2017. As a standing member of the Climate and National Security Working Group co-chaired by the National Security Council and the Office of Science and Technology Policy, the Department worked to ensure that the current impacts of climate change, and those anticipated in the coming decades, be identified and considered in the development and implementation of relevant national security doctrine, policies, and plans. DHS was a key player in the development of the pre-decisional draft of the Climate and National Security Action Plan. The Committee was halted in March 2017 with the issuance of Executive Order 13783: *Promoting Energy Independence and Economic Growth.*

The DHS Climate Change and Health Disaster Resilience Group was established in early FY 2017. The Department hosted two teleconferences with participation from most of the States, including Hawaii and Alaska, as well as representatives from the Canadian government, private sector, educational institutions, State and Local Governments, as well as Federal Agencies. The DHS-led group focuses on climate change health issues and is exploring methods to improve community and health resilience and form collaborations across the U.S. and Canada and will continue its work during FY 2018 with the goal of having quarterly teleconference meetings.

In FY 2017, the Department commenced the adjudication of public comments received in response to 1) FEMA proposed amendments to regulations on *"Floodplain Management and Protection of Wetlands" to Implement Executive Order 13690*, which establishes the Federal Flood Risk Management Standard (FFRMS) and 2) FEMA proposed supplementary policy (FEMA Policy: 078-3) which further clarifies how FEMA applies the FFRMS. In compliance with Executive Order 13783: *Promoting Energy Independence and Economic Growth*, rulemaking activities were ceased.

Planned Actions and Key Milestones: During FY 2018, DHS intends to advance the following initiatives:

- Establish a DHS headquarters-led program focused on evaluating the potential impacts of extreme weather events on DHS infrastructure resilience to minimize mission impacts.
- Advance the DHS Flood Apex Program designed to bring together new and emerging technologies designed to increase communities' resilience to flood disasters and provide flood predictive analytic tools to FEMA, state and local governments, and other stakeholders.
- Develop a "One DHS" system for governance and oversight of infrastructure management which includes the incorporation of the Department's largest utility consumer data and expansion of current analytical capabilities.
- Publish a study on the Arctic Information Sharing Environment. Through collaboration with interagency and international partners, the USCG will develop methods for improving shipping and environmental data obtained from space-based and unmanned aircraft systems.

GAO High-Risk Area: Improving the Management of IT Acquisitions and Operations (Government-wide)

Overview: More than $80 billion is invested annually in information technology (IT) across the Federal Government. GAO has determined that agencies continue to struggle with IT projects due to overly broad scopes and goals of delivering functionality several years after initiation. Also, executive-level governance and oversight across the Federal Government is often ineffective because chief information officers (CIOs) do not have the authority to review and approve their entire agency IT portfolios and overall authority is limited. Congress has reacted through the *Federal Information Technology Acquisition Reform Act*, which is intended to strengthen CIO authority and provide proper oversight for IT projects.

DHS has launched improvement efforts on multiple fronts to improve the management of IT acquisitions as well as existing IT systems, positioned itself as a leader in various efficiency initiatives, and stood up the JRC to evaluate high priority, and cross-departmental opportunities.

Lead Office and Official: Management Directorate Office of the CIO, Melissa Bruce, Executive Director for the Enterprise Business Management Office

Progress: The Department's actions to implement FITARA have produced many successes. DHS updated IT management processes and established additional elements to support a compatible, cohesive infrastructure; standardized operating procedures related to improving the transparency and management of IT acquisitions and operations; and strengthened the Office of the Chief Information Officer's (OCIO) authority to provide the needed direction and oversight. Since the implementation of FITARA at the Department, OCIO has:

- Established the Agency Software Manager within the IT Services Office (ITSO) as well as established an Enterprise and Software License Branch, which is focused on standardizing IT across the DHS enterprise, simplifying software license management, and providing support to ensure that DHS maintains a performance advantage, while increasing employee productivity. In order to coordinate and integrate the software license approach across the Department, DHS established an IT Category Management Working Group in April 2017 to address the direction outlined in Category Management Policy 16-1. The working group is co-led by leadership from

OCIO, the Office of the Chief Procurement Officer (OCPO), and the Office of Chief Financial Officer (OCFO).

- Continued to employ mature enterprise-wide governance processes, including program reviews, IT Acquisition Reviews, and CIO approval of acquisition plans and reprogramming requests. OCIO is a key contributor to the DHS JRC process and reviews. Additionally, DHS continues to mature its Enterprise IT Services Board (EITSB) and Enterprise Architecture Board (EAB) activities.
- Partnered with the OCFO for the second year to conduct an in-depth review of DHS IT infrastructure requirements. In 2017 an IT Infrastructure Assessment measured the performance and risks of IT infrastructure end point, hardware, and telecom assets across DHS. The study analyzed 201 systems, which included mission essential systems and the top 40 percent of IT steady-state spending, and identified aging, end-of-life, insufficient disaster recovery, or underperforming assets. OCIO and OCFO made recommendations and are taking actions to put the policies, funding, and ongoing monitoring in place to reduce the risks related to legacy infrastructure. In FY 2018, OCIO and OCFO have initiated the next annual IT Infrastructure Assessment and will be refining performance measures for end point, telecom, and server assets, with additional emphasis on collecting information on all DHS systems to inform planning for cloud migration and reducing reliance on DHS data centers. The results of this study are expected to inform FY 2020-2024 budget formulation and data center-related procurements.
- Continued to update the IT Federal Dashboard, which has resulted in approximately 300 Program Health Assessments in the calendar year.
- Established the DHS Headquarters Agile Acquisition Integrated Project Team (IPT) to bring together representatives from the Office of Program Accountability and Risk Management (PARM), JRC, OCIO, OCPO, OCFO, OCIO's Chief Technology Officer (CTO), S&T, and Digital Services. This IPT successfully completed the DHS IT Agile Acquisition Pilots, which included five program-level IPTs that piloted the acquisition process improvements that facilitate increased customer value, accountability, and oversight; faster time-to-market; and reduced cost and risk. The pilot programs all successfully achieved Acquisition Decision Event (ADE) 2A/2B, and two have commenced ongoing six-month program reviews to show incremental progress to the Acquisition Review Board (ARB). In July 2017, the Agile Acquisition Working Group IPT concluded, and the implementation of the Action Plans will be managed by the existing Information Technology Program Management Center of Excellence, along with the FITARA action items assigned to that body.
- Ensured that a minimum of 80 percent of DHS's major IT software delivery acquisitions deliver usable functionality every 12 months. In FY 2017 Q1 and Q2, OCIO reached out to every major IT investment program and associated project to validate which were conducting software development. OCIO interacted with program and project managers to ensure they were delivering usable functionality in 6- to 12-month increments, and that they were reporting the development methodology and release dates appropriately. DHS surpassed the minimum of 80 percent of major IT software delivery acquisitions delivering usable functionality every 12 months. As of September 30, 2017, 90 percent of the projects supporting Level 1, Level 2, and special interest investments are reporting use of agile software development and 86 percent of these projects are delivering usable functionality in increments of 6 months or less. The Agile Instruction was edited to include the FITARA requirement for the CIO to certify that software development projects are appropriately implementing incremental development. The INVEST system is being updated to provide a field for OCIO staff to indicate the CIO certification for appropriate projects.
- Addressed the lack of sufficient program management capabilities for major high-priority IT investments, by developing a number of IT-focused support and oversight capabilities, in addition to those generally available, including:

  - Taking a leading role at the federal level to implement competency standards for IT Project and Program Managers in the form of the Federal Acquisition Certification for Program and Project Managers (FAC-P/PM) from the Office of Federal Procurement Policy;
  - Operating a successful program for training and certifying IT program managers. This OCIO-led program has conducted three one-year IT Program Manager Development Program Tracks to provide IT Program Management training, hands-on experience and certification to DHS employees who manage IT programs and projects. This initiative is governed by the revised federally-mandated OMB, FAC-P/PM policy accompanied by the newly released FAC-P/PM IT Core Plus Specialization requirement;
  - Establishing technical centers of excellence with resources, best practices, templates, and tools to assist program managers. These centers of excellence enable experts to serve as mentors to help other employees develop skills and experience in different technical and managerial areas that support program execution;
  - Establishing a Systems Engineering Life Cycle course that teaches this methodology to program managers to help them deliver their investments according to DHS guidance; and
  - Offering an in-house opportunity for certified project management professionals to meet continuing education requirements through OCIO. The Project Management Institute approved DHS OCIO as a registered education provider for government-led project management training.
  - Optimized DHS Commodity IT beginning in FY 2011. Optimizing hosting across the Department has resulted in the consolidation of 45 data centers. The cumulative savings achieved from these transitions is over $355 million as of the end of FY 2016, which is more than ten times the $24.4 million cumulative data center savings that was originally projected through FY 2016. Similarly, DHS Components have migrated to one or more “as-a-service” private cloud offerings and/or strategically-sourced enterprise contract vehicles. The cumulative savings achieved from these strategically-sourced transitions is $1.03 billion as of the end of FY 2016, which is more than 2.5 times the $327 million originally projected through FY 2016. Finally, cumulative savings from all business process improvement and optimization/consolidation initiatives was originally projected to reach $504 million by FY 2016. Instead, DHS has saved or avoided $1.47 billion through FY 2016 alone, which is over two and half times the original $504 million projection.

Planned Actions and Key Milestones: DHS will continue to implement OMB initiatives to improve IT management, reduce duplication and costs, and improve services to the public with ongoing in-person TechStat reviews of IT programs, monthly reporting to the federal IT Dashboard, and leveraging strategic sourcing opportunities. Planned actions and key milestones include:

- In accordance with OMB Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing, the Department of Homeland Security (DHS) has taken into consideration key requirements and processes that need to be implemented to develop a comprehensive Software License Centralization Plan. DHS fully recognizes and understand the challenges pertaining to the centralization of software management. During FY 2017, the Department took the initial steps to implement a COTS tool to support the inventory management processes (CDM) and appointed an agency Software Manager. Thus far in FY 2018, the Department has outlined the key processes, practices, and steps to be undertaken as a part of a comprehensive centralization plan and management adoption framework, which will be completed in FY 2018. As DHS for begins its implementation of the processes outline within the plan, we will utilize an agile methodology and the concept of progressive elaboration so that as more detailed information becomes available the plan for software licenses may continuously and constantly be modified.

- In accordance with OMB M-16-19 Data Center Optimization Initiative (DCOI), the Department of Homeland Security (DHS) completed and delivered "Implementing DCOI: DHS Enterprise Computing Services (DHS ECS) Strategic Plan," on February 28, 2017 and is currently working with Component CIO organizations to update and deliver the final DHS optimization plan in April 2018. The DHS CIO, or delegations, will be the final decision authority and will provide oversight for execution of the DHS ECS Strategic Plan, exercising appropriate governance to ensure an efficient orchestration of change, and highly adaptive capabilities that must remain within the physical and operational control of the Department. Simultaneously, the DHS and its Component's will continue rationalization of existing systems, applications and data sources while determining the most appropriate cloud service / deployment models for migration. DHS intends to rapidly capitalize on FedRAMP and DHS-approved government and commercial cloud providers to the maximum extent possible to reduce sustainment and operating costs, shorten implementation timelines, more effectively keep pace with emerging technologies, and allow the DHS to take advantage of the larger economies of scale that typically lower costs.
- In accordance with OMB Category Management Policies Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops (15-1) and Mobile Devices and Services (16-3), DHS has established the IT Mobility Sub-Category Management Working Group (MSCM WG) to assist in accomplishing a smooth and transparent transition of current DHS Mobility Managed Service(s) to Next Generation Mobility Managed Service(s). The MSCM WG Charter encompasses mobile, desktop, and laptop devices usage and service. The combination of these device and service categories represents the current DHS mobile computing base and will be considered in DHS's requirements for the evolution of computing technology and next generation enterprise contract solution(s). During FY 2018, the working group will identify Component Mobility related requirements and priorities; validate the delivery of transition activities to satisfy those requirements; and support and drive the planning, execution, monitoring and tracking of the Component transition to the Next Generation Mobility Managed Service(s).
- The 2018 IT Infrastructure Assessment findings and recommendations will be completed by the end of Q2 FY 2018 for input into the DHS budget formulation review and decision process. Further analysis will provide input to the DHS Cloud Strategy that is planned for completion in FY 2018.
- The draft IT infrastructure technology refresh policy will be completed by the Q1 FY 2018 for review and approval by the Under Secretary of Management (USM). An additional policy for Cloud computing will be drafted by Q3 FY 2018 for subsequent review and approval by the USM.
- The Office of the Chief Technology Officer (OCTO) will create an internal high level roadmap of strategy and proposed performance metrics for measuring progress by Q1 FY 2018.
- The OCTO will establish an Open Source Community of Practice (COP) to include representatives from all major DHS components to collaborate and determine existing Open Source repository implementations across DHS by Q2 FY 2018.
- The OCTO will collaborate with Open Source COP and other agencies to compare and combine existing best practices and tools into a consolidated DHS Open Source repository strategy by Q4 FY 2018.
- The OCTO will commence a pilot implementation of Open Source software into a shared repository by Q4 FY 2018.

Low-Priority Program Activities

The President's Budget identifies the lower-priority program activities, as required under the *GPRA Modernization Act*, 31 U.S.C. 1115(b)(10). The public can access the volume at: http://www.whitehouse.gov/omb/budget

Acronyms

ADE – Acquisition Decision Event

AIS – Automated Indicator Sharing

ALOS – Average Length of Stay

APG – Agency Priority Goal

AQI – Agricultural Quarantine Inspection

ARB – Acquisition Review Board

ARM – Agriculture Risk Management

ATS – Automated Targeting System

A&O – Analysis and Operations

BASE – Baseline Assessment for Security Enhancement

BOD – Binding Operational Directive

CA-Plan – Climate Action Plan

CBP – U.S. Customs and Border Protection

CDM – Continuous Diagnosis Mitigation

CERTS – Cargo Enforcement Reporting and Tracking System

CFATS – Chemical Facility Anti-terrorism Standards

CFO – Chief Financial Officer

CHCO – Chief Human Capital Office

CIO – Chief Information Officer

CIP – Critical Infrastructure Protection

CISR – Critical Infrastructure Security and Resilience

COO – Chief Operating Officer

CROPs – Component Recruitment and Outreach Plans

CSD – Cyber Security Division

CSAT – Chemical Security Assessment Tool

CS&C – Office of Cybersecurity and Communications

CTHA – Continued Temporary Housing Assistance

CTO – Chief Technology Office

C-TPAT – Customs-Trade Partnership Against Terrorism

DEFEND – Dynamic Emerging Federal Enterprise Network Defense

DHS – U.S. Department of Homeland Security

DMO – Departmental Management and Operations

DNDO – Domestic Nuclear Detection Office

DOS – Department of State

DPIO – Deputy Performance Improvement Officer

E2C2 – Export Enforcement Coordination Center

EAB – Enterprise Architecture Board

EEI – Employee Engagement Index

EEIWG – Export Enforcement Intelligence Working Group

EITSB – Enterprise IT Services Board

EO – Executive Order

ERO – Enforcement and Removal Operations

ESC – Enterprise Computing Services

EXD – Explosives Division

FAC-P/PM – Federal Acquisition Certification for Program and Project Managers

FEMA – Federal Emergency Management Agency

FEVS – Federal Employee Viewpoint Survey

FIMA - Federal Insurance and Mitigation Administration

FLETC – Federal Law Enforcement Training Centers

FMS – Foreign Military Sales

FPS – Federal Protective Service

FSA - Facility Security Assessment

FY – Fiscal Year

FYHSP – Future Years Homeland Security Program

GAO – Government Accountability Office

GCC - Government Coordinating Council

GFS – Government Facility Sector

GPRA – Government Performance and Results Act

GPRAMA – GPRA Modernization Act

HCOP – Human Capital Operating Plan

HME – Homemade Explosives

HOMECORT – Homeland Criminal Organization Target

HPRDS – Human Portable Rad/Nuc Systems

HQ – Headquarters

HRM – Human Resource Management

HSI – Homeland Security Investigations

HVA – High Value Assets

IC – Intelligence Community

ICE – U.S. Immigration and Customs Enforcement

IEFA – Immigration Examination Fee Account

IPT – Integrated Project Team

IRS – Internal Revenue Service

ISC – Interagency Security Committee

ISP – Internet Service Provider

IT – Information Technology

ITDS – International Trade Data System

I&A – Office of Intelligence and Analysis

JIOCC – Joint Intelligence and Operation Coordination Centers

JOA – Joint Operating Areas

JTF – Joint Task Force

LEO – Law Enforcement Officer

MCO – Mission Critical Occupation

MEXUS – Mexico-US Joint Contingency Plan

MFR – Modular Firing Range

MT – Mandatory Training

MS-13 – Mara Salvatrucha drug cartel/gang

NCATS – National Cybersecurity Assessment and Technical Services

NCCIC – National Cybersecurity and Communications Integration Center

NCEPP – National Cyber Exercise and Planning Program

NCMEC – National Center for Missing and Exploited Children

NCPS – National Cybersecurity Protection System

NFIP – National Flood Insurance Program

NIST – National Institute of Standards and Technology

NOC – National Operations Center

NPPD – National Protection and Programs Directorate

NTAG – National Targeting and Analysis Group

NSSE – National Special Security Event

OCHCO – Office of the Chief Human Capital Officer

OCPO – Office of the Chief Procurement Officer

OCRSO – Office of the Chief Readiness Support Officer

OEWG – Organizational Effectiveness Working Group

OGC – Office of the General Counsel

OHA – Office of Health Affairs

OIG – Office of Inspector General

OMB – Office of Management and Budget

OPCON – Operational Control

OPLA – Office of Principal Legal Advisor

OPM – Office of Personnel Management

OPMAT – Operations Matador

OPS – Office of Operations Coordination

PARM – Program Accountability and Risk Management

PA&E – Office of Program Analysis and Evaluation

PCoE – Protection Center of Excellence

PIO – Performance Improvement Officer

PMDF – Performance Measure Definition Form

PMCO – Priority Mission Critical Occupation

PPA – Program, Project, and Activity

PTI – Priority Trade Issue

RFID – Radio Frequency Identification

RIG – Regional Integration Group

RPM – Radiation Portal Monitors

RVA – Risk and Vulnerability Assessments

SBA – Small Business Administration

STT – Sample Tracking Tool

S&T – Science and Technology Directorate

TCO – Transnational Criminal Organizations

THIRA – Threat and Hazard Identification and Risk Assessment

TRIP – Traveler Redress Inquiry Program

TSA – Transportation Security Administration

USCG – U.S. Coast Guard

USCIS – U.S. Citizenship and Immigration Services

USDA – U.S. Department of Agriculture

USM – Under Secretary for Management

USSS – U.S. Secret Service

VBIED – Vehicle–Borne Improvised Explosive Device

WDP – Workforce Development Plan

WYO – Write-Your-Own

Homeland
Security

Homeland
Security