



# U.S. Department of Homeland Security Annual Performance Report

Fiscal Years 2015 – 2017



Homeland  
Security

# About this Report

---

The *U.S. Department of Homeland Security Annual Performance Report for Fiscal Years (FY) 2015-2017* presents the Department's performance measures and applicable results aligned to our missions, provides the planned performance targets for FY 2016 and FY 2017, and includes information on the Department's Strategic Review and our Agency Priority Goals. In addition, this report presents several FY 2015 Department-wide management initiatives followed by a summary of major management and performance challenges and high-risk areas identified by the DHS Office of Inspector General and the Government Accountability Office. The report is consolidated to incorporate our annual performance plan and annual performance report.

The *FY 2015 – 2017 Annual Performance Report* is one in a series of three reports which comprise the Department's performance and accountability reports:

- ***DHS Agency Financial Report:*** Delivery date – November 13, 2015.
- ***DHS Annual Performance Report:*** Delivery date – February 9, 2016.
- ***DHS Summary of Performance and Financial Information:*** Delivery date – February 16, 2016.

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

For more information, contact:

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

Information may also be requested by sending an email to [par@hq.dhs.gov](mailto:par@hq.dhs.gov) or calling (202) 447-0333.



Homeland  
Security



Visit Our Website  
[www.dhs.gov](http://www.dhs.gov)

## Table of Contents

Introduction .....	2
Organization .....	2
Missions and Goals for Homeland Security .....	3
How Our Measures Align to Our Strategic Plan .....	4
Organizational Performance Management Framework in DHS .....	4
Performance Community .....	5
Annual Process to Review and Improve Performance Measurement .....	6
Performance Data Verification and Validation Process .....	6
Strategic Reviews .....	8
Planning, Programming, Budgeting, and Execution (PPBE) and the Performance Budget.....	10
DHS Performance by Strategic Goal .....	11
Summary of Results and Plan.....	11
Mission 1: Prevent Terrorism and Enhance Security .....	13
Mission 2: Secure and Manage Our Borders .....	27
Mission 3: Enforce and Administer Our Immigration Laws .....	39
Mission 4: Safeguard and Secure Cyberspace.....	48
Mission 5: Strengthen National Preparedness and Resilience.....	64
Mature and Strengthen Homeland Security.....	80
Priority Goals .....	89
FY 2014 – 2015 Agency Priority Goals .....	89
FY 2016 – 2017 Agency Priority Goals .....	94
Cross-Agency Priority Goals.....	97
Management Initiatives .....	99
Unity of Effort .....	99
Customer Service.....	102
Human Capital Management .....	112
Acquisition Management/Strategic Sourcing .....	117
Information Technology .....	118
Sustainability .....	123
Financial Stewardship.....	124
Major Management and Performance Challenges and High-Risk Areas – Summary of Progress .....	126
Low-Priority Program Activities.....	152
Acronym List.....	153

[Appendix A: Measure Descriptions, Data Collection Methodologies, and Verification and Validation Information](#)

[Appendix B: Program Evaluations](#)

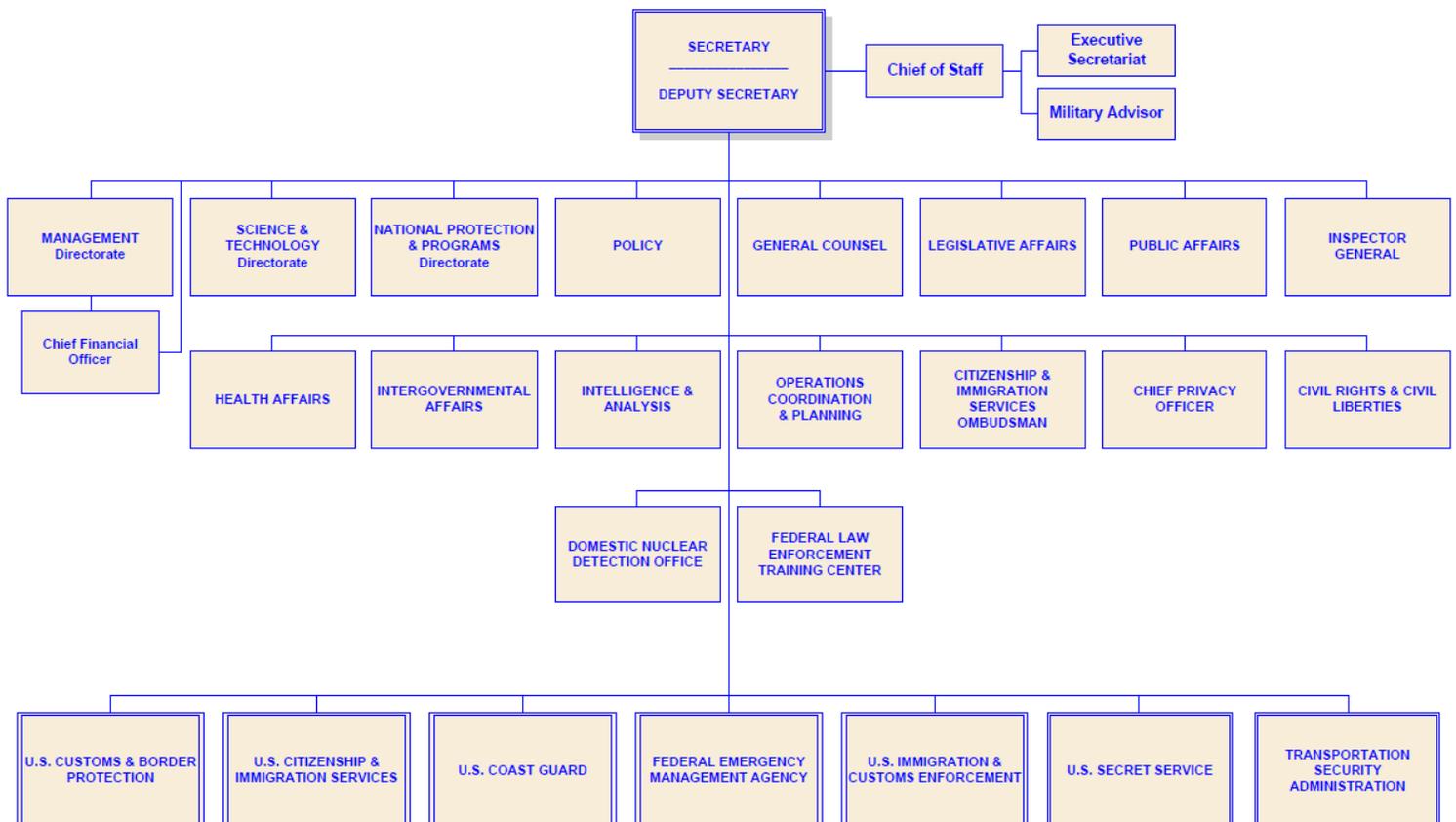
## Introduction

The *U.S. Department of Homeland Security (DHS) Annual Performance Report (APR) for Fiscal Years (FYs) 2015-2017* presents the Department’s performance measures and applicable results for FY 2015, associated performance targets for FY 2016 and FY 2017, and includes information on the Department’s FY 2015 Strategic Review and our Agency Priority Goals (APGs). In addition, this report presents several FY 2015 Department-wide management initiatives followed by a summary of major management and performance challenges and high-risk areas identified by the DHS Office of Inspector General and the Government Accountability Office.

The FY 2015-2017 APR satisfies the *Government Performance and Results Act (GPRA)* and the *GPRA Modernization Act (GPRAMA) of 2010* requirement to publish the Department’s Annual Performance Report and Annual Performance Plan.

## Organization

DHS’s operational Components lead the Department’s frontline activities to protect our Nation. The remaining DHS Components 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>.



## Missions and Goals for Homeland Security

Performance information in this report is organized around the missions and goals identified in the Department's [FY 2014-2018 Strategic Plan](#). The *FY 2014-2018 Strategic Plan* continues the Department's efforts to prioritize front-line operations while maximizing effectiveness and efficiency. The missions and goals of the Department are provided below.

### Mission 1: Prevent Terrorism and Enhance Security

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

### Mission 2: Secure and Manage Our Borders

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

### Mission 3: Enforce and Administer Our Immigration Laws

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

### Mission 4: Safeguard and Secure Cyberspace

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

### Mission 5: Strengthen National Preparedness and Resilience

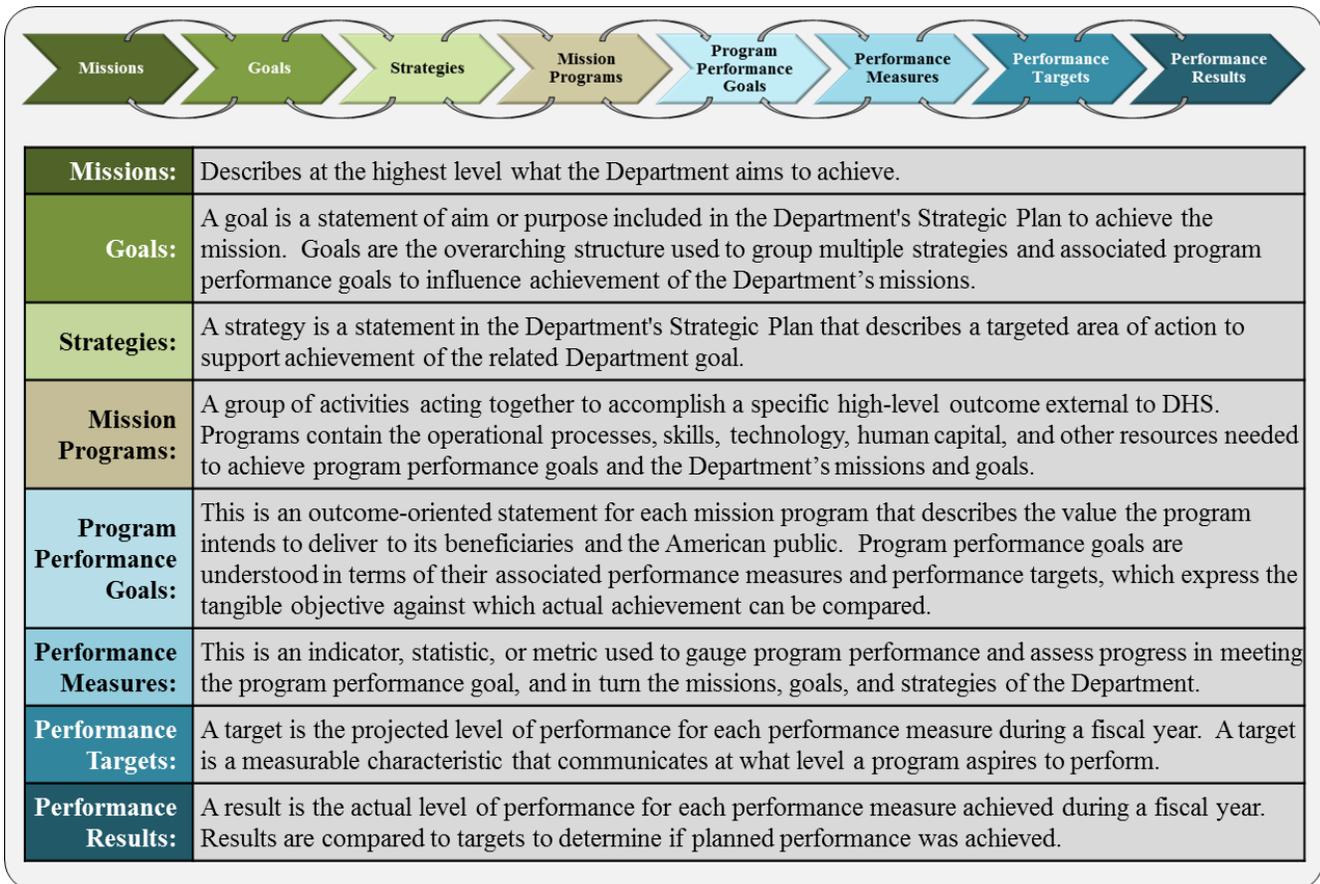
- Goal 5.1: Enhance National Preparedness
- Goal 5.2: Mitigate Hazards and Vulnerabilities
- Goal 5.3: Ensure Effective Emergency Response
- Goal 5.4: Enable Rapid Recovery

### Mature and Strengthen Homeland Security

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

## How Our Measures Align to Our Strategic Plan

The figure below shows the linkage between our strategic plan, the Department’s mission programs, and the measures we use to gauge performance. This approach to measurement ensures that DHS can assess the achievement of our missions as identified in our strategic framework. In the following section, we describe our performance management framework and how this gets implemented.



## Organizational Performance Management Framework in DHS

DHS created a robust performance framework that drives performance management and enables the implementation of performance initiatives. This approach also facilitates the reporting of results within the Department for a comprehensive set of measures aligned to the missions and goals of the Department. The DHS Organizational Performance Management Framework consists of:

- The DHS performance community;
- An annual process to review and improve performance measures;
- A rigorous measure verification and validation process;
- The quarterly reporting and review of performance measure results;

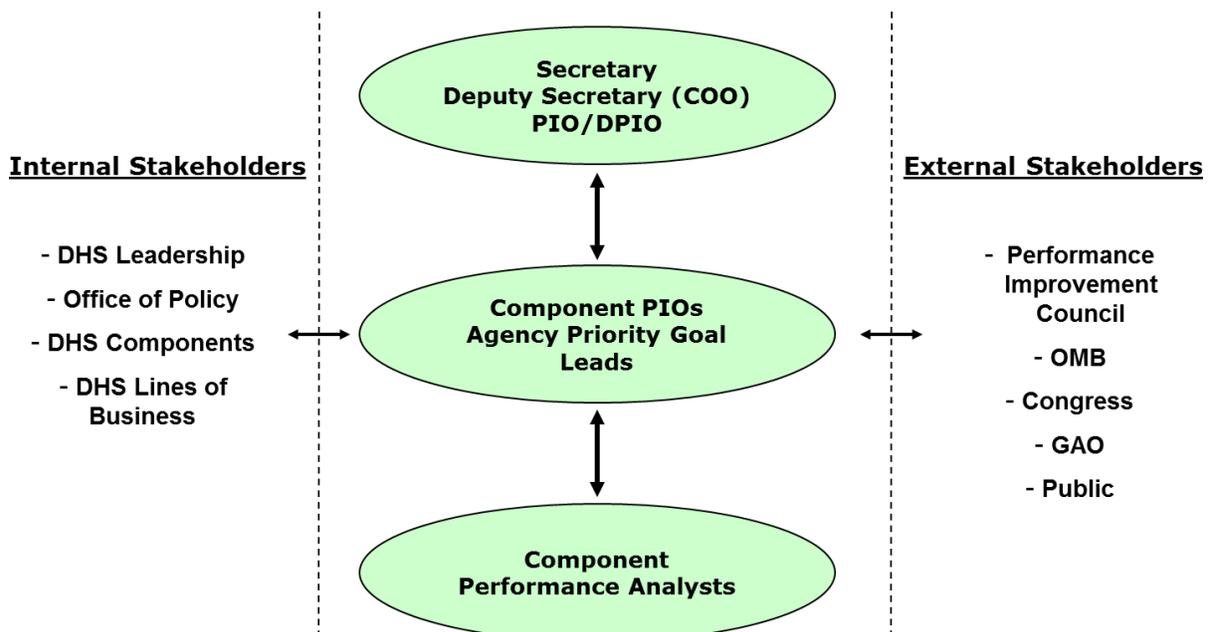
- A web-based system for performance data;
- An annual Strategic Review; and
- The development of a performance budget in conjunction with the Department’s Planning, Programming, Budgeting, and Execution (PPBE) process.

## Performance Community

The DHS performance community is led by the Chief Operating Officer (COO), the Performance Improvement Officer (PIO), and the Deputy PIO (DPIO) who are supported by the Office of Program Analysis and Evaluation (PA&E) located under the 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 APG Leads, the senior leaders driving performance management efforts in their respective Components, and 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, CFO/PA&E performance analysts facilitate and manage GPRAMA performance initiatives for the Department under the direction of the COO, PIO, and DPIO 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.

*DHS Organizational Performance Community*



## Annual Process to Review and Improve Performance Measurement

With the support of leadership, CFO/PA&E initiates the annual measure improvement process each spring to enhance our set of publicly reported measures to more effectively convey the results delivered to meet our missions. 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. This process typically begins in March, with proposed changes from programs in DHS Components submitted 30 June each year. These proposals are reviewed by Component leadership and by Headquarters performance analysts. Approved changes are then submitted to OMB for their review and approval. Our publicly reported measures associated with our performance budget deliverables are then published in the Department's APR, the Component Strategic Context Chapters of the Congressional Justification, the Future Years Homeland Security Program (FYHSP) Report to Congress, and support other strategic management processes such as Senior Executive Service certification and personnel performance plans.

## Performance Data Verification and Validation Process

The Department recognizes the importance of collecting complete, accurate, and reliable performance data since this helps determine progress toward achieving program and Department goals and objectives. 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 agency heads to attest to the completeness and reliability of the performance data they report and put procedures in place to ensure valid data as part of the Management Assurance process.

DHS 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 the: 1) Performance Measure Definition Form (PMDF); 2) Performance Measure Checklist for Completeness and Reliability; and 3) annual assessments of the completeness and reliability of a sample of our performance measures by an independent review team.

### *Performance Measure Definition Form (PMDF)*

CFO/PA&E implemented 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. This information is maintained in a Department IT system, and is published annually as Appendix A to our Annual Performance Report. The PMDF is also 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. GAO recently cited DHS's thoroughness in collecting and reporting this information in their review of the quality of performance information in their report: *Managing for Results: Greater Transparency Needed in Public Reporting Quality of Performance Information for Selected Agencies' Priority Goals* ([GAO-15-788](#)).

### ***Central Information Technology Repository for Performance Measure Information***

All of DHS's approved measures are maintained in a Department-wide 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 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 is then used as the source for all quarterly and annual Performance and Accountability Reporting. Finally, the performance data in the FYHSP System is 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 Secretary's assertion whether or not the Department has effective controls over financial and performance reporting as well as efficiencies of our operations.

### ***Independent Assessment of the Completeness and Reliability of Performance Measure Data***

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. An independent review team assesses selected Component GPRAMA measures using the methodology prescribed in the *DHS Performance Measure Verification and Validation Handbook*, documents their findings, makes recommendations for improvement, and may perform a subsequent follow-up review to observe the implementation of recommendations. Corrective actions are required for performance measures determined to be unreliable. The Handbook is distributed and 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 Head assertions over the reliability of its performance information reported in the Performance Measure Checklist and

Component Head Assurance Statement. DHS has shared our process with other Agencies in support of their measure data verification and validation improvement efforts.

***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 attesting to the completeness and reliability of performance measure information in our Performance and Accountability Reports. 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):

- Performance Measure: Percent of adults that participated in a preparedness exercise or drill at their workplace, school, home or other community location in the past year (Federal Emergency Management Agency (FEMA))
  - In an effort to streamline the survey in FY 2015, FEMA shortened the composite questions that provided data for this measure resulting in a methodology error. FEMA has taken corrective action to return to the original methodology in the FY 2016 survey.

**Strategic Reviews**

DHS conducted its second annual Strategic Review of progress and results delivered for the 16 strategic goals in the DHS FY 2014-2018 Strategic Plan. For each strategic goal, an assessment team was guided by a senior executive who assembled a team from Components who play a significant role in implementing operations that affect goal performance. DHS leveraged the expertise of those working directly to advance progress on the strategic goals to conduct the first phase of the review, which is a self-assessment. Then a Headquarters team conducted a cross cutting review, independently and then as a team, by examining the findings from the 16 assessment teams. This analysis is summarized with major conclusions and recommendations and used for leadership discussion.



The Assessment Teams conducted their review during the January to March timeframe, the Headquarters review occurred in April, and leadership briefings and delivery of summary results to OMB occurred in May. This approach is designed to support the OMB-established timeline in order to make the information available to the Agency and OMB during the budget development process. The assessment teams involved over 250 participants who used a variety of evidence to evaluate progress in four areas: performance results, learning and innovation, planning and foresight, and challenges and opportunities. Assessment teams provided summaries of progress in these four assessment areas, along with highlighting accomplishment and challenges using results delivered and evidence from FY 2014 and the first quarter of FY 2015 if available.

The following graphic identifies the progress findings<sup>1</sup> for all 16 mission goals evaluated. Detailed Summaries of Progress are provided for each goal in the [DHS Performance by Strategic Goal](#) section.

 <h2 style="text-align: center;">Strategic Review Progress Results</h2>				
Mission 1 Prevent Terrorism and Enhance Security	Mission 2 Secure and Manage Our Borders	Mission 3 Enforce and Administer Our Immigration Laws	Mission 4 Safeguard and Secure Cyberspace	Mission 5 Strengthen National Preparedness and Resilience
				
Goal 1.1: Prevent Terrorist Attacks	Goal 2.1: Secure U.S. Air, Land, and Sea Border and Approaches	Goal 3.1: Strengthen and Effectively Administer the Immigration System	Goal 4.1: Strengthen the Security and Resilience of Critical Infrastructure against Cyber Attacks and other Hazards	Goal 5.1: Enhance National Preparedness
Goal 1.2: Prevent and Protect Against the Unauthorized Acquisition or Use of CBRN Materials and Capabilities	Goal 2.2: Safeguard and Expedite Lawful Trade and Travel	Goal 3.2: Prevent Unlawful Immigration	Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise	Goal 5.2: Mitigate Hazards and Vulnerabilities
Goal 1.3: Reduce Risk to the Nation's Critical Infrastructure, Key Leadership, and Events	Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations and Other Illicit Actors		Goal 4.3: Advance Cyber Law Enforcement, Incident Response, and Reporting Capabilities	Goal 5.3: Ensure Effective Emergency Response
			Goal 4.4: Strengthen the Cyber Ecosystem	Goal 5.4: Enable Rapid Recovery
<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="border: 1px solid black; padding: 5px; background-color: #0070C0; color: white; text-align: center;">Noteworthy Progress</div> <div style="border: 1px solid black; padding: 5px; background-color: #70AD47; color: white; text-align: center;">Satisfactory Performance</div> <div style="border: 1px solid black; padding: 5px; background-color: #FFD700; color: black; text-align: center;">Focus Areas for Improvement</div> </div>				

<sup>1</sup> OMB Circular A-11 directs all CFO Act agencies to identify a subset of goals as “Demonstrating Noteworthy Progress” and a subset of goals as “Focus Areas for Improvement.”

## Planning, Programming, Budgeting, and Execution (PPBE) and the Performance Budget

Performance management is relevant to each stage of the Department's PPBE process. PPBE is an annual process that incorporates long-term strategic planning and serves as the basis for developing the Department's annual budget submission and out year spending profile as enumerated in the FYHSP Report to Congress, in accordance with the provisions of the [Homeland Security Act of 2002](#).

In Planning, goal setting, risk assessment, and mission scoping are conducted to determine and prioritize the capabilities necessary to deliver results aligned to the DHS Strategic Plan. In Programming, resources are allocated to best meet the prioritized needs within projected resources, considering potential performance gains in the process. In Budgeting, budget estimates are developed ensuring the efficient and effective use of funding to meet priorities and the planned levels of performance are integrated with the levels of funding requested. Finally, in Execution, program execution and performance results are compared to plans to assess accomplishments and shortfalls, and to inform future execution efforts and the other phases of the PPBE cycle.

To further Department-wide PPBE integration, Secretary Johnson issued the "[Strengthening Departmental Unity of Effort](#)" initiative in 2014 that continues today. In this initiative, the Secretary directed specific activities across four main lines of effort: inclusive senior leader discussion and decision-making forums that provide an environment of trust and transparency; strengthened management processes for investment, including requirements, budget, and acquisition processes, that look at cross-cutting issues across the Department; focused, collaborative Departmental strategy, planning, and analytic capability that supports more effective DHS-wide decision-making and operations; and enhanced coordinated operations to harness the significant resources of the department more effectively. These changes have led to better traceability through each step of the PPBE process, while supporting our broader goal of better understanding of the broad and complex DHS mission space, and empowering DHS Components to effectively execute their operations.

## DHS Performance by Strategic Goal

This section of the Annual Performance Report provides an analysis of the Department’s performance aligned with the goals in the DHS FY 2014 – 2018 Strategic Plan.

### Summary of Results and Plan

When reviewing the results at the close of FY 2015, 64 percent of the Department’s measures<sup>2</sup> met their targets. The results for the percent of measures that met their targets by mission are shown in the table below by the black diamond. When looking at trends in the results, 77 percent of measures sustained or improved performance from FY 2014; the results by mission for those that sustained or improved is shown in the table below by the white diamond. The FY 2016-2017 performance plan includes a total of 91 measures, representing 9 measures that were retired from our previous performance plan and the introduction of 15 new measures.

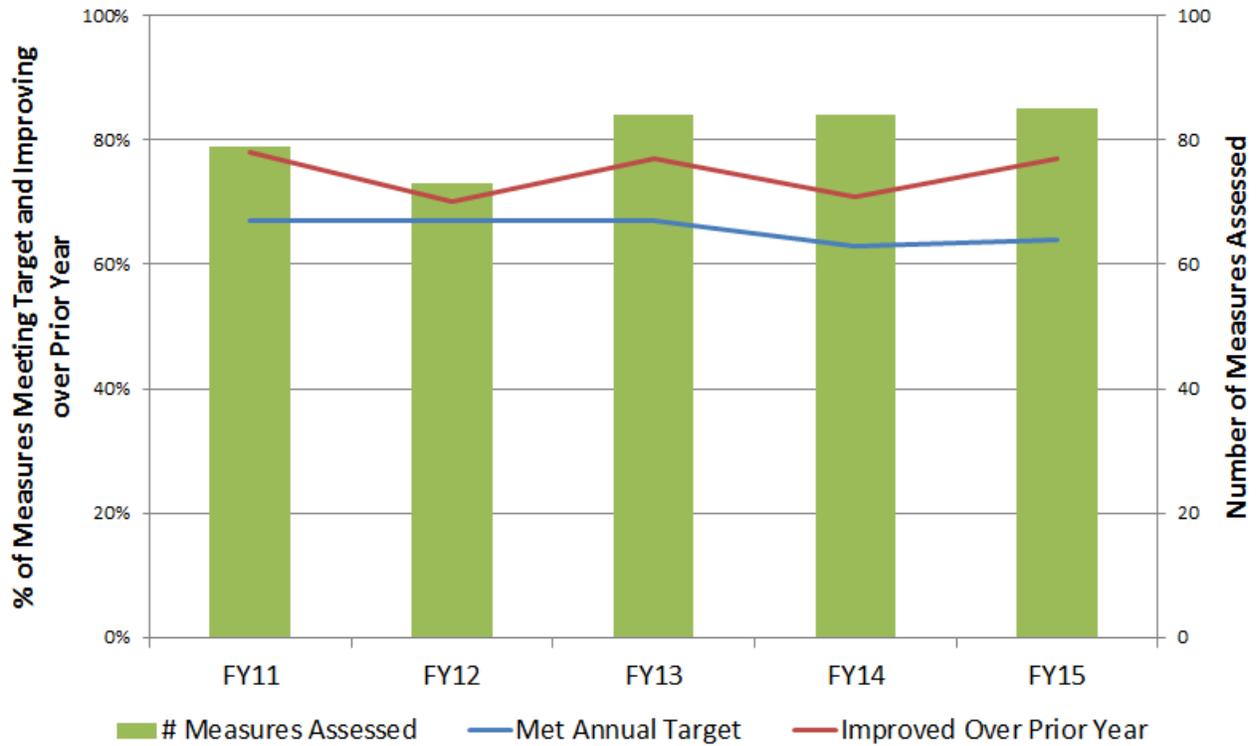
Mission	Performance Summary					
	Scale:	0%	25%	50%	75%	100%
Mission 1: Prevent Terrorism and Enhance Security				◆		◆
Mission 2: Secure and Manage Our Borders			◆◆			
Mission 3: Enforce and Administer Our Immigration Laws			◆◆			
Mission 4: Safeguard and Secure Cyberspace				◆		◆
Mission 5: Strengthen National Preparedness and Resilience				◆		◆

◆ - Percent of measures that met their FY 2015 target.

◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

This year’s overall results are consistent with historical results. The chart on the following page shows that the measures meeting their target on an annual basis varied between 63 to 67 percent from FY 2011 through FY 2015. Likewise, the percent of measures that maintained or improved over the prior year ranged from 71 to 78 percent.

<sup>2</sup> This report presents our “strategic set” of measures. These measures have been developed over time to align with the strategy published in the DHS FY 2014 – 2018 Strategic Plan, as required by GPRAMA. These measures best communicate our progress in the delivery of results and the assessment of our success in achieving our strategic goals. DHS also manages a larger set of measures, known as our “management set.” These measures are available in the Strategic Context chapter of each Component’s Congressional Budget Justification located on the DHS budget webpage at: <http://www.dhs.gov/dhs-budget>. In addition, Components and their programs manage a large number of operational measures to inform program management and specific implementation activities. Our capital investment plans for major investments also contain measures that relate to key performance indicators and may link to our strategic or management measures sets.



The remainder of the report presents information for each of our strategic goals. Each goal begins with a statement of the goal and its strategies, which are described in more detail in the FY 2014-2018 DHS Strategic Plan. Next, a *Strategic Review Summary of Progress* narrative is presented as a result of the Department’s Strategic Review assessment. This is followed by *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. Finally, to continually improve our set of performance measures, new measures are introduced and measures are retired each year and are identified in the measure tables.

## Mission 1: Prevent Terrorism and Enhance Security

### Goal 1.1: Prevent Terrorist Attacks

#### Strategies

- *Analyze, fuse, and disseminate terrorism information*
- *Deter and disrupt operations*
- *Strengthen transportation security*
- *Counter violent extremism*

#### Strategic Review Summary of Progress

Assessment Lead      Ken Fletcher, Chief Risk Officer, Transportation Security Administration (TSA), Office of the Chief Risk Officer

The Department of Homeland Security (DHS), in consultation with the Office of Management and Budget (OMB), has determined that performance toward this goal is making noteworthy progress.

#### Introduction

DHS applies a multifaceted approach to preventing terrorist attacks in the United States, focusing on risk-based passenger and cargo screening, intelligence and information-sharing, and working beyond our borders to deter and disrupt threats at the earliest point possible. DHS performs and oversees security operations at the Nation's airports, screening hundreds of millions of passengers annually to ensure the freedom of movement of people and commerce. Through these efforts, DHS has continued to increase security, achieve system-wide efficiencies, and shortened wait times for the traveling public.

#### Major Achievements

DHS continues to fuse and analyze information from the Intelligence Community, other government agencies, and our foreign partners. DHS created and disseminated products—such as *Roll Call Releases*, *Joint Intelligence Bulletins*, *Intelligence Assessments*, and *TRIPwire*—to frontline security and law enforcement partners to assist in their counterterrorism efforts.

DHS developed new technologies to aid in video surveillance, biometrics, and identity management to be used to detect, deter, and disrupt potential terrorist activities. DHS reduces risk of the flow of passengers and commerce by scanning cargo identified as high risk, updating terrorist watchlists used in vetting and screening operations, implementing biometric vetting systems to better assess immigration benefits applicants, and enhancing security at maritime and surface transportation facilities.

DHS enrolled over 3.6 million travelers in its Trusted Traveler Programs, advanced participation by 11 airlines, and implemented some form of expedited aviation/customs and immigration screening at over 120 airports as of September 30, 2014. These efforts increased security effectiveness, improved the passenger experience, and achieved efficiencies through targeted reallocation of screening resources.

DHS created programs to counter violent extremism, including Community Awareness Briefings and Community Resiliency Exercises to help communities understand and address terrorist recruitment tactics, and to build partnerships between communities and law enforcement. In addition, DHS held over 100 community engagement events (as of September 30, 2014) and provided cultural competency trainings to law enforcement personnel across the country.

Major Challenges & Opportunities for Improvement

A dynamic threat environment—coupled with lengthy technology development, testing, acquisition, and deployment processes—presents challenges in quickly responding with the most current technology. Consequently, DHS must accurately determine the best use of resources in most efficiently and effectively fulfilling its mission. Intelligence-driven, risk-based approaches, supported by streamlined operations, have proven successful in several instances. Public-private partnerships also present opportunities to share security costs. The implementation of risk-based screening to identify potential threats while providing a positive experience for the traveling public is a careful balancing act. DHS is responding to information released by the DHS Office of the Inspector General after this review was completed so as to best manage risk, cost, and impact on the traveling public.

**Performance Highlight**

Below is a highlighted accomplishment demonstrating our efforts to prevent terrorist attacks.



**Record Number of Firearms Detected at Passenger Checkpoints**

Over the past decade, TSA has developed a highly trained federal workforce that has safely screened more than five billion airline passengers and their possessions, and established a multi-layered security system reaching from curb to cockpit. Every day, in airports around the country, TSA Transportation Security Officers (TSO) routinely detect prohibited items in carry-on and checked bags, as well as on passengers. In May 2015 alone, TSOs intercepted a record 243 firearms at airport security checkpoints and prevented the illegal transport of such items on airplanes. In FY 2015,

TSOs detected more than 2,547 firearms, in addition to thousands of knives, weapons, and other prohibited items.

TSA continues to focus on risk-based, intelligence-driven security procedures, to direct greater focus on high-risk passengers while still maintaining an effective overall security program, as evidenced by the volume of prohibited items found at airport security checkpoints.

**Performance Results and Plan**

In FY 2015, there were eleven performance measures used to assess the Department’s efforts for this goal. For the FY 2016-2017 performance plan, three new measures are being introduced and three measures are being retired. In FY 2015, 64 percent of the measures met their target and 100 percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary					
	Scale:	0%	25%	50%	75%	100%
Goal 1.1: Prevent Terrorist Attacks						

- ◆ - Percent of measures that met their FY 2015 target.
- ◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below are two highlighted strategic measures that gauge efforts to prevent terrorist attacks.

Percent of intelligence reports rated “satisfactory” or higher in customer feedback that enable customers to understand the threat (Analysis and Operations (AO))								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	90%	93%	95%	94%	95%	94%	94%

This measure gauges the extent to which the DHS Intelligence Enterprise is satisfying its customers' needs related to anticipating emerging threats. This measure encompasses reports produced by all DHS component intelligence programs and provided to federal, state, and local customers. This measure aggregates customer ratings of the relevance, timeliness, and usefulness of intelligence reports disseminated. The annual target was met based on voluntary customer response to a survey attached to the subset of finished intelligence reports and is consistent with previous results.

Percent of international air enplanements vetted against the terrorist watch list through Secure Flight (TSA)								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	100%	100%	100%	100%	100%	100%	100%	100%

Secure Flight is a risk-based passenger prescreening program that enhances security by identifying passengers by potential risk before they arrive at the airport by matching their names against trusted traveler lists and watchlists. This serves to prevent individuals on the No Fly List from boarding an aircraft and to identify individuals for enhanced screening. After matching passenger information against government watch lists, Secure Flight transmits the matching results back to airlines before they can issue passenger boarding passes. TSA continues to vet 100 percent of international air enplanements against the terrorist watch list for those known or suspected terrorists with a full name and date of birth through the Secure Flight Program and has maintained this achievement for the past five years.

The remaining strategic measures used to gauge our efforts to prevent terrorist attacks are displayed below. For those measures that did not meet their targets, an explanation with corrective action is provided. In addition, changes to measure names and targets from the previous year’s report are identified.

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
<b>TSA</b>									
Percent of overall compliance of domestic airports with established aviation security indicators	96.0%	95.9%	95.0%	94.4%	94.0%	100%	95.0%	100%	100%
The performance results indicate the percentage which domestic airports have been found to comply with transportation security regulations through TSA inspections. TSA aggressively works with the airports and air carriers to ensure they comply with all security requirements and takes enforcement and other actions when necessary. TSA has taken actions to increase the rate of									

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
compliance, including increased industry outreach and Compliance Security Enhancement Through Testing activities, a risk-based testing program for leading security indicators.									
Average number of days for DHS Traveler Redress Inquiry Program (TRIP) redress requests to be closed	---	99	93	52	62	< 70	50	< 60	< 60
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	---	---	---	100%	100%	100%	100%	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	23%	28%	39%	69%	78%	82%	80%	86%	86%
Results were impacted by changes in the American Public Transportation Association assessment criteria which increased the number of mass transit and passenger rail systems included in the measure. Baseline Assessment for Security Enhancement (BASE) assessments were conducted during Q4 for these systems but none were officially closed during this time. Surface Inspectors will continue meeting with the transit agency to provide them with guidance on improving their BASE scores. The guidance consists of best practices specific to the Security Action Items (SAI) on which the transit agency scored poorly and also giving the agency contact information for other transit agencies that have scored well on that particular SAI, so the transit agencies can learn from their peers.									
Percent of air carriers operating from domestic airports in compliance with leading security indicators	98.0%	99.2%	98.1%	98.0%	98.0%	100%	98.0%	100%	100%
The performance results indicate the percentage of air carriers found to comply with transportation security regulations through TSA inspections. TSA aggressively works with the airports and air carriers to ensure they comply with all security requirements and takes enforcement and other actions when necessary. TSA has taken actions to increase the rate of compliance, including increased industry outreach and Compliance Security Enhancement Through Testing activities, a risk-based testing program for leading security indicators.									
Percent of air cargo screened on commercial passenger flights originating from the United States and territories	100%	100%	100%	100%	100%	100%	100%	Retired <sup>1</sup>	
Percent of domestic cargo audits that meet screening standards	---	---	---	---	---	New Measure		95%	96%

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
Percent of inbound air cargo screened on international passenger flights originating from outside the United States and Territories	---	---	93.0%	99.5%	100%	100%	100%	Retired <sup>2</sup>	
Percent of international cargo audits that meet screening standards	---	---	---	---	---	New Measure		95%	96%
Percent of domestic air enplanements vetted against the terrorist watch list through Secure Flight	---	100%	100%	100%	100%	100%	100%	100%	100%
Number of daily travelers eligible to receive expedited physical screening based on assessed low risk	---	---	---	---	698,025	900,000	891,802	Retired <sup>3</sup>	
<p>During FY 2015, TSA re-balanced the risk level accepted through expedited screening in response to changes in threat and recommendations from the DHS Inspector General. As part of the shift in emphasis, TSA removed or decreased opportunities for travelers to receive expedited screening without directly enrolling in a DHS Trusted Traveler Program. These changes impacted the ability to reach the FY 2015 goal of 900,000 travelers. TSA continues to increase the population of known travelers, expand airline and airport participation in TSA Pre✓<sup>®</sup>, and conduct risk assessments to increase the number of passengers eligible for expedited screening.</p>									
Percent of daily passengers receiving expedited physical screening based on assessed low risk	---	---	---	---	---	New Measure		50%	50%

- Note 1: TSA is retiring this measure and introducing the measure “Percent of domestic cargo audits that meet screening standards” as it more accurately assesses performance. Measuring cargo screening audits is a much more effective measure of cargo screening security because it directly reflects TSAs actions and abilities to affect screening compliance of shippers.
- Note 2: TSA is retiring this measure and introducing the measure “Percent of international cargo audits that meet screening standards” as it more accurately assesses performance. Measuring cargo screening audits is a much more effective measure of cargo screening security because it directly reflects TSAs actions and abilities to affect screening compliance of shippers.
- Note 3: TSA is unable to control the number of people who fly so the measure “Percent of daily passengers receiving expedited physical screening based on assessed low risk” is being introduced to better reflect the goal of expedited screening operations.

## Mission 1: Prevent Terrorism and Enhance Security

### *Goal 1.2: Prevent and Protect Against the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities*

#### Strategies

- *Anticipate chemical, biological, radiological, and nuclear emerging threats*
- *Identify and interdict unlawful acquisition and movement of chemical, biological, radiological, and nuclear precursors and materials*
- *Detect, locate, and prevent the hostile use of chemical, biological, radiological, and nuclear materials and weapons*

#### Strategic Review Summary of Progress

Assessment Lead      John Zabko, Assistant Director, Domestic Nuclear Detection Office (DNDO), Architecture & Plans Directorate

The Department of Homeland Security (DHS) has determined that performance toward this goal is making satisfactory progress.

#### Introduction

DHS Components implemented programs to enhance the security of the global supply chain and chemical facilities; biological threat detection and surveillance; and nuclear detection efforts and nuclear forensics activities (investigation of nuclear materials to find evidence to support attribution of the materials and identification and prosecution of smuggling networks). These programs have improved and sustained a reduction in the risks of chemical, biological, radiological, and nuclear (CBRN) threats.

#### Major Achievements

In coordination with federal partners, DHS Components led interagency planning efforts, risk assessments, and requirements development activities to address the threat of CBRN terrorism. DHS Components also supported capacity building efforts and worked collaboratively through training, exercises, and technical exchange programs for CBRN security issues, nuclear forensics, and risk analysis with international, federal, state, local, tribal, and territorial, and private sector partners.

As of September 30, 2014, DHS conducted over 1,000 inspections at high-risk chemical facilities and approved nearly 900 chemical facility site security plans (SSPs) under the Chemical Facility Anti-Terrorism Standards (CFATS) program. In recognition of DHS's work to implement and improve chemical facility security, Congress enacted the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (the Act) (P.L. 113-254), providing long-term authorization for CFATS to ensure DHS has the authority necessary to more effectively protect these facilities.

The Department's Joint Requirements Council formed topic-specific teams to conduct CBRN assessments to identify common capability needs and challenges. The Department also invested in

technology evaluations that are shaping global standards and knowledge about equipment. Homeland security research and development is transitioning from laboratories to manufacturers and operators including two models of handheld chemical vapor detectors and new scintillator materials ready for manufacturers to use in detectors that will improve radiological and nuclear detection capabilities.

#### Major Challenges & Opportunities for Improvement

DHS is actively looking at the challenges and opportunities legislative authorization provides in terms of guiding the work being done within the Department to enhance security. Legislative authority helps clarify requirements related to CBRN and may assist in engaging partners to ensure compliance. For example, CFATS legislation gives the Department a unique opportunity to strengthen the CFATS program, but also requires a number of activities to be completed in relatively short timeframes, while continuing to implement the CFATS program. Meeting these new requirements and developing updated regulations while implementing the CFATS program at its current pace will be a challenge. In addition, DHS is reviewing capabilities and risk assessments to align operator training and equipment selection to ensure future operational tactics and procedures address emerging threats.

#### **Performance Highlight**

Below is a highlighted accomplishment demonstrating our efforts in detecting nuclear and radiological materials.



#### **Improving Security and Efficiency at U.S. Ports of Entry**

Purchased by DNDO and operated by U.S. Customs and Border Protection (CBP), Radiation Portal Monitors (RPMs) are deployed at our ports of entry to scan incoming maritime containerized cargo, trucks, and personally-owned vehicles for radiological or nuclear threats prior to entering the United States. However, there are many legitimate uses for radioactive materials, including medical and industrial uses, and these materials are often present in the stream of commerce and people entering our borders. In addition to scanning for threats, the monitors routinely discover these benign radioactive materials, resulting in a significant

operational burden for CBP officers who resolve these types of alarms.

In order to improve the efficiency of security measures to ensure the flow of legitimate commerce and travelers, CBP and DNDO worked closely to implement a new approach using revised operational settings for deployed RPM systems. Through the implementation of the revised setting, alarm rates have been reduced at seaports by an average of 78 percent and at land border crossings by an average of 44 percent, equating to a reduction of more than 200,000 RPM alarms per year. The reduction in RPM alarm rates and decrease in secondary security inspections permitted officers in the field to be redirected to other high priority law enforcement duties and made selected RPMs available for refurbishment and redeployment. As a result, the Department improved performance, gained efficiency at ports, and secured the Nation against radiological and nuclear threats. DNDO and CBP are continuing to collaborate to identify capabilities to further improve security and operational efficiencies at Ports of Entry.

**Performance Results and Plan**

In FY 2015, there were four performance measures used to assess the Department’s efforts in this goal. In FY 2015, 75% percent of the measures met their target and 100% percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary					
	Scale:	0%	25%	50%	75%	100%
Goal 1.2: Prevent and Protect Against the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities					◆	◆

◆ - Percent of measures that met their FY 2015 target.

◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below are two highlighted strategic measures that gauge efforts to prevent and protect against the unauthorized acquisition or use of chemical, biological, radiological, and nuclear materials and capabilities.

**Number of people covered by Securing the Cities program preventive radiological and nuclear (rad/nuc) detection capabilities (in millions) (DNDO)**

FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	---	23.0	23.0	23.0	37.0*	37.0

The Securing the Cities (STC) program provides financial assistance to state, local, and tribal organizations to develop a robust regional radiological/nuclear detection program. For the STC program to count the population as covered by a robust radiological/nuclear detection capability, the region must demonstrate that 10% or more of its standing law enforcement are trained and equipped to conduct primary screening and patrolling as part of their daily routine duties and there are equipped and trained personnel to conduct secondary screening and alarm adjudication. In addition, the region must conduct at least one multi-jurisdictional exercise a year, and allow the exchange of information among regional partners and with federal agencies, and mutually assist each other in performing the radiological/nuclear detection mission. The Securing the Cities program continues to provide indirect support of the development and sustainment of radiological and nuclear detection capabilities in the greater New York City / Jersey City / Newark region, which covers 23 million people. Work is ongoing in the Los Angeles and Long Beach, California region and the National Capital Region in Washington, DC that will enable the Domestic Nuclear Detection Office to meet future goals.

\* Note: The FY 2016 target previously published as 37.5 in the FY 2014 – 2016 Annual Performance Report was changed to 37.0 based on updated program implementation planning.

**Percent of performance standards implemented by the highest risk chemical facilities and verified by DHS (National Protection and Programs Directorate)**

FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	46%	78%	95%	93%	95%	95%

This measure reports the percent of risk based performance standards that are approved and implemented within site security plans or alternative security programs for Tier 1 and Tier 2 facilities that are compliant with CFATS regulation. Over the past two years, the CFATS program has made significant progress, inspecting and approving nearly all Tier 1 and 2 regulated facilities.

Due to previously approved facilities no longer contributing to the result, the target for FY 2015 was narrowly missed. Plans are in place to meet the target of 95 percent in FY 2016. The CFATS program target is set below 100 percent based on a changing population of regulated facilities and the multiple steps necessary to reach the approval stage. The CFATS program is an important part of our Nation’s counterterrorism efforts as the Department works with our industry stakeholders to keep dangerous chemicals out of the hands of those who wish to do us harm. Since the CFATS program was created, we have engaged with industry to identify and regulate high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with the possession of chemicals of interest.

The remaining strategic measures are used to gauge our efforts to prevent and protect against the unauthorized acquisition or use of radiological and nuclear materials and capabilities. Due to the potential impact on national security, the information for these measures is For Official Use Only (FOUO).

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
<b>DNDO</b>									
Percent of cargo conveyances that pass through radiation portal monitors upon entering the nation via land border and international rail ports of entry	FOUO	FOUO	FOUO	FOUO	FOUO	FOUO	FOUO	FOUO	FOUO
Percent of containerized cargo conveyances that pass through radiation portal monitors at sea ports of entry	FOUO	FOUO	FOUO	FOUO	FOUO	FOUO	FOUO	FOUO	FOUO

## Mission 1: Prevent Terrorism and Enhance Security

### *Goal 1.3: Reduce Risk to the Nation's Critical Infrastructure, Key Leadership, and Events*

#### Strategies

- *Enhance security for the Nation's critical infrastructure from terrorism and criminal activity*
- *Protect key leaders, facilities, and national special security events*

#### Strategic Review Summary of Progress

Assessment Lead John Eric Skelton, U.S. Secret Service (USSS), Deputy Assistant Director

The Department of Homeland Security (DHS), in consultation with the Office of Management and Budget (OMB), has highlighted this goal as a focus area for improvement.

#### Introduction

The American way of life depends upon the effective functioning of the nation's critical infrastructure and key resources, and the protection of key leaders and events. Due to a variety of challenges in program execution for protective services provided by the USSS and the ability to protect critical infrastructure and improve federal building security, this goal is as a focus area for improvement.

#### Major Achievements

The USSS continued to prevent and defend against attacks on protected persons, locations, and events, to protect the integrity of U.S. currency, and to successfully prosecute individuals conducting financial crimes.

To improve security for the Nation's critical infrastructure, the National Protection and Programs Directorate (NPPD) published the [Joint National Priorities for Critical Infrastructure Security and Resilience](#) in October 2014. In addition, the Federal Protective Service (FPS), at the direction of DHS leadership, enhanced its presence and security at high risk federal buildings and the surrounding communities in targeted cities throughout the country by deploying staff to augment the existing law enforcement staffing in those cities to meet surge operational objectives. NPPD also developed national and departmental policies on countering improvised explosive devices and worked with Intelligence & Analysis to publish a strategic threat assessment for the Electricity subsector. The U.S Coast Guard (USCG) conducted domestic port security vulnerability assessments, and coordinated support for protective operations during National Special Security Events. The Office of Operations Coordination performed risk assessments for nearly 8,000 special events (as of September 30, 2014).

#### Major Challenges & Opportunities for Improvement

In terms of protecting key leaders and facilities, challenges in the areas of staffing, training, and protective countermeasures have resulted in the potential increased risk and decreased program effectiveness for the USSS, as was evidenced by certain protective challenges at the White House Complex. In light of these challenges, the DHS Secretary established an independent Protective

Mission Panel to review USSS policies, staffing, and operations, and to provide recommendations for enhancing the USSS protective mission.

Recent heightened threat-level events, both domestically and internationally, and the subsequent focus on reinforcing the protection of critical infrastructure and enhancing federal building security—managed by the Federal Protective Service in NPPD—has stretched the FPS law enforcement capacity and availability to conduct facility security assessments to diagnose vulnerabilities and work with critical infrastructure owners to address shortfalls while maintaining an increased security presence at federal facilities.

#### Highlighted Future Actions

USSS has begun to adopt strategies recommended by the United States Secret Service Protective Mission Panel to address programmatic risks. The Mission Panel recommended focusing on specific areas to improve which include: 1) conducting additional training and obtaining additional personnel; 2) improving perimeter infrastructure; and 3) improving technology and operations. Currently the USSS is actively working to implement near term solutions in response to the Panel's recommendations, and is aggressively pursuing additional funding and resources to achieve robust and permanent solutions.

To sustain the enhanced security and protective measures associated with federal building security managed by FPS, OMB authorized a fee increase for FPS for fiscal year 2017. To provide a long term solution to this situation, NPPD will develop alternative operational models and a path forward that relies less heavily on voluntary compliance and a fee-based structure to enforce recommended countermeasures. In addition, the Government Accountability Office audit recommendations will continue to be implemented to improve future operations.

## Performance Highlight

Below is a highlighted accomplishment demonstrating success in reducing risk to critical infrastructure.



### Papal Visit and United Nations General Assembly

USSS successfully orchestrated one of the largest domestic security operations in the history of this country providing security for the United Nations (UN) General Assembly and the visit by Pope Francis to the United States. In addition to the Pope, USSS was the lead U.S. government agency for the security of over 160 world leaders, in addition to over 70 of their spouses, who came to the U.S. for the UN General Assembly and other reasons. These world leaders included

President Xi Jinping of China, President Vladimir Putin of Russia, Prime Minister David Cameron of the United Kingdom, King Abdullah of Jordan, Prime Minister Haider Al-Abadi of Iraq, President Hassan Rouhani of Iran, Prime Minister Matteo Renzi of Italy, President François Hollande of France, Prime Minister Benjamin Netanyahu of Israel, President Abdel Fattah el-Sisi of Egypt and President Raul Castro of Cuba. Almost all of these leaders were in our country at the same time.

The security for this convergence of world leaders was a massive and intense undertaking. These events required, among many things:

- The assignment of thousands of special agents and uniform personnel of the USSS from around the country to be primarily responsible for these leaders while they were anywhere in the United States;
- Months of detailed discussions and planning with city officials and police departments in New York, Philadelphia, and Washington, D.C., to plan and prepare parade and motorcade routes, and outdoor and indoor events;
- Months of direct negotiations with the staff and security details of almost all these world leaders about the logistics and security for their visits, to include a visit by Director Clancy and other USSS personnel to the Vatican; and
- Security screening of an estimated 130,000 people in Washington, D.C.; over one million people in Philadelphia, and over 200,000 in New York.

The security for the all these leaders (and the public) surrounding their visits to the U.S. was by no means limited to the USSS. Other components of the Department of Homeland Security were heavily involved. All these forces, working together, brought about safe and successful visits to the United States by the Pope and the other world leaders, in a highly professional, precise and well-coordinated manner. The Pope and others got to see and experience the United States, our people, and our free and democratic society, at our very best.

## Performance Results and Plan

In FY 2015, there were seven performance measures used to assess the Department's efforts for this goal. In FY 2015, 57 percent of the measures met their target and 71 percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary					
	Scale:	0%	25%	50%	75%	100%
Goal 1.3: Reduce Risk to the Nation's Critical Infrastructure, Key Leadership and Events						

- ◆ - Percent of measures that met their FY 2015 target.
- ◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below are two highlighted strategic measures that gauge efforts to reduce risk to the Nation's most critical infrastructure, key leadership, and events.

Percent of tenants satisfied with the level of security provided at federal facilities (NPPD)								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
81.3%	77.8%	78%	82%	76%	86%	71%	87%	88%

This measure assesses the effectiveness of security services provided by FPS to the Government Services Agency tenants through the use of a formal customer satisfaction survey. FPS uses the feedback from this survey to identify opportunities for improvement in the security services provided to its customers. In FY 2015, 13,260 out of 18,653 respondents answered that they were satisfied or highly satisfied with the level of security provided at federal facilities. A customer's satisfaction with the facility security support can be influenced by many factors such as: onsite protective security officer guard performance levels, countermeasure equipment performance levels, lack of guards and/or countermeasures that a customer deems necessary at a facility. To increase customer satisfaction with FPS service delivery, FPS will continue its Customer Portfolio Engagement activities sponsored at the Executive level for standardized implementation across every FPS region to address the downward trend.

Financial crimes loss prevented through a criminal investigation (in billions) (USSS)								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
\$6.56	\$4.85	\$2.75	\$4.20	\$3.04	\$2.70	\$1.47	\$1.80*	\$1.90

This measure is an estimate of the direct dollar loss to the public that was prevented due to USSS intervention or interruption of a criminal venture through a criminal investigation. This estimate is based on the likely amount of financial crime that would have occurred had the offender not been identified nor the criminal enterprise disrupted. This year's target was not met for a few primary reasons which include: many financial cases are very large in scope and take a long time to investigate; the field special agent workforce has reached a historic low; and some agents were diverted to support campaign protection and the visit from the Pope. USSS will improve performance by addressing staffing shortfalls in the recently developed Human Capital Plan.

\* FY 2016 target reflects USSS allocation of personnel to support campaign protection. The FY 2016 target previously published as \$2.50 in the FY 2014 – 2016 Annual Performance Report was changed to \$1.80. The FY16 and out year targets were adjusted based on FY15 results and the unpredictable size, scope, and closure rate of these types of investigations.

The remaining strategic measures used to gauge our efforts to reduce risk to the Nation's most critical infrastructure, key leadership, and events are displayed below. For those measures that did not meet their targets, an explanation with corrective action are provided.

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
<b>USCG</b>									
Security compliance rate for high risk maritime facilities	---	99.9%	98.7%	99.3%	99.3%	100%	99.6%	100%	100%
<p>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 99.6%, a 0.3% improvement over FY 2014 results. In total, only 15 of more than 3,400 high risk facilities were not in compliance. USCG will continue to partner with the maritime industry to assist in the development and execution of effective Maritime Transportation Security Act regulated maritime facility security programs.</p>									
<b>USSS</b>									
Percent of currency identified as counterfeit	0.0087%	0.0078%	0.0085%	0.0072%	0.0068%	< 0.0088%	0.0058%	< 0.0090% <sup>1</sup>	< 0.0088%
Percent of National Special Security Events that were successfully completed	100%	100%	100%	100%	100%	100%	100%	100%	100%
Percent of protectees that arrive and depart safely <sup>2</sup>	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 <sup>2</sup>	100%	100%	100%	100%	99.7%	100%	100%	100%	100%

Note 1: FY 2016 target reflects USSS allocation of personnel to support campaign protection.

Note 2: FY 2010 to FY 2014 data was previously aggregated in a single measure from these two measures.

## Mission 2: Secure and Manage Our Borders

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

#### Strategies

- Prevent illegal import and entry
- Prevent illegal export and exit

#### Strategic Review Summary of Progress

Assessment Lead Co-Lead: Woody Lee, Chief, U.S. Customs and Border Protection (CBP), U.S. Border Patrol Directorate for Strategic Planning and Analysis  
Co-Lead: John Prince, CAPT, U.S. Coast Guard (USCG), Director of Law Enforcement, Maritime Security & Defense Operations Policy

The Department of Homeland Security (DHS), in consultation with the Office of Management and Budget (OMB), has highlighted this goal as a focus area for improvement.

#### Introduction

The Department has made progress in its ability to identify and apprehend individuals trying to illegally enter the United States, smuggle contraband across our borders, and identify weapons of mass destruction in the supply chain. Over the past several years, DHS has focused personnel, assets, technology, and infrastructure resources on the U.S. air, land, and sea borders and approaches, and made critical security improvements along the Northern and maritime borders. Although progress is being made, DHS has identified a greater need to integrate and unify efforts across multiple components, and thus determined that this goal was a focus area for improvement.

#### Major Achievements

DHS experienced an increase in the volume of illicit people, including unaccompanied children and goods attempting to enter and exit the United States, but despite this increase DHS maintained steady interdiction rates in the land, air, and maritime domains. Concurrently, DHS made moderate progress disrupting or dismantling transnational criminal organizations operating on the nation's borders. Biometric system improvements allowed for better detection of illicit entry attempts and improved awareness of those entering the country.

DHS also strengthened international partnerships and bolstered international capabilities, helping to combat threats as far from the border as possible. Examples include: expanded participation by foreign ports in the Container Security Initiative; and installation of maritime interdiction and prosecution support specialists in a transit zone nation as a step toward disrupting or dismantling transnational criminal organizations.

#### Major Challenges & Opportunities for Improvement

DHS cannot fully achieve its strategic outcomes in securing the border until its component operations are synchronized against a single set of prioritized threats. The implementation of the Southern Border and Approaches Campaign plan by the Secretary will reinforce the unity of effort

required across DHS components to define overall success, coordinate law enforcement activities, and improve performance in securing the Nation.

Future Actions

DHS will implement a Southern Border and Approaches Campaign Strategy with the overarching goals to: enforce our immigration laws and interdict individuals seeking to illegally cross our land, sea, and air borders; degrade transnational criminal organizations; and decrease the terrorism threat to the Nation, all without impeding the flow of lawful trade, travel, and commerce. DHS has formed three Joint Task Forces (JTFs), cross-populated by DHS components and partners. JTF-West will focus on the southwest land and maritime borders and approaches, while JTF-East will focus on the southeast maritime border and approaches. JTF-Investigations will coordinate integrated joint investigations and operations across the entire Southern Border. Together, the three task forces will deploy DHS assets in a strategic and coordinated way in order to secure the Southern border and approaches of the United States across land, sea, and air domains.

**Performance Highlight**

Below is a highlighted accomplishment demonstrating efforts to improve border security.



**DHS Sponsors Analytical Exercise to Advance Joint Intelligence Capabilities on the Southwest Border**

In June 2015, the Joint Task Force-West (JTF-W), the National Targeting Center, and the Human Smuggling Cell sponsored a two-week joint analytical exercise for DHS personnel from all four JTF-W corridors (California, Arizona, New Mexico/West Texas, and South Texas).

The exercise introduced a system known as Falcon to corridor intelligence and operations teams. A total of 35 intelligence specialists and 18 operations personnel representing ICE’s Homeland Security Investigations, and CBP’s Border Patrol and Office of Field Operations attended the working-group style

exercise. Participants learned how to import data sets from various sources and then use the combined data to create a three-dimensional operating picture of the illicit organizations within their respective areas of responsibility. The participants spent the second week analyzing the threat pictures and drafting courses of action (COAs) that would be used to target the newly identified threats by executing counter-network operations.

On the final day, each corridor workgroup presented their briefings and COAs to JTF-W Director Robert L. Harris, JTF-Investigations Deputy Director Pete Hatch, and National Targeting Center Executive Director Troy Miller. Director Harris later stated how impressed he was with the capabilities of the participants and the outcomes of their final briefings and how this new system can provide new capabilities to help secure the southwest border.

**Performance Results and Plan**

In FY 2015, there were six performance measures used to assess the Department’s efforts for this goal. In FY 2015, 83 percent of the measures met their target and 83 percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary				
	Scale:	0%	25%	50%	75%
Goal 2.1: Secure U.S. Air, Land, and Sea Borders and Approaches					

- ◆ - Percent of measures that met their FY 2015 target.
- ◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below are two highlighted strategic measures that gauge efforts to secure U.S. air, land, sea borders, and approaches.

Percent of people apprehended multiple times along the southwest border (CBP)								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	16%	14%	≤ 17%	14%	≤ 17%	≤ 17%

This measure examines the percent of deportable individuals who have been apprehended multiple times by the Border Patrol. The Border Patrol uses the Consequence Delivery System (CDS) on the Southwest Border as a means to employ an analytical process that standardizes decision making in the application of consequences and examines the efficiency and effectiveness of individual consequences on various types of deportable aliens. Recidivism and the average number of apprehensions per recidivist are the strongest indicators of CDS effectiveness. Since CDS implementation in FY 2011, the annually reported recidivism rate has decreased each year from an average of 27 percent to 14 percent in FY 2015 and average apprehensions per recidivist decreased from 2.71 to 2.38 in FY 2015. Contributing factors to the reduction included reducing the percent of apprehensions resulting in a Voluntary Return, the least effective and efficient consequence, from 59 percent in FY 2010 to 4 percent in FY 2015; and applying more effective and efficient consequences to illegal aliens with a higher probability of making subsequent illegal entries.

Rate of interdiction effectiveness along the Southwest Border between ports of entry (CBP)								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	---	79.28%	80.00%	81.01%	81.00%	81.00%

This measure reports the percent of detected illegal entrants who were apprehended or turned back after illegally entering the United States between the ports of entry on the southwest border. The U.S. Border Patrol uses a risk-based strategy to deploy resources and address emerging threats. Risk is assessed qualitatively and quantitatively and is informed by multiple indicators, including the Interdiction Effectiveness Rate (IER). The IER is the percent of detected illegal entrants who were apprehended or turned back after illegally entering the U.S. between the Southwest Border ports of entry. The IER focuses on positive outcomes (apprehensions or turnbacks) of recent entrants made in the immediate border area, and excludes apprehensions made over 30 days after entry and apprehensions made beyond our area of operations. Through recent process improvements that identify capability gaps, as well as additional man hours attained through the Overtime Transition Plan, CBP was able to strategically deploy resources based on risk and end the year with an IER of 81.01 percent, exceeding the 80 percent target. Using this strategic approach, CBP plans to accomplish the goal of an 81 percent IER in FY 2016.

The remaining strategic measures are used to gauge our efforts to secure U.S. air, land, sea borders, and approaches. For those measures that did not meet their targets, an explanation with corrective action are provided

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
<b>CBP</b>									
Percent of detected conventional aircraft incursions resolved along all borders of the United States	---	95.3%	96.0%	99.3%	98.8%	100%	99.3%	100%	100%
<p>During FY 2015, 269 of 271 border incursions were resolved for an overall 99.3% success rate. The two unresolved aircraft were visually spotted by Border Patrol and Office of Field Operations agents on the border and reported to the Air and Marine Operations Center. Responding law enforcement could not locate the target to identify and resolve. The Air and Marine Operations Center will continue to increase surveillance capability through integration of Federal Aviation Administration and Department of Defense radar technology along the border environment to better detect low flying aircraft incursions.</p>									
Amount of smuggled outbound currency seized at the ports of entry (in millions)	---	\$47.0	\$31.9	\$36.9	\$37.7	\$30.0	\$37.6	\$30.0	\$30.0
Number of smuggled outbound weapons seized at the ports of entry	---	---	---	731	411	400	505	400	400
<b>USCG</b>									
Migrant interdiction effectiveness in the maritime environment	---	---	---	---	---	73.0%	74.8%	74.0%	74.5%

## Mission 2: Secure and Manage Our Borders

### Goal 2.2: Safeguard and Expedite Lawful Trade and Travel

#### Strategies

- *Safeguard key nodes, conveyances, and pathways*
- *Manage the risk of people and goods in transit*
- *Maximize compliance with U.S. trade laws and promote U.S. economic security and competitiveness*

#### Strategic Review Summary of Progress

Assessment Lead Colleen Manaher, Director, U.S. Customs and Border Protection (CBP), Office of Field Operations

The Department of Homeland Security (DHS), in consultation with the Office of Management and Budget (OMB), has determined that performance toward this goal is making noteworthy progress.

#### Introduction

Lawful trade and travel provides tremendous economic benefits to our society, evident by a substantial increase in the number of tourist and business travelers and in the value of U.S. exports and imports, and is underscored by projections for continued growth at an average of six percent annually through 2030. DHS and our partners work to secure and expedite these flows of people and goods, as they are a main driver of U.S. economic prosperity.

#### Major Achievements

As of September 30, 2014, DHS screened over 370 million people entering the U.S.; investigated nearly 11,000 visa overstays; collected more than \$48 billion in fees, duties, and tariffs on imports valued at \$2.4 trillion; ensured safe transit of \$3.2 trillion in commerce over 25,000 miles of U.S. waterways; maintained over 49,000 aids to navigation; issued 51 permits for bridge projects valued at \$10.3 billion; and expended over 15,000 hours supporting movement through ice impeded lakes and waterways. DHS aggressively expanded risk-based approaches to the screening of people using Global Entry and Transportation Security Administration (TSA)Pre✓<sup>®</sup>, time-saving technologies such as Automated Passport Control kiosks, experiments, and pilot programs with the creation of the Entry/Exit Test Facility, and expansion of the Automated Commercial Environment. The U.S. Coast Guard (USCG) bolstered domestic icebreaking operations, reduced permitting-process review time, and improved operations to manage U.S. aids to navigation.

New international agreements included establishing a new Preclearance port at Abu Dhabi, United Arab Emirates, expanding the Container Security Initiative to three additional foreign ports, expanding the Customs-Trade Partnership Against Terrorism to Singapore, conducting a Truck Cargo Preclearance Pilot with Canada, and completing the roll-out of 100 percent screening of all international inbound air cargo transported on passenger aircraft.

Major Challenges & Opportunities for Improvement

DHS challenges include developing a complete Entry/Exit system at the ports of entry and successfully managing further expansion of the Trusted Trader and Trusted Traveler programs, with a special focus on Global Entry and TSA Pre✓®. Global aviation security risks are increasing and are a growing challenge to combat effectively. DHS will refine the TSA International Risk Framework, a systematic decision-making framework that identifies international aviation security risk and supports the targeted application of direct and indirect risk mitigation measures.

**Performance Highlight**

Below is a highlighted accomplishment demonstrating our ability to safeguard lawful trade.



**Operation Atlantic**

In 2014, CBP, the United Kingdom Border Force, and the United Kingdom Association of Chief Police Officers - Vehicle Crime Intelligence Service, formulated Operation Atlantic targeting shipments of Land Rover Defenders and Austin Mini Coopers imported from the United Kingdom (UK) which may have been modified in a fraudulent manner to take advantage of exemptions within the statutes and regulations administered by the Department of Transportation and the Environmental Protection Agency that allow the importation of older, nonconforming vehicles more than 25 years old. This continuing national operation

is being led by the Import Safety Commercial Targeting and Analysis Center, part of the Office of International Trade in Washington, DC. By sharing law enforcement information, CBP and UK law enforcement have identified many illegal shipments at various ports of entry across the United States.

Since joint targeting efforts began, approximately 700 imported vehicles have been targeted for examination at over 20 ports in the U.S., with over 100 vehicles stopped from entering because they failed to meet US safety standards. The operation has also led to several criminal investigations in the U.S. and the UK. With the assistance of the Office of Public Affairs, over 30 million people have watched, read, or viewed an Operation Atlantic news story online. Operation Atlantic is an important initiative as it clearly demonstrates the significance and benefits of multi-lateral information exchanges in the enforcement of the laws of the U.S. and other countries, which are in progress this Fiscal Year.

**Performance Results and Plan**

In FY 2015, there were seven performance measures used to assess the Department’s efforts for this goal. In FY 2015, 43 percent of the measures met their target and 29 percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary					
	Scale:	0%	25%	50%	75%	100%
Goal 2.2: Safeguard and Expedite Lawful Trade and Travel			◆	◆		

◆ - Percent of measures that met their FY 2015 target.

◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below are two highlighted strategic measures that gauge efforts to safeguard and expedite lawful trade and travel.

Percent of imports compliant with U.S. trade laws (CBP)								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
98.89%	97.67%	96.46%	97.66%	97.99%	97.50%	98.89%	97.50%	97.50%

Ensuring that all imports are compliant and free of major discrepancies allows for lawful trade into the United States. This measure reports the percent of imports that are compliant with U.S. trade laws including customs revenue laws. CBP works with our international trade partners through several [trade programs](#) to build—and improve upon—a solid and efficient trade relationship to accomplish safer, faster, and more compliant trade. In FY 2015, 98.89 percent of imports were found to be compliant with U.S. trade laws. These results are an improvement from FY 2014, are consistent with prior year results, and have improved three years in a row. CBP closely monitored importers to reduce the non-compliance rates through Importer Self-Assessment, Customs-Trade Partnership programs, and Centers of Excellence and Expertise instituted in FY 2013.

Percent of import revenue successfully collected (CBP)								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	99.12%	98.88%	98.73%	99.56%	100%	98.61%	100%	100%

CBP has the statutory responsibility to collect all revenue due to the U.S. Government that arises from the importation of goods. This amounts to more than \$48 billion annually based on import tariffs, duties, and fees on nearly \$2.5 trillion of imports into the United States. However, not all importers pay their tariffs, duties, and fees, which in FY 2013 saw estimated under-collections of \$736.7 million and over-collections of \$108.8 million. FY 2015 results are consistent with long term trends; however the target was missed. While there remains a very small percentage of under collections, it is due to some importers unintentionally or intentionally failing to pay the correct amount of duties, taxes, and fees. CBP will continue to apply various enforcement methods such as audits, targeting, and statistical random sampling to bridge the revenue gap and identify non-compliance with U.S. trade laws, regulations and agreements.

The remaining strategic measures are used to gauge our efforts to safeguard and facilitate lawful trade and travel. For those measures that did not meet their targets, an explanation with corrective action are provided. In addition, changes to measure names and targets from the previous year’s report are identified.

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
<b>CBP</b>									
Percent of cargo by value imported to the U.S. by participants in CBP trade partnership programs	---	55.1%	54.7%	55.2%	53.9%	54.0%	52.2%	53.0%	62.0%
Over 67 importers were suspended from the C-TPAT program during FY 2015 for various instances of non-compliance (e.g., negative validations and narcotics). As required by the Safe Port Act, immediate remediation efforts have been implemented.									

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
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	---	---	98%	98%	99.22% <sup>1</sup>	100%	99.76%	100%	100%
<p>This measure gauges the overall percent of inbound cargo in the sea, air, and land environments identified as potentially high risk by the Automated Targeting System that is reviewed, scanned, or otherwise examined prior to lading or at arrival at a US port of entry. A small percentage of cargo is not reviewed due to status changes en route, information processing and data entry errors, or logistical and scheduling anomalies. To improve measure results, the CBP Office of Field Operations is working with the Targeting &amp; Analysis Systems Program Directorate to resolve status tracking problems and information processing errors and with shippers and carriers to rectify logistical and scheduling issues.</p>									
<b>USCG</b>									
Availability of maritime navigation aids	98.5%	98.5%	98.3%	98.2%	98.2%	97.5%	97.7%	97.5%	97.5%
Number of detected incursions of foreign fishing vessels violating U.S. waters	82	122	160	189	198	< 215	224	< 220	< 224
<p>There were 224 detected foreign fishing vessel incursions in FY 2015, 26 more than reported in FY 2014 and 9 more than expected when the FY 2015 target was set. The prior year variance is less than .001% of the estimated number of Mexican vessels fishing in adjacent waters capable of encroaching into the U.S. Exclusive Economic Zone. To deter future incursions, the U.S. Coast Guard will continue aerial and surface patrols of the U.S./Mexico Maritime Boundary Line.</p>									
Fishing regulation compliance rate	97.2%	97.4%	98.3%	98.1%	97.5%	96.5%	97.1%	96.5%	97.0%

Note 1: The program began reporting to the one hundredth decimal place in FY 2014 since a small change in percent is a large volume of cargo.

## Mission 2: Secure and Manage Our Borders

### *Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations and Other Illicit Actors*

#### Strategies

- *Identify, investigate, disrupt, and dismantle transnational criminal organizations*
- *Disrupt illicit actors, activities, and pathways*

#### Strategic Review Summary of Progress

Assessment Lead Tracey Bardorf, Director, U.S. Immigration and Customs Enforcement (ICE), Office of Policy

The Department of Homeland Security (DHS) has determined that performance toward this goal is making satisfactory progress.

#### Introduction

Transnational criminal rely on revenues generated through the sale of illegal drugs and counterfeit goods, human trafficking and smuggling, and other criminal activities. They also gain strength by taking advantage of the same innovations in management and supply chain structures that are propelling multinational corporations.

DHS is making satisfactory progress in its strategies to disrupt and dismantle transnational criminal organizations and other illicit actors. Progress is made by targeting illicit financing activities that transnational criminal organizations depend on, creating a deterrent effect from injecting uncertainty into criminal decision making, and using intelligence to target and interdict people and illicit goods through a rapid response workforce, as well as surveillance and enforcement assets.

#### Major Achievements

Investigative work based on ICE's Significant Case Report (SCR) process led to an increase of significant cases - including those focused on Transnational Criminals or Criminal Organizations (TCOs) - directly resulting in either a disruption or dismantlement. "Disruption" is defined as impeding the normal and effective operation of the targeted organization. "Dismantlement" is defined as destroying the organization's leadership, financial base, and network to the degree that the organization is incapable of operating and/or reconstituting itself.

Additionally, U.S. Coast Guard (USCG) continued to expand its international capabilities to counter TCOs by gaining approval to permanently assign USCG interdiction and prosecution experts to Panama, a country adjacent to active maritime smuggling routes.

#### Major Challenges & Opportunities for Improvement

With regard to opportunities, USCG's Western Hemisphere Strategy provides a framework for addressing the greatest maritime threats and challenges for DHS in the Western Hemisphere over the next 10 years. The recent acquisition and deployment of new National Security Cutters has

provided enhanced capability and reliability in the transit zones. The ongoing work to replace the Coast Guard’s aging fleet of Medium Endurance Cutters with more capable Offshore Patrol Cutter will further help compensate for the shift of naval assets from the this region to support the U. S. Navy’s pivot to the Pacific.

An opportunity exists to operationalize the Homeland Criminal Organization Target Priority Investigations, otherwise known as “HOMECORT.” Led by the Joint Task Force – Investigations and including representatives from U.S. Customs and Border Protection (CBP), USCG, and ICE, HOMECORT integrates DHS criminal investigations and investigative activities to enhance the Department’s efforts to suppress crime, illicit flow, surges, and hotspots; as well as improve law, order, and governance on the border and in the approaches.

**Performance Highlight**

Below is a highlighted accomplishment demonstrating success in this combatting transnational crime.



**HOMECORT—Prioritizing Criminal Networks**

Joint Task Force – Investigations (JTF-I) has changed the course of investigative business within the Department by developing and implementing the Homeland Criminal Organization Target Priority Investigations, otherwise known as HOMECORT. JTF-I, comprised of representatives from CBP, USCG, and Homeland Security Investigations created the HOMECORT process with the emphasis of a secretarial validated, departmental investigative priority, which integrates DHS criminal investigations and investigative activities to enhance the JTFs’ efforts to suppress crime, illicit flow, surges and hotspots; as well as improve law, order and governance on the border and in the approaches.

A key role of the HOMECORT process involves the development of an interagency approved action plan that integrates DHS Components’ authorities, capabilities, expertise, and resources to counter these Department-level priority targets, networks, problem sets, and crises.

The development and implementation of the HOMECORT process was an innovative approach to place DHS on the forefront of federal law enforcement. As a result, the HOMECORT process has achieved great success by identifying and enhancing top-tier investigations within the Department; facilitated the development of counter-network and investigative strategies from an operational level; synchronized multiple investigations involving the same network to arrive at a common desired criminal justice outcomes; and leveraged departmental capabilities within ICE, CBP, U.S. Citizenship and Immigration Services, USCG, and others in DHS, as well as our interagency partners to maximize the effectiveness of DHS investigations.

The establishment of HOMECORT—similar to the Drug Enforcement Agency’s Consolidated Priority Organization Target list or the Federal Bureau of Investigation’s Top International Criminal Organizations Target list—will be recognized as DHS’s premier investigative capability to fight transnational criminal organizations.

**Performance Results and Plan**

In FY 2015, there were three performance measures used to assess the Department’s efforts for this goal. In FY 2015, zero percent of the measures met their target and zero percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary					
	Scale:	0%	25%	50%	75%	100%
Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations and Other Illicit Actors						

- ◆ - Percent of measures that met their FY 2015 target.
- ◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below is one highlighted strategic measure that gauges efforts to disrupt and dismantle transnational criminal organizations and other illicit actors.

Percent of significant child exploitation or child sex trafficking investigations that resulted in a disruption or dismantlement* (ICE)								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	23.5%	59.0%	41.0%	18.1%	20.0%**	21.0%

This measure reports the percent of significant child exploitation or child sex trafficking investigations resulting in the disruption or dismantlement of high-threat criminal organizations/individuals. "Child exploitation" is defined as manufacturing and distributing sexual or perverted acts or images of children under the age of 18. ICE has established a Child Exploitation Investigations Center to serve as a central coordination point for state, local, and tribal offices, the National Center for Missing and Exploited Children, and other federal law enforcement agencies, as well as international law enforcement agencies dedicated to combating the sexual exploitation of children. The significant decline in the percent of disruptions or dismantlements is due to two primary reasons: 1) a reduction in current year disruptions or dismantlements due to prior year SCR surge operations; and 2) a coding error which led to inconsistent data collection that overstated prior year results. ICE will continue its successful SCR process and has provided data collection corrections to the process going forward.

\* - Previous measure name: Percent of transnational child exploitation or sex trafficking investigations resulting in the disruption or dismantlement of high-threat child exploitation or sex trafficking organizations or individuals.  
 \*\* - The FY 2016 target previously published as 42% in the FY 2014 – 2016 Annual Performance Report was changed to 20%. The program is reducing its targets to account for the data collection issue discovered in FY 2015.

The remaining strategic measures are used to gauge our efforts to disrupt and dismantle transnational criminal organizations and other illicit actors. For those measures that did not meet their targets, an explanation with corrective action are provided.

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
<b>ICE</b>									
Percent of significant drug investigations that resulted in a disruption or dismantlement <sup>1</sup>	---	---	---	42.6%	45.0%	29.0%	14.5%	15.0% <sup>2</sup>	16.0%

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
The significant decline in the percent of disruptions or dismantlements is due to two primary reasons: 1) a reduction in current year disruptions or dismantlements due to prior year SCR surge operations; and 2) a coding error which led to inconsistent data collection that overstated prior year results. ICE will continue its successful SCR process and has provided data collection corrections to the process going forward.									
Percent of significant transnational gang investigations that resulted in a disruption or dismantlement <sup>3</sup>	---	---	---	60.8%	44.0%	41.0%	12.0%	13.0% <sup>4</sup>	14.0%
The significant decline in the percent of disruptions or dismantlements is due to two primary reasons: 1) a reduction in current year disruptions or dismantlements due to prior year SCR surge operations; and 2) a coding error which led to inconsistent data collection that overstated prior year results. ICE will continue its successful SCR process and has provided data collection corrections to the process going forward.									

Note 1: Previous measure name: Percent of transnational drug investigations resulting in the disruption or dismantlement of high-threat transnational drug trafficking organizations or individuals.

Note 2: The FY 2016 target previously published as 30% in the FY 2014 – 2016 Annual Performance Report was changed to 15%. The program is reducing its targets to account for the data collection issue discovered in FY 2015.

Note 3: Previous measure name: Percent of transnational gang investigations resulting in the disruption or dismantlement of high-threat transnational criminal gangs.

Note 4: The FY 2016 target previously published as 42% in the FY 2014 – 2016 Annual Performance Report was changed to 13%. The program is reducing its targets to account for the data collection issue discovered in FY 2015.

## **Mission 3: Enforce and Administer Our Immigration Laws**

### ***Goal 3.1: Strengthen and Effectively Administer the Immigration System***

#### **Strategies**

- *Promote lawful immigration*
- *Effectively administer the immigration services system*
- *Promote the integration of lawful immigrants into American society*

#### **Strategic Review Summary of Progress**

Assessment Lead: Joe Moore, Chief Financial Officer, U.S. Citizenship and Immigration Services (USCIS), Office of the Chief Financial Officer

The Department of Homeland Security (DHS) has determined that performance toward this goal is making satisfactory progress.

#### Introduction

DHS continually seeks better ways to provide accurate and useful immigration information to our customers, more effectively grant immigration and citizenship benefits, and promote an awareness and understanding of citizenship. Since any good immigration system must be able to rapidly respond to changes in demand, DHS is leveraging technology to better administer benefits and make information more accessible and secure.

#### Major Achievements

DHS processed over 6.7 million benefit requests, including applications for naturalization, lawful permanent residence, change of status, refugee and asylum protection, and initiatives such as deferred action for childhood arrivals through USCIS. USCIS maintained an average cycle time of 4.1 months for adjudicating all form types, narrowly missing the target of less than 4 months. USCIS also conducted 66,870 refugee interviews and admitted 69,987 refugees, which is 99.9 percent of the presidential cap and the closest the refugee program has come to reaching the cap in over 30 years. In addition, USCIS also made the correct decision in 99 percent of all approved naturalization and permanent residence applications. Furthermore, USCIS achieved an overall National Customer Service Center satisfaction rating of 86 percent. To promote lawful immigration, USCIS hosted 3,145 public engagements, reaching over 124,000 individuals. Finally, the Office of the Citizenship and Immigration Services Ombudsman took action to resolve 89 percent of case-related inquiries regarding the delivery of citizenship and immigration services within 90 days of receipt, exceeding the target of 85 percent. All statistics are as of September 30, 2014.

#### Major Challenges & Opportunities for Improvement

Achieving target processing times for certain form types remains a challenge primarily due to increased application receipt volumes. DHS will continue to address workload challenges by redirecting incoming cases to optimize capacity, shifting immigration services officers' adjudication priorities so that more time is allocated to the application types with the largest volume of pending cases, and encouraging the use of overtime.

**Performance Highlight**

Below is a highlighted accomplishment demonstrating success in immigrant integration.



**White House Task Force on New Americans**

Recognizing the importance of immigrant integration for our Nation’s continued success, President Obama created the White House Task Force on New Americans on November 21, 2014. The Task Force includes 16 federal departments, agencies, and White House offices. The Task Force is led by co-chairs Cecilia Muñoz, director of the White House Domestic Policy Council, and León Rodríguez, director of USCIS. On April 14, 2015, the Task Force submitted its report, [Strengthening Communities by Welcoming All Residents: A Federal Strategic Action Plan on Immigrant & Refugee Integration](#), to President Obama. The

report establishes a federal immigrant integration strategy that allows new Americans to contribute to society to their fullest potential. The report provides an action plan that sets 16 core goals that will be achieved, in part, through 48 recommended actions that Task Force members will pursue to help: build welcoming communities; strengthen existing pathways to naturalization and promote civic engagement; support skill development, foster entrepreneurship, safeguard workers; and expand opportunities for linguistic integration and education.

These efforts will build on three critical integration pillars: civic, economic, and linguistic. To examine current federal efforts across each pillar, the Task Force identified and catalogued current federal initiatives that further the civic, economic, and linguistic integration of immigrants. The Task Force’s assessment indicated achieving key integration objectives will require greater action by federal agencies, but also by states, local communities, the private sector, philanthropic organizations, and immigrants and refugees themselves.

On July 6, 2015, under the umbrella of the Task Force on New Americans and President Obama’s executive actions on immigration, USCIS released a series of promotional materials for the [Citizenship Public Education and Awareness Initiative](#). The new messages include digital and print advertisements in English, Spanish, Chinese, and Vietnamese; radio public service announcements in Spanish and Chinese; and video public service announcements in English and Spanish. This initiative aims to provide those seeking citizenship with information on the naturalization process and USCIS educational resources.

**Performance Results and Plan**

In FY 2015, there were four performance measures used to assess the Department’s efforts for this goal. In FY 2015, 50 percent of the measures met their target and 75 percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary					
	Scale:	0%	25%	50%	75%	100%
Goal 3.1: Strengthen and Effectively Administer the Immigration System				◆	◆	

◆ - Percent of measures that met their FY 2015 target.

◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below are two highlighted strategic measures that gauge efforts to strengthen and effectively administer the immigration system.

<b>Percent of customers satisfied with the citizenship and immigration-related support received from the National Customer Service Center* (USCIS)</b>								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	80%	93%	87%	86%	85%	88%	85%	85%

This measure gauges the overall rating of the immigration process and is based on the results from the following areas: 1) accuracy of information; 2) responsiveness to customer inquiries; 3) accessibility to information; and 4) customer satisfaction. The FY 2015 result for this measure, 88 percent, is consistent with the results for the past three years and is indicative of the attention USCIS has given to the customer service approach. In addition, these results continue to exceed industry customer satisfaction averages. Throughout the year, USCIS has met the target by constantly listening to customer feedback and taking deliberate steps to improve the level of service provided to its customers. The professionalism of the Immigration Services Officers and the Customer Service Representatives, along with the accuracy of the information they provide, have consistently contributed to high ratings. Additionally, the use of innovative technology has also helped maintain this high satisfaction. For example, USCIS uses Interactive Voice Response, the automated voice that callers hear when they call the National Customer Service Center, which provides public access to current information (e.g., about case status) and guides the caller to live assistance when needed. USCIS has been able to meet this goal by maintaining the high performance of these factors throughout the fiscal year.

\* - Previous measure name: Overall customer service rating of the immigration process.

<b>Average of processing cycle time (in months) for naturalization applications (N-400) (USCIS)</b>								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
4.5	4.6	4.6	4.7	5.5	≤ 5.0	5.0	≤ 5.0	≤ 5.0

The N-400, Application for Naturalization, is filed by an individual applying to become a U.S. citizen. The average processing time for an N-400 in FY 2015 was five months, meeting the annual target and a significant improvement from the FY 2014 result. This result reverses the prior trend in processing time for this form. USCIS has maintained production levels and met cycle time goals for the N-400. USCIS overcame workload challenges that had the potential to decrease quality and increase cycle times. The changes made to address the challenges included: redirecting incoming cases between service centers and field offices to utilize available capacity, increasing clerical support to receive and prepare cases, and shifting Immigration Services Officer adjudication hours across application types with the greatest pending volumes. USCIS remains committed to meeting N-400 cycle time targets and continues to implement strategies to improve the efficiency of case processing, such as increasing and strengthening employee training and increasing supervisory engagement.

The remaining strategic measures were used to gauge our efforts to strengthen and effectively administer the immigration system. For those measures that did not meet their targets, an explanation with corrective action are provided. In addition, changes to measure names and targets from the previous year’s report are identified.

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
<b>USCIS</b>									
Average of processing cycle time (in months) for adjustment of status to permanent resident applications (I-485)	3.8	4.4	5.1	4.7	6.0	≤ 4.0	6.4	≤ 4.0	≤ 4.0
<p>USCIS experienced an increase in the I-485 cycle time as a result of ongoing workload challenges. Despite the increase in cycle time, the accuracy of I-485 decisions has remained consistent. USCIS remains committed to meeting the I-485 cycle time targets and will continue making changes to address the workload challenges by redirecting incoming cases to better utilize capacity and shifting Immigration Services Officer adjudication hours across application types with the greatest pending volumes. USCIS will also strengthen the quality of employee training and supervisory engagement to increase the efficiency of case processing. In addition, USCIS will encourage the use of overtime to improve cycle times without compromising the accuracy of benefit decisions.</p>									
Percent of students enrolled in classes under the Citizenship and Integration Grant Program that show educational gains	---	---	---	---	---	80%	75%	80%	80%
<p>USCIS did not meet its target for two primary reasons. First, a significant percentage of enrolled students were not both pre- and post-tested. USCIS believes that the students who did not return to post-test are those that are more likely to have achieved measurable educational gains and as a result have a higher level of confidence in their ability to be successful in the naturalization process. Second, the testing and reporting requirement were new to FY 2014 grant recipients. For some grant recipients, the nationally normed, standardized tests were not part of their curricula prior to receiving this grant. USCIS believes that this lack of experience working with standardized tests may also have contributed to the lower results. With additional experience, we expect the negative impacts of this factor to diminish. The Office of Citizenship will continue to monitor grant performance and provide technical assistance to grant recipients regarding the use of pre and post testing, stressing that pre and post testing is required for all enrolled students under USCIS grant guidelines. USCIS will also explore strategies for grantees to provide incentives for students to complete the post-test requirement.</p>									

## Mission 3: Enforce and Administer Our Immigration Laws

### Goal 3.2: Prevent Unlawful Immigration

#### Strategies

- Prevent unlawful entry, strengthen enforcement, and reduce drivers of unlawful immigration
- Arrest, detain, and remove criminals, fugitives, and other dangerous foreign nationals

#### Strategic Review Summary of Progress

Assessment Lead: Tracey Bardorf, Director, U.S. Immigration and Customs Enforcement (ICE), Office of Policy

The Department of Homeland Security (DHS) has determined that performance toward this goal is making satisfactory progress.

#### Introduction

The increased movement of people and goods across our borders provides many legitimate opportunities but also provides more places to conceal illicit goods, unauthorized migrants, and threats to the United States. Unlawful migration is influenced by many factors, including weak rule of law and violence in other countries. In addition, violent extremists and criminals can hide within this larger flow of migrants who intend no harm.

DHS is pursuing a number of strategies, including: increasing situational awareness at our borders; ensuring that only those abroad who are eligible receive travel documents to the United States; and identifying, arresting, detaining, and removing criminal aliens, fugitives, individuals who pose a threat to public safety, repeat immigration violators, and other dangerous foreign nationals.

#### Major Achievements

While total criminal removals declined from the previous year, a significant percentage of ICE's interior removals—85 percent as of September 30, 2014—remained focused on criminal aliens, demonstrating the organization's increasing adherence to stated criminal priorities. Also, 98 percent of all removals, totaling 309,477 individuals, clearly met one or more of ICE's stated civil immigration enforcement priorities: aliens who pose a danger to national security or a risk to public safety; recent illegal entrants; and aliens who are fugitives or otherwise obstruct immigration controls

As of September 30, 2014, U.S. Citizenship and Immigration Services (USCIS) referred more than 19,100 cases to ICE for investigation and or enforcement actions, investigated over 117,200 fraud referrals, and conducted more than 11,700 site visits to verify claims made in requests for immigration benefits and completed more than 13,000 Compliance Reviews (CRs) as part of the Administrative Site Visit and Verification Program. CRs are conducted to establish the legitimacy of the petitioning organization and to verify the accuracy of the information pertaining to the employment offer, thereby ensuring the integrity of the immigration benefits system.

Major Challenges & Opportunities for Improvement

Expansion and implementation of additional immigration benefit granting programs that are driven by executive actions on immigration presents inherent challenges associated with workload management, systems capabilities, integrity assurance, budgetary constraints, and legal considerations. A decline in criminal alien removals can partially be attributed to challenges presented by state and local laws, executive orders, and policies in hundreds of jurisdictions that have limited local law enforcement’s ability to cooperate with ICE detainers.

**Performance Highlight**

Below is a highlighted accomplishment demonstrating success in reducing drivers of unlawful immigration.



**Discovery of Honduran National Wanted for Murder and Attempted Murder**

In July 2015, ICE ERO obtained information from the Honduran National Police via the Criminal History Information Sharing (CHIS) initiative, indicating Juan Jesus Cabrera-Morales was wanted for illegal possession of commercial firearms, attempted murder, and murder in Honduras. Cabrera-Morales was arrested by Border Patrol near Calexico, California for illegally entering the United States.

Information pertaining to the discovery of warrants in Honduras for Cabrera-Morales was made possible because

of ERO’s CHIS program. CHIS is a vital international public safety tool that provides participating nations with criminal history information in advance of an alien’s removal. CHIS also facilitates the exchange of foreign criminal history information to ICE that would have previously gone unknown. These records assist ICE in the identification and classification of additional illegal immigrants within the agency’s criminal removal priorities and enable the discovery of international fugitives.

**Performance Results and Plan**

In FY 2015, there were eight performance measures used to assess the Department’s efforts for this goal. For the FY 2016-2017 performance plan, three new measures are being introduced and three measures are being retired. In FY 2015, 50 percent of the measures met their target and 50 percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary					
	Scale:	0%	25%	50%	75%	100%
Goal 3.2: Prevent Unlawful Immigration				◆		

◆ - Percent of measures that met their FY 2015 target.

◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below are two highlighted strategic measures that gauge efforts to prevent unlawful immigration.

Percent of workers determined to be "Employment Authorized" after an initial mismatch (USCIS)*								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	0.28%	0.24%	0.22%	0.19%	≤ 0.90%	0.17%	≤ 0.80% **	≤ 0.70%

E-Verify is a fast and free Internet-based system that allows employers to confirm the eligibility of their employees to work in the United States. This measure gauges the accuracy of the E-Verify process. The FY 2015 results for this measure, 0.17 percent, demonstrate a year-over-year improvement since FY 2011. E-Verify continues to be very successful in verifying employees with their government records during the initial electronic matching phase to ensure only those individuals who have a right to work are employed. In those cases where the electronic check does not find a match, it is very rare that the applicant will be found to be employment authorized after contesting the initial determination. USCIS continues to improve its processes through E-Verify enhancements such as further action letter notices to employees, myE-Verify, a free online service that permits individuals to create a secure account to manage use of their information in E-Verify, and Self Check, a free online service that allows an individual to check his or her employment eligibility.

- \* - Previous measure name: Percent of initial mismatches for authorized workers that are later determined to be "Employment Authorized."
- \*\* - The FY 2016 target previously published as ≤ 0.90% in the FY 2014 – 2016 Annual Performance Report was changed to ≤ 0.80% based on FY2015 results and historical trends.

Percent of detention facilities found in compliance with the national detention standards by receiving an acceptable inspection rating (ICE)								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	95%	97%	100%	100%	100%	100%	100%	100%

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

The remaining strategic measures are used to gauge our efforts to prevent unlawful immigration. For those measures that did not meet their targets, an explanation with corrective action are provided. In addition, changes to measure names and targets from the previous year’s report are identified. Finally, to continually improve our set of performance measures, new measures are introduced and measures are retired each year, and are identified in the measure tables.

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
<b>ICE</b>									
Average length of stay in detention of all convicted criminal aliens prior to removal from the United States (in days)	37.0	34.7	31.9	33.5	37.5	≤ 34.5	40.3	≤ 37.5	≤ 37.0
<p>The average length of stay (ALOS) in detention for convicted criminal aliens increased by an average of 2.8 days from FY 2014 to FY 2015. This coincided with substantial variations in ALOS in different Areas of Responsibility (AORs). Criminal ALOS increased in particular in the Ninth Circuit AOR, with overall criminal ALOS increasing 12%, from 39 days in FY 2014 to 44 days in FY 2015. Aliens who went through formal hearings contributed the most to criminal ALOS increase, increasing 10 days from FY 2014 to FY 2015. This substantial jump coincides with the 2014 Southwest Border surge, which resulted in a prioritization of Unaccompanied Alien Children (UACs) and family units in the case docket. To address these issues, Enforcement and Removal Operations (ERO) will continue to employ the Criminal Alien Program Surge Enforcement Team initiative at additional state and local facilities. In FY 2015, ERO increased the number of removals of criminal aliens in the Probation &amp; Parole program over FY 2014 by 54%, and in FY 2016 ICE will continue this focus to maintain this positive trend. In FY 2015, Transportation and Removal Program worked with Central American governments to negotiate the removal of 50 Failure to Comply (FTC) cases. In FY 2016 ICE will continue to work FTC cases to reduce processing time on these lengthy cases.</p>									
Number of convicted criminal aliens removed per fiscal year	195,772	216,698	225,390	216,810	177,960	198,000	139,368	158,664 <sup>1</sup>	161,060
<p>As of the end of FY 2015, ICE removed 139,368 convicted criminal aliens, compared to 177,960 in FY 2014. Between FY 2014 and FY 2015, criminal encounters fell 13%. This drop was caused by policies limiting state and local law enforcement cooperation with ICE and a reduction in Border Patrol turnovers. Between January 1, 2014 and September 13, 2015, ICE recorded 18,499 instances of detainers that were declined by local jurisdictions, 8,389 of which were declined between October 1, 2014 and September 13, 2015. When local jurisdictions decline ICE detainers, ICE must dedicate additional officer resources to locate and arrest criminal aliens in the public domain, thereby increasing processing times and risking officer and public safety. Comparing FY 2014 to FY 2015, Border Patrol turnovers were down 26%. Roughly one quarter of border patrol turnovers are convicted criminals, meaning that there were 12,000 fewer convicted criminal turnovers to ICE in FY 2015 than FY 2014. Enforcement and Removal Operations will continue to employ the Criminal Alien Program Surge Enforcement Team initiative at additional state and local facilities. In FY 2015, ERO increased the number of removals of criminal aliens on Probation &amp; Parole over FY 2014 results by 54%, and in FY 2016 ICE will continue to focus on this target area to maintain this positive trend. In FY 2015, the Transportation and Removal Program worked with Central American governments to negotiate the removal of 50 FTC cases. In FY 2016 ICE will continue to work FTC cases to reduce processing time on these lengthy cases.</p>									
Percent of total aliens removed that are criminal aliens	---	---	---	---	---	New Measure		57%	57%
Percent of removal orders secured by ICE attorneys that Support ICE's Civil Enforcement Priorities (CEP)	---	---	---	---	58%	60%	43%	Retired <sup>2</sup>	
<p>This measure indicates the percent of total removal orders secured by the Office of the Principal Legal Advisor (OPLA) attorneys that support the agency's civil enforcement priorities (CEP). However, in November 2014 Secretary Johnson issued a memorandum that altered the definition of what was considered a priority removal, causing ICE to focus their efforts on removing individuals that would not count towards the CEP-based target. ICE will retire the measure and will develop a replacement measure that will better reflect enduring priorities.</p>									
Percent of removal orders secured by ICE attorneys that support current enforcement priorities	---	---	---	---	---	New Measure		60%	60%

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
Number of employers audited, sanctioned, or arrested for violating immigration-related employment laws or otherwise brought into compliance with those laws	---	---	---	4,743	2,191	1,854	1,928	1,854	1,854
<b>USCIS</b>									
Percent of religious worker site visits where potential fraud or other technical noncompliance concerns were identified	---	1%	7%	7%	5%	≤ 10%	5%	Retired <sup>3</sup>	
Percent of non-immigrant worker (H1-B) site visits where potential fraud or other technical noncompliance concerns were identified	---	1%	15%	12%	11%	≤ 15%	9%	Retired <sup>3</sup>	
Percent of applications for citizenship and immigration benefits not approved following a potential finding of fraud	---	---	---	---	---	New Measure		90%	90%

Note 1: The FY 2016 target previously published as 177,314 in the FY 2014 – 2016 Annual Performance Report was changed to 158,664. Targets have been adjusted for FY16 and out years due to changes impacting these results, including: 1) state and local laws, and policies in hundreds of jurisdictions limiting cooperation with ICE detainers; and 2) federal court precedent, leading to a greater number of individuals released on immigration judge-determined bonds and transferred from the detained docket to the non-detained docket.

Note 2: Due to the November 20, 2014 revisions to immigration enforcement removal policies, ICE is retiring this measure and has developed a replacement measure of ICE immigration court activities.

Note 3: USCIS is retiring these two measures and introducing the measure “Percent of applications for citizenship and immigration benefits not approved following a potential finding of fraud” which replaces the two measures with a better outcome oriented measure.

## Mission 4: Safeguard and Secure Cyberspace

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

#### Strategies

- *Enhance the exchange of information and intelligence on risks to critical infrastructure and develop real-time situational awareness capabilities that ensure machine and human interpretation and visualization*
- *Partner with critical infrastructure owners and operators to ensure the delivery of essential services and functions*
- *Identify and understand interdependencies and cascading impacts among critical systems*
- *Collaborate with agencies and the private sector to identify and develop effective cybersecurity policies and best practices*
- *Reduce vulnerabilities and promote resilient critical infrastructure design*

#### Strategic Review Summary of Progress

Assessment Lead      Bob Kolasky, Deputy Assistant Secretary for Infrastructure Protection, National Protection and Programs Directorate (NPPD), Infrastructure Protection

The Department of Homeland Security (DHS) has determined that performance toward this goal is making satisfactory progress.

#### Introduction

Our critical infrastructure is increasingly connected and interdependent. Securing and enhancing its resilience is an economic and national security imperative. As most of the nation's infrastructure is owned and operated by the private sector, DHS partners with industry stakeholders and federal, state, local, territorial, and tribal governments to manage risks that may have national-level impacts. During FY 2014, these endeavors produced satisfactory results in strengthening the security and resilience of critical infrastructure against cyberattacks and other hazards.

#### Major Achievements

In FY 2014, DHS continued to implement mandates from the *2013 National Infrastructure Protection Plan (NIPP)*, *Presidential Policy Directive 21-Critical Infrastructure Security and Resilience*, and *Executive Order 13636 Improving Critical Infrastructure Cybersecurity* by facilitating the sharing of timely and actionable risk products. DHS provides a wide range of risk assessment tools and support to stakeholders that promote risk-based decisions on physical and cyber security measures. DHS initiated the implementation of NIPP 2013 through the release of the Secretary's Joint National Priorities for critical infrastructure, updates of Sector Specific Plans, and the stand-up of a working group to measure progress and coordinate efforts to meet the NIPP Call to Action to leverage partnerships, innovate for risk, and focus on outcomes. Notably, DHS launched the Critical Infrastructure Cyber Community Voluntary Program as the coordination point within the Federal Government for critical infrastructure stakeholders, both public and private, to improve their cyber risk management processes.

### Major Challenges & Opportunities for Improvement

DHS lacks a holistic and coordinated risk management approach that includes both physical and cyber security. Employing an all-hazards approach, DHS continues to work with stakeholders to coordinate policies, tools, capabilities, and human capital that address both physical and cyber security. DHS also lacks robust performance measures that demonstrate the impacts of efforts undertaken by the DHS and its stakeholders. DHS continues to work with its partners to develop security and resilience measures that will aid in understanding Critical Infrastructure Security and Resilience program effectiveness. Lastly, with the persistent and evolving threats posed by cyber incidents, DHS continues to work with its industry partners to define public and private sector roles and responsibilities for responding to significant cyber incidents. Ensuring a timely and coordinated response is key to mitigating impacts in order to better protect both organizations and the American public.

### **Performance Highlight**

Below is a highlighted accomplishment demonstrating success in strengthening the security and resilience of critical infrastructure.



### **Enhanced National Infrastructure Coordinating Center (NICC) Fusion Cell Enhances Situational Awareness**

In spring 2015, Under Secretary Spaulding approved the Interim Capability Plan for an enhanced NICC to be staffed with representatives from all NPPD program offices to provide enhanced situational awareness for all of NPPD's operations. The enhanced NICC is providing: 1) integrated near-real time situational awareness; 2) synthesis and fusion of briefing and reporting products; and 3) executive briefing functions for steady state operations, incidents, and special events.

In early May 2015, the enhanced NICC responded when a suspicious item in a locker triggered an evacuation of New York's Statue of Liberty. The Enhanced NICC's Fusion Cell quickly coordinated information between Federal Protective Service (FPS), and the Office of Infrastructure Protection's Protective Security Coordination Division and Sector Outreach and Programs Division to ensure all personnel, resources and equities were informed. The ability to connect all pertinent divisions effectively and efficiently ensured timely and accurate reporting to senior NPPD leadership and provided enhanced situational awareness for field forces.

The Enhanced NICC's Fusion Cell is comprised of Fusion Action Officers, who are NPPD personnel assigned on detail from a number of operational programs: the FPS, the Office of Cyber and Infrastructure Analysis, National Cybersecurity and Communications Integration Center, and several divisions within the Office of Infrastructure Protection including the Infrastructure Security Compliance Division, Protective Security Coordination Division, and Sector Outreach and Programs Division. The Fusion Action Officers work side by side with the existing NICC team and are directly involved in daily operations, such as information corroboration and coordination calls. This effort will help provide a more integrated and comprehensive level of situational awareness and corresponding briefing capabilities.

Another example of the Fusion Cell at work enhancing situational awareness occurred during the recent civil unrest in Baltimore, Md. The Enhanced NICC's Fusion Cell served as the central point for NPPD operations by identifying and accounting for FPS officers deployed to support law enforcement operations, tracking Protective Security Advisor support to the state Emergency Operations Center, as well as the overall state of infrastructure in the Baltimore area. The Fusion Action Officers were able to coordinate with field and headquarters-based staff to gather information on activities throughout the event, ensuring timely and accurate information and situational awareness for DHS officials.

"The Enhanced NICC is serving a critical role in carrying out NPPD's integrated situational awareness efforts," notes Under Secretary Suzanne Spaulding. "Having a steady-state understanding of the state of the Nation's infrastructure is a key part of our mission and this cross-NPPD initiative will provide this function going forward."

**Performance Results and Plan**

In FY 2015, there were five performance measures used to assess the Department’s efforts for this goal. For the FY 2016-2017 performance plan, two new measures are being introduced. In FY 2015, 60 percent of the measures met their target and 80 percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary					
	Scale:	0%	25%	50%	75%	100%
Goal 4.1: Strengthen the Security and Resilience of Critical Infrastructure				◆	◆	

◆ - Percent of measures that met their FY 2015 target.

◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below are two highlighted strategic measures that gauge efforts to strengthen the security and resilience of critical infrastructure.

**Percent of intelligence reports rated “satisfactory” or higher in customer feedback that enable customers to manage risks to cyberspace (Intelligence and Analysis (I&A))**

FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	88%	94%	94%	95%	93%*	95%	95%

In today’s interconnected world, every second can make a difference in either preventing an incident or responding to an event that affects the Nation. The ability of federal, state, local, tribal, territorial, and private sector partners to share accurate information quickly is essential to the Nation’s security and resilience. This measure assesses how well the Department provides actionable intelligence to our partners to manage risks to cyberspace. In FY 2015, I&A achieved a 93 percent rating and is pursuing other ways to gauge customer feedback and will work to update the measure set with improved customer service feedback measures.

\* - The FY 2015 results were previously reported as 94% in the DHS FY 2014 Agency Financial Report and have been restated based on additional information received.

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

FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	100%	63%	60%	100%	100%*	100%

This measure addresses the extent to which critical infrastructure owners and operators use the results of cybersecurity vulnerability and resiliency assessments to improve their cybersecurity posture. During FY 2015, 26 feedback forms were received from sites that participated in a cyber resilience review (CRR) or used the cyber security evaluation tool (CSET). Of those 26 forms, Strategic Risk Assessment and Mitigation received seven, and Industrial Control System-Cyber Emergency Response Team received nineteen. Each one of the organizations that submitted a feedback form indicated the implementation of at least one enhancement resulting from the CRR or CSET.

\* - The FY 2016 target previously published as 65% in the FY 2014 – 2016 Annual Performance Report was changed to 100% based on FY 2015 results.

The remaining strategic measures are used to gauge our efforts to partner to reduce cyber and physical risk to critical infrastructure. For those measures that did not meet their targets, an

explanation with corrective action are provided. In addition, changes to measure names and targets from the previous year’s report are identified. Finally, to continually improve our set of performance measures, new measures are introduced and measures are retired each year, and are identified in the measure tables.

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
<b>NPPD</b>									
Percent of facilities that are likely to integrate vulnerability assessment or survey information into security and resilience enhancements	---	---	---	---	89%	80%	90%	80% <sup>1</sup>	80%
Percent of high risk facilities that receive a facility security assessment in compliance with the Interagency Security Committee (ISC) schedule	---	---	---	34%	93%	100%	100%	100%	100%
Percent of respondents indicating that operational cybersecurity information products provided by DHS are timely and actionable	---	---	58%	74%	79%	82%	81%	85% <sup>2</sup>	90%
Feedback responses received in the fourth quarter of FY 2015 were lower than in any previous quarter. Of the 31 responses to the customer satisfaction survey that were received in FY 2015, 25 responses indicated that the National Cybersecurity and Communications Integration Center (NCCIC) provided information that was both timely and actionable. The Office of Cybersecurity and Communications continues to use the Cyber Information Sharing and Collaboration Program's analyst-to-analyst exchange opportunities to understand customer preferences with respect to NCCIC products, and to make product improvements where possible. For FY 2015, the final result of 81% narrowly missed the target of 82% by one percentage point. The Department continues to improve the quality and timeliness of the cybersecurity indicators shared with external stakeholders. In FY 2016, DHS will institute an automated process to share indicators with stakeholders.									
Percent of survey respondents that were satisfied or very satisfied with the timeliness and relevance of cyber and infrastructure analysis based products	---	---	---	---	---	New Measure <sup>3</sup>		80%	82%
Percent of respondents reporting that DHS critical infrastructure information will inform their decision making on risk mitigation and resilience enhancements	---	---	---	---	---	New Measure <sup>4</sup>		71%	74%

Note 1: There are a few reasons that the targets remain at 80%. Facilities volunteer to receive initial assessments and recurring assessments every three years. It is anticipated that facilities will implement enhancements at a much slower rate after their initial assessment. In addition, the program has seen a drop in total assessments from FY 2014 as fewer facilities are volunteering to participate, thus resulting in a shrinking denominator for this measure.

Note 2: The FY 2016 target previously published as 90% in the FY 2014 – 2016 Annual Performance Report was changed to 85% based on FY 2015 results and trends from previous years.

Note 3: NPPD is introducing this measure to evaluate the Office of Cyber and Infrastructure Analysis, which informs the federal, state, local and private sector to improve their cyber and infrastructure resiliency efforts or plans.

Note 4: NPPD is introducing this measure to evaluate a range of training, exercise, and information sharing activities developed and implemented for the six sectors led by the Office of Infrastructure Protection, which include chemical, commercial facilities, critical manufacturing, dams, emergency services, and nuclear sectors, as well as cross-sector engagements with state, regional, and local partners.

## Mission 4: Safeguard and Secure Cyberspace

### Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise

#### Strategies

- *Coordinate government purchasing of cyber technology to enhance cost-effectiveness*
- *Equip civilian government networks with innovative cybersecurity tools and protections*
- *Ensure government-wide policy and standards are consistently and effectively implemented and measured*

#### Strategic Review Summary of Progress

Assessment Lead Mike Darling, Director of Enterprise Performance Management Office, National Protection and Programs Directorate (NPPD), Office of Cybersecurity and Communications

The Department of Homeland Security (DHS) has determined that performance toward this goal is making satisfactory progress.

#### Introduction

The Federal Government provides essential services and information on which many Americans rely. Not only must the government protect its own networks, it must serve as a role model to others in implementing security services. DHS itself plays a leading role in securing federal civilian networks, allowing the Federal Government to do its business securely.

#### Major Achievements

Among our successes, the Continuous Diagnostics & Mitigation (CDM) program significantly improved initial operating capacity, and the Chief Information Officer (CIO) team conducted extensive engagements with stakeholders and partners across the federal civilian government to increase CIO's knowledge on the cybersecurity services available to them by DHS and to foster collaboration and coordination.

As of December 31, 2014, DHS reached a total of 62 signed Memoranda of Agreement (covering all 23 non-defense Chief Financial Officer Act agencies in addition to 40 small/micro agencies and the U.S. Postal Service) to permit DHS to provide the full suite of EINSTEIN program capabilities for internet security situational awareness. The EINSTEIN Program is an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal civilian government so that federal agencies will be aware of the threats to their infrastructure in nearly real-time and can act swiftly to take corrective measures. DHS increased EINSTEIN 2 coverage to 79 departments or agencies, including 18 of 18 .gov Trusted Internet Connection Access Providers.

DHS also established intrusion prevention services with two additional internet service providers (ISPs), putting three "Tier 1" critical ISP Intrusion Prevention Security Service contracts in place. DHS deployed Einstein 3 Accelerated capabilities to one ISP, providing the capacity to protect

500,000 federal users from malicious e-mail attacks (such as e-mail-initiated spear phishing campaigns) or malware installed on .gov networks from communicating with external entities attempting to control that malware.

As of December 31, 2014, CIO increased the number of required Personal Identification Verification (PIV) card users to authenticate to a DHS network from 16 percent to 84 percent. DHS CIO also designed and hosted the first Small and Micro Agency Cybersecurity Support Workshop, providing information to small agency Chief Information Security Officers (CISOs) and CIOs on the cybersecurity services available to them through DHS.

Through outreach activities, DHS was able to receive all Secured Content Automation Protocol (SCAP) feeds from the departments/agencies for the first time. This effort also included a Performance Analysis Console which was implemented within CyberScope that includes vulnerability risk scoring charts on Agencies' Federal Information Security Management Act (FISMA) and SCAP submissions over periods of time, furthering our understanding of risk through data.

#### Major Challenges & Opportunities for Improvement

Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing, granted DHS authorities in developing a unique standards organization for information sharing. DHS has an opportunity to collaborate with both public and private sector partners to increase the exchange of threat information beyond the current capabilities by creating a common set of standards to govern the creation and function of Information Sharing Analysis Organizations. Deploying our technical tools can present a challenge as CDM will not operate at full capacity until the sensors are fully installed at participating agencies and the Federal dashboard is operational. In addition, the interpretation of the implementation of HSPD-12 Mandatory PIV varies from agency-to-agency across government, creating a disparity when results are rolled up.

## Performance Highlight

Below is a highlighted accomplishment demonstrating success in expanding enhanced cybersecurity services.

### DHS Continues to Expand Enhanced Cybersecurity Services Program

As part of our effort to share timely and actionable cyber threat information with the private sector, the DHS has expanded the [Enhanced Cybersecurity Services \(ECS\)](#) program beyond those entities classified as “critical infrastructure” to all interested U.S.-based public and private organizations.

ECS solves a difficult challenge for the U.S. government: sometimes, the government has information so sensitive that the information is classified. If information is classified, DHS cannot share it broadly with the private sector to let companies protect themselves. The solution is ECS. Through ECS, DHS shares sensitive and classified cyber threat indicators from across government with Commercial Service Providers (CSPs).

In turn, these CSPs use this information to protect their customers, via a commercial agreement, from cyber threats. CSPs are thus a managed security service: a company can pay to receive the security service that these CSPs offer.

Until recently, only critical infrastructure sector entities could receive ECS. Now, CSPs are able to offer ECS to all interested U.S.-based public and private organizations. In FY 2015, ECS accredited two additional CSPs, Verizon, and Lockheed Martin, who are now able to provide ECS intrusion prevention capabilities to customers. CSP accreditation is a time and labor intensive process, sometimes taking well over two years to deploy security systems and finalize security requirements. In addition to Lockheed and Verizon, AT&T and CenturyLink are also accredited to provide ECS, with numerous other companies currently proceeding through the accreditation process. DHS does not endorse any one particular service or business.

ECS currently offers two countermeasure services, Domain Name System Sinkholing and Email Filtering. The program expects to add a third service to its line-up in FY 2016. Since inception, ECS has blocked approximately 1,000,000 instances of malicious activity from customer networks. The Federal Government and five sectors (Communications, Commercial Facilities, Defense Industrial Base, Energy, and Finance) currently use ECS. The program is now accelerating outreach efforts in the hopes of bringing more sectors to the table. ECS has proven to be a highly effective part of a layered defense, and is recommended for any organization seeking to implement additional protections against sophisticated threats.

## Performance Results and Plan

In FY 2015, there were two performance measures used to assess the Department’s efforts for this goal. In FY 2015, 100 percent of the measures met their target and 100 percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary				
	Scale:	0%	25%	50%	75%
Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise	◆◆				

- ◆ - Percent of measures that met their FY 2015 target.
- ◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below are two highlighted strategic measures that gauge efforts to secure the federal civilian government information technology enterprise. Changes to measure names and targets from the previous year’s report are identified.

Percent of traffic monitored for cyber intrusions at civilian Federal Executive Branch agencies (NPPD)								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	73.0%	82.4%	88.5%	89.0%	94.3%	95.0%*	95.0%

This measure assesses DHS’s scope of coverage for potential malicious cyber-activity across participating civilian Federal Government agencies.<sup>3</sup> Federal Executive Branch network monitoring uses EINSTEIN 2 network flow and intrusion detection system sensors which are deployed to trusted Internet connection locations at agencies or Internet service providers. These sensors capture network flow information and provide alerts when signatures, indicative of malicious activity, are triggered by inbound or outbound traffic. The long-term trend is positive for this measure and there continues to be an aggressive plan to consolidate Internet traffic of the civilian Federal Government agencies through the EINSTEIN intrusion detection system sensors. In FY 2015, 94.3 percent of the Federal Executive Branch agencies network traffic was monitored for cyber-intrusions.

\* - The FY 2016 target previously published as 89% in the FY 2014 – 2016 Annual Performance Report was changed to 95% based on the FY 2015 year-end results to be more ambitious.

Percent of known malicious cyber traffic prevented from causing harm at federal agencies (NPPD)								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	---	100%	85%	100%	100%*	100%

This performance measure assesses the percent of known malicious activity that is mitigated on federal agencies’ networks through an active defense capability known as EINSTEIN 3 Accelerated. This is achieved by actively defending against malicious activity through detection and prevention, and applying countermeasures if needed for protection. Each currently deployed indicator of a malicious threat is paired with a countermeasure to prevent the malicious threat from harming those networks. DHS has met the FY 2015 annual target; however, results may fall below 100% in future fiscal years as the program expands the number of indicators and countermeasures it uses.

\* - The FY 2016 target previously published as 90% in the FY 2014 – 2016 Annual Performance Report was changed to 100% to reflect current capabilities of the deployed EINSTEIN systems.

<sup>3</sup> Defined as Chief Financial Officers (CFO) Act agencies (other than the Department of Defense) as well as non-CFO Act agencies that are Trusted Internet Connection Access Provider agencies.

## Mission 4: Safeguard and Secure Cyberspace

### Goal 4.3: Advance Cyber Law Enforcement, Incident Response, and Reporting Capabilities

#### Strategies

- Respond to and assist in the recovery from cyber incidents
- Deter, disrupt, and investigate cybercrime

#### Strategic Review Summary of Progress

Assessment Lead      Co-Lead: Kenneth Jenkins, Deputy Assistant Director, U.S. Secret Service (USSS), Office of Investigations  
Co-Lead: Mike Darling, Director of Enterprise Performance Management Office, National Protection and Programs Directorate (NPPD), Office of Cybersecurity and Communications

The Department of Homeland Security (DHS) has determined that performance toward this goal is making satisfactory progress.

#### Introduction

Online criminal activity threatens the Internet's safe and secure use. Law enforcement performs an essential role in achieving our Nation's cybersecurity objectives by detecting, investigating, and preventing a wide range of cybercrimes, from theft and fraud to child exploitation, and apprehending and prosecuting those responsible. In addition to criminal prosecution, there is a need to rapidly detect and respond to incidents, including through the development of quarantine and mitigation strategies, as well as to quickly share incident information so that others may protect themselves. Safeguarding and securing cyberspace requires close coordination among federal law enforcement entities, network security experts, state, local, tribal, and territorial officials, and private sector stakeholders.

#### Major Achievements

The USSS and the United States Computer Emergency Readiness Team (US-CERT) provided information to UPS Stores Inc. to protect itself and its customers from criminal activity; UPS identified 51 impacted stores in 24 states and stopped this cyber incident before it developed into a major data breach. DHS's Science and Technology Directorate developed methods and tutorials for acquiring and analyzing information from 13 different disposable phone models, regardless of the presence of Universal Serial Bus or any active device locks. The tutorials are available free of charge to federal, state, local, and select international law enforcement partners.

DHS's National Cybersecurity and Communications Integration Center (NCCIC) substantially reduced the number of federal Heartbleed vulnerability instances from 265 to 2 over a three week period during April, 2014. This was a 99 percent reduction in Heartbleed exposures across the federal government. During this timeframe the NCCIC conducted over 1,000 network scans and delivered over 100 Heartbleed reports to federal partners.

**Major Challenges & Opportunities for Improvement**

Using the situational awareness available from the NCCIC and the Federal Network Resilience’s understanding of Federal agency cybersecurity challenges and requirements, DHS will have an opportunity to leverage the authorities provided by the *National Cybersecurity Protection Act of 2014* and the *Federal Information Security Management Act Modernization Act of 2014*. These requirements give the NCCIC the opportunity to become the federal civilian center for sharing cybersecurity risks, incidents, analysis, and warnings for federal and non-federal entities. A challenge associated with this opportunity will be managing the potential increased demand with current staffing levels. In addition, DHS law enforcement entities (USSS and U.S. Immigration and Customs Enforcement) face the challenge of maintaining a highly trained cadre of agents and analysts with computer and network knowledge to lead DHS cyber protection and investigations in the future.

**Performance Highlight**

Below is a highlighted accomplishment demonstrating success in cyber law enforcement, response, and reporting.



**Global Cyber Mastermind Extradited**

In June 2015, a multi-year cyber investigation, led by the USSS, culminated in Brooklyn federal court with the arraignment of an alleged architect of a massive global cybercrime operation. Ercan Findikoglu, 33, was arrested by the German BKA (Federal Investigative Police) pursuant to an arrest warrant issued by the United States District Court.

Since 2010, it is alleged that an elite team of hackers, led in part by Findikoglu, targeted payment processors and financial institutions involved in processing prepaid debit cards. The group specialized in

breaching databases associated with prepaid debit cards, raising the withdrawal limits of accounts, disabling security features, and utilizing the accounts to orchestrate worldwide cash-out events. The group has allegedly been linked to at least three of these types of cyber intrusions with actual losses in excess of \$55 million.

Over the past year, several other high ranking members of this criminal organization have been apprehended locally and abroad by both members of USSS, and members of foreign law enforcement agencies working in conjunction with the USSS New York Field Office. As a result of forging new, unprecedented relationships with various international law enforcement partners, USSS has been able to expand both its knowledge of this organization, and maintain itself on the forefront of upcoming malicious trends and tactics.

**Performance Results and Plan**

In FY 2015, there were five performance measures used to assess the Department’s efforts for this goal. For the FY 2016-2017 performance plan, one new measure is being introduced. In FY 2015, 80 percent of the measures met their target and 100 percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary					
	Scale:	0%	25%	50%	75%	100%
Goal 4.3: Advance Cyber Law Enforcement, Incident Response, and Reporting Capabilities					◆	◆

◆ - Percent of measures that met their FY 2015 target.

◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below are two highlighted strategic measures that gauge efforts to advance law enforcement, incident response, and reporting capabilities.

Percent of incidents detected by the U.S. Computer Emergency Readiness Team for which targeted agencies are notified within 30 minutes (NPPD)								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	89.0%	87.2%	92.0%	96.6%	94.0%	96.0%

US-CERT detects malicious cyber activity targeting Federal agencies. This measure assesses the percent of incidents directed at Federal agencies and detected by the US-CERT for which agencies are informed of this malicious activity within 30 minutes. This measure demonstrates the US-CERT's ability to share situational awareness of malicious activity with its federal agency stakeholders through the EINSTEIN intrusion detection systems and other tools. In FY 2015, US-CERT detected a total of 536 incidents, responding to 518 of these incidents within 30 minutes for a 96.6 percent response rate—a significant improvement from FY 2014.

Amount of dollar loss prevented by Secret Service cyber investigations (in millions) (USSS)								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	\$1,119	\$384	\$727	\$589	\$575*	\$600

The measure reflects USSS's efforts to reduce cyberrelated financial losses to the public. The USSS maintains [Electronic Crimes Task Forces](#), which focus on identifying and locating international cyber criminals connected to cyber intrusions, bank fraud, data breaches, and other computer-related crimes. In FY 2015, \$589 million were prevented by USSS cyber-investigations. This year's target was not met for a few primary reasons which include: many financial and cybercrime cases are very large in scope and take a long time to investigate; the field special agent workforce has reached a historic low; and some agents were diverted to support campaign protection and the visit from the Pope. USSS will improve performance by addressing staffing shortfalls in the recently developed Human Capital Plan.

\* - FY 2016 target reflects USSS allocation of personnel to support campaign protection. The FY 2016 target previously published as \$727 in the FY 2014 – 2016 Annual Performance Report was changed to \$575. The FY16 and out year targets were adjusted based on FY15 results and the unpredictable size, scope, and closure rate of these types investigations.

The remaining strategic measures below were used in FY 2015 to gauge our efforts to advance cyber law enforcement, incident response, and reporting capabilities. For those measures that did not meet their targets, an explanation with corrective action are provided. In addition, changes to measure names and targets from the previous year's report are identified.

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
<b>USSS</b>									
Number of law enforcement individuals trained in cyber crime and cyber forensics both domestically and overseas	---	---	---	1,517	1,533	1,300	2,070	1,800 <sup>1</sup>	1,900
Number of financial accounts recovered (in millions)	---	---	---	3.90	0.29	0.40	0.93	0.40	0.40
Terabytes of data forensically analyzed for criminal investigations	---	---	---	4,002	4,902	3,800	6,052	6,000 <sup>2</sup>	7,000
Number of cyber mitigation responses	---	---	---	---	---	New Measure <sup>3</sup>		410	430

Note 1: The FY 2016 target previously published as 1,300 in the FY 2014 – 2016 Annual Performance Report was changed to 1,800 based on previous trends and expected performance in the future.

Note 2: The FY 2016 target previously published as 3,800 in the FY 2014 – 2016 Annual Performance Report was changed to 6,000 based on previous trends and expected performance in the future.

Note 3: New measure added to assess area of importance in this goal.

## Mission 4: Safeguard and Secure Cyberspace

### Goal 4.4: Strengthen the Cyber Ecosystem

#### Strategies

- Drive innovative and cost effective security products, services, and solutions throughout the cyber ecosystem
- Conduct and transition research and development, enabling trustworthy cyber infrastructure
- Develop skilled cybersecurity professionals
- Enhance public awareness and promote cybersecurity best practices
- Advance international engagement to promote capacity building, international standards, and cooperation

#### Strategic Review Summary of Progress

Assessment Lead      Pete Fonash, Chief Technology Officer, National Protection and Programs Directorate (NPPD), Office of Cybersecurity and Communications

The Department of Homeland Security (DHS) has determined that performance toward this goal is making satisfactory progress.

#### Introduction

DHS made satisfactory progress in its efforts to strengthen a healthy cyber ecosystem through innovating and developing cost effective security products, conducting research and transitioning it to market, developing and executing programs and initiatives to cultivate skilled cybersecurity professionals, enhancing public awareness of cybersecurity, and advancing international engagements to promote capacity building and cooperation around cybersecurity.

#### Major Achievements

DHS strengthened the cyber ecosystem by driving innovative and cost effective security products, services, and solutions through the Transition to Practice Program which brokered a deal to license Los Alamos National Lab's quantum encryption package. This new technology creates encryption keys impervious to cryptanalysis and contains Quantum Key Distribution technology that secures communications. DHS conducted and transitioned research and development to enable a trustworthy cyber infrastructure through the Software Assurance Marketplace (SWAMP), an online, open-source, collaborative research environment. SWAMP allows software developers to test software for security weaknesses, software tool developers to improve tools by offering a wide range of software packages to test against, and software researchers to interact and exchange ideas.

Furthermore, skilled cybersecurity professionals were developed by expanding access to cybersecurity training through expanding the Federal Virtual Training Environment and the Federal Cybersecurity Training Events programs. Public awareness of cybersecurity was enhanced and best practices promoted through the hosting and support of National Cybersecurity Awareness Programs, including the Stop.Think.Connect.™ campaign. And finally, DHS strengthened operational information sharing and coordination with America's closest allies and key partners to

foster new relationships in key regions by providing training and promoting DHS cybersecurity resources and participated in global standards bodies and cybersecurity fora to promote DHS leadership on global cybersecurity discussions.

### Major Challenges & Opportunities for Improvement

The cybersecurity landscape and environment continually changes. As this is an inherent challenge to cybersecurity, DHS capitalized on a vulnerability (i.e., Heartbleed) to develop Memorandums of Understandings with federal agencies and departments to scan networks. This allows DHS to scan these networks on a periodic ongoing basis, to quarantine, and to investigate potential vulnerabilities to assess threat levels and to mitigate them.

### **Performance Highlight**

Below is a highlighted accomplishment demonstrating success in developing skilled cybersecurity professionals.



### **Expanded Access to FedVTE Provides Free Cybersecurity Training**

America needs a strong cybersecurity workforce to keep up with evolving technology and increasing cybersecurity risks. To help meet this need, DHS has expanded access to the Federal Virtual Training Environment ([FedVTE](#)) – an online training center featuring a wide range of cybersecurity courses – to

state, local, tribal, and territorial (SLTT) government employees and U.S. veterans across the country.

DHS is coordinating outreach about the program to SLTT governments through the Multi-State Information Sharing and Analysis Center (MS-ISAC), which is a part of the nonprofit Center for Internet Security. With a mission to improve the overall cyber security posture of SLTT governments, the MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's SLTT governments. SLTT government personnel may contact [info@msisac.org](mailto:info@msisac.org) with any account approval questions.

DHS also has coordinated efforts with the non-profit Hire Our Heroes to enable U.S. veterans' access to FedVTE. Hire our Heroes' goal is to train, mentor, and coach transitioning veterans. Veterans may register for a FedVTE account at <https://hireourheroes.org/veterans-training/>.

Sponsored by DHS and supported by the Department of Defense's Defense Information Systems Agency, FedVTE provides:

- Government-wide, on-demand access to cybersecurity training to help the workforce maintain expertise and foster operational readiness;
- Courses ranging from beginner to advanced levels;
- Training available at no cost to users; and
- Training accessible from any Internet-enabled computer.

On average, FedVTE delivers more than 35,000 hours of training per month and in 2014 alone, FedVTE saved the Federal Government approximately \$72 million in training costs.

For more information about FedVTE, please visit the National Initiative for Cybersecurity Careers and Studies portal at: <http://niccs.us-cert.gov/training/fedvte>. Qualified users may access the system at [fedvte.usalearning.gov](http://fedvte.usalearning.gov).

**Performance Results and Plan**

In FY 2015, there was one performance measure used to assess the Department’s efforts for this goal. In FY 2015, zero percent of the measures met their target and zero percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary				
	Scale:	0%	25%	50%	75%
Goal 4.4: Strengthen the Cyber Ecosystem					

◆ - Percent of measures that met their FY 2015 target.

◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below is a strategic measure that gauges efforts to strengthen the cyber ecosystem.

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

FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	89%	93%	80%	60%	73%*	80%

This measure reflects the percent of identified and completed planned transitions of cybersecurity products and/or services (e.g. technologies, tools, capabilities, standards, knowledge products) within S&T’s Cyber Security Division (CSD) projects to government, commercial or open sources. The percent reported is reviewed using the number of planned transition milestones stated in CSD’s budget execution plan for the fiscal year. Sixty percent of CSD’s identified products and services have transitioned as of the end of the year. These included a broad range of capabilities, tools, and services, such as technology pilots that were deployed at several federal agencies (such as Health and Human Services, DHS) and local governments (City of Tulsa), a privacy policy reasoning engine, and a risk assessment tool for cloud based systems. Reasons for not meeting the target include: 1) for the Computer Security Incident Response Team milestone, publication of the handbook was delayed in order to incorporate feedback from training sessions that are planned for several stakeholder organizations; and 2) funding constraints impacted the milestones relating to research on the best practices of hardware and user identification on a network. S&T completed three of the four missed transitions in the first quarter of FY 2016. To help ensure milestones are met next year, CSD will implement a more robust review process each quarter with each responsible program manager. The review will include a schedule, budget, and technical progress analysis.

\* - The FY 2016 target previously published as 80% in the FY 2014 – 2016 Annual Performance Report was changed to 73%. Based on the transition plan in FY 2016, the target has been adjusted to be ambitious yet achievable.

## Mission 5: Strengthen National Preparedness and Resilience

### Goal 5.1: Enhance National Preparedness

#### Strategies

- Empower individuals and communities to strengthen and sustain their own preparedness
- Build and sustain core capabilities nationally to prevent, protect against, mitigate, respond to, and recover from all hazards
- Assist federal entities in the establishment of effective continuity programs that are regularly updated, exercised, and improved

#### Strategic Review Summary of Progress

Assessment Lead Kathleen Fox, Assistant Administrator for National Preparedness Directorate, Federal Emergency Management Agency (FEMA)

The Department of Homeland Security (DHS) has determined that performance toward this goal is making satisfactory progress.

#### Introduction

Preparedness against hazards, such as natural disasters, acts of terrorism, and pandemics is a shared responsibility that calls for the involvement of everyone—known as the “whole community” approach—in preparedness efforts. DHS continued to expand its whole community implementation of the National Preparedness System to build and sustain core capabilities identified in the National Preparedness Goal. States and territories begin by assessing risks and identifying capability gaps and DHS supports the enhancement of national preparedness by implementing data-driven national programs that provide planning, training, exercise support, and resources. DHS made significant strides engaging the whole community and incorporating lessons learned from previous incidents into future planning.

#### Major Achievements

Every state and territory submitted a Threat and Hazard Identification and Risk Assessment (THIRA)<sup>4</sup>, identified their capability gaps, and assessed progress. As of September 30, 2014, 71 percent of states are meeting the DHS THIRA guidance which is significant in that the implementation of this comprehensive planning process to assess risk and capabilities is still in the early stages. Over 5,400 contributors across all levels of government, private sector, and non-governmental organizations (NGOs) participated in the THIRA process, an increase of 4,191 contributors over last year due to improved communication, planning, and outreach efforts. America’s PrepareAthon! had over 17 million participants register to conduct preparedness actions in events across the country as of September 30, 2014.

<sup>4</sup> The THIRA process is a comprehensive assessment for identifying community-specific threats and hazards, setting capability targets for each core capability identified in the National Preparedness Goal, and estimating resources needed to meet the capability targets.

DHS brought together federal, state, local, and territorial jurisdictions, NGOs, and private industry partners to exercise significant planning and preparedness needs through the 2014 CAPSTONE series of exercises designed to educate and prepare participants for potential catastrophic events. In addition, the Spill of National Significance Executive Seminar identified three major policy initiatives and established workgroups to address those initiatives. In response to the Ebola virus outbreak, DHS coordinated with federal, state, and local responders and quickly developed and delivered training and exercises on Personal Protective Measures for Biological Events to first responders to meet significant nationwide demand.

### Major Challenges & Opportunities for Improvement

The greatest challenge in emergency management lies in preparing for a catastrophic disaster. DHS continues to improve its capacity to respond to incidents while engaging non-traditional partners. The National Preparedness Report identified Access Control and Identity Verification core capabilities as a new national area for improvement, along with cybersecurity, housing, infrastructure systems, long-term vulnerability reduction, and economic recovery. The increased potential for landside and maritime disasters, natural disasters or manmade disasters, will continue to challenge the Nation's current capacity to prepare for and respond to incidents while encouraging innovation to adapt to changing circumstances.

### **Performance Highlight**

Below is a highlighted accomplishment demonstrating success in enhancing national preparedness.



### **Non-Disaster Grant Funding in Action**

In 2014, the City of Philadelphia, which is part of the Southeastern Pennsylvania Regional Task Force (SEPA RTF), developed and conducted the Medical Surge Exercise Program, a series of exercises that improved the region's ability to implement an integrated approach to mass casualty incidents. Components of this exercise program included the Family Assistance Workshop, the Mass Fatality Workshop, the Mass Fatality Tabletop Exercise, and the Family Assistance Center Functional Exercise. The exercise series validated and finalized two new response plans and evaluated the ability of participating agencies

to establish an incident command structure that properly supported fatality management operations and perform patient tracking and family reunification operations.

The exercises and planning were timely—on May 12, 2015, an Amtrak train traveling from Washington, D.C. to New York City derailed in North Philadelphia. This level 3 mass casualty incident resulted in eight fatalities and more than 200 injuries. During the response, the City of Philadelphia activated its Family Assistance Services and Mass Fatality plans and conducted medical surge operations, activities supported by recent preparedness investments made using FEMA Urban Areas Security Initiative (UASI) funding.

The SEPA RTF spent \$188,950 in UASI funding on the Medical Surge Exercise Program, an investment that directly contributed to the ability of first responders at the scene of the Amtrak derailment to successfully execute incident response operations and support survivor needs.

**Performance Results and Plan**

In FY 2015, there were five performance measures used to assess the Department’s efforts for this goal. For the FY 2016-2017 performance plan, one new measure is being introduced and one measure is being retired. In FY 2015, 60 percent of the measures met their target and 80 percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary					
	Scale:	0%	25%	50%	75%	100%
Goal 5.1 Enhance National Preparedness				◆	◆	

◆ - Percent of measures that met their FY 2015 target.

◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below are two highlighted strategic measures that gauge efforts to enhance national preparedness.

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

FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	86%	71%	100%	77%	100%	100%

The National Preparedness Goal is, “A secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.” The THIRA is a four step common risk assessment process that helps the whole community—including individuals, businesses, faith-based organizations, nonprofit groups, schools and academia and all levels of government—understand its risks and estimate capability requirements. FEMA has set the target for this measure to be 100 percent in light of its importance to the “whole community.” In FY 2015, all 56 states and territories submitted THIRAs as required; 77 percent have developed a THIRA that meets all 4 steps of the current DHS guidance. Thirteen states experienced challenges with developing measurable capability targets, understanding resource requirements, and identifying National Incident Management System resource types. These results informed FEMA’s Threat and Hazard Identification and Risk Assessment technical assistance, which will assist states and territories to achieve alignment with DHS guidance in FY 2016.

**Percent of federal agencies ready to initialize continuity of essential functions and services in the event of a catastrophic disaster (FEMA)**

FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	---	---	94.0%	96.6%	95.5%	97.0%

This measure assesses the percent of federal agencies ready to respond immediately to a continuity of operations event. This measure encompasses federal agencies that are required to respond to notification tests and real-world incidents within four hours. The FY 2015 target of this measure was met with 96.6 percent of required federal departments and agencies successfully acknowledging receipt of continuity readiness alerts and notifications within four hours of their issuance.

The remaining strategic measures are used to gauge efforts to enhance national preparedness. For those measures that did not meet their targets, an explanation with corrective action are provided. In addition, changes to measure names and targets from the previous year’s report are identified.

Finally, to continually improve our set of performance measures, new measures are introduced and measures are retired each year, and are identified in the measure tables.

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
<b>FEMA</b>									
Number of states and territories that have demonstrated improvement towards achieving their core capability targets established through their Threat and Hazard Identification and Risk Assessment (THIRA)	---	---	---	---	28	29	31	Retired	
Percent of states and territories that have achieved an intermediate or above proficiency to address their targets established through their THIRA	---	---	---	---	---	New Measure <sup>1</sup>		68%	70%
Percent of high-priority core planning capabilities <sup>2</sup> rated as proficient by states and territories	---	---	39.6%	38.3%	44.3%	44.0%	46.3%	46.0%	48.0%
Percent of adults that participated in a preparedness exercise or drill at their workplace, school, home or other community location in the past year	---	---	---	---	43%	44%	N/A	46%	48%
This measure is being reported as unreliable for the FY 2015 reporting cycle. In an effort to streamline the survey in FY 2015, FEMA shortened the composite questions that provided data for this measure resulting in a methodology error. FEMA has taken corrective action to return to the original methodology in the FY 2016 survey.									

Note 1: FY 2015 baseline results for this measure were 67.8%.

Note 2: Please see the [National Preparedness Goal](#) for a description of the core capabilities.

## Mission 5: Strengthen National Preparedness and Resilience

### Goal 5.2: Mitigate Hazards and Vulnerabilities

#### Strategies

- *Promote public and private sector awareness and understanding of community-specific risks*
- *Reduce vulnerability through standards, regulation, resilient design, effective mitigation, and disaster risk reduction measures*
- *Prevent maritime incidents by establishing, and ensuring compliance with, standards and regulations*

#### Strategic Review Summary of Progress

Assessment Lead      Co-Lead: Roy Wright, Deputy Associate Administrator for Insurance & Mitigation, Federal Emergency Management Agency (FEMA)  
Co-Lead: Jonathon Burton, CAPT, U.S. Coast Guard (USCG), Director, Inspections and Compliance

The Department of Homeland Security (DHS) has determined that performance toward this goal is making satisfactory progress.

#### Introduction

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

#### Major Achievements

As of September 30, 2014, more households and communities are taking steps to mitigate property damage and adopt disaster-resistant building codes than in previous years. Maritime mitigation efforts included screening 212,000 vessels, 30 million vessel crewmembers & passengers, and updating the 43 Area Maritime Security Plans to assess cyber vulnerabilities and marine transportation system recovery capacities. These efforts ensured the 5-year average number of chemical discharge incidents, oil spills, and commercial mariner and recreational boating deaths and injuries all were reduced.

The implementation of SUMMIT<sup>5</sup> software by FEMA allowed responders and decision makers to access the nation's modeling & simulation resources to analyze and prepare for incidents. The Mitigation Framework Leadership Group developed a Federal Flood Risk Management Standard to

<sup>5</sup> SUMMIT is a modeling & simulation software environment that enables analysts, emergency planners, responders, and decision makers to seamlessly access integrated suites of modeling tools & data sources for planning, exercise, or operational response. SUMMIT is being used in small and large-scale exercises to accelerate scenario planning, provide scientifically-grounded scenario data, and enhance the realism and common operating picture.

ensure federally-funded projects are built to account for flood risk. Other flood mitigation actions included: expansion of FEMA’s flood mapping program (Risk MAP) to cover 53 percent of the U.S. population, a new test tunnel for testing inflatable tunnel plug prototypes designed to prevent flooding in mass transit systems, development of an APEX Flood Program implementation strategy to increase community resilience, and 25 pilot programs to provide accurate assessments of communities’ flood risks.

### Major Challenges & Opportunities for Improvement

Though DHS made advances in mitigating hazards and vulnerabilities, significant challenges lie ahead. The National Flood Insurance Program (NFIP) currently owes the U.S. Department of the Treasury \$23 billion. DHS will consider changes to address both the sustainability and affordability of the NFIP for the 2017 reauthorization of the program.

### **Performance Highlight**

Below is a highlighted accomplishment demonstrating success in preventing incidents by establishing, and ensuring compliance with, standards and regulations.



### **Benefits of Flood Mapping and Mitigation Action**

FEMA’s Risk Mapping, Assessment, and Planning program provides updated Flood Insurance Rate Maps, planning, and outreach support throughout the country, working with communities to take action and mitigate future flood risk. This analysis empowered community officials in Colorado to make informed mitigation decisions, such as enacting stricter building codes, improving drainage issues, and restricting construction in Special Flood Hazard Areas (SFHA). These efforts paid off when disaster struck. For eight days in 2013, Colorado experienced unprecedented rainfall along the Front Range of the Rocky Mountains that flooded 18 counties with more than 17 inches of

rain. Despite these extraordinary conditions, homes inside the city limits were damaged, but remained standing. Critical water and wastewater facilities stayed open during the surge. Businesses reopened the day after the rains stopped. While property owners could have never predicted the intensity of the storm—they were prepared.

On March 30, 2015, FEMA issued a case study on the Colorado floods called *Reducing Losses through Higher Regulatory Standards* focused on Boulder, Larimer, and Weld counties. The study’s goal was to identify, evaluate, and quantify the cost effectiveness of the practices used by local communities during the 2013 floods and showcase which policies saved lives and property. The study found that requiring freeboard—a safety factor, expressed in feet, above the base flood elevation—as part of design standards saved \$154 million; restricting construction of basements in the new or expanded SFHAs reduced damages by \$50 million; and restricting developments in floodplains reduced potential damages by \$148 million. In addition, the study found a direct correlation between decreased losses and participation in FEMA’s Community Rating System, which encourages communities to implement local mitigation, floodplain management, and conduct outreach activities that exceed the minimum NFIP requirements.

FEMA will continue to work with Colorado to make informed decisions about higher regulatory standards, reward communities for their participation in the Community Rating System, and employ other cost effective mitigation measures that will protect lives and livelihood.

**Performance Results and Plan**

In FY 2015, there were four performance measures used to assess the Department’s efforts for this goal. For the FY 2016-2017 performance plan, one new measure is being introduced and one measure is being retired. In FY 2015, 75percent of the measures met their target and 100 percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary				
	Scale:	0%	25%	50%	75%
Goal 5.2: Mitigate Hazards and Vulnerabilities				◆	◆

◆ - Percent of measures that met their FY 2015 target.

◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below is a highlighted strategic measure that gauges efforts to mitigate hazards and vulnerabilities.

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

FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	48%	56%	57%	61%	61%	63%	62%	63%

This measure assesses the number of communities adopting building codes containing provisions that adequately address earthquake, flood, and wind hazards. FEMA works with code adoption and enforcement organizations to support community implementation of disaster resistant building codes, defined as being in compliance with the National Flood Insurance Program regulations, equivalent to the National Earthquake Hazards Reduction Program recommended provisions, and in compliance with the provisions of the International Codes as designated by the International Codes Council. FEMA also works with the Insurance Services Office Building Code Effectiveness Grading Schedule data to track the number of high-risk communities subject to flood, wind, earthquake, and combined perils that have adopted disaster resistant building codes over time. Over the past five years, significant improvement in the number of communities in high earthquake, flood, and wind-prone areas adopting disaster-resistant building codes has been seen as evidenced by the FY 2015 results of 63 percent—a 31 percent increase since FY 2011. Steady progress continues to be made due to training, education, outreach, and associated adoption of building codes by both communities and businesses.

The remaining strategic measures are used to gauge our efforts to mitigate hazards and vulnerabilities. For those measures that did not meet their targets, an explanation with corrective action are provided. In addition, changes to measure names and targets from the previous year’s report are identified. Finally, to continually improve our set of performance measures, new measures are introduced and measures are retired each year, and are identified in the measure tables.

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
<b>FEMA</b>									
Percent of U.S. population (excluding territories) covered by planned mitigation strategies	---	68.7%	71.0%	76.7%	79.6%	78.0%	80.8%	79.0%	79.0%

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
Reduction in the potential cost of natural disasters to communities and their citizens (in billions)	\$2.98	\$3.40	\$2.97	\$3.21	\$3.92	\$2.60	\$4.40	Retired	
Benefit to cost ratio of the hazard mitigation grants	---	---	---	---	---	New Measure <sup>1</sup>		1.3	1.4
<b>USCG</b>									
Three-year average number of serious marine incidents	---	---	---	---	---	≤ 693	696	≤ 701	≤ 698
<p>The three-year average number of serious marine incidents (SMI) for Q4 FY 2015 was 696, exceeding the 2015 target by 0.5%, despite a positive performance trend over the past two years. This measure reports the three-year average number of SMI's as defined by 46 Code of Federal Regulations 4.03-2, which include: death or injury requiring professional treatment beyond first aid; reportable property damage greater than \$100,000; actual or constructive loss of certain vessels; discharge of oil of 10,000 gallons or more; or a discharge of a reportable quantity of a hazardous substance. The USCG strives to consistently improve performance. Through our commitment to excellence across our broad suite of prevention activities, the USCG endeavors to drive down the occurrence of SMIs. Given current performance and projections, we anticipate achieving performance targets in FY 2016.</p>									

## Mission 5: Strengthen National Preparedness and Resilience

### Goal 5.3: Ensure Effective Emergency Response

#### Strategies

- Provide timely and accurate information
- Conduct effective, unified incident response operations
- Provide timely and appropriate disaster assistance
- Ensure effective emergency communications

#### Strategic Review Summary of Progress

Assessment Lead      Co-Lead: Robert J. Fenton, Regional Administrator, Region IX, Federal Emergency Management Agency (FEMA)  
Co-Lead: Julia Hein, CAPT, U.S. Coast Guard (USCG), Director, Incident Management and Preparedness Policy

The Department of Homeland Security (DHS) has determined that performance toward this goal is making satisfactory progress.

#### Introduction

Striving to protect the nation and its citizens against major accidents, disruptions, natural disasters and deliberate attacks, DHS acts as the federal coordinator during emergency response, supporting state, local, tribal, territorial and regional governments, while working with Non-Government Organizations and the private sector to leverage needed resources.

#### Major Achievements

DHS enhanced operational readiness and national preparedness by making significant strides in response communications and operational planning, drafting new or updating plans that include lessons learned from major incidents like Deepwater Horizon and Superstorm Sandy. DHS successfully executed a pilot program that tested the City of Baltimore's response capabilities and focused on various aspects of response risk assessment methodologies and technology assessments validating Baltimore's response capabilities—and DHS plans to expand this program to other cities in the future. USCG executed new Search and Rescue agreements with Cuba that improved responses in the Caribbean. Other notable innovations include the rollout of a more efficient and robust emergency response personnel management database that provides the ability for more comprehensive and effective incident workforce management for pre-event (availability), event (deployment), and post event (de-mobilization) cycles, and improved communications through a wireless alert system that supports our emergency communications strategy.

#### Major Challenges & Opportunities for Improvement

DHS aims to provide guidance and support to the response community to ensure continuity of operations during all hazards and incidents. Still, opportunities exist to improve strategic planning and management. Emergency communications are ever-evolving, and DHS must consider major changes in policy, legislation, budget, technology, and the establishment of the First Responder

Network Authority, which is charged with ensuring the implementation of a Nationwide Public Safety Broadband Network.

Cyber security presents a significant challenge and DHS is focused on building collaborative capabilities to combat cyber threats and respond to consequences of cyber events by developing the Annexes to the Federal Interagency Operations Plan.

### Performance Highlight

Below is a highlighted accomplishment demonstrating success in ensuring effective emergency response.



### FINDER Locates Four Buried Under Earthquake Damage

Four men in Nepal, trapped for several days under as much as 10 feet of bricks, mud and other debris, [were rescued](#) on April 25, 2015, thanks to a new search-and-rescue technology developed in partnership with the Science and Technology Directorate (S&T) and the National Aeronautics and Space Administration's Jet Propulsion Laboratory.

The device, [FINDER](#) (Finding Individuals for Disaster and Emergency Response), uses microwave-radar technology to detect heartbeats of victims trapped in wreckage. It had previously demonstrated capabilities to detect people buried under up to 30 feet of rubble, hidden behind 20 feet of solid concrete, and from a distance of 100 feet in open spaces. A recently added locator feature not only provides search and rescue responders with confirmation of a heartbeat, but also the approximate location of trapped individuals within about five feet, depending on the type of rubble. In disaster scenarios, such as earthquakes and tornadoes, wreckage is made up of twisted and shattered materials. Radar signals bounce back so signals are complex. FINDER's advanced data processing systems pick out the faint signals and are sensitive enough to distinguish the unique signature of a human's breathing pattern and heartbeat. The advantage of this technology is in allowing first responders to quickly ascertain if a living human victim is present in the debris and, if so, to ensure effective emergency response. The technology is sensitive enough that victims, whether conscious or not, can easily be detected, which helps responders decide the most efficient course of action.

FINDER's human-finding abilities were demonstrated through multiple test searches over the past several years with urban search and rescue teams in Virginia, Oklahoma, Indiana, New Jersey, Georgia, California, and Illinois. This year's earthquakes in Nepal presented the first opportunity to test the technology and the new locator feature in a real-world operational scenario. S&T [announced](#) on May 7, 2015, that two commercial partners have been licensed to manufacture the device.

**Performance Results and Plan**

In FY 2015, there were six performance measures used to assess the Department’s efforts for this goal. For the FY 2016-2017 performance plan, four new measures are being introduced and one measure is being retired. In FY 2015, 83 percent of the measures met their target and 83 percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary					
	Scale:	0%	25%	50%	75%	100%
Goal 5.3: Ensure Effective Emergency Response						◆

- ◆ - Percent of measures that met their FY 2015 target.
- ◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below are two highlighted strategic measures that gauge efforts to ensure effective emergency response.

**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)**

FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	100%	100%	100%	100%	100%	100%

This measure reflects FEMA's role in effectively responding to any threat or hazard, with an emphasis on saving and sustaining lives within 72 hours, in support of state, local, tribal, and territorial governments. Actions necessary to stabilize an incident are defined as those functions that must be initiated immediately following an incident in order to ensure the best outcomes for survivors. These actions include establishing joint federal/state incident objectives and interoperable communications between FEMA-supported incident sites, deploying urban search and rescue resources, rapidly activating response coordination centers, and issuing timely alerts, warnings, operations orders, and situation reports. All response incident management and support actions initiated in FY 2015 met required timeframes and requirements for Incident Management Assistance Teams, Urban Search and Rescue, Mobile Emergency Response Support, National Response Coordination Center, FEMA Operations Center, and National Watch Center resources. FEMA has met this target three consecutive years.

\* Previous measure name: Percent of incident management and support actions necessary to stabilize a jurisdiction within 72 hours or by the agreed upon time

**Percent of orders 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)**

FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
97.5%	93.3%	92.8%	95.4%	97.9%	95.0%	97.6%		Retired

This measurement evaluates the percentage of orders from FEMA distribution centers or logistics partners that arrive at the specified location by the validated and agreed upon delivery date. Orders include but are not limited to: meals, water, tarps, plastic sheeting, cots, blankets, and generators. Overall results are at the high end of FEMA’s performance trend for this measure. FEMA is retiring this measure and introducing a similar measure “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” which provides more

granularity of for measuring and reporting this important response activity. FEMA met their target this year, delivering 82 of 84 deliveries on time.

\* Previous measure name: Percent of orders 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.

The remaining strategic measures are used to gauge our efforts to ensure effective emergency response. For those measures that did not meet their targets, an explanation with corrective action are provided. In addition, changes to measure names and targets from the previous year’s report are identified. Finally, to continually improve our set of performance measures, new measures are introduced and measures are retired each year, and are identified in the measure tables.

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
<b>FEMA</b>									
Percent of the U.S. population directly covered by FEMA connected radio transmission stations	72%	84%	85%	90%	90%	90%	90%	90%	90%
Percent of Incident Management Assistance Teams establishing joint federal and state response objectives within 18 hours	---	---	---	100%	100%	100%	100%	100%	100%
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	---	---	---	---	---	New Measure <sup>1</sup>		95%	95%
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	---	---	---	---	---	New Measure <sup>2</sup>		99.9%	99.9%
Operational readiness rating of FEMA’s specialized incident workforce cadres	---	---	---	---	---	New Measure <sup>3</sup>		69%	74%
<b>National Protection and Programs Directorate (NPPD)</b>									

Performance Measures	Prior Year Results					FY 2015		Planned Targets	
	FY10	FY11	FY12	FY13	FY14	Target	Results	FY16	FY17
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	---	---	---	---	---	New Measure <sup>4</sup>		55%	56%
Percent of calls made by National Security/Emergency Preparedness users during emergency situations that DHS ensured were connected	99.4%	97.8%	99.4%	96.8%	99.3%	97%	99.3%	97.5%	98.0%
<b>USCG</b>									
Percent of people in imminent danger saved in the maritime environment	74.4%	77.3%	77.3%	79.0%	79.0%	100%	80%	100%	100%
<p>In FY 2015 there were 16,456 Search and Rescue (SAR) cases resulting in 3,536 lives saved. This performance measure excludes SAR responses which had greater than 10 lives at risk; there were 21 such cases. Factors beyond USCG control often led to tragic outcomes despite response efforts to achieve a favorable outcome. Distress victims may, for example, succumb to traumatic injuries incurred in a boating accident before first responders reach the scene. In such cases, the opportunity to influence the outcome is diminished, but USCG nonetheless responds with the intent to save lives. There are numerous variables that affect the percentage of people saved from imminent danger, many of which are beyond USCG control. While the FY 2015 target was not realized, the percentage of people in imminent danger saved is consistent with previous years. USCG SAR will continue to analyze SAR data to determine potential causes for variances and other contributing factors.</p>									

- Note 1: New measure added to replace “Percent of orders 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” to better measure the overall delivery to the group in need. A full order is made up of multiple shipments which can arrive on-time with respect the need.
- Note 2: Although this is a new publicly reported measure, FEMA has been tracking this information and is able to provide previous results: FY 2013 = 98.0%; FY 2014 = 98.4%; and FY 2015 = 99.7%.
- Note 3: This measure is also included as part of the set of measures in FEMA’s Agency Priority Goal.
- Note 4: NPPD is introducing this new measure to assess state and territorial preparedness across a broad array of communications capabilities. The Office of Emergency Communications impacts the results of this measure in multiple ways to include providing technical assistance events to help develop communication interoperability plans, coordinating various stakeholder groups, and providing state and local officials with recommendations to improve their long-term emergency communications capabilities.

## Mission 5: Strengthen National Preparedness and Resilience

### Goal 5.4: Enable Rapid Recovery

#### Strategies

- *Ensure continuity and restoration of essential services and functions*
- *Support and enable communities to rebuild stronger, smarter, and safer*

#### Strategic Review Summary of Progress

Assessment Lead Robert J. Fenton, Regional Administrator, Region IX, Federal Emergency Management Agency (FEMA)

The Department of Homeland Security (DHS) has determined that performance toward this goal is making satisfactory progress.

#### Introduction

DHS plays a key role in facilitating recovery following a disaster by supplementing communities' recovery core capabilities; promoting infrastructure resilience guidelines and use of standards; and encouraging the development of continuity plans for communities, government entities, and private sector organizations. The devastating effects of recent disasters have highlighted the need to reform our national approach to long-term recovery. Communities devastated by a disaster, particularly large-scale events such as Hurricane Sandy, face complex and difficult challenges including restoring economic viability, rebuilding infrastructure and public services, and establishing resilience against future hazards.

#### Major Achievements

Disaster recovery coordination and resources for data analysis, joint planning, infrastructure projects, and funding for a local disaster recovery coordinator expanded under the National Disaster Recovery Framework following the Enhanced F-4 major tornado disaster that killed 16 and destroyed 85 percent of businesses as it tracked through the cities of Vilonia and Mayflower in Faulkner County, Arkansas. Expanded recovery coordination resulted in a consortium of state, local, private sector, philanthropic, and federal partnerships working in concert to increase the capacity of the impacted communities to achieve recovery and improve sustainability. The cities of Vilonia and Mayflower, Arkansas, have signaled ownership of their recovery by finalizing their recovery strategies, producing redevelopment designs, and identifying projects. These initiatives received a jump-start from facilitated recovery peer-to-peer workshops with key community representatives from Joplin, Missouri, county and state officials, three state universities, and the private sector.

FEMA improved the Public Assistance program through implementation of key sections of the *Sandy Recovery Improvement Act*, such as small project thresholds allowing for more flexibility in supporting recovery efforts.

#### Major Challenges & Opportunities for Improvement

FEMA Recovery completed a review of the Public Assistance program to assess the current construct for implementing the program and to begin the process for developing a new model for

the delivery of assistance after major disasters and emergencies. The diagnostic analysis confirmed previous concerns, highlighted additional areas of focus, and refined our understanding of the inefficiencies and challenges in the current model. The results of the diagnostic analysis are being shared with regional and state stakeholders and form the basis of the Public Assistance Re-engineering Business Case currently under development. DHS is also building collaborative capabilities to recover from consequences of cyber events by developing the Annexes to the Federal Interagency Operations Plan. FEMA improved the Public Assistance program through implementation of key sections of the *Sandy Recovery Improvement Act*, such as small project thresholds. FEMA is also addressing Government Accountability Office findings to improve administrative cost for major disasters by establishing a robust Disaster Administrative Cost Integrated Project Team with programmatic experts responsible for effectively delivering the mission as well as business managers accountable for finding efficiencies in service delivery.

**Performance Highlight**

Below is a highlighted accomplishment demonstrating success in enabling rapid recovery.



**FEMA Providing Resilient Rebuilding and Recovery in New York**

The *Sandy Recovery Improvement Act* authorizes alternative procedures for the Public Assistance Program that allows FEMA to implement innovative pilot programs. One such pilot is the alternative procedures for permanent work that provides communities with greater flexibility in meeting their needs for more resilient rebuilding and recovery. Two examples of success stories are the New York University Langone Medical Center and the Nassau County Wastewater Treatment Facilities, which both accepted consolidated fixed grant estimates to restore the pre-

disaster function of their facilities and eliminate or reduce future damages through cost-effective mitigation measures.

FEMA provided \$1,130,072,880 in assistance to New York University Langone Medical Center (NYULMC) for consolidating 10 disaster damaged facilities into one fixed capped grant. Under this grant, NYULMC is taking steps to reduce future flood damage by reinforcing and installing exterior flood doors/barriers/egress, elevating mechanical, electrical, and plumbing systems, installing internal flood doors, installing check valves/backflow preventers and installing pumps and sump pumps. Nassau County also accepted FEMA assistance of \$729,637,539 to restore the Bay Park wastewater treatment plant, two water pollution control plants, and 32 pump stations and make the reconstructed plants and pump stations more resilient to future flooding events through the construction of a protective berm, dewatering capability, and electrical system improvements.

Applicants like NYULMC and Bay Park Wastewater Treatment Plant, who are participating in the consolidated fixed grant estimate, benefit from receiving expedited funding allowing them to rebuild and recover faster than the traditional FEMA grant process

**Performance Results and Plan**

In FY 2015, there were two performance measures used to assess the Department’s efforts for this goal. In FY 2015, 50 percent of the measures met their target and 100 percent maintained or improved actual results compared to FY 2014.

Goal	Performance Summary					
	Scale:	0%	25%	50%	75%	100%
Goal 5.4: Enable Rapid Recovery				◆		◆

- ◆ - Percent of measures that met their FY 2015 target.
- ◇ - Percent of measures that maintained or improved actual performance results compared to FY 2014.

Below are two highlighted strategic measures that gauge efforts to enable rapid recovery. Changes to measure names and targets from the previous year’s report are identified. In addition, with efforts to continually improve our set of performance measures, new measures are introduced and measures are retired each year, and are identified in the measure tables.

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)								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	94.5%	91.5%	93.0%	96.9%	94.0%	95.0%

Recovery assistance helps individuals affected by disasters and emergencies return to normal quickly and efficiently. Individual Assistance (IA) performed very well this year. There were nine IA declarations in FY 2015. Ninety-nine of all housing assistance cases were awarded within 60 days. Disaster Case Management had only one case and it was processed within the establish timeframe. Disaster Assistance Improvement Program experienced 59.03 hours of downtime, while IA Grants Management System experienced 14.32 hours of downtime for the year. Call Centers have answered 605,124 calls, of which 602,131 (99.51 percent) have been answered within two minutes. During the year there was a transition of IA staff, and the percent of positions filled were within annual target. Customers receiving IA assistance have expressed an increasing satisfaction concluding the year within target.

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)								
FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	86.2%	90.9%	93.0%	92.0%	93.0%	93.0%

This measure reflects a weighted percent of how FEMA delivers services to communities following a disaster based upon three categories: program services; supporting infrastructure; and customer satisfaction. Sub-elements within these three categories include: ensuring timely kickoff meetings following requests for public assistance; having available grant management systems; assuring that business staff are in place; and delivering these services to enhance customer satisfaction of those receiving public assistance. Supporting and ensuring our citizens have quality support after a disaster is critical to facilitating a community's recovery. FEMA did not achieve the planned results this year primarily due to a surge in activity in the second half of FY 2015; however, program results are trending positively over the past three years. In FY 2016, FEMA will complete a reengineering effort that will serve to enhance customer satisfaction and improve the processing time from a request for public assistance to the kick-off meeting.

## Mature and Strengthen Homeland Security

### Goal: *Integrate Intelligence, Information Sharing, and Operations*

#### Strategies

- Enhance unity of regional operations coordination and planning
- Share homeland security information and analysis, threats, and risks
- Integrate counterintelligence
- Establish a common security mindset with domestic and international partners
- Preserve civil rights, civil liberties, privacy, oversight, and transparency in the execution of homeland security activities

#### Performance Highlight

Below is a highlighted accomplishment demonstrating success in integrating intelligence, information sharing, and operations.



#### Information Sharing

The Office of Intelligence and Analysis (I&A) has a unique mandate within the Intelligence Community and is the Federal Government lead for sharing information and intelligence with state, local, tribal and territorial governments and the private sector. It is these non-federal partners who are integral to the Homeland Security Enterprise in preventing and responding to evolving threats to the homeland. I&A supports [state and major urban area fusion centers](#) with deployed personnel and systems, training, and collaboration. This National Network

of fusion centers is the hub of much of the two-way intelligence and information flow between the Federal Government and our state, local, tribal and territorial partners. The fusion centers represent a shared commitment between the Federal Government and the state and local governments who own and operate them. Individually, each represents a vital resource for merging information from national and local sources to prevent and respond to all threats and hazards. Collectively, their collaboration with the Federal Government, one another (state-to-state and state-to-locality), and with the private sector represents the new paradigm through which we view homeland security. [Fusion centers have contributed](#) and will continue to contribute to improvements in information sharing and collaboration that will enhance the nation's overall preparedness.

I&A assumes the program management role for the Department's engagement with the [Nationwide Suspicious Activity Reporting \(SAR\) Initiative \(NSI\) Program Management Office \(PMO\)](#). As part of that role, I&A is a direct liaison with the NSI PMO and facilitates the efforts of DHS components and fusion centers in becoming active NSI participants. Additionally, I&A leverages SAR data to create analytical products that assist federal, state, local, and tribal partners in their respective homeland security missions.

## Mature and Strengthen Homeland Security

### Goal: *Enhance Partnerships and Outreach*

#### Strategies

- *Promote regional response capacity and civil support*
- *Strengthen the ability of federal agencies to support homeland security missions*
- *Expand and extend governmental, nongovernmental, domestic, and international partnerships*
- *Further enhance the military-homeland security relationship*

#### Performance Results and Plan

Below is a highlighted strategic measure that gauges efforts to enhance partnerships and outreach.

#### Percent of National Center for Missing and Exploited Children (NCMEC) examinations requested that are conducted (U.S. Secret Service (USSS))

FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	100%	100%	100%	100%	100%	100%	100%	100%

This measure represents the percentage of USSS computer and polygraph forensic exams conducted in support of any investigation involving missing or exploited children in relation to the number of computer and polygraph forensic exams requested. USSS met its goal and supported the Department in its objective of expanding partnerships by conducting 100% of computer forensic and polygraph exams in support of any investigation involving missing and exploited children in relation to the number of exams requested by NCMEC—with 351 polygraph and 137 computer forensic exams conducted.

## Performance Highlight

Below is a highlighted accomplishment demonstrating success in enhancing partnerships and outreach.



### Community Engagement Exchange on Countering Violent Extremism

Since 2011, the DHS Office for Civil Rights and Civil Liberties (CRCL), in partnership with the Department of State, has coordinated an annual bilateral community engagement program on countering violent extremism (CVE). The program pairs two cities in the United States with two in each European country, and the delegations—representing civil society and local government—exchange information and best practices that support CVE efforts. The exchange program is designed to help community stakeholders, educators, youth leaders, and local law enforcement partners exchange best

practices that may benefit trust-building efforts, further the protection of civil rights and civil liberties, reduce alienation, promote effective integration, and help communities that are resilient and able to counter the narrative of violent extremist groups.

The 2014 city pair program started with a June 2014 visit by a U.S. delegation (including DHS) to Vilvoorde, Belgium in order to discuss and exchange best practices on CVE, community engagement, and building community resilience to combat the recruitment of community members by violent extremist groups. On September 22-26, 2014, DHS hosted a CVE Exchange Program delegation from Vilvoorde in both Washington, D.C. and Columbus, Ohio. The delegation participated in a series of meetings and events with partners from federal, state, and local governments, as well as nongovernmental organizations and academia. The events ranged from CRCL-led community engagement roundtables with diverse communities, to visiting schools to meet with student leaders and administrators. The delegation included the Mayor of Vilvoorde and the Vilvoorde Chief of Police, as well as key local and community officials and members of the city council elected from key demographic populations representing disaffected communities. The visit culminated in a roundtable event at the Noor Islamic Center in Columbus, hosted by Secretary Johnson. Secretary Johnson remarked at the roundtable on the ways we can remain vigilant in countering violent extremism, including offering people – particularly young people – opportunities to channel their energy and passion in different directions.

The exchange program produced tangible results for the town of Vilvoorde. In an April 7, 2015 meeting, Vilvoorde Mayor Hans Bonte told the U.S. Ambassador to Belgium, Denise Campbell Bauer, which he credits the decreased flow of foreign fighters from Vilvoorde to strong community engagement efforts implemented at the local level. He reported that Vilvoorde was about to celebrate the one-year mark of no residents departing for Syria to fight in the conflict there, noting that other towns in Belgium were still facing several departures a month. Bonte believes his city's recipe for success is rooted in the deep personal commitments by local officials to counter violent extremism, which have resulted in the formation of closer ties with diverse communities, and increased support for front line practitioners and first responders like teachers and police officers. Mayor Bonte cited the implementation of community engagement activities and best practice exchanges he learned about while participating in the exchange program as directly influencing programming in Vilvoorde, resulting in the notable decrease in the flow of foreign fighters to Syria from his city.

## Mature and Strengthen Homeland Security

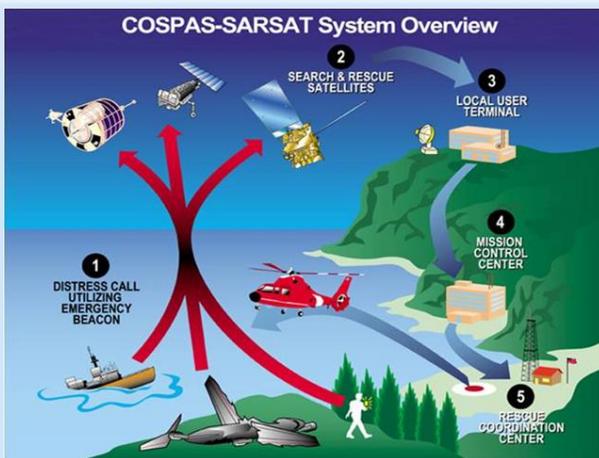
**Goal: Strengthen the DHS International Affairs Enterprise in Support of Homeland Security Missions**

### Strategies

- Establish strategic priorities for the Department’s international affairs enterprise
- Establish a coordination and communication mechanisms across the DHS international affairs enterprise

### Performance Highlight

Below is a highlighted accomplishment demonstrating success in DHS international partnerships.



### USCG Partnering to Improve Search and Rescue

The International COSPAS SARSAT Program<sup>6</sup> (ICSP) is an international collaboration that provides global space-based alerting and locating for 406 MHz distress beacons. These beacons are required on most commercial boats and planes by both the International Maritime Organization and the International Civil Aviation Organization. At the same time, a growing population of terrestrial users, including U.S. citizens, numerous government agencies, and various parts of the military are now utilizing personal locator beacons for distress alerting and locating services in places where conventional communications are either non-existent or unreliable. Since the inception and launch

of the first COSPAS satellite in 1982, more than 39,000 people have been rescued around the world as a result of the ICSP program, including more than 7,500 in the United States Search and Rescue region. Many of these cases have been led by the U.S. Coast Guard (USCG), which is the largest user of SARSAT alert data in the world.

The legacy ICSP satellite system is nearing the end of its operational life and the USCG is working closely with the U.S. Air Force, the National Aeronautics and Space Administration (NASA), the National Oceanic and Atmospheric Administration (NOAA), and the international community to transition to a more capable second-generation SARSAT system, known internationally as MEOSAR (Mid-Altitude Earth-Orbiting Search and Rescue) and domestically as SAR/GPS (Search and Rescue/Global Positioning System). The agencies have partnered together to integrate recently developed NASA technology onto the SAR/GPS radio repeaters aboard Air Force GPS satellites, which will transmit distress alerts through a local user terminal to the U.S. Mission Coordination Center, which is overseen by NOAA. The alerts are then distributed to the appropriate USCG, Air Force, or International Rescue Coordination Center. The new MEOSAR system will improve detection rates and location accuracy, allow more timely detection of distress, and provide enhanced two-way information flow—advantages that will reduce search times and lead to more lives saved in the future.

<sup>6</sup> COSPAS is an acronym for the Russian words "Cosmicheskaya Sistema Poiska Avaryinyh Sudov," which translates to "Space System for the Search of Vessels in Distress". SARSAT is an acronym for Search And Rescue Satellite-Aided Tracking

## Mature and Strengthen Homeland Security

### Goal: Conduct Homeland Security Research and Development

#### Strategies

- *Employ scientific study to understand homeland security threats and vulnerabilities*
- *Develop innovative approaches and effective solutions to mitigate threats and vulnerabilities*
- *Leverage the depth of capacity in national labs, universities, and research centers*

#### Performance Highlight

Below is a highlighted accomplishment demonstrating success in conducting homeland security research and development.



#### Apex Programs: Restructuring Research and Development across the Homeland Security Enterprise

Early in FY 2015, the Under Secretary for S&T asked leaders within S&T, S&T's stakeholders, and the American public what they thought the big threats to the Nation would be in the next 20-30 years. Using this input, S&T developed and publicized a set of [visionary goals](#). They include: Screening at Speed: Security that Matches the Pace of Life; A Trusted Cyber Future: Protecting Privacy, Commerce, and Community; Enable the Decision Maker: Actionable Information at the Speed of Thought; Responder of the Future: Protected, Connected, and Fully Aware; and Resilient Communities: Disaster-Proofing Society.

With these goals, S&T realized they needed to rethink their projects and how they interact with the Homeland Security Industrial Base. Using the goals as their guide, S&T created complimentary Apex Programs to lead S&T investments toward closing identified homeland security gaps in mission capability within a timeframe of five years or less. S&T carefully refocused some projects toward a more strategic end state, integrating them into Apex Programs. Remaining projects retained their operational focus while still supporting the DHS mission and S&T's visionary goals. Some Apex Programs have as many as 40 individual projects all working toward the accomplishment of a specific Apex goal.

Apex Programs include: [Air Entry/Exit Re-Engineering](#); Border Situational Awareness; Real-Time Bio-threat Awareness; Relational, Adaptive Processing of Information and Display; Next Generation Cyber Infrastructure; Aviation Checkpoint Screening at Speed; and the Next Generation First Responder.

Consolidating and road mapping multiple project efforts under these refocused programs allows S&T to look strategically at the Nation's security and address future challenges while continuing to support today's operational needs. This new construct allows S&T the flexibility of leveraging cross-cutting expertise within S&T, while at the same time engaging smart industry advisors to develop a homeland security industrial base.

Other complementary innovative actions include S&T's National Conversation on Homeland Security Technology, better align industry insight with Homeland Security Enterprise, a series of online and in person discussions designed to help solve the Nation's security challenges. S&T also added their first [prize competition](#) and kicked off their first [business accelerator](#) program.

**Performance Results and Plan**

Below is a highlighted strategic measure that gauges efforts to conduct homeland security research and development.

**Percent of Apex technologies or knowledge products transitioned to customers for planned improvements in the Homeland Security Enterprise (Science and Technology Directorate (S&T))**

FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
---	---	---	---	---	80%	82%	80%	80%

This measure gauges the transition of high priority, and high value research and development projects known as Apex projects. Apex technologies and knowledge products are quickly delivered to improve homeland security operations. Apex products consist of cross-cutting, multi-disciplinary efforts which employ 3 to 5 year innovation cycles from project inception through operational testing. Eighty-two percent of the Apex high priority technologies and knowledge products, namely Border Enforcement Analytics (BEAP) and Air Entry/Exit Re-Engineering (AEER), were transitioned in FY 2015. Apex AEER completed Sequence 3 data analysis. The Sequence 3 report includes CONOPS configuration recommendations for additional sequence testing and field evaluation. Recommended biometric exit CONOPs have been submitted to the U.S. Customs and Border Protection. Several of the scheduled BEAP transitions were delayed until FY 2016. The Apex BEAP program modified several of its contracts to achieve expanded capabilities required by U.S. Immigration and Customs Enforcement (ICE). The goal of delivering the high speed transaction processing to ICE Homeland Security Investigations SI Roadrunner/BEAP programs through the Big Data Environment has changed from FY 2015 to late FY 2016 due to this requirement modification.

## Mature and Strengthen Homeland Security

### Goal: *Ensure Readiness of Frontline Operators and First Responders*

#### Strategies

- *Support systems for training, exercising, and evaluating capabilities*
- *Support law enforcement, first responder, and risk management training*

#### Performance Highlight

Below is a highlighted accomplishment demonstrating success in training and exercising frontline operators and first responders.



#### Forging Private-Public Partnerships through Training

On June 1, 2015, nearly 175 mall executives, mall security directors, and local law enforcement officers and leaders gathered to participate in the inaugural Private-Public Partnership Academy (PPPA) at FLETC in Glynco, Georgia. FLETC collaborated with the National Protection and Programs Directorate (NPPD) and private sector stakeholders to plan this first-of-its-kind training event at FLETC. The PPPA brought together three distinct groups to participate in training pertinent to securing public venues, with a broader goal of improving coordination, security, and resiliency across traditional public and private sector areas of responsibility.

The pilot PPPA featured training in topics applicable to all segments of the audience, and the planners tailored the training to address both public and private sector roles and responsibilities in securing commercial facilities. Training in topics such as terrorism awareness, weapons of mass destruction, improvised explosive devices, leadership in a crisis, special event security planning, and tactical medical culminated with a final practical exercise, during which four teams competed to identify threat indicators during a large-scale event. FLETC collaborated with NPPD's Federal Protective Service to inject simulated threats into a FLETC-wide event open to all staff. For example, they staged a suspicious package, a person wearing unseasonable clothing, a role player handing out literature indicative of his association with domestic terrorism, an abandoned vehicle containing suspicious materials, and a role player conducting video surveillance with a smart phone. Afterward, FLETC instructors led them through a de-briefing to discuss the injected threats and their responsibilities during an actual event.

Participant feedback indicated that one of the greatest values of the PPPA was learning about others' roles, which leads to improved coordination during emergent situations. Additionally, participants observed that the PPPA underscored the private and public sectors' collective responsibility in ensuring safety and security. FLETC is considering how it can replicate this experience for additional private and public sector stakeholders, potentially in other subsectors besides commercial facilities. Through the inaugural PPPA, FLETC concretely incorporated the private sector into the work it does every day to advance training excellence through partnerships.

**Performance Results and Plan**

Below are two highlighted strategic measures that gauge efforts to train and exercise frontline operators and first responders. Changes to measure names and targets from the previous year’s report are identified.

**Number of federal law enforcement training programs and/or academies accredited or re-accredited through the Federal Law Enforcement Training Accreditation process (Federal Law Enforcement Training Centers (FLETC))**

FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
52	66	83	97	107	113	114	118*	123

This performance measure reflects the cumulative number of federal law enforcement training programs and/or academies accredited or re-accredited through the Federal Law Enforcement Training Accreditation (FLETA) process. Agencies realize that FLETA provides a return on their investment and ensures a systematic approach to developing and providing consistent training for agencies. This measure has had a positive trend for the past six years.

\* - The FY 2016 target previously published as \$119 in the FY 2014 – 2016 Annual Performance Report was changed to 118. FLETC has experienced increasing difficulty achieving success on these measures due to the number of programs that have been cancelled by the controlling agency or allowed to lapse due to controlling agency internal budget issues or changes in priorities.

**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)**

FY10 Result	FY11 Result	FY12 Result	FY13 Result	FY14 Result	FY15 Target	FY15 Result	FY16 Target	FY17 Target
96%	98.5%	96%	100%	91%	94%	98%	95%	95%

This performance measure reflects the satisfaction of Partner Organizations that FLETC training programs address the right skills needed for their officers/agents to perform their law enforcement duties such as the prevention of the introduction of high-consequence weapons of mass destruction, terrorism, and other criminal activity against the U.S. and our citizens. This measure was met through FLETC's collaboration with Partner Organizations in order to: 1) promote partnership; and 2) invite and respond to their input on research, development, and revision of training programs in order to effectively address the right skills needed for their officers/agents to perform their law enforcement duties.

## Mature and Strengthen Homeland Security

### Goal: Strengthen Service Delivery and Manage DHS Resources

#### Strategies

- *Recruit, hire, retain, and develop a highly qualified, diverse, effective, mission-focused, and resilient workforce*
- *Manage the integrated investment life cycle to ensure that strategic and analytically based decisions optimize mission performance*
- *Manage and optimize financial resources, property/assets, procurements, security, and DHS IT*
- *Establish and execute a comprehensive and coordinated DHS health and medical system*

#### Performance Highlight

Below is a highlighted accomplishment demonstrating success in this goal.



#### Long-Term Success in Cost Savings

Since DHS implemented its Strategic Sourcing Program in 2005, DHS has saved more than \$3.00 billion, of which nearly \$2 billion was saved in the last five years, and more than \$450 million in FY 2015 alone. The DHS Strategic Sourcing Program, viewed as a ‘best in class’ efficiency model across the Federal Government, has been endorsed by the Office of Management and Budget, Government Accountability Office, and several members of Congress.

Strategic Sourcing supports the DHS Secretary’s “Unity of Effort” initiative by convening working groups comprised of DHS subject matter experts, acquisition professionals, legal staff, and other stakeholders that are focused on developing acquisition streamlining tools and shared acquisition vehicles that effectively leverage the Department’s buying power, reduce administrative costs through the elimination of redundant contracts and processes, and foster continuous cooperation on future challenges and events.

Extensive collaboration across the Department has been vital to DHS’s strategic sourcing success. For example, the Office of the Chief Information Officer community has worked with the Strategic Sourcing Program Office on nearly 30 initiatives, and consistently work together to identify new opportunities. These efforts have helped to identify ways to enhance enterprise-level capabilities and reduce the total lifecycle cost of commodities by focusing not only on a reduction in purchase price, but also by including beneficial terms and conditions in the contract vehicles that further lower the costs of maintaining and using the commodity.

## Priority Goals

### FY 2014 – 2015 Agency Priority Goals

In the FY 2014 Budget, the Obama Administration defined Agency Priority Goals (APG) which represent areas in which the Administration has identified opportunities to significantly improve near-term performance. DHS's FY 2014 – 2015 APG's are a set of focused initiatives that support the Agency's longer-term strategic framework. A brief overview of each of the Department's APGs is provided below. Quarterly updates and additional detail is available at [www.performance.gov](http://www.performance.gov).

#### ***Agency Priority Goal 1: Strengthening Aviation Security through Risk-based Decisions*** ***(Aligns to DHS Mission 1)***

Strengthen aviation security counterterrorism capabilities and improve the passenger experience by using intelligence driven information and risk-based decisions: By September 30, 2015, the Transportation Security Administration (TSA) will expand the use of risk-based security initiatives to increase the percentage of travelers eligible for expedited screening at airports to 50 percent and enhance the passenger experience.

**Overview:** TSA performs and oversees security operations at the nation's airports, screening over 660 million passengers annually, to ensure the freedom of movement of people and commerce. In an effort to strengthen aviation security while enhancing the passenger experience, TSA is focusing on risk-based, intelligence-driven security procedures and enhancing its use of technology. Since 2011, the agency has implemented several risk-based initiatives including the TSA Pre✓<sup>®</sup> expedited screening program; the nationwide implementation of modified screening protocols for passengers 12 and younger, passengers 75 and over, and active duty service members; expediting physical screening of Veterans on chartered Honor Flights; and providing modified screening to Wounded Warriors. A number of initiatives will further enable TSA to reach its goal of expanding expedited screening for known populations in order to focus on those that are unknown including the development and deployment of the TSA Pre✓<sup>®</sup> Application and TSA Risk Assessment programs; expansion of TSA Pre✓<sup>®</sup> participation to international air carriers; continued expansion of the Known Crew Member program; and developing operational policies, procedures, and other activities such as the evolution of checkpoint screening technologies to support deployment of Risk Assessments that will grow the volume of passengers eligible for expedited screening.

As of December 2013, on a weekly basis, more than 32 percent of passengers received some form of expedited screening, and TSA continued to grow that number. While driving the growth of eligible populations is key to the initiative's long term success, TSA faces challenges in aligning, planning, and executing activities for incorporating these various populations. The success of achieving TSA's risk-based security milestones is in many ways reliant upon external and internal partners that TSA continues to work with to mitigate these challenges.

**Progress Update:** Over the past two years, TSA worked to achieve the targets for the measures in this APG, and in most instances, TSA met or surpassed the goal. Through ongoing efforts to accelerate efforts to promote enrollment in DHS Trusted Traveler Programs (TTPs) and expand

TSA Pre✓<sup>®</sup> to trusted, pre-vetted populations, TSA has strengthened security at screening checkpoints while simultaneously increasing its operational efficiency and improving the passenger experience.

- On December 4, 2013, TSA implemented the TSA Pre✓<sup>®</sup> Application Program, permitting U.S. citizens and U.S. lawful permanent residents the opportunity to apply directly to TSA Pre✓<sup>®</sup>. To date, 329 enrollment centers—including 37 at 34 airports, and 292 in high-traffic off-airport locations around the country—process, on average, more than 4,600 applications daily. As of the end of FY 2015, TSA has received more than 1.6 million enrollment applications since the program’s inception.
- TSA has taken policy decisions to extend TSA Pre✓<sup>®</sup> to members of low risk populations (LRPs), and continues efforts to “onboard” additional federal agencies and departments. During the reporting period, TSA has extended TSA Pre✓<sup>®</sup> eligibility to the following LRPs:
  - Department of Defense and U.S. Coast Guard civilian employees
  - Cadets and midshipmen at the five U.S. service academies
  - Department of State Top Secret clearance holders
  - TSA employees
  - Members of the Aviation Security Advisory Committee, National Fusion Center Association, and The Flag and General Officers’ Network
- To meet the demand from travelers and airports that did not have a dedicated TSA Pre✓<sup>®</sup> lane, TSA launched an initiative to permit TSA Pre✓<sup>®</sup>-eligible travelers expedited screening traveling through airports with single-lane checkpoints.
- TSA continues to encourage domestic and foreign air carriers’ participation in TSA Pre✓<sup>®</sup>. As of the end of FY 2015, ten U.S. and two foreign carriers (Air Canada and WestJet) participate in TSA Pre✓<sup>®</sup>. Currently, more than 86 percent of domestic passengers are flying aboard a TSA Pre✓<sup>®</sup>-participating carrier.
- The TSA Secure Flight (SF) program enhances the Nation’s transportation system by operating a risk-based, intelligence-driven watch list matching capability. Using an automated process to match Secure Flight Passenger Data (SFPD) against various watch lists—e.g., No Fly list, Selectee list, Center for Disease Control and Prevention’s Do Not Board list—SF flags travelers who pose a potential risk to transportation, allowing for appropriate mitigating actions to be taken. SF has successfully vetted 100% of SFPD over the reporting period.
- DHS Traveler Redress Inquiry Program (TRIP) has consistently met its processing-time goal by continually improving processes; identifying phases that could be made more efficient and steps that could be eliminated; and conducting pilots of potential process changes that could improve cycle times. DHS TRIP has made steady and significant improvements in the processing times.
- During the second half of FY 2015, TSA began adjusting the risk posture associated with expedited passenger screening in response both to changes in the threat, and also to recommendations from the DHS Inspector General. These changes resulted in travelers not directly enrolled in a DHS TTP or members of an LRP having a decreased opportunity to receive expedited screening.

**Agency Priority Goal 2: Prioritized Detention and Removal of Criminal Aliens**  
(Aligns to DHS Mission 3)

Enforce and administer our immigration laws through prioritized detention and removal of criminal aliens: By September 30, 2015, U.S. Immigration and Customs Enforcement (ICE) will increase criminal alien removals, as a percentage of total removals, by 5%.

**Overview:** ICE is committed to identifying, arresting, detaining, prosecuting, and removing aliens who present a danger to national security or are a risk to public safety, as well as those who otherwise undermine the integrity of our immigration laws and our border control efforts. These include, but are not limited to aliens engaged in or suspected of terrorism or espionage, violent criminals, felons and repeat offenders, and organized criminal gang members. Also critical to ICE enforcement priorities are recent illegal border crossers.

This goal is a continuation of effort began in FY 2012 to increase efficiencies in the process of detaining and removing illegal aliens. The focus for the next two years will be to showcase ICE's abilities to remove criminal aliens from the United States. These efforts include identifying and apprehending at-large criminal aliens, and expanding coverage in jails and prisons in order to identify and process removable incarcerated foreign-born detainees.

ICE uses prosecutorial discretion which improves efficiencies by identifying and eliminating low priority cases clogging the immigration system. The use of prosecutorial discretion also allows ICE to prioritize the use of its enforcement personnel, detention space, and removal assets to ensure that the aliens it removes represent, as much as reasonably possible, the agency's enforcement priorities, namely the promotion of national security, border security, public safety, and the integrity of the immigration system.

**Progress Update:** In November of 2014, Secretary of Homeland Security, Jeh Johnson, issued the memorandum [\*Policies for the Apprehension, Detention and Removal of Undocumented Immigrants\*](#), outlining the Department's revised civil enforcement priorities. The memorandum directs that the nation's limited immigration enforcement resources be used in the most effective and efficient way possible, focusing on the removal of the greatest threats to national security, public safety, and border security. The revised civil enforcement priorities strengthen the Department's focus on recent border crossers and serious criminals. Successful execution of the Secretary's memorandum was supported by the following contributing programs in FY 2015:

**Enforcement:**

- ICE Enforcement and Removal Operations (ERO) continued to utilize the Criminal Alien Program Surge Enforcement Team (CAPSET), which is capable of deploying to areas needing additional assistance. ERO completed four CAPSET operations specifically targeting facilities with a high population of detainees scheduled to be released in November 2015 pursuant to the 2014 United States Sentencing Commission Amendment 782. These operations resulted in 777 encounters, 247 detainees, 161 charging documents issued, and 55 arrests.
- ICE continues to expand the Criminal History Information Sharing (CHIS) program, allowing ERO to share information regarding the criminal convictions of foreign nationals

being removed from the U.S. and to receive information about foreign criminal convictions for individuals in ICE custody. In FY 2015, ERO concluded negotiations with Jamaica and the Bahamas, and official CHIS agreements are expected to be signed in FY 2016.

- Fugitive Operations Teams made 20,961 arrests, approximately 89 percent of which were criminal arrests, the highest percentage in the program's history.
- ICE continued National Criminal Analysis and Targeting Center support to the Sex Offender Registration initiative to identify, target, and remove foreign-born sex offenders, leading to 55 arrests in FY 2015.

***Detention:***

- In FY 2015, nearly 99 percent of ICE detainees were subject to mandatory detention or otherwise met an enforcement priority.
- The Alternatives to Detention (ATD) program continued to provide monitoring of non-detained criminal aliens and increased the average daily population by approximately 3,625 from FY 2014 (approximately 23,000) to FY 2015 (approximately 26,600).
- The ATD program developed and implemented numerous staging areas (S sites) that allow for initial ATD evaluation and enrollment of individuals before they are released from Border Patrol facilities or Family Residential Centers. ICE assigns a GPS unit to such individuals, and allows them to transit across the U.S. to their final destination in the appropriate AOR, where their status in the program will then be further evaluated. The S sites enable oversight of those individuals in transit, where previously they were not monitored unless and until they reported in at their final destination. ICE enrolled 6,308 participants on the southwest border and over 2,099 participants at the three Family Residential Centers.

***Removal:***

- ERO established a process with the government of El Salvador to acquire travel documents in order to advance Failure to Comply (FTC) removal cases. FTC cases are those comparatively small number of cases where ICE has been unable to obtain the necessary travel documents to effectuate repatriation of an individual in its custody. This resulted in the removal of over 50 FTC cases in FY 2015.
- On March 27, 2015, ICE ERO signed a MOU with the People's Republic of China facilitating the travel of Chinese experts to the U.S. to verify the identity and citizenship of Chinese nationals who are under final removal orders. Chinese officials have already interviewed 82 such individuals, and verified the Chinese citizenship of 30 of them. These individuals are now awaiting removal. The remaining cases are ongoing.
- On September 4, 2015, ERO established a process to obtain birth certificates from the Government of Jamaica for individuals who are subject to a final order of removal.

***Challenges:***

In FY 2015, many of ICE's performance outcomes were negatively impacted by laws and policies in jurisdictions across the country that limit state and local law enforcement cooperation with ICE detainees, and federal court precedent that has resulted in the release of a greater number of criminal aliens on bonds and their placement on the slower, non-detained docket. Consistent with Secretary Johnson's November 2014 memorandum [\*Secure Communities\*](#), ICE is working with state and local jurisdictions to increase cooperation through requests for notification of certain priority aliens prior to the alien's release in order to mitigate the impact of detainer non-compliance.

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

Ensure Resilience to Disasters by Strengthening Disaster Preparedness and Response Capabilities: By September 30, 2015, states and territories will demonstrate improvement towards achieving their core capability targets established through their Threat and Hazard Identification and Risk Assessment (THIRA).

**Overview:** To enhance national preparedness and resilience, FEMA established the THIRA to provide a common approach for identifying and assessing risks and documenting their associated impacts. Developing an understanding of its risks from natural, technological, and human-caused threats and hazards allows a community to make informed decisions about how to manage risk and develop needed capabilities.

In addition, states and territories assess their current capability and set targets for improvement for preventing, protecting against, mitigating, responding to, and recovering from these threats and hazards. FEMA expects states and territories to demonstrate improvement towards achieving their capability targets over the next two years through their THIRAs.

**Progress Update:**

**Results:**

- Thirty-one states and territories demonstrated improvement in their State Preparedness Reports toward achieving core capability targets established through their Threat and Hazard Identification and Risk Assessments, compared to 28 states and territories in fiscal year 2014. As the Threat and Hazard Identification and Risk Assessment process matures, states and territories will continue to refine capability targets by making them more specific and measurable. Since the initial assessment in 2012, roughly 43 percent of targets became more specific, seven percent of targets were made more challenging, and only two percent of targets were revised downward. Given the improved refinement of targets, FEMA has confidence that results of this measure demonstrate an increase in state and territory preparedness capabilities as indicated through the State Preparedness Report assessment.
- Forty-three out of the 56 state and territory Threat and Hazard Identification and Risk Assessment submissions achieved alignment with DHS Comprehensive Preparedness Guide 201, Second Edition, compared to 48 states and territories in fiscal year 2013. Analysis of the fiscal year 2015 results showed that 13 states experienced challenges with developing measurable capability targets, understanding resource requirements, and identifying National Incident Management System resource types. These results informed FEMA's Threat and Hazard Identification and Risk Assessment technical assistance in the fourth quarter, which will assist states and territories to achieve alignment with DHS guidance in their December 2015 submission.
- States and territories rated themselves as proficient in planning for 46.3 percent of their high-priority core capabilities in fiscal year 2015, compared with 38.3 percent in fiscal year 2013. Planning is a key indicator of preparedness.

**Milestones:**

- During fiscal years 2014 and 2015, FEMA conducted a total of 12 in-person technical assistance visits within the regions and 36 virtual technical assistance sessions addressing various aspects of the Threat and Hazard Identification and Risk Assessment and State Preparedness Report.
- During fiscal years 2014 and 2015, all 56 states and territories with Threat and Hazard Identification and Risk Assessments attended in-person and/or virtual technical assistance sessions. All states and territories with 2013 and 2014 Threat and Hazard Identification and Risk Assessments that did not align to DHS guidance participated in one or more technical assistance sessions.
- FEMA completed outreach activities started in fiscal year 2014 to share the results of calendar year 2013 and 2014 Threat and Hazard Identification and Risk Assessments and State Preparedness Reports with other Federal departments and agencies.
- FEMA is using OMB MAX, a platform run by the Office of Management and Budget, to help share 2013 and 2014 State Preparedness Report results with offices across the Federal government. Sharing State Preparedness Report results supports data-driven decision making to ensure Federal preparedness programs are targeting their resources to help state, local, tribal, and territorial governments improve their preparedness capabilities.
- The 2014 National Preparedness Report was released on August 6, 2014 and the 2015 National Preparedness Report was released on May 28, 2015. The National Preparedness Report summarizes national progress in building, sustaining and delivering the 31 core capabilities outlined in the National Preparedness Goal.

**FY 2016 – 2017 Agency Priority Goals**

For the FY 2016 – 2017 APG's, the Department is introducing three new APGs described below. More information about these can be found on [www.performance.gov](http://www.performance.gov).

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

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

**Overview:** Transnational criminal organizations (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.

Transnational Criminal Organizations (TCO's) 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 (SB&A) 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 Joint Task Forces (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.

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

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% of the participating federal civilian executive branch agencies so that they can monitor their networks.

**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.

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

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

**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.

## **Cross-Agency Priority Goals**

Per the GPRM Modernization Act requirement to address Cross-Agency Priority (CAP) Goals in the agency strategic plan, the annual performance plan, and the annual performance report please refer to [www.Performance.gov](http://www.Performance.gov) for the agency’s contributions to those goals and progress, where applicable. DHS currently contributes to the following CAP Goals:

- Mission Oriented:
  - Cybersecurity (Lead);
  - Improve energy efficiency to affect climate change;
  - Mitigate insider threat risks;
  - Identify job-creating opportunities;
  - Modernize infrastructure permitting modernization; and
  - Improve science, technology, engineering and mathematics education opportunities.

- Management Focused:
  - Deliver world class customer service;
  - Improve IT delivery customer service and outcomes;
  - Improve government's buying power through strategic sourcing;
  - Expand agencies use of shared services to improve performance and efficiency; improve administrative effectiveness and efficiency through benchmarking;
  - Support the interoperability and openness of data;
  - Improve the transfer of new technologies from the laboratory to the commercial marketplace; and
  - Build the workforce we need for tomorrow.

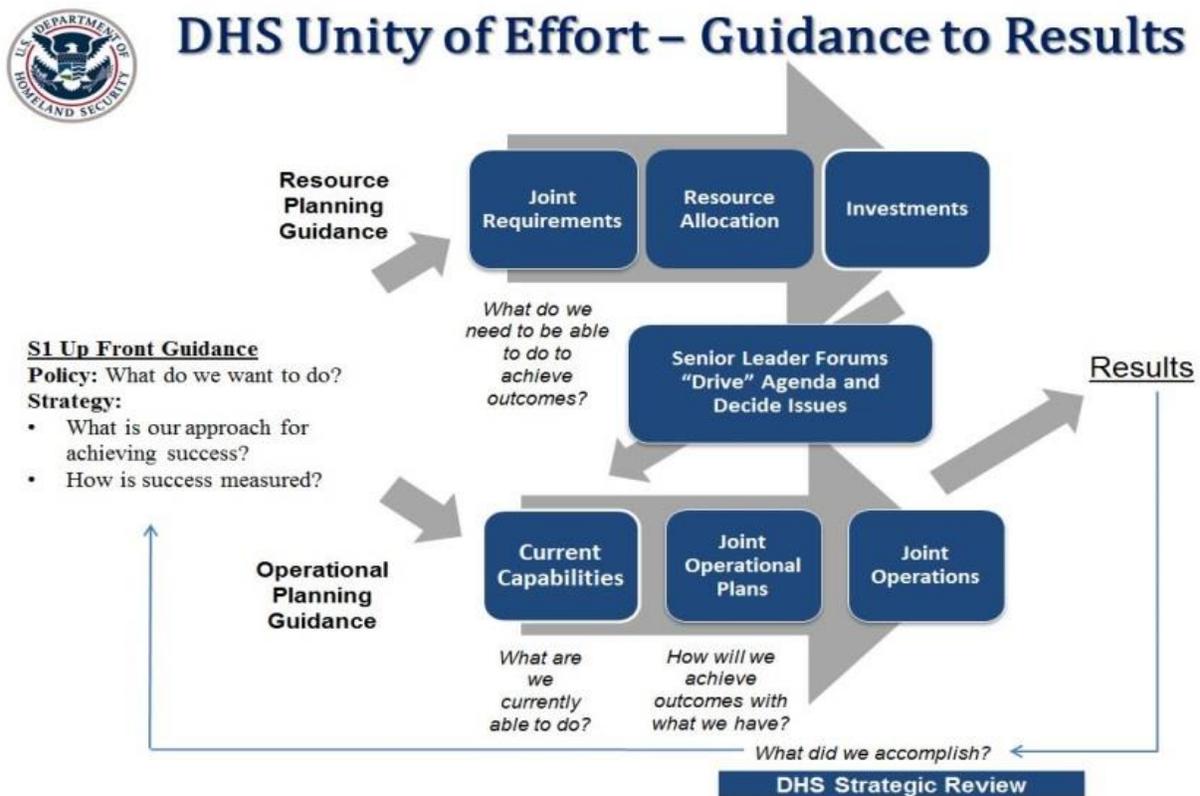
## Management Initiatives

This section discusses several of the FY 2015 Department-wide management programs and initiatives that are delivering greater service and protection to American citizens and our other customers. The initiatives are presented in the following categories:

- Unity of Effort
- Customer Service
- Human Capital Management
- Information Technology
- Acquisition Management/Strategic Sourcing
- Sustainability
- Financial Stewardship

## Unity of Effort

One year following the introduction of Secretary Jeh Johnson’s “Strengthening Departmental Unity of Effort” initiative (April 14, 2014), the Department of Homeland Security remains committed to institutionalizing transparent, unified, decision-making processes and empowering DHS Components to collectively address the Department’s complex mission space. Over the past fiscal year, DHS has made great strides associated with this vital initiative in spite of challenges such as a sustained period of budgetary constraints. That progress is more than just words: by examining



results through undertakings such as the DHS Strategic Review and the Annual Performance Report, the Department continues to improve its ability to measure success via the alignment of guidance to results.

Specific notable Unity of Effort initiative accomplishments include:

- The Joint Requirements Council (JRC) was created by the Secretary to help build a more unified, operationally effective and efficient Department through the creation of a Component-driven joint requirements process. The JRC oversees the Department's requirements generation process and provides recommendations for investment, as well as changes to training, organization, laws, and operational processes and procedures. Within FY 2015, the JRC made significant progress in building the Joint Requirements Integration and Management System (JRIMS), the process by which the Department reviews and validates capability requirements, associated gaps, and proposed fulfillment options to mitigate those gaps. The JRC has developed a draft DHS Management Directive, and associated Instruction Manual, to govern the execution of JRIMS and to establish initial roles and responsibilities. These documents are expected to be approved in December 2015. The JRC has also worked simultaneously to build an electronic tool called Knowledge Management/Decision Support (KM/DS) that will serve as the Department's system for JRIMS management. An associated training effort on JRIMS and KM/DS is being developed for relevant DHS stakeholders, with initial courses scheduled for early 2016.
- On February 27, 2015 Secretary Johnson signed the inaugural DHS Resource Planning Guidance (RPG) - a document called for as part of the Unity of Effort initiative. The FY 2017-2021 RPG outlined leadership priorities for Components and helped inform their respective budget development. This annual document is crucial to transforming the Secretary's guidance into results by codifying resource planning priorities that enable DHS Components to address budget challenges with cross-Departmental solutions. The RPG development and implementation process continues to be more institutionalized with the Secretary signing the FY 2018-2022 RPG months earlier, tangibly driving improvements and harmonization in the areas of Joint Requirements, Resource Allocation, and Investments.
- The initial group of Winter Studies was a central output from the 2017-2021 RPG. These Component-led efforts developed analytically informed solutions to some of the Department's highest priority areas, with several informing the FY 2017-2021 Program and Budget Review. In addition, a number of Winter Studies added value beyond the Program and Budget Review. For example, the Joint Duty Winter Study explored the creation and design of a workforce rotation program to enhance unity of effort and strengthen the Department's greatest resource—its workforce. It sought to do so by identifying and incentivizing participation in professional development work rotations outside member's home Component. This program will improve overall mission effectiveness and also Department-wide morale by providing meaningful career opportunities at various levels throughout the Department. The study was broadly endorsed at DHS senior leader forums and has resulted in follow-on instructions to create and implement a Joint Duty pilot program by summer 2016.
- In April 2015, the underlying concepts of the Unity of Effort initiative were applied to overhaul the Department's acquisition and procurement process via the Acquisition Innovations in Motion (AIiM) plan. This on-going series of events and initiatives has two goals: 1) institutionalizing a consistent and recurring approach to industry engagement and 2) implementing targeting initiatives designed to improve the DHS acquisition process.

- The continued productivity and evolution of both Senior Leader Forums - the Deputy's Management Action Group (DMAG) and the Senior Leaders Council (SLC), which both meet twice monthly to address the Department's most challenging issues in a transparent, collaborative fashion. Specifically, the SLC has met to discuss and decide on future Component goals and challenges (October, 2014) and approaches to the Congressional budget debate (March, 2015). During that timeframe, the DMAG has made several key decisions ranging from the approval of the FY 2017-2021 RPG (October 15, 2014), the realignment of certain DHS headquarters offices and their corresponding functions (February 10, 2015), investment options during the FY 2017-2021 Program and Budget Review (July 2015), and the implementation of the DHS Data Framework (June 11, 2015).
- The new DHS Southern Borders and Approaches Campaign Plan and new DHS Joint Task Forces East, West, and Investigations—another direct extension of the Unity of Effort initiative—achieved full operational capability on July 31, 2015. The introduction of the Campaign and three joint task forces reflects DHS's new focus on collective missions with a unified emphasis on joint operations.
- The Department has begun to deepen its analytical capabilities to assess and address challenges as well as utilize those capabilities to assist how it measures future Departmental achievements and results. This Analytic Agenda will allow DHS to acquire, develop, and implement the basic tools required for data-driven management of its missions. This effort will build and institutionalize the necessary data, models, and underlying business processes to provide a unified baseline that can assist leadership in its decision-making. An early example of this is the development of new strategic outcome metrics for the Department's border security mission. These strategic outcome measures, linked to Goal 2.1 of DHS's Strategic Plan, enable the Department to optimize the allocation of its limited resources to minimize the level of illegal entry of people and goods into the United States. As the Department continues to foster better analytical capabilities, its self-evaluation processes will similarly continue to mature. The second annual Strategic Review, completed in May 2015, provided insight into Departmental areas to address; in the future DHS can further refine this tool to answer how it met or failed to meet its outlined goals.

These achievements are only the beginning of the Department's strategic direction to unify efforts to better address the diverse set of challenges DHS faces today and in the future. The challenges, which include everything from a contested and fraught cyberspace realm, domestic and international terrorists, and more, all demand an agile, strategic and unified Department.

Looking forward, the processes and organizations the Unity of Effort initiative has put into place will continue to grow in institutional strength and provide the driving force behind the Department's new strategic approach. As the Department begins work on the 2018 Quadrennial Homeland Security Review, the Unity of Effort initiative will underscore that when Components are collective in action, the Department more effectively executes its missions.

## Customer Service

### *Internal Customer Service Initiatives*

The Under Secretary for Management (USM) oversees the Management Directorate lines of business, delivers quality mission support services and provides leadership and oversight for Management functions, while eliminating redundancies and reducing support costs. Through this effort, the USM is continuing to implement the integrated mission support structure for the Department to improve the efficiency and effectiveness of mission support services.

Efforts to improve customer service occur in a variety of forums, which include:

- **Acquisition Innovations in Motion (AiM)** - Implemented AiM, an effort that institutionalizes a consistent and recurring approach to industry engagement, and executes targeted initiatives designed to improve the DHS acquisition process and increase operational capability. A series of initiatives, industry engagement events, and conversations focused on reciprocal learning between DHS and industry provides an improved understanding of the marketplace, increased trust between the two, and lays the groundwork for increased competition and effective execution of the DHS mission. For example, under *AiM*, DHS implemented the Procurement Innovation Laboratory (PIL), which highlights innovative techniques for increasing efficiencies and effectiveness in the procurement process. Lab successes will advance mission delivery by removing entry barriers for innovative, non-traditional contractors to compete for DHS business opportunities; shorten time-to-award; and increase probabilities of successful IT system development.
- **Transparency in Hiring** - Collaborated with Component human resource directors to improve the hiring process through greater consistency, timeliness and transparency in hiring. There are several departmental and Component level initiatives to ensure that hiring processes are effective and efficient, and provide a positive experience for applicants. By improving hiring, the Department is better positioned to attract the best and brightest candidates.
- **Consolidate the DHS Footprint** - Developed recommendations to identify co-location and real property efficiencies to fulfill common administrative and logistical needs. The Boston regional cross-component team made 32 recommendations, which included coordinated training, streamlined mission support administrative services, shared asset operations and maintenance service contracts, and the consolidation and improved utilization of real property. A cross-Component implementation team is currently at work in the region. DHS will expand this model to 11 additional regions of the United States in FY 2016.

In FY 2016, the Management Directorate will continue to enhance customer service and effectiveness by making the Department an employer of choice, enhancing mission capability through innovative procurement approaches, and optimizing the use of DHS assets and shared services. In addition, the Management Directorate will continue its Management Forums, which allows customers to provide input on their needs and give feedback on current service. Moving forward, DHS will continue these efforts and find new ways to improve the delivery of services to its customers.

## *Air Passenger Screening Customer Service Initiatives*

The Transportation Security Administration (TSA) performs and oversees security operations at the nation's airports, screening more than 660 million passengers annually, to ensure the freedom of movement of people and commerce. In an effort to strengthen aviation security while enhancing the passenger experience, TSA focuses on risk-based, intelligence-driven security procedures, as well as initiatives to enhance its use of technology thereby lessening the burden on the flying public. By analyzing available data and information currently provided by the traveler and combining that information with our multi-layered system of aviation security, TSA can better focus limited resources on higher-risk and unknown passengers.

TSA has taken several steps to improve customer satisfaction while maintaining a strong security posture. These steps include, but are not limited to:

- **Social Media Updates:** Customer service is evolving to match the rapid growth and development of digital and social media. TSA launched an @AskTSA Twitter account in August 2015 in order to improve the public perception of TSA by providing helpful and friendly real-time responses to the traveling public before, during and after travel. By taking on the role of customer service with social media, TSA has the opportunity to better prepare passengers arriving at security checkpoints. The @AskTSA Twitter account consists of an eight member team that will be located at the Transportation Security Operations Center and will mirror the hours of the TSA Contact Center to include weekends and holidays. The Partnership for Public Service fellowship team, comprised of representatives from the U.S. Department of Defense, Department of Veteran's Affairs, National Health Institute, and the Import-Export Bank of the United States are collaborating on this initiative so that other Federal agencies have the opportunity to pilot the same type of program. In addition, during 2015, TSA expanded its Instagram presence to more than 300 thousand followers and was recognized by Rolling Stone as number four in the top 100 Instagram accounts to follow. TSA's use of interesting photographs via Instagram raises awareness about TSA Pre✓<sup>®</sup>, TSA initiatives and policies, and the items that are not permitted at the checkpoint.
- **TSA Website:** TSA's website serves as the primary public source of information available 24/7 regarding activities to protect the nation's transportation systems with an average of more than 3.5 million visitors per month. TSA launched a completely revamped and redesigned website in August 2015 focused on customer centric content and responsive design. This includes a two-click navigation system based on the most accessed and needed information for the public as well as rewritten content; lower page count; easy access to popular programs and services on the homepage; an interactive map showing TSA Pre✓<sup>®</sup> airports and airlines; a robust news section and photo and video galleries; and it is designed to work on any device. In addition, TSA focused on visitors learning something new about the mission of TSA when they access the site with top news stories on the homepage, which are updated each week.
- **Expedited Screening:** Through ongoing efforts to accelerate enrollment in DHS Trusted Traveler Programs (TTPs) and expand TSA Pre✓<sup>®</sup> to trusted, pre-vetted populations, TSA has strengthened security at screening checkpoints while simultaneously increasing its operational efficiency and improving the passenger experience. As of September 30, 2015, TSA Pre✓<sup>®</sup> was available at more than 160 airports through 12 participating airlines,



including Air Canada as the first international participating airline. Expedited screening benefits include members of TSA's Pre✓<sup>®</sup> application program, members of U.S. Customs and Border Protection's Trusted Traveler programs, members of Congress, federal judges, all members of the U.S. Armed Forces including those serving in the National Guard and reserves, and government employees from select agencies. In March 2015, the TSA Pre✓<sup>®</sup> application program enrollment reached one million passengers and thousands continue to apply on a daily basis. TSA is evaluating options for leveraging the private sector to increase passenger enrollment in TSA Pre✓<sup>®</sup>. Through these combined

efforts, as of September 30, 2015, approximately 41 percent of the traveling public was receiving expedited screening.

During the second half of FY 2015, TSA initiated several changes resulting in an overall decrease in the percentage of travelers eligible to receive expedited screening. These changes include halting the use of Managed Inclusion 2 at all airports across the system (Note: Managed Inclusion 2 was a real time threat assessment process at the screening checkpoint using a combination of Explosive Trace Detection (ETD) and behavioral assessment, and then random selection for expedited screening); eliminating some groups of travelers from consideration as potentially eligible for TSA Pre✓<sup>®</sup> on a trip-by-trip basis via Secure Flight (SF) Risk Assessment Rules; implementing enhancements to strengthen the risk assessment algorithm; decreasing the opportunity for inclusion in TSA Pre✓<sup>®</sup> via SF Risk Assessment rules from any single factor by approximately one-third; and other adjustments to the risk assessment rules process driven by recent intelligence information.

As a result of these changes, the overall proportion of daily travelers eligible for expedited screening has decreased overall by approximately 20 percent from peak levels of eligible travelers achieved earlier in FY 2015, while at the same time the number of pre-vetted trusted travelers and other approved low-risk passengers has increased, and now accounts for more than 12 percent of daily passenger volume (up from 5.7 percent at the beginning of 2015).

In FY 2016, TSA will continue to focus on increasing the number of known travelers; this will allow TSA enhance security effectiveness, while improving the passenger experience.

- Traveler Redress Inquiry Program (TRIP):** In FY 2015, the DHS TRIP program implemented a new process, released by the White House in April 2015, providing enhancements to DHS TRIP by offering additional transparency for U.S. citizens and lawful permanent residents who have been denied boarding on a commercial aircraft because they are on the No Fly List. When a U.S. citizen or lawful permanent resident applying for redress is, in fact, on the No Fly List, DHS TRIP will now inform that applicant of his or her status on the List. These applicants will be provided with an opportunity to request and receive additional information regarding their status, as well as submit any information that they consider potentially relevant to that status. Following a review (including an

examination of any information provided by the applicant), DHS TRIP will inform applicants of the results regarding their status on the No Fly List.

- **TSA Contact Center (TCC):** The TCC fields inquiries by telephone, email, or online portal. These direct inquiries from travelers concern a wide variety of issues, ranging from prohibited and permitted items to identification requirements to trusted traveler program enrollment. In FY 2015, the TCC modified two current customer satisfaction surveys to increase participation. Both the TCC survey and EEO intake survey have a participation rate of approximately 30 percent. As a result of survey scores, TSA has proposed changes in the EEO intake triage process which are intended to increase response time. The TCC also established a modified response process which allows individuals with advanced yet less complex inquiries to receive a more timely response. In addition, the Interactive Voice Response system was modified to provide callers with better self-service options.
- **Multicultural Training:** In FY 2015, TSA developed an Image Awareness Passenger Engagement Training Module and the Passenger Engagement Briefing that all Transportation Security Officers (TSOs) will receive. The training entails presentation of various screening checkpoint scenarios, such as sexual orientation, religious headwear, and African-American female hair pat-downs, for example, and focuses on the perceptions that travelers have when interacting with TSA employees. This training allows the TSOs to learn and discuss how to better handle situations so that negative perceptions of TSA are not reinforced.
- **Disability Training:** In FY 2015, TSA launched a targeted webinar series wherein members of TSA's Disability and Medical Condition Coalition share insights, experiences, and best practices in live, webinar-based presentations to the TSOs related to a particular disability or medical condition. Through this engagement, TSOs ask questions and learn best practices from the coalition member presenter about how to ensure successful interactions with passengers with disabilities at the security checkpoints.
- **TSA Claims Process:** TSA screens millions of passengers and bags each year. Occasionally TSA will damage an article. To ensure passengers have an easy to navigate and file claim system, information on how to file a claim is available on TSA's public website. The website is easy to follow and provides contact information for the public. Any contacts made are responded to within two business days. Claims may be presented to TSA by email, fax, or standard mail. Travelers who have filed a claim with TSA may easily find status information on their claim at [www.TSA.gov](http://www.TSA.gov). TSA is working to reduce any claims, and over the last six years claims have gone down by 54 percent. This is the result of TSA educating officers on actions that may lead to claims and promoting efficient baggage tracking, lost and found systems, and other procedural changes to reduce claims and keep the public's trust.

## *Ports of Entry Customer Service Initiatives*

### **Key Accomplishments in FY 2015**

On February 13, 2015, DHS and the Department of Commerce released a report to President Obama titled "*Supporting Travel and Tourism to Grow Our Economy and Create More Jobs: a National*

*Goal on the International Arrivals Process and Airport-Specific Action Plans.*” The report defines a national goal that was developed through extensive consultation with leaders from the airline industry, airport authorities, state, and local governments, as well as other industry leaders in the customer experience space:

*“The United States will provide a best-in-class international arrival experience, as compared to our global competitors, to an ever-increasing number of international visitors while maintaining the highest standards of national security. Together, the public and private sectors endeavor to ensure that legitimate travelers feel secure and welcome and view their arrival experience as the very best as compared to our global competitors.”*

Working in full partnership with private industry and local government stakeholders, U.S. Customs and Border Protection (CBP) continues to demonstrate its commitment to facilitating economic growth while reducing wait times for international travelers. CBP is committed to establishing the metrics and processes necessary to support ongoing improvement, and is working to increase officer use of mobile technologies to maximize efficiencies.

Airport-specific Action Plans have been developed through close partnerships with airports, airlines and industry, and include significant steps to drive innovation to increase security while simplifying and streamlining the entry process at the top 17 airports. Compulsory quarterly updates are carefully reviewed by the Office of Field Operation senior management and posted to the Travel and Tourism website on CBP.gov to provide the traveling public the latest information and ensure accountability and transparency. Terminal Level Metrics Dashboards are published to the CBP.gov site once a month.

CBP continues to aggressively pursue new and innovative technology that will assist officers in their efforts to provide national security and efficiently facilitate trade and travel through our nation’s ports of entry. To address the substantial increases in travel volume to the U.S. and the continuing growth in worldwide travel, CBP continues to make substantial improvements in traveler facilitation through automation, innovation, and trusted traveler programs. In FY 2015, CBP deployed more than 1,000 Automated Passport Control (APC) kiosks to 37 locations. Mobile Passport Control (MPC) has been developed and is in a pilot testing phase at airports in Atlanta (ATL), Miami (MIA), Seattle (SEA), Chicago (ORD), and San Francisco (SFO). Expansion of MPC continues, with business requirements to be released soon. Global Entry kiosks are installed at 57 airports and over 3.5 million travelers have Global Entry benefits. The kiosks have been used over 15.4 million times. CBP is continuing to expand Global Entry membership as quickly as possible and international Global Entry partnerships will continue to expand to additional countries.

### **Key Challenges**

CBP is relentlessly pursuing new and innovative technology to assist officers in their efforts to provide national security and efficiently facilitate trade and travel through our nation’s ports of entry.

To achieve the national goal of a best-in-class arrival experience, we need a substantial transformation of CBP’s business processes. Creating the CBP Arrivals Area of the Future, based on a Technology First vision that places mobile applications in the hands of CBP Officers (CBPOs)

performing different roles and tasks, giving them the information they need at their fingertips, requires significant expansion of CBPO use of mobile technology and a consolidation of all CBP operations in one location of the Federal Inspection Services (FIS) area. To realize this vision, the unique features of each airport and the airport-identified “pain points” must be addressed individually at the local level.

When the vision is fully realized, technology like APC and MPC will first allow travelers to self-segregate after claiming baggage and will meter passenger flow into the baggage area. Consolidated CBP staffing will be located in one area of the FIS. Secondary inspection areas and office space will always be adjacent to Primary. CBP Officers will have both the traveler and baggage in one place for quick decision making. This configuration can potentially lead to more roving and increased enforcement while also speeding the overall inspection process. This will provide one clear picture of the international arrivals process, enabling CBP to develop more accurate metrics and encouraging airlines and airports to be timely with baggage delivery.

A major challenge at many locations is facility capacity, including sufficient space for the passenger queue and enough distance between booths or podiums to accommodate travelers with baggage. Significant baggage delivery delays may cause bottlenecks that impact overall passenger processing.

### **Next Steps**

Over the next few years, CBP will continue to aggressively pursue the initiatives included in the 17 Airport Action Plans. These efforts will be supported by quarterly reports to management and timely updates to information for stakeholders and the traveling public. CBP will complete simulation modeling to prove the potential positive outcomes of the CBP Arrivals Area of the Future, and continue working with willing private sector partners at Seattle and Ft. Lauderdale to incorporate new concepts into their designs. The Airport Technical Design Standard will be updated and new facilities or major reconstruction should be geared towards the concept of the CBP Arrivals Area of the Future.

### ***Disaster Assistance Customer Service Initiatives***

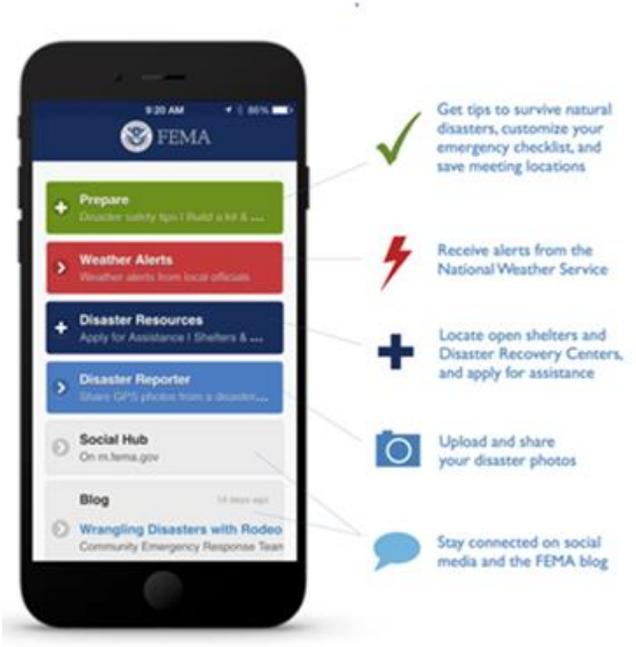
The Federal Emergency Management Agency (FEMA) coordinates the Federal Government’s role in preparing for, preventing, mitigating the effects of, responding to, and recovering from all domestic disasters, including natural disasters and acts of terror. FEMA strengthens the resilience of the nation in the wake of a disaster, and serves survivors by providing disaster assistance such as grants to repair homes, temporary rental assistance, and reimbursement for damaged property. To ensure that disaster survivors have timely information and access to disaster assistance, FEMA is working to disseminate information and connect with communities in a variety of ways to improve customer satisfaction:

- **FEMA Language Line:** Following Hurricane Sandy, FEMA established a language line that provides callers direct access to disaster assistance information in more than 50 languages. This line has been promoted through community outreach, engagement with State and local government officials, flyer distribution, news releases and media interviews. While

initiated during Hurricane Sandy, this line is still active and will be a resource for Limited English Proficiency (LEP) callers during future disasters.

- Phone and Online Disaster Assistance Applications:** FEMA’s three National Processing Service Centers provide professional services for disaster survivors and ensure correct processing of customers’ applications. As part of FEMA’s strategic objective to enhance and expand services for survivors, efforts are currently underway to modernize the existing Call Center platform, enabling FEMA to leverage emerging technologies and services to improve the survivor experience and become a Government Center of Excellence in contact center service and performance. Successful modernization will enable the call centers to more effectively meet survivor needs in a timely and effective manner in addition to allowing for faster response to disaster-related change. During FY 2015, FEMA awarded the contract to begin the modernization effort with a full implementation target set for the end of FY 2017. [DisasterAssistance.gov](http://DisasterAssistance.gov) continues to provide survivors with an online and mobile registration vehicle for FEMA individual assistance. Seventeen Federal partner agencies participate in the program with DHS/FEMA acting as the managing partner. Sharing survivor data among the partnership elevates the ability of the government and the whole community to serve survivors efficiently. The Disaster Assistance Improvement Program has been approved to reengineer DisasterAssistance.gov as a single source of information for disaster survivors and a single entry-point to apply for disaster assistance from multiple federal agencies. The Disaster Assistance Re-engineering Effort will provide an agency-neutral, survivor centric portal for disaster assistance; offering a tailored experience for survivor needs based on information they provide.
- Mobile Device Applications:** FEMA launched the National Weather Service (NWS) alerting capability for the FEMA app on April 14, 2015 and added Spanish language capability for NWS alerts on May 18, 2015. The NWS alerts feature allows the public to stay informed and prepare for weather events in 5 US locations of their choosing on their mobile device. Additionally, operating system and maintenance updates were applied on a

quarterly basis for both iOS and Android platforms. FEMA will be adding additional features such as event reminders, social media integration, sharing, enhanced disaster preparedness features, integration with additional 3rd party support tools (i.e. Salesforce), and technology refresh. FEMA also deployed Spanish language support and a web based subscribe/unsubscribe feature for Text Messaging. Future enhancements of Text Messaging include additional keywords and additional messaging capability. Key challenges include continuous security enhancements and adapting to constant mobile technology changes.



- Customer Satisfaction Surveys:** The Customer Satisfaction Analysis (CSA) group has redesigned the Follow-up Program Effectiveness & Recovery survey to focus on

survivor centric support and align with strategic plan objectives. Requests from Recovery Directorate, National Preparedness Directorate, External Affairs, and the Office of Disability Integration & Coordination indicated a need for a redesign of the questionnaire to gather valuable feedback from our disaster survivors not previously collected. The rewritten and renamed “Survivor Centric Customer Satisfaction Survey” includes topics on preparing for a disaster, post disaster information and communications, accessibility to FEMA resources and services, financial assistance, expectations, household’s level of recovery, and overall customer satisfaction. The survey was designed for flexible deployment for specific types of disasters and can be performed in any timeframe ranging from 30 days to 24 months after declaration. The sampling methodology is also flexible in that a random sample can include eligible applicants, ineligible applicants, or both as well as a follow-up survey with those who previously participated in past CSA satisfaction surveys. The Survey is currently approved and in use, with the first disaster for the second quarter on calendar year 2015. Future surveys will be conducted quarterly on non-duplicate eligible applicants from those disasters surveyed with the Program Effectiveness and Recovery surveys.

- **Public Assistance Re-engineering:** Public Assistance, which services state, local, tribal, and qualified private non-profits, accounts for the majority of FEMA’s grant funding and typically awards more than \$4 billion annually. Recovery has embarked on a reengineering project that is designed to increase the overall efficiency, address known shortcomings in the program, and become more aligned with FEMA leadership’s vision of how the PA program should operate beginning in late FY 2014. The reengineering efforts are intended to increase interaction with the customer, standardize processes, decrease administrative costs, improve quality of work, and reduce errors through the enhanced communications on the front end of the process.
- **Public Assistance Appeals and Audits Branch (PAAB):** The PAAB has implemented several approaches to improving the consistency, timeliness, and processing of first appeals nationwide. Through establishing new dedicated appeal analyst positions at all ten FEMA regions, developing procedures by which overburdened regions can transfer appeals to those with lighter workloads, and creating a First Appeals Section at Headquarters to serve as a national resource, FEMA has made progress in constructing the capacity, flexibility, and system needed to address the current backlog of appeals and meet future demands of the States and communities. At this point, the biggest challenge for the Agency is hiring and training the personnel necessary to carry out these functions. Until current vacant staffing positions are filled, FEMA will continue to balance the competing demands of reducing existing overdue appeal backlogs with the timely processing of new appeals.



### ***U.S. Citizenship and Immigration Services Customer Service Initiatives***

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

On an average day, USCIS: completes 23,000 applications for various immigration benefits; welcomes 3,200 new citizens; answers 44,000 phone calls to our toll-free customer service line; serves 9,500 customers at 84 local offices; fingerprints and photographs 15,000 applicants at 136 application support centers; conducts 148,000 national security background checks; and processes 2,040 petitions filed by employers to bring workers to the United States.

USCIS has a rich customer-centric business model to provide services and benefits to a wide range of customers, including but not limited to:

- Individuals seeking to enter the country as a nonimmigrant (e.g. a temporary visitor or student) or as a lawful permanent resident (LPR), along with LPRs who choose to become U.S. citizens through the naturalization process;
- Individuals who live overseas and seek to be reunified with relatives in the United States;
- Employers who file a petition on behalf of a potential worker;
- Individuals fleeing oppression, persecution and torture because of their race, religion, nationality, membership in a particular social group, or political opinion;
- Individuals confronting an urgent humanitarian situation and needing authorization to enter the United States on a temporary basis;
- Employers who use the E-Verify program to determine the employment eligibility of new employees; and
- Federal, state, and local government agencies that use the Systematic Alien Verification for Entitlements (SAVE) program to confirm immigration status before issuing public benefits.

Below are a few of USCIS's recent efforts to improve the customer experience:

- **USCIS Electronic Immigration System:** USCIS continues to modernize the process for receiving and adjudicating immigration benefit requests by using its electronic immigration system to change from a paper-based process to an electronic process and gradually expand the system to cover all USCIS citizenship and immigration benefits.
- **National Customer Service Center (NCSC):** Through the NCSC, USCIS provides nationwide telephone assistance to customers calling about immigration services and benefits. Assistance is available in English and Spanish. During the next fiscal year, the NCSC will improve how the agency interacts with its customers by offering an Interactive Virtual Assistant (IVA), Web chat, and email.

In FY 2015, USCIS introduced the following:

- **Virtual Hold** – Customers who call the NCSC have the option to request live assistance. If a caller has case specific questions, the call can be transferred to a Tier 2 USCIS Officer. While waiting for a Tier 2 Immigration Services Officer to become available, customers are placed in a virtual hold that allows the customer to hold their place in queue, with the option to disconnect and receive a call back.
- **Change of Address (COA)**

- The COA tool was redesigned based on stakeholder feedback and now provides clearer instructions and navigation. At the same time, it eliminated the need, in most cases, to file a separate AR-11 (Alien's Change of Address Card). Additional steps have also been taken to protect customers' privacy.
  - In addition, the tool is compatible with multiple web browsers and guides customers through the change of address process and sends customers a confirmation email.
- **Case Status Online (CSOL)**
  - CSOL was updated to make it easier for customers to modify their profiles. This update works in conjunction with myUSCIS, which allows the customers to check the status of their pending cases and receive updates.
  - A help feature was also added to assist the customers with questions.
- **Customer Engagement Center:** USCIS is moving toward a new customer service model, evolving from traditional call centers to a full-scale customer engagement center that will include live chat and secure messaging. USCIS is actively working to provide customers with the following features:
  - A searchable knowledge database that allows customers to enter immigration questions in plain language and receive a clear answer, along with relevant supporting materials;
  - A single, personalized portal that will enable them to access case status information; make case inquiries and submit requests for service; view personalized case and contact history; schedule in-person appointments; and communicate securely with USCIS via chat and email about their cases; and
  - Customers will be able to enter data about themselves to identify immigration benefits that they may qualify for, along with information on associated forms, fees, and required documentary evidence.
- **Public Engagement Efforts:** USCIS holds a variety of external stakeholder events to share information and obtain feedback on USCIS programs and policies. As of September 30, 2015, USCIS hosted 73 national engagements and 3,787 local engagements reaching more than 189,773 individuals. This included 714 engagements on deferred action for childhood arrivals with 66,873 attendees; 1,017 multilingual outreach events with more than 63,225 participants; and more than 418 engagements with underserved populations that reached more than 27,348 people. During FY 2015, USCIS also expanded its public education and customer awareness efforts by enhancing communications on immigration scams and the unauthorized practice of immigration law; more than 1,621 engagements reached more than 106,379 customers. In FY 2015, USCIS trained more than 236 librarians, and had approximately 3,105 librarians registered to receive information specific to USCIS outreach.
- **Citizenship Outreach Partnerships:** USCIS continues to expand municipal partnerships to increase the capacity of communities to prepare immigrants for naturalization and raise awareness of the rights and responsibilities of citizenship. In FY 2015, USCIS signed letters of agreement with the cities of Atlanta, GA; New York, NY; Boston, MA; Seattle, WA; and Houston, TX. Under this initiative, USCIS has distributed more than 398,000 educational

materials on citizenship and the unauthorized practice of immigration law and established 348 citizenship corners in municipal facilities.

- **Verification Outreach:** The Verification Outreach program promotes awareness and correct use of the Employment Eligibility Verification Form I-9, E-Verify, employee rights, and the SAVE program. To achieve this, approximately 40 public webinars are offered monthly totaling 529 webinars to 25,295 participants in FY 2015.

## Human Capital Management



The Office of the Chief Human Capital Officer (OCHCO) continued to strengthen the human capital line of business with the transition to a new Human Capital Strategic Plan (HCSP) and operational framework for completing cross-cutting human capital strategic priorities in FY 2015 and beyond. The HCSP represents the second five year strategic planning cycle emphasizing management integration, accountability tracking, and the use of human capital data analysis to meet DHS mission needs. FY 2015 also was the first year DHS has developed and implemented an annual

operational plan jointly developed by OCHCO and the components to support continuing performance improvements. OCHCO also completed a full year of quarterly, data-driven performance reviews through its HRstat program. 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 a “Fully Addressed” rating for implementing the Human Capital Strategy (HCM #1) in its February 2015 High Risk Report.

Under the FY 2015 Operational Plan, DHS accomplished a number of significant outcomes – several provided near term benefits to the workforce and some positioned DHS for high impact outcomes in FY 2016 and beyond. Key human capital accomplishments and priorities for the next 1-2 years are outlined below and align with the human capital goals established in the DHS HCSP.

### **Goal 1: Provide human capital strategies to successfully achieve the DHS mission and mitigate risks.**

#### Accomplishments:

- Transitioned to a new Human Capital Strategic Plan and a sustainable operational framework that advances human capital programs, improves performance, and better supports DHS mission accomplishment.
- Enhanced its human capital decision support capabilities by standardizing the key indicators reported on the DHS Human Capital Dashboard. With common definitions and a common approach to data collection across DHS components, human capital leadership is better able to assess and guide departmental efforts to improve the efficiency and effectiveness of HR policies/programs.
- Developed component-specific workforce plans according to the DHS Workforce Planning Guide framework with quarterly status updates on action plans to close gaps for select

Mission Critical Occupations. A central source library was established to foster collaboration among the workforce planning community and includes best practices, guidance, and tools related to skill gap analysis and closure activities.

- Developed and implemented component language access plans to address gaps in foreign language skills across the Department. This effort addresses a GAO recommendation (GAO-1-714) to assess language needs, capabilities and shortfalls.
- Updated the Workforce Planning Guide and tools to guide component action planning in FY 2016 and beyond to ensure consistent, more streamlined workforce planning processes throughout the Department.
- Strengthened and enhanced the Balanced Workforce Strategy (BWS) program by launching an internal audit process for the implementation and use of the Balanced Workforce Assessment Tool (BWAT). Mandated for use for all new resource requirements, BWAT helps components maintain an appropriate mix of federal and contractor resources. Audits of ICE, NPPD, USCIS, and FEMA were completed as planned in FY 2015.
- Developed recommendations and initiated implementation of a DHS Succession Planning Framework. Linked closely with workforce analysis, the success planning framework provides components with a consistent approach for identifying succession risks along with the development of strategies to address leadership pipeline or workforce gaps.
- Matured DHS benchmarking data and capabilities through participation in a government-wide effort led by OMB and OPM to provide comparative data for agency performance improvement planning. The resulting benchmark data informed FY 2016 operational planning and provided focus areas for more in-depth analysis and action planning in FY 2016.

#### 1-2 Year Priorities:

- Mature value of HRstat emphasizing data analysis and actions for high impact outcomes that improve performance.
- Strengthen and enhance the value and use of human capital data through the implementation of the Five Year Human Capital Data Plan.
- Broaden the use of the Workforce Planning framework to additional Mission Critical Occupations and implement skill gap measurement strategies to assess the effectiveness of gap closure actions implemented by the components.
- Complete DHS-wide implementation of the Succession Planning Framework to assist in workforce planning and skill gap closure strategies.

#### **Goal 2: Acquire a highly qualified and diverse workforce.**

##### Accomplishments:

- Developed and published policy, guidance, and tip sheets to DHS managers, employees, and HR professionals to help them navigate the hiring process.
- Continued to execute the DHS Coordinated Recruitment and Outreach Strategy, which was key to GAO awarding DHS a “Mostly Addressed” rating for the Targeted Outreach and Recruitment outcome on the February 2015 High Risk Report.

- Strengthened information collection and coordination on component recruitment events for added efficiency which closed GAO audit 13-742, *DHS Is Generally Filling Mission-Critical Positions, but Could Better Track Costs of Coordinated Recruiting Efforts*.
- Drafted the DHS Strategic Outreach and Recruitment Plan (DHS SOAR) to replace the current DHS Coordinated Recruitment and Outreach Strategy, and which will continue to drive diversity at DHS which is among the best in government.
- Revised the Component Recruitment and Outreach Plan (CROP) template to enhance recruiting efforts to meet current and long-term workforce needs through collaboration between Component recruiters, workforce planners, and diversity/EEO staff.
- Coordinated DHS engagement at high-value diverse recruiting opportunities, including the five major annual law enforcement training events targeting diverse populations to enhance DHS presence and branding at major recruiting events.
- Analyzed DHS' performance on major entry programs such as the Pathways Program and the DHS Millennial workforce. Pathway Programs continue to increase in use each year and the millennial workforce is even more diverse than the overall DHS workforce.
- Signed memoranda of understanding with the major diverse Higher Education Associations that together represent over 1,500 Minority Serving Institutions to increase communication between DHS and the associations, including employment opportunities.
- Reformatted the DHS Recruiter Training into a virtual format. The training is designed to reduce costs and enhance collaboration by enabling DHS to send local recruiters with general knowledge about employment opportunities across DHS. To date, over 400 DHS Recruiters have been trained through this program.
- Awarded two Blanket Purchase Agreements to third party providers for internships to supplement the Pathways Programs and enhance diversity efforts.
- Strengthened oversight on the hiring process with the development of the first department-wide quarterly time-to-hire report which includes component-by-component data as well as shared successes, obstacles and effective practices.
- Initiated a pilot program with CBP, TSA, and USSS focused on an improved time-to-hire data collection methodology by focusing on specific phases of the hiring process for five Mission Critical Occupations, which will enable the Department to have a stronger understanding of obstacles that need to be addressed in the hiring process.
- Enhanced the DHS hiring process by implementing notifications to hiring managers on the status of recruitment at critical points in the hiring process.

#### 1-2 Year Priorities:

- Execute the DHS Strategic Recruitment and Outreach Plan to ensure outreach to diverse populations and enhance the efficiency and effectiveness of DHS recruiting efforts.
- Enhance recruiting and onboarding programs to include new forms of media to attract, engage, and hire employees, including broadening recruitment efforts to women regarding law enforcement careers and to minority serving institutions.

### **Goal 3: Foster a departmental culture of excellence through inclusion and engagement.**

#### Accomplishments:

- Improved Federal Employee Viewpoint Survey (FEVS) administration and follow-up by developing a streamlined FEVS action planning tool to better support component employee engagement planning. Also conducted component training on root cause analysis and metrics to support development of more rigorous actions plans. Integrated employee engagement measures into the quarterly HRstat performance reviews and used FEVS results to better inform employee engagement planning activities, consistent with department leadership and the President's Management Agenda Cross Agency Priority goal on People and Culture.
- Developed and published a toolkit for DHS program managers and human capital support staff to use Cyber Security and IT hiring flexibilities and incentives effectively.
- Collaborated with the Department of Defense to develop a course aimed at identifying, assessing, and preparing the next-generation of cybersecurity operators to protect and defend U.S. interests.
- Strengthened the tracking and reporting for the 12-hour "give-back" requirement for every supervisory employee as part of the Department's Cornerstone leadership development program. This improvement enabled DHS to highlight the many forms of "give back" available to supervisory employees such as mentoring and serving on selection panels for development programs. Through this program, DHS promotes employee engagement and a culture of continuous learning and development.
- Developed Departmental guidance for evaluating, consolidating, and assessing the effectiveness of mandatory training on an annual basis. The guidance helps ensure quality standards are consistently applied and the effectiveness of mandatory training is assessed annually. Launched an online training course for first time supervisors of bargaining unit employees to develop understanding and help strengthen DHS's commitment to fostering productive relationships with the unions. The training, information, and job aids provided by components targeted topics relevant to their respective collective bargaining agreement and labor practices.
- Created and field tested a series of tools for enhancing leadership capabilities; including an innovation toolkit, a guide to conducting a great town hall meeting, and a stay interview guide. Set up the Leadership Resource Center, a site on the DHS intranet, to house all these resources. We are initiating a communications campaign this month to distribute the info to all DHS executives, managers, and supervisors.
- Created and distributed a "welcome to DHS" video that is being incorporated into all new employee orientation at the Department
- Launched a behavioral interview question bank to help hiring managers identify positive, engagement-oriented attitudes and behaviors among senior executive job candidates.
- Released the requirements all Components will have to align to for all five tiers of the DHS Leader Development Framework, and are working towards fully implementing all of the tiers.
- Created the capacity to target communications specifically to various tiers of leadership, and created new communications tools – Leader Alerts (for executives, supervisors, and managers, as appropriate) and Connected (a monthly all-employee e-newsletter)

- Continued the commitment to hold an annual Secretary's Awards Ceremony after a multi-year hiatus, with the sixth ceremony having occurred in November.
- All DHS Components have created or are in the process of creating peer-to-peer recognition programs
- DHS Components have submitted new Employee Engagement Action Plans to the Under Secretary for Management; signed, for the first time, by Component heads.
- DHS completed a Joint Duty Winter Study to evaluate a comprehensive Joint Duty Program to enhance operations and mission execution, support unity of effort, and enhance leadership and professional development. As a result of the Winter Study, the Deputy's Management Action Group directed a survey of Joint Duty positions across DHS, and development of a general policy and an implementation plan for a DHS-wide Joint Duty Program.

#### 1-2 Year Priorities:

- Implement the first phase of the Joint Duty Program (Summer 2016 – 2017) to include development of operation policies and procedures, establishment of Joint Duty Assignment roles and processes, and the initiation of staffing.
- Continue to analyze 2015 FEVS results to identify component-specific trends including key driver analysis, and develop robust action plans to achieve change across the Department. Foster employee engagement by completing a train-the-trainer program for DHS in partnership with OPM based on positive feedback from the FY 2015 New Inclusion Quotient (New IQ) pilot sessions on diversity, inclusion, and employee engagement.
- Continue to develop and launch employee tools to build awareness of promotion, joint duty, and rotational opportunities within and across the DHS components.
- Continue to support the DHS Labor Management Forum and its efforts to foster labor-management cooperation and component action planning.

#### **Goal 4: Achieve human resources operational excellence.**

##### Accomplishments:

- Piloted the use of HR Service Level Agreements (SLAs) and quarterly results reporting for Headquarters HR customers. Based on positive feedback, a plan was developed for implementing SLA's throughout the Department.
- Launched a cross-component initiative to develop and implement a departmental framework for training HR professionals. The framework will help DHS maintain the high performing HR workforce needed to support the DHS mission areas.
- Deployed the AXIS human capital reporting tool to all components and developed a 5 year plan for enriching the data used to build models and develop visualizations to help human capital leaders make better informed business decisions.

##### 1-2 Year Priorities:

- Continue to improve HR services and customer satisfaction levels throughout the Department through the implementation and monitoring of HR Service Level Agreements.
- Refine and expand the use of the Department's automated position description tool, which assists managers and human capital support in effectively describing positions performing mission critical work.

- Continue component deployments of the Department’s Performance and Learning Management System according to the approved implementation plan.
- Continue to enrich the human capital data in the AXIS analytics and reporting system to help human capital leaders make better-informed business decisions.

Tightening budgets and the growing competition for cybersecurity and other critical skills suggest that hiring, training, and employee morale (as measured by the Federal Employee Viewpoint Survey) will remain near-term challenges for the DHS human capital line of business. In view of this the Under Secretary for Management has identified three strategic priorities to address these challenges and to advance DHS an employer of choice:

- Improve employee morale;
- Refine department-wide human capital plans, policies and programs to support the cybersecurity workforce; and
- Improve the efficiency and effectiveness of the hiring process.

## **Acquisition Management/Strategic Sourcing**

The Department of Homeland Security (DHS), Strategic Sourcing Program Office (SSPO) resides within the Office of the Chief Procurement Officer. The SSPO enhances mission efficiency and reduces the cost of delivering the mission by critically analyzing data on what we buy and how we buy it across the Department to identify ways to leverage spend, reduce redundancy, increase standardization, and streamline the acquisition of products and services. Through the development of department-wide contracts, strategic sourcing consolidates resources (both dollars and people) to save millions in taxpayer dollars.

The DHS Strategic Sourcing Program, viewed as a ‘best in class’ efficiency model across the Federal Government, has been endorsed by the Office of Management and Budget, Government Accountability Office, and several members of Congress. Since the program’s inception in 2005, DHS has saved more than \$3 billion, of which nearly \$2 billion was saved in the last five years, and more than \$450 million in FY 2015 alone. These savings accomplishments are a direct result of effective collaboration amongst stakeholders across the Department.

Strategic Sourcing supports the DHS Secretary’s “Unity of Effort” initiative by convening working groups comprised of DHS subject matter experts, acquisition professionals, legal staff, and other stakeholders that are focused on developing acquisition streamlining tools and shared acquisition vehicles that effectively leverage the Department’s buying power, reduce administrative costs through the elimination of redundant contracts and processes, and foster continuous cooperation on future challenges and events.

Extensive collaboration across the Department has been vital to DHS’s strategic sourcing success. For example, the Office of the Chief Information Officer community has worked with the Strategic Sourcing Program Office on nearly 30 initiatives, and consistently work together to identify new opportunities. These efforts have helped to identify ways to enhance enterprise-level capabilities and reduce the total lifecycle cost of commodities by focusing not only on a reduction in purchase

price, but also by including beneficial terms and conditions in the contract vehicles that further lower the costs of maintaining and using the commodity.

Other organizations that the Strategic Sourcing Program Office has successfully collaborated with include the Office of the Chief Readiness Support Officer to establish the Bulk Fuel, Furniture, Employee Shuttle Service, and the Government-wide Domestic Delivery and Print Management initiatives; the Office of the Chief Human Capital Officer to develop and implement the Enterprise Talent Management System and Medical Case Management contract vehicles; and the Office of the Chief Financial Officer to deliver a suite of contract vehicles that are dedicated specifically to the DHS financial community, including Financial Management and Reporting Support Services, Assessment of Internal Controls Support Services, and Compliance, Performance, and Statistical Sampling of Internal Controls Support Services.

In addition to internal programs, the DHS Strategic Sourcing Program Office provides innovations to the entire federal acquisition community. For example, in fiscal year 2015, DHS has worked with several other agencies, including the Federal Bureau of Investigation, Department of Commerce, Department of State, and Department of Treasury, to share its strategic sourcing best practices and lessons learned to support continued adoption of strategic sourcing across government. While DHS recognizes the importance of collaboration across the federal community, DHS does not believe that all commodities and services are suited for government-wide implementation as one, consolidated solution. A key challenge for DHS is finding the right balance between supporting and adopting federal-wide initiatives and maintaining a portfolio of contract vehicles which provide the agility necessary to support its robust mission. The fulfillment of DHS mission needs takes priority over utilization and adoption of federal-wide contracts. DHS has evolved its strategic sourcing program to increase its focus on vehicles which enhance the Department's mission capability, such as ammunition, cyber security skills, detection equipment, and tactical communications equipment.

With a portfolio of over 70 active strategic sourcing vehicles covering nearly 500 individual contracts, the program faces other challenges that may eventually impede growth and continued success. For example, the program operates with a fixed number of resources yet the demand for new vehicles, information, and collaboration on strategic sourcing continues to grow. Additionally, the program is finding it increasingly difficult to find dedicated subject matter experts and volunteers to support the development, evaluation, and implementation of new strategic sourcing initiatives. Recognizing these challenges are primarily due to decreasing budgets and increased mission requirements, the program continues to identify best practices and innovative approaches from both government and industry to achieve DHS mission objectives.

## **Information Technology**

The Department continues to enhance its Information Technology (IT) and management practices through the implementation of administration priorities. Below are a few areas where progress has been made in FY 2015.

## **DHS IT Strategic Plan**

Information technology plays a critical role in the ability of DHS to deliver effective, efficient services and solutions that ultimately provide for the security of the American people. The 2015-2018 DHS IT Strategic Plan was developed as a guide for the IT communities as we work together to improve the Department's operational efficiency, provide mission-enabling services, and support management initiatives across the Department.

## **FITARA Implementation**

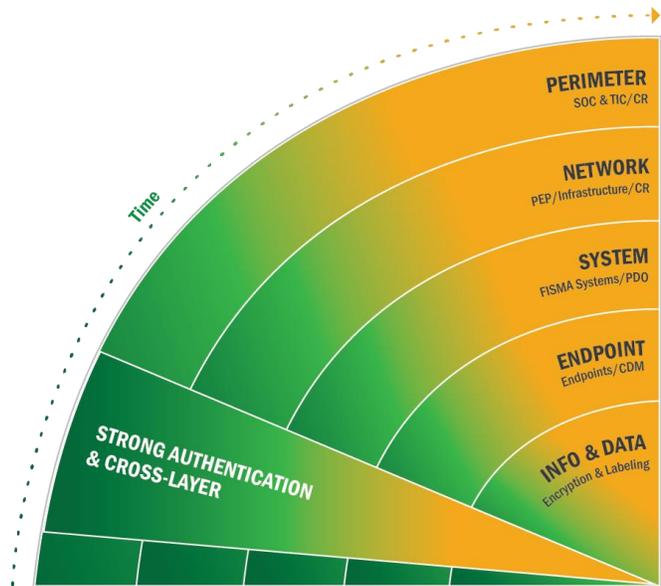
In 2015, final guidance was released by OMB for implementation of the Federal IT Acquisitions Reform Act (FITARA). FITARA aims to ensure agency Chief Information Officers (CIOs) have significant involvement in procurement, workforce, and technology-related budget matters in order to help agencies to use modern digital approaches to achieve the objectives of effective and efficient programs and operations. The DHS Office of the Chief Information Officer (OCIO) has led the implementation of FITARA across the DHS lines of business, targeting core business processes aligned to the areas of budget formulation and execution, acquisition, and organization and workforce. DHS established the FITARA Component Integrated Planning Team to assist in the development of the agency action plans in order to document the business processes that align with FITARA and identify opportunities to better incorporate the CIO in the management and oversight of IT resources. In FY 2016, the Department will continue the work to update policies based on FITARA requirements, and identify and document the policies and processes throughout the acquisition lifecycle where we will incorporate the CIO and IT assessments.

## **IT Security**

The growing number of cyber-attacks on Federal Government networks is becoming more sophisticated, aggressive, and dynamic. In FY 2015, breaches around the Federal Government led to an OMB-directed 30-day cyber sprint designed to quickly improve the cybersecurity posture of federal systems by implementing key actions to mitigate risks, including: network scanning, critical vulnerabilities patching, tightened policies for privileged user access, identification of high value assets (data, systems, infrastructure, applications, equipment), and accelerated implementation of multi-factor authentication for access to the networks and systems. DHS led the efforts for the OMB cyber sprint, achieving 99 percent PIV card usage for privileged users and 95 percent for unprivileged users—exceeding OMB's goal for unprivileged users by 20 percent and enhancing network security across the Department. As the model agency for IT security, the Under Secretary for Management also directed DHS Components to work with Component CIOs to adopt within 30 days, six additional cybersecurity measures designed to strengthen our infrastructure.

To successfully protect the Homeland, the DHS workforce must be able to access information services anytime, from anywhere. The Department is transforming its IT infrastructure to meet the demands of employees to ensure access to services 24/7 from any approved access point. At the same time, the Department also needs to protect the Homeland from one of the most challenging threats—the advanced, persistent threat initiated by highly-skilled and organized cyber adversaries. To significantly improve our cyber defense, DHS is moving to a threat-based defense strategy. Threat-based defense uses the knowledge gained from single, often disparate, attacks and related events to reduce the likelihood of successful future attacks. DHS foundational cybersecurity activities for improving the Department's internal cyber security posture include the development

and rollout of a Cyber Capabilities Maturity Model and roadmap. The maturity model outlines a defense-in-depth approach encompassing five distinct layers and one cross cutting layer for identity management, enabling authorization and authentication to each layer. This model will be used to implement baseline operational measures, identify the most critical capability gaps, and use the results to identify strategic sourcing opportunities, coordinate research and development, prioritize resource allocation requests and inform resource allocation decisions, and ultimately strengthen and improve the DHS cybersecurity posture. In consultation NPPD, the CIO, Deputy CIO, and Component CIOs have identified the major threats to cyberspace and are reviewing current cybersecurity capabilities and gaps across the department. The Office of the Chief Financial Officer is collaborating with them to develop a funding plan to mitigate threats and reduce risk.



**Defense In Depth**

DHS, through NPPD, also helps federal agencies identify and fix problems inside their networks in near real-time using the Continuous Diagnostics and Mitigation program (CDM). CDM offers federal agencies commercial off-the-shelf (COTS) tools, with robust terms for technical modernization as threats change. 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 of implementation. Phase 1 focuses on implementing the tools and sensors required for hardware and software asset management, configuration settings management, and vulnerability management, which will protect systems and data. Phase 2 capabilities will cover user account and network privilege management; and Phase 3 covers boundary protection and event management. The current CDM task order for DHS for Phase 1 provides the foundation for cybersecurity FISMA reporting, integrating the security tools into a “One DHS” tool set. Implementation of the CDM tools will begin in FY 2016 and continue through FY 2017.

**Winter Study**

In FY 2015, the DMAG selected an IT Infrastructure Assessment as an area for a Winter Study for FY 2018-2022. Per the FY 2018-2022 RPG, the IT Infrastructure Assessment Winter Study will assess aging infrastructure technology to identify and resolve gaps, identify redundancies, and coordinate operational readiness and optimal performance of mission essential systems across the Department’s Components. This study will develop a repeatable management and planning approach to: 1) enable prioritized phasing of the refresh of information technology; 2) implement common performance standards for mission essential systems; 3) support interoperability and architectural compatibility; 4) improve planning to upgrade legacy infrastructure to allow for the

adoption of new and emerging technologies; and 5) further leverage strategic sourcing practices by continuously improving and re-evaluating the purchasing of information technology assets.

### **Mobility**

This past year, DHS also created the Mobility Initiative Working Group, known as the MI-5. The MI-5 is a cross-organization group of both strategic and operational partners working to create a common deployable mobility solution across the Department that will enable the agile, secure, and cost-effective delivery of mobile computing capabilities to support the DHS mission. The goal of the MI-5 is to be an enabling force to the DHS mission as “mobility” changes the way we interact with and support the needs of the American citizens. As IT capabilities continue to evolve in this space, the MI-5 provides the collaborative foundation for business and IT to quickly respond to support the mission. To address the rapidly evolving environment and the manner in which the business adapts, the MI-5 employs an agile, 90-day approach to address the most critical issues in mobility and gain incremental progress towards solutions. The DHS MI-5 received the 2015 FedScoop 50 “Tech Program of the Year” award, which recognizes the extraordinary achievements of leaders in the federal IT community.

Over the course of FY 2016, the MI-5 will be establishing a collaboration site on Homeland Security Information Network (HSIN) complete with a resource plan to fully implement and maintain and a mobile application development playbook to be a resource for mission and IT personnel. MI-5 will also provide several position papers and recommendations to the CIO community on the best path forward for integration of mobile IT capabilities with our desired business models.

### **IT Information Sharing**

The Homeland Security Information Network (HSIN) is the trusted network for homeland security mission operations to share Sensitive But Unclassified information. Federal, state, local, territorial, tribal, international, and private sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and in general, share the information they need to do their jobs. HSIN increased its membership by 81 percent in FY 2014. Starting in FY 2014, HSIN now has federated access with the Department of Justice Regional Information Sharing System and the Law Enforcement Enterprise Portal, as well as simplified sign-on capabilities for fusion centers and other mission critical DHS systems like Tripwire and the IP Gateway. These connections expand the ability to collaborate with more than 8,900 law enforcement and criminal justice agencies, including more than 117,000 law enforcement officers across the nation. OCIO also developed the National Information Exchange Model (NIEM) Emergency Management Domain, which supports emergency-related services and information sharing to increase disaster preparedness. DHS launched NIEM 3.1 which includes human services as a key component for demographic information exchange.

### **Industry Engagement**

In order to improve the industry capture, bid, and proposal processes for IT across the Department, the DHS Office of the Chief Procurement Officer and the OCIO collaborated to develop the Joint Industry Engagement Plan (JIEP), a logical extension of AiIM, to provide a framework for and a means of communicating the Department’s overarching approach to industry engagement and

acquisition initiatives for IT. The JIEP includes multiple industry engagement activities throughout 2015 and 2016 and will support AIiM and other high-level initiatives.

### **IT Digital Services**

In September 2015, DHS became the third agency to formally establish an in-house Digital Service Team, reporting to the DHS CIO. The DHS Digital Service works on high visibility IT projects across DHS to address risks and challenges, and to provide IT subject matter expertise and experience in leading large technology initiatives, change management, web development, user-centered design, and technology policy. The DHS Digital Service is currently supporting the USCIS Transformation, myUSCIS, and CBP International Trade Data System programs. Digital Service involvement has driven significant engineering and product design enhancements and supported three major releases, including electronic filing and processing of USCIS Form I-90 (renewal / replacement of a green card) and Immigrant Visa Fee payment along with myUSCIS Explore My Options, Help Center, and Practice Civics Test features. The DHS Digital Service will gain additional team members and new projects in FY 2016 and beyond.

In addition, the DHS Chief Technology Officer (CTO) is working closely with the DHS Program Accountability and Risk Management (PARM) Office to transform the overall IT acquisition and oversight process, in order to align and support the USDS Playbook. Initially, this effort is being executed as a series of pilot initiatives with Component programs (such as FEMA NFIP), but ultimately will result in a more agile and effective IT acquisition process for the entire department.

### **IT Services**

The way to deliver IT is changing. It is critical that DHS adapt to the ever changing environment and reimagine operating processes and organizational models to take advantage of technology advancements and commercial market drivers. The move to a more mobile workforce has our customers re-envisioning the possibilities and the way they conduct business. “Cloud” and “Mobile” both bring an expectation of a rapid delivery cycle which has the IT community working feverishly to transition traditional management processes to a new delivery model. DevOps, as a conceptual construct, and Agile, as a methodology, present a way to bring the IT development and IT operations communities closer and achieve an accelerated and iterative delivery of IT services. The DevOps construct and the agile methodology are important for government to adopt and necessary to meet the current and expected business demands. In FY 2015, DHS restructured its Data Center contracts to make the move to cloud technologies easier for our customers, while also improving service levels and pricing options. The DHS Enterprise Computing Services initiative will leverage public cloud services that offer the same or a greater level of protection necessary for the DHS mission and information systems. The next generation Enterprise Computing Services (ECS) initiative is in development and will establish an Enterprise Compute Services Framework to manage the use, performance, and synchronized delivery of cloud service offerings within the Department, from both Federal and commercial providers. The ECS Framework will make it easier, safer, cost effective, and more productive for DHS Components and consumers to discover, access, and integrate cloud services to support their mission.

## Sustainability

DHS continues to ensure that its operations are carried out in a manner that is both environmentally and fiscally sound and fulfills our legal requirements. The DHS Strategic Sustainability Performance Plan (SSPP) is the backbone for successful integration of sustainable practices into the daily business processes and decision-making that supports the DHS mission. The SSPP reflects the Department's strategic vision for doing business in a more efficient and sustainable way, and incorporates environmental compliance. Sustainable practices conserve energy and natural resources, reduce pollution and contamination releases, enhance the workplace through reduced exposure to hazardous materials and chemicals, and strengthen national security by encouraging energy independence.

DHS continues to move forward with implementing performance contracts (public-private ventures) in an effort to meet its federal \$73.2M commitment by December 2016. Currently, DHS is conducting program management reviews with Components which include updated plans of action and milestones for performance contracts. The newly appointed Deputy Under Secretary for Management/Chief Sustainability Officer has indicated he will conduct quarterly sustainability meetings at which performance contract status updates will be discussed.

During the past year, GSA offered opportunities to convert conventionally-fueled vehicles to hybrid electric sedans at no additional cost. USCG, USCIS, TSA, and FLETC have taken advantage of this program resulting in the acquisition of over 1,900 alternative fuel and hybrid vehicles. DHS will continue to take advantage of these type opportunities as they arise, without impacting the ability to meet the Department mission. DHS also implemented a Fuel Sharing Pilot Program along the Southwest Border where fuel owned by CBP will be available to other DHS Components in an effort to increase operational efficiencies.

DHS updated the Motor Vehicle Acquisition Guide. This "Acquisition Guide" was developed to provide acquisition procedures for the DHS Motor Vehicle Fleet Program, which requires Components to justify acquisitions prior to additional or replacement vehicles being ordered and to ensure compliance with sustainability mandates. The Acquisition Guide also includes a checklist for new and replacement vehicles that must be approved by the DHS Fleet Manager before vehicles are acquired.

In FY 2015<sup>7</sup>, DHS achieved the following:

- Reduced scope 1&2 greenhouse gas emissions by 21 percent and scope 3 emissions by 31 percent;
- Reduced 2408 vehicles from the owned fleet inventory;
- Achieved a 23.5 percent energy intensity reduction goal against a 2003 baseline;
- Realized a 6.9 percent electricity usage from renewable energy sources;
- Used conservation initiatives at facilities across DHS to reduce the potable water intensity by 22 percent; and

---

<sup>7</sup> FY 2015 measure reports reflect FY 2014 actual results.

- Executed \$53 million in performance-based contracting to further reduce energy usage and cost.

In FY 2015, the DHS Sustainable Practices Awards program had eleven winners. Among these, the United States Secret Service (USSS) entered into an initiative with the Maryland Department of Natural Resources to transform lawns to woodlands at its James J. Rowley Training Center in Laurel, Maryland. Under this initiative, 6,780 trees were planted at no cost to the USSS. These trees will reduce pollution by intercepting 112 million gallons of storm water and conserve about 2.2 million kilowatt/hours of cooling electricity needs per year. Trees are an excellent way to reduce greenhouse gas emissions and the USSS trees are estimated to reduce atmospheric carbon by 7.9 million pounds per year which is equivalent to the emissions from about 720 automobiles.



U.S. Secret Service Award winners Tom Franklin (left) and David Brown stand by newly planted trees.

Continued success in integrating sustainability across the Department requires investment in suitable projects, raising awareness and promoting success. Executive Order (EO) 13693, *Planning for Federal Sustainability in the Next Decade* and the SSPP form the basis for DHS actions for the next two years. In accordance with the EO, DHS plans to establish accelerated greenhouse gas reductions that support the federal government goal of achieving a 40 percent reduction in greenhouse gas emissions by 2025.

Attaining this goal will require investments in

energy conservation projects, building on-site renewable energy installations such as solar power and constructing sustainable buildings. DHS plans to continue development of the Office of the Chief Readiness Support Officer Consolidated Asset Portfolio and Sustainability Information System (CAPSIS) which improves sustainability reporting data quality and enables more timely and easily defended management decisions. The Sustainability Performance Management piece of CAPSIS links key data with real property, fleet and personal property information which can be used to identify opportunities for improvements in sustainability. Recent reductions in budgets for these initiatives means delays in full utilization and efficiency of these systems.

DHS is developing systems to assist in measuring and reporting our progress, and will initiate course corrections to achieve our goals. In support of these goals, the Department will comply with all environmental and energy laws, regulations, and Executive Orders. DHS remains committed to pursuing and achieving the strategies and goals established in its Sustainability Plan.

## Financial Stewardship

As a responsible steward of federal funds, the Department has been diligently working to strengthen financial management to produce timely and reliable financial information. In addition to sustaining the clean financial statements audit opinion, the Department is able to provide reasonable assurance that internal controls over financial reporting were operating effectively as of September 30, 2015, with the exception of the material weakness identified in the Secretary's Assurance Statement. These achievements demonstrate the Department's dedication to proper

stewardship of taxpayer dollars and are the result of strong commitment from DHS leadership and the expertise and hard work of our financial management community.

In FY 2015, DHS continued to make substantive progress across its Components in its Financial Systems Modernization (FSM) initiative. The Federal Law Enforcement Training Center (FLETC) completed a technical refresh of their Accounting and Budgeting System (FABS) in the first quarter. The U.S. Coast Guard (USCG), Transportation Security Administration (TSA), and Domestic Nuclear Detection Office (DNDO) completed a global configuration phase with the Department of the Interior's Interior Business Center (DOI IBC), a federal shared service provider, in the second quarter. This phase determined the common baseline for the three Components on the DOI IBC financial management shared service.

Following the global configuration phase, DNDO entered into the implementation phase, which continued throughout FY 2015, with go-live scheduled in FY 2016. TSA and USCG implementations are scheduled in subsequent years.

Additionally, U.S. Citizenship & Immigration Services (USCIS), the Science & Technology (S&T) Directorate, the National Protection & Programs Directorate (NPPD), and the Management Directorate (MGMT) have obtained approval from the FSM Executive Steering Committee on their business cases for financial systems modernization. These four Components are working with DHS procurement to execute inter-agency agreements for a discovery phase with a federal shared service provider for financial management system services. The discovery phase began in the fourth quarter in FY 2015.

Finally, in the third quarter of FY 2015, the Federal Emergency Management Agency (FEMA) received Treasury's Office of Financial Innovation and Transformation (FIT) recommendation to OMB to proceed with modernization. FEMA continues to follow the Treasury FIT's Agency Modernization Evaluation process and is conducting pre-discovery activities and preparing required documentation.

As we move into FY 2016, DHS will continue to implement a risk-based approach to audit remediation and work closely with Components to mitigate risks of new material weaknesses or audit qualifications, while sustaining prior-year successes. The Department will monitor critical corrective action milestones to ensure they are completed on schedule and assist Components with implementation efforts to remediate and downgrade the severity of internal control deficiencies, as it has done in prior years.

Specific FSM goals for FY 2016 include the DNDO go-live on the DOI IBC system and continuing to make significant progress on the TSA and USCG migration to DOI IBC. After USCIS, S&T, NPPD, and MGMT complete their discovery phase, they will seek approval from the DHS Acquisition Review Board to move forward into an implementation phase.

## 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 both 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. OIG’s Fiscal Year (FY) 2015 Major Management and Performance Challenges report identified challenges in nine broad areas.

- DHS Management and Operations Integration
- Financial Management
- Transportation Security
- Disaster Preparedness and Response
- Infrastructure Protection and Cybersecurity
- Acquisition Management
- IT Management and Technology
- Border Security and Immigration Enforcement
- Employee Accountability and Integrity

More specific information about these challenges, the Department’s progress addressing them and next steps can be found in the OIG’s report “Major Management and Performance Challenges Facing the Department of Homeland Security” located at:

<https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-07-Nov15.pdf>.

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. GAO maintains these high-risk items on the list until it is satisfied that acceptable progress has occurred to address them. The most recent report, “High Risk Series: An Update” ([GAO-15-290](#)), was published in February 2015. The two areas in which DHS is the lead federal agency, as well as eight 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
	Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland	2005
	Ensuring the Effective Protection of Technologies Critical to U.S. National Security Interests	2007
	Improving Federal Oversight of Food Safety	2007

Scope	Issue Area	Year Issue First Added to GAO's High Risk List
	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. Although the Department continually strives to improve the efficiency and effectiveness of its programs and operations, the areas identified above merit a higher level of focus and attention. Overcoming challenges in these areas requires long-term strategies for ensuring stable operations, sustained management attention, and resources.

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

<b>GAO High-Risk Area:</b> Strengthening DHS Management Functions (DHS-specific)
<p><b>Overview:</b> 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 acquisition, information technology (IT), financial and human capital management.</p>
<p>In response to this high-risk designation, DHS semi-annually publishes the <i>Integrated Strategy for High Risk Management</i>, which GAO has stated “provides a path for DHS to be removed from GAO’s high-risk list,” if implemented and sustained. In 2013, GAO acknowledged DHS’s significant maturation and narrowed this high risk area from “Implementing and Transforming DHS” to “Strengthening DHS Management Functions.” This refocusing by GAO is a reflection of “the considerable progress in transforming [DHS’s] original component agencies into a single cabinet-level department.”</p>
<p><b>Lead Office and Official:</b> Office of the USM, Michelle Benecke, executive director for Management Integration</p>
<p><b>Progress:</b> In June 2015, DHS published its ninth <i>Integrated Strategy for High Risk Management</i>, 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.</p>
<p>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. Making major strides in the past two years, the Department has:</p>

- Fully met three of the five (60 percent) criteria for list removal (leadership commitment, a framework to monitor progress and corrective action plans) and partially met the two remaining criteria (capacity [i.e., resources] and demonstrated, sustained progress).
- Developed a solid strategy and framework to strengthen DHS management functions and reduced the level of risk from “high” to “moderate” or “low.” Overall, DHS reports that it has fully or mostly addressed over 63 percent of the GAO outcomes.
- Achieved a third unmodified (i.e., clean) audit opinion on all five financial statements in November 2015 – a confirmation of the Department’s ongoing commitment to sound financial management practices. DHS received its first unmodified audit opinion in December 2013 and its second in November 2014. These successes led to GAO rating the associated outcomes as fully addressed.
- Operationalized the Joint Requirements Council (JRC), which enables cross-Component requirements and develops recommendations for investment. The JRC is actively assessing joint requirements for several investment portfolios, including information-based screening and vetting, aviation commonality, information sharing, chemical-biological-radiological-nuclear, and cybersecurity.
- Ensured all Components with major acquisition programs have Component Acquisition Executives (CAEs) or acting CAEs in place. Further, the Chief Acquisition Officer has established more rigorous oversight of major acquisition programs through the CAE structure.
- Successfully completed two cycles of strategic human capital planning and implementation with program actions, which demonstrates sustainability and contributed to GAO’s fully addressed assessment for the associated outcome.

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 Secretary’s *Unity of Effort* initiative. *Unity of Effort* is a framework that is 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 make significant progress in implementing the *Integrated Strategy for High Risk Management* and strengthening Departmental *Unity of Effort*. During the next fiscal year, DHS expects to accomplish the following:

- Support the Component-driven JRC, as well as changes to training, organization, laws, and operations process and procedures.
- Obtain the fourth consecutive clean audit opinion by executing an aggressive risk-based approach to audit remediation, working closely with Components to sustain prior-year successes, and mitigate the risk of new material weaknesses or audit qualifications.
- Continue integrating the DHS acquisition oversight framework, focusing on all acquisitions, including IT programs by creating common standards, integrated processes,

and greater visibility of performance across all acquisition programs. Further, it will reduce the burden on program managers, while improving accountability and transparency.

- Continue to integrate functions and mature capability to understand critical management information through the Business Intelligence initiative, led by the Management Dashboard Executive Steering Committee.
- Maintain current leadership commitment, fully address the outstanding GAO outcomes, monitor the effectiveness of resource mitigation strategies, and fully implement and sustain the *Integrated Strategy for High Risk Management*.

**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 from the 2005 hurricanes or future catastrophic losses within ten years, possibly more. The lack of sufficient revenues highlights structural weaknesses in how the program is funded. Also, weaknesses in NFIP management and operations, including financial reporting processes and internal controls, and oversight of contractors place the program at risk. FEMA has begun to address these issues, including implementing legislation, improving contractor oversight, and taking the first steps toward financial systems modernization with the NFIP Phoenix 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. As NFIP had already begun implementing the required premium rate increases, this required issuing refunds to many 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 continues to address the structural and operational challenges confronting NFIP and continues to make progress in GAO-identified areas of concern. For example:

- NFIP successfully prioritized and implemented 30 of 60 sections of BW-12 and HFIAA requiring action within a year of passage. More specifically, FEMA (1) effectively issued

the vast majority of refunds from October 2014 to January 2015; (2) adjusted premium rate increases; (3) applied new surcharges; (4) released new rates and mapping standards; and (5) established its Office of the Flood Insurance Advocate in June 2015 to connect policyholders with information needed to better understand the program

- 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 “Need” Phase (ADE-1), completed in the first quarter of FY 2016. This ADM gave the PMO permission to proceed to the “Analyze/Select” phase and garner approval for existing requirements documentation as well as finalizing an Analysis of Alternatives (AoA) to help identify the appropriate solution for NFIP’s needs.
- FEMA enhanced its contractor oversight activities by:
  - ✓ Establishing Best Practices for Contracting Officer’s Representatives (CORs). These Best Practices align performance of COR duties with the achievement of NFIP’s goals and objectives. They also provide transparency in the oversight and administration of NFIP contracts. They also ensure effective and efficient administration of NFIP contracts and adherence to Federal Acquisition Regulation.
  - ✓ Establishing a quality assurance and surveillance plan to monitor and evaluate contracts is based on the premise that NFIP will maintain high-quality standards for all contractor services and deliverables.

**Planned Actions and Key Milestones:** FEMA will continue to implement provisions of BW-12 and HFIAA. NFIP will expedite flood insurance reform and implement program changes through policy and by leveraging existing processes to release program updates every six months. Specifically, FEMA will:

- Begin planning the transition of NFIP matters (including NFIP Rate Guidance, mapping standards, program integration, reports and studies, and major acquisition lifecycle milestones) from the NFIP Transformation Task Force to FIMA in December 2015.
- Publish the NFIP Rate Guidance Issue in WYO bulletins to NFIP insurers in April and October 2016, allowing the mandated six months required for consultation and notice of changes impacting systems.
- Release mapping standards by publishing them on [FEMA.gov](http://FEMA.gov) in May and November 2016, allowing the mandated time required for public comment.
- Integrate the following requirements into its ongoing program and reporting processes:
  - ✓ Set 25 percent annual premium rate increases for businesses, mandated under BW-12, to take 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.
  - ✓ Apply 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.
  - ✓ NFIP insurers, working with WYO companies, will collect current flood zone determinations to populate FEMA’s HFIAA-mandated clear communication of risk to property owners.

As NFIP integrates critical rate requirements into the program, it will refocus to longer-term initiatives, including program updates and rulemaking initiatives. This fall, new reports and studies will provide information critical to shaping NFIP’s next steps in meeting the following requirements:

- The Technical Mapping Advisory Council, authorized under BW-12, will deliver its BW-12 future conditions and annual reports in October 2015 and begin a HFIAA-required technical review to inform the administrator’s certification of a national mapping program which produces technically credible data.
- The National Academies of Science delivered the second phase of the affordability study required under BW-12 and HFIAA for the administrator’s consideration in November 2015. This study informs delivery of the required affordability framework for the program by proposing an analytical approach FEMA might use to evaluate affordability policy options such as those described in phase one.
- FEMA will issue a brochure on alternative flood mitigation methods for buildings to help communities and policyholders mitigate flood risk and rates.

Major acquisition lifecycle framework milestones for FEMA’s insurance system modernization activities include:

- ADE-2A: FEMA currently anticipates completing ADE-2A by the end of calendar year 2016. This milestone involves the approval of requirements, concept of operations, and AoA artifacts before proceeding to a potential acquisition.
- NFIP Phoenix Program appeared at an Acquisition Review Board (ARB) in September 2015. This milestone involves the incorporation of NFIP Reform initiatives including claims data processing, and internal and external Customer Experience information and data considerations.

**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)/Enterprise Performance Management Office, Matthew Shabat, director, Performance Management

**Progress:** DHS continues to advance its ability to develop and share situational awareness of cyberthreats and vulnerabilities while taking actions to protect federal agencies from malicious activity.

DHS improved its cyber-analytical and technical capabilities. For example:

- DHS’s National Cybersecurity Assessment and Technical Services team increased its cyber-hygiene scanning activities. This has resulted in an increasing number of detected vulnerabilities in federal agencies’ Internet-facing systems each FY (see table below).

<u>FY</u>	<u>Vulnerabilities Detected</u>
2013	11,350
2014	59,937
Through Q3 of FY 2015	65,752

- Under the *Federal Information Security Modernization Act of 2014*, the Secretary can now issue binding operational directives, which are directions to agencies to mitigate risks to their information systems. DHS released its first binding operational directive in May 2015, which requires agencies to quickly patch their most critical cyber vulnerabilities.
- DHS has enhanced the Continuous Diagnostics and Mitigation (CDM) program which, in turn, will improve DHS’s influence on protecting federal agencies from malicious activity. This program provides federal civilian agencies with tools to monitor agencies’ internal networks divided into three phases. Phase 1 identifies vulnerabilities on computers and software on agency networks. Phase 2 will monitor users on agencies’ networks and detect if they are engaging in unauthorized activity. Phase 3 will assess activity happening within agencies’ networks to identify anomalies and alert security personnel.

DHS also strengthened the effectiveness of its partnerships with the private sector and other federal agencies in securing cybercritical infrastructure. For example:

- DHS has made efforts to provide CDM to other federal agencies. As of June 2015, DHS had provided CDM Phase 1 capabilities to 8 agencies, covering over 50 percent of the civilian Federal Government. Although each agency must still take action to implement these systems, DHS expects increased CDM coverage across the civilian Federal Government.
- 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. EINSTEIN 3A protects approximately 45 percent of the civilian Federal Government with at least one of its two security “countermeasures.”
- DHS’s National Cybersecurity and Communications Integration Center (NCCIC) has enhanced support to state, local, tribal, and territorial governments and to the private sector by providing incident management and response support, including network and malware analysis. As of the third quarter of FY 2015, NCCIC provided onsite incident response to 32 incidents – nearly double the total for FY 2014. NCCIC also coordinates responses to

significant incidents to (1) give senior leaders a clear understanding of the situation; (2) give operators the information they need to respond effectively; and, (3) enable NCCIC to identify indicators of compromise that can then be shared with other agencies and applied to EINSTEIN.

- NCCIC has improved public-private sector partnerships by improving information sharing so they can block threats before penetrating networks. As of the third quarter of FY 2015, NCCIC disseminated over 6,000 alerts, warnings, and bulletins. DHS now has a system to automate the sharing of cyberthreat indicators, and DHS is building this capability so that participants can share this information in near-real-time. One agency is already receiving cyber threat information via this automated system.

DHS improved privacy compliance and protected PII and other sensitive information. For example:

- DHS's Privacy Office (PRIV) serves a unique role as both an advisor and oversight body for the Department. DHS employs a layered approach to privacy oversight for the Department's cybersecurity activities which includes extensive collaboration with the NPPD Office of Privacy.
- 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. For example, 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 analytically relevant to predefined known or suspected cyberthreats.
- DHS conducts a separate privacy compliance review (PCR) process to assess performance of the privacy requirements established through PIAs and other compliance documentation. In January 2012, PRIV conducted a PCR on the EINSTEIN program which is publicly available at [DHS.gov](http://DHS.gov). In response to the recommendations from that review, NPPD's Office of Privacy developed and implemented quarterly privacy reviews (QPR) of PII handling to ensure that NCCIC, through its U.S. Computer Emergency Readiness Team (US-CERT) program, is following their standard operating procedures for PII handling. NPPD conducted the first QPR in October 2012, with subsequent reviews quarterly. The scope of the QPR has increased to include all CS&C indicator and signature activities. In 2014, PRIV conducted an update to the EINSTEIN PCR, and conducted a separate PCR for the ECS program.
- In response to a recommendation from the initial EINSTEIN QPR, NPPD's Office of Privacy, in coordination with the DHS Office of General Counsel and Office of Civil Rights and Civil Liberties; and NCCIC, developed role-based training addressing PII handling as articulated in the US-CERT Information Handling Guidelines. This training commenced in May 2014 and due to the high demand across CS&C, it has been provided monthly both in-person and via webinar sessions to both federal and contractor analysts.

GAO referenced specific reports and recommendations tied to DHS in its February 2015 high risk list. There were six recommendations directed at NPPD. Of those six recommendations, two have been closed-implemented and four have estimated completion dates during the fourth quarter of FY 2015.

**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, continue procuring CDM capabilities, and enable automated indicator sharing.

During the next year, 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 CDM for 97 percent of the civilian Federal Government by the end of FY 2015.
- Work aggressively to build an automated sharing of cyberthreat indicators across government and to the private sector so that participants can share this information in near real-time. DHS expects that multiple agencies and private sector partners will begin sharing and receiving information through this system by the end of the first quarter of FY 2016.

**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*. These laws grant the Secretary additional flexibility with regard to hiring and compensating cybersecurity positions, while also instructing the Department to increase its cybersecurity workforce analysis and planning efforts. More specifically, DHS is now required to develop a comprehensive cybersecurity workforce strategy covering the readiness, capacity, training, recruitment, and retention of the Department’s cybersecurity workforce. In addition, DHS must conduct that workforce analysis which:

- Identifies and categorizes all open and filled cybersecurity positions, and determining critical gaps in coordination with the Office of Personnel Management (OPM); and,
- Addresses a variety of factors including: the readiness and capacity of the workforce to meet the DHS cybersecurity mission, the location of positions and vacancies, and the training provided to employees.

**Lead Office and Official:** Management Directorate, Office of the Chief Human Capital Officer (OCHCO), Catherine V. Emerson, chief human capital officer (CHCO)

**Progress:** DHS has moved from the implementation phase of its strategic human capital plan framework to the sustainment phase and is applying strategic human capital planning actions to ensure DHS has the talent and skills necessary to meet present and future mission-related challenges. In February 2015, GAO released its high risk list rating DHS as fully addressed for one of the human capital management outcomes of the “Strengthening DHS Management Functions”

area, “Implement the Human Capital Plan.” Addressing the remaining human capital management outcomes remains a high priority. DHS continues to mature the human capital strategic planning process and is demonstrating sustainability of this program through several activities:

- The Human Capital Leadership Council (made up of the human resource directors of each operational Component and OCHCO executives) met for the third annual offsite session in June 2015 to initiate the annual human capital planning cycle. A key outcome was a draft FY 2016 operational plan that establishes the program priorities for the upcoming year and aligns to the Human Capital Strategic Plan (HCSP) for FYs 2015 through 2019.
- The enhanced operational planning features of the new human capital planning framework build on the operational planning that supported the earlier DHS workforce strategy and demonstrates the sustainability GAO required for providing a fully addressed rating.
- In preparation for FY 2016 operational planning, DHS conducted an environmental scan of factors affecting the workforce and human capital programs, an analysis of human capital data and trends, and an evaluation of key priorities including improving the hiring process, improving employee morale, and supporting the cybersecurity workforce.
- The Office of Strategic Workforce Planning and Analysis (SWPA) reports the operational plan status to the CHCO monthly and to DHS-wide human capital leadership quarterly. This level of progress reporting promotes transparency and enables timely corrective actions on operational activities where needed.
- By the second quarter of FY 2015, DHS had completed a full year’s cycle of CHCO-led, quarterly, data-driven performance reviews known as HRstat.
- Over the last year, DHS has continued to mature the HRstat program by strengthening quarterly measures to be more relevant and enhancing the human capital dashboard.
- SWPA made considerable progress in strengthening its workforce planning capabilities by completing trend analysis on the Human Resources Operations Audits (HROA) and demonstrating how audit results directly linked to tactics and success indicators included in HCSP. SWPA also adopted a feedback process to follow up with Components after publication of each HROA final audit report.
- In February 2015, OCHCO established an online repository to serve as a central source for the DHS workforce planning community to share best practices, guidance, and tools and stay abreast of skill gap initiatives. The central source library fosters enhanced collaboration and *Unity of Effort* in the identification, assessment, and closure of skill gaps.
- In July 2015, OCHCO published departmental guidance on competency modeling and assessment based on the DHS Competency Framework, ensuring integration of initiatives across OCHCO program offices.
- In July 2015, OCHCO also published an updated workforce planning guide which includes guidance and tools that integrate feedback from a Component-led focus group, lessons learned from the workforce planning cycle, government-wide practices, and external research.

Since January 2015, the Department began refining strategies to implement the new cybersecurity workforce legislation. The Cyberskills Management Support Initiative continues to work with Components to track and monitor the current cybersecurity workforce through the Cybersecurity Workforce Inventory reporting process. Current efforts focus on three key areas:

- Drafting a regulation to implement the new legislative authorities;

- Initiating an assessment of the current DHS cyberskills workforce; and,
- Continuing the Secretary’s Honors Program Cyber Student Volunteer Initiative.

DHS is responsible for drafting regulations, in coordination with OPM, for new cybersecurity workforce authorities. DHS human capital and legal experts have reviewed the legislation and OPM’s accompanying analysis to ensure there is consensus concerning the scope of new authorities. In addition, the Department’s draft regulation, which would implement the staffing-related provisions of the legislation, is in an advanced stage of review within DHS.

In May 2015, DHS initiated a two-phase data collection effort to assess the Department’s cyberworkforce. This data collection effort will produce a consolidated, DHS-wide inventory of the makeup and distribution of its cyberworkforce.

**Planned Actions and Key Milestones:** To sustain a GAO rating of fully addressed for implementing the Human Capital Plan and continue progressing toward a fully addressed rating for the remaining outcomes, the Department-wide human capital community and its key stakeholders will:

- Continue to implement the HCSP through annual operational plans and data-driven performance reviews.
- Monitor and evaluate the human capital dashboard.
- Assess FY 2016 Component recruiting and outreach plans using the Accountability Checklist by November 30, 2015.
- Evaluate and report the results of gap closure strategies, including analyzing trends, identifying risk areas, and ensuring integration into human capital strategic and operational plans by December 31, 2015.
- Analyze quarterly DHS recruiting and marketing costs.
- Receive results from the 2015 Federal Employee Viewpoint Survey, and continue cycle of communication and employee engagement action plan implementation by December 31, 2015.
- Issue final training and development, and rotations policies by December 31, 2015.
- Launch and evaluate the third cycle of Component workforce planning according to the DHS Workforce Planning Guide framework beginning by January 31, 2016.
- DHS Components continue to host students for volunteer positions in the 2015 cycle of the Cyber Student Volunteer Initiative. As of May 2015, a cohort of 51 students have served in 8 Components and 30 DHS locations nationwide. A majority of these students will complete these short-term assignments by September 30, 2015, and in October, the volunteers and their Component managers will be invited to Washington, D.C. for an end of program event with DHS senior leadership.

**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. Despite a high level of leadership commitment to improve real property data, the Federal Government continues to face challenges with the accuracy and consistency of the Federal Real Property Profile causing the Federal Government to report inaccurate inventory and outcome information.

With more than 99 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 account for 81 percent of annual DHS operating outlays for real estate at \$1.7 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), Facilities and Operational Support, Karl Johnson, acting assistant deputy director for Facilities and Operational Support

**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 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. For example:

- DHS worked with all of its Components to build its Real Property Efficiency Plan (RPEP) in response to the Administration's Reduce the Footprint initiative. The RPEP illustrates the Department's maturation process, highlighting robust efforts to reduce the footprint, while supporting mission and maintaining operational performance. DHS's RPEP 5-year plan for FY 2016 through 2020 estimates a 6.5 percent reduction in square footage from a DHS FY 2015 projected office and warehouse baseline of 25.5 million SF. Within the 5-year plan, DHS projects to reduce its office space by 1.1 million SF and its warehouse space by 558,207 SF for a total reduction of 1.7 million SF. DHS finalized the RPEP on October 15, 2015. This follows DHS's adoption of its single Workplace Standard in September 2014, which provides criteria for the development of requirements for office and related spaces (conference rooms, break rooms, file rooms, etc.). The standard is an extension of work pattern studies and associated design processes used to design efficient and effective space layouts incorporating shared workstations. The use of shared workstations is intended to minimize the amount of dedicated and assigned employee workstations; provide effective collaborative space; and provide flexibility to account for telework.
- In collaboration with GSA, DHS updated the development strategy from the last OMB Approved Revised Baseline in June 2013 to a new enhanced plan for the St. Elizabeths campus. The enhanced plan delivers the goals of the original consolidation plan at a lower cost and in a shorter timeframe than earlier plans by: (1) adopting new and smaller space standards; (2) implementing flexible workplace strategies; and (3) realigning the lease expirations to dovetail with and support the construction schedule. The enhanced plan reduces overall construction at St. Elizabeths by nearly 900,000 gross SF and reduces space requirements at other anchor locations within the National Capital Region (NCR). It will save over \$800 million in construction costs and projects 30 year net present value cost

avoidance to DHS of \$1.2 billion over the best case alternative of replacing expiring leases with new commercial leases.

- DHS has further developed its flexible workplace strategies, as demonstrated by a continuing increased level of flexible workplace pilots occurring at headquarters locations within the Department.
- DHS completed a top 10 cities review, an assessment of opportunities for office space consolidation and efficiencies. This review identified potential opportunities for consolidation and/or footprint reduction in administrative office occupancies (excluding the National Capital Region). Progress will be monitored and annual updates completed in conjunction with study and evaluation of project feasibility. This effort will be expanded as additional markets with significant DHS administrative office occupancies and opportunities for reconfigurations and consolidation are identified.
- DHS continued to collaborate with GSA and other DHS lines of business (LOBs) to deliver strategies that leverage expiring leases; seek opportunities for consolidation and co-location; and expand its field efficiency initiative.
- DHS continued aggressive implementation of the DHS Workspace Standard, effective September 30, 2014, to improve its business processes.

DHS continued efforts to ensure protection of our Nation's federal facilities. For example:

- FPS implemented surge efforts to increase post inspections. FPS is on track to exceed FY 2015 projections for inspections completed. FPS also implemented process improvements to increase capabilities to capture the results of completed inspections.
- FPS successfully implemented the Modified Infrastructure Survey Tool (MIST) version 2.0, a Web-based application that supports the successful completion of approximately 4,000 facility security assessments (FSAs) reports and actions with a specific focus on high-risk facilities and in accordance with the Interagency Security Committee (ISC) standards. This application includes structured question sets from earlier versions of MIST, builds in FPS specific workflows, links facility inventory data with assessment data, and provides enhanced reporting capabilities. The application has successfully operated since it deployed in December 2014 and is being used by FPS's law enforcement workforce to accomplish all assessment related work. The ISC has reviewed the FPS process and indicated all the necessary elements for certification. Nevertheless, because the elements are not included in the software program, certification was not achieved. The ISC provided six recommendations for achieving the certification of the software. Two of which have already been implemented and the remaining recommendations have been included in the Mission Needs Statement required for inclusion in the software.
- FPS continued conducting operations at federal facilities to serve as visual deterrents to potential terrorist operations and criminal activity in and around federal buildings. FPS also continued engaging with state and local law enforcement agencies in advance planning and after-action reporting. Operations included law enforcement and security personnel testing and validating the effectiveness of FPS countermeasures, conducting perimeter patrols and explosive detection sweeps, interviewing suspicious persons, and evaluating access control and screening operations, and recommending appropriate enhancements.
- FPS led the effort to establish an ISC Real ID working group. This working group developed strategies that were incorporated in the development of the first edition of the *Real ID Act of 2005 Implementation: An Interagency Security Committee Guide*, which

outlines the phased implementation schedule for enforcement and access control procedures, among other items.

- FPS launched the Train the Trainer Protective Security Office Training Pilot program in April 2014. The program aims to train and certify FPS contract guard instructors to teach the agency’s National Weapons Detection Training Program.
- FPS drafted a concept paper for developing a Protection Center of Excellence (PCE) that addresses training, doctrine, research, and professional development gaps for security professionals protecting our Nation’s critical infrastructure. FPS entered into a memorandum of agreement (MOA) with the Federal Law Enforcement Training Center (FLETC) that establishes a PCE which leverages the parties’ training expertise and FLETC’s consolidated training model for federal law enforcement to identify, develop, and deliver training courses for security professionals based on the ISC’s standards and guidelines. FPS is working with the ISC and FLETC to assess the PCE concept.
- FPS has increased its visibility and responsibilities within the ISC by assigning designated representatives to every ISC subcommittee and working group. FPS also chairs the Training Subcommittee and the Countermeasures Subcommittee.
- FPS also coordinated efforts to include cyberbased events in the tenth edition of the ISC Design Basis Threat (DBT) report, while finalizing crime statistics and other intelligence based products necessary to inform the upcoming elicitation by the DBT subcommittee.

**Planned Actions and Key Milestones:** DHS has strategic plans for several initiatives related to the managing real property as a high risk program area. Over the next year, DHS expects to make important progress in strengthening real property portfolio planning and management functions by:

- Completing a review of DHS’s Sensitive Compartmented Information Facility spaces and demand by September 2016 to include a multi-year data accuracy and quality improvement initiative based on Six Sigma methodologies.
- Maintaining focus on the enhanced plan for the St. Elizabeths campus by advocating for funding the campus completion to optimize DHS Headquarters operations and ensure the most efficient use of space and resources.
- Continuing contingency planning efforts in support of a lease consolidation strategy for NCR pending receipt of sufficient funding to further the St. Elizabeths campus plans.
- Monitoring Component lease requirements to include lease prospectuses to ensure alignment with departmental objectives including the utilization rate target of 150 usable SF per person for new assignments.
- Increasing outreach efforts through the Field Efficiency initiative to provide guidance and consulting services to DHS Headquarters elements and field operations beyond NCR.
- Institutionalizing a single, unified DHS strategy on real property portfolio planning, asset management, and efficiency across all DHS elements.

**GAO High-Risk Area:** Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland (Government-wide)

**Overview:** In January 2005, GAO designated “Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland” as high risk. GAO has since monitored federal efforts to implement the Federal Information Sharing Environment (ISE), because the government faces serious challenges in analyzing key information and sharing

information among federal, state, local, tribal, territorial, and other security partners in a timely, accurate, and useful manner to protect against terrorist threats. The ISE serves as an overarching solution to strengthening the sharing of intelligence, terrorism, law enforcement, and other information. DHS is a key federal participant in the ISE. Continued progress toward improved information sharing is critical in order to reduce the risks of threats to the homeland and to respond to the changing nature of domestic threats.

In its 2013 high -risk list, GAO identified nine action items that are critical for moving the ISE forward, and noted that two had been completed. In the 2015 update, GAO reported that the program manager for the ISE and key Departments, including DHS, had achieved four of the seven remaining action items and had partially met the remaining three action items.

**Lead Office and Official:** Office of Intelligence and Analysis, Glenn Krizay, executive director for plans, integration and evaluation

**Progress:** To establish an enterprise architecture management capability and use it to guide selection of projects for substantially achieving the environment:

- DHS created, published, and implemented the DHS Information Sharing Segment Architecture (ISSA) which serves as a roadmap to guide strategy implementation and project investment selection efforts to achieve the future state of the DHS ISE. It aligns the DHS mission and enterprise functions with the business policies, strategies, leadership, architecture, and governance needed to identify a consistent set of information sharing and safeguarding services and capabilities internal to DHS and the broader ISE.
- DHS participates in ISE Ready which promotes awareness of the ISSA, verifies that DHS is deploying its key information sharing and safeguarding capabilities using the ISSA, and serves as a platform for DHS leadership to make informed decisions relating to resource management and project investment alignment.
- DHS developed the International Information Sharing Architecture under the ISSA which ensures consistency in policies implemented with foreign partners, and is a tool for providing architectural oversight and governance of DHS's interfaces with foreign partners.
- The Information Sharing and Safeguarding Governance Board (ISSGB) adopted the ISSA to identify other enterprise information sharing and safeguarding initiatives. It drives the use of common processes, services, and standards that will ensure DHS is interoperable with and participates in the ISE.

To improve sharing under the environment and more fully develop a set of metrics and processes to measure results achieved:

- The ISSA and the Department's overall enterprise architecture management capability improved DHS's ability to interface with state, local, tribal, and territorial partners. For example, the Simplified Sign-on project, focused on increasing efficiency for fusion center personnel by improving uniform, timely, and appropriate access to more DHS data.
- DHS implemented the National Information Exchange Model (NIEM) to provide standards, data models, tools, and technical support services to improve information sharing, particularly for sharing terrorism related information, across multiple federal, state, and local platforms. DHS also developed NIEM's Emergency Management Domain (EMD), which supports emergency-related services and information sharing to increase readiness.

DHS launched NIEM 3.1 which includes human services as a key component for demographic information exchange.

- DHS is developing and evaluating several critical projects to enhance the overall international information sharing and safeguarding program. For example, DHS is centralizing Components' programs that share information with foreign partners through technology and operational infrastructures suitable to managing agreements.
- DHS deployed the Trusted Automated eXchange of Indicator Information system which allows organizations to share actionable cyberthreat information across organization and product/service boundaries and thereby mitigate cyberthreats.
- DHS implemented the Critical Infrastructure Information Sharing and Safeguarding Enhancement (CIISSE) Program to expand private sector information sharing activities by (1) providing access to Intelligence and Information; (2) ensuring that engagement enhances CIISSE requirements, processes, information flows, and products; (3) better integrating departmental processes for the private sector information sharing; and (4), developing a CIISSE coordination and management function.
- DHS continues to improve sharing and collaboration through the Homeland Security Information Network (HSIN) to disseminate critical secured information sharing within the ISE. DHS increased HSIN membership by 81 percent in FY 2014.
- DHS continues to use common operating pictures, geospatial optimization to provide real-time notifications with cross-domain capabilities. This enables the integration of maritime security common operating data for sharing across Components and with state, local, and international partners for the detection, classification, and interdiction of small maritime targets.
- DHS is developing a performance management framework to capture objective, standardized data to evaluate the value and impact of individual fusion centers and the National Network of Fusion Centers in supporting national information sharing and homeland security outcomes. This assessment, to be conducted annually, enables DHS to coordinate access to capabilities, resources, and expertise necessary for state and local partners to share information and intelligence.

To establish milestones and time frames as baselines to track and monitor progress on individual projects and in substantially achieving the overall environment:

- DHS created the Information Sharing and Safeguarding Strategy Implementation Plan (the Plan) which defines milestones with delivery dates and measures that show progress toward DHS objectives and the realization of the environment. The FY 2016 draft Plan currently has 45 milestones, each with defined timelines that show progress toward the Plan's 17 programs, projects, and initiatives. ISSGB reviews the Plan to ensure its activities and milestones are consistent with the most pressing mission priorities and needs.
- ISSGB monitors several executive steering committees for its major information sharing and safeguarding programs; each has a work plan with defined milestones and delivery dates; and, performance metrics for DHS and Environment goals and objectives.

In addition, of 12 open recommendations to DHS in GAO reports related to this high risk area, GAO has closed 5 recommendations, related to increasing field-based entity coordination, collaboration, and co-location efforts; and, strengthening information sharing with transportation stakeholders; and is taking actions to address the other 7 recommendations.

**Planned Actions and Key Milestones:** DHS has the following planned actions to address the remaining three partially met action items:

- The DHS Data Framework will have 20 total data sets by the end of FY 2016. DHS will develop data tagging workbooks to capture all data elements in the data set and will assign access permissions to each one. DHS will also conduct privacy analyses to determine what, if any, changes are necessary to public-facing privacy documentation and coordinate the technical details on the transfer of the data.
- DHS initiated an FY 2016 refresh of the Plan to focus as an enabler to the agenda for the ISSGB and sub-working groups and stakeholder across the DHS enterprise. The refresh will address enterprise-wide plans, frameworks, responsibilities, priority objectives, and mission impact related initiatives that develop mission capabilities and that focus on mission impact. This will allow for drafting performance measures and milestones for monitoring progress moving forward.
- During FY 2016, DHS will deliver NIEM Version 3.2 and continue to support increased adoption of the NIEM across federal, state, local and international partners by enhancing NIEM EMD content and publishing the NIEM Surface Transportation Domain. DHS will complete re-signing of expired DHS NIEM Domain Stewardship Agreements and execute the action plan derived from "Future of NIEM" strategic discussions. In the long term, DHS plans to deliver NIEM Version 4.0, an updated Unified Modeling Language profile. DHS will also establish and implement performance metrics for DHS NIEM adoption, domain ownership, and the creation of NIEM-conformant information exchanges.
- NPPD will update key portions of the Stakeholder Engagement and Requirements Management plans, to better incorporate stakeholder outreach and requirements management. The final plans on how and when sector-specific agencies will be engaged will be released during the fall of 2015.
- During the remainder of FY 2015, FEMA will implement an additional in-depth desk review of all projects that states have categorized as fusion center projects. Each fusion center project review will include an examination of project progress, impediments to timely completion, and verification of funding data provided by the state. Information verified will be compared to state submissions during the application and reporting processes.
- During FY 2016, FEMA will move the reporting functionality currently supported by the Grants Reporting Tool to the Non-Disaster Grants System, which will provide more advanced to review project progress.

**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 Policy, Daniel Price, acting principal director (Transborder)

**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. The E2C2 Intelligence Cell, once fully established, will develop the required standard operating procedures and determine implementation of these procedures for facilitating intelligence-law enforcement information sharing at E2C2. The E2C2 Intelligence Cell should then have sufficient data to establish baseline and trend data analysis. DHS is committed to working with E2C2 partner agencies to fully staff the intelligence cell.

To improve security cooperation and disclosure, DHS has made improvements to FMS oversight. In 2014, CBP and the U.S. Department of Defense (DOD) established an informal working group to share information and work toward implementing an automated system to provide data regularly on FMS cases. This system would strengthen CBP accounting for FMS articles exported under an FMS contract. CBP holds biweekly teleconferences with DOD’s Defense Security Cooperation Agency (DSCA), which have resulted in progress in several areas, including:

- Near agreement on the final data elements that CBP needs from FMS cases to monitor compliance of FMS exports electronically. The list of data elements is in the process of being finalized.
- Access to FMS for select CBP employees to review current value and status of FMS cases. As of August 2015, CBP had gained access to the Security Cooperation Information Portal via the tokens provided by DSCA. This access has enabled CBP to view FMS case data within the system.
- CBP and DSCA are drafting an MOA that will allow DSCA to send FMS data to CBP electronically for review and completion.

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

- ICE has requested assistance from the National Security Council (NSC) in securing detailees for E2C2. The NSC is currently working to gain support for cooperating departments and agencies.
- CBP is on track to create and implement a centralized process for tracking FMS shipments and enhancing the FMS export data validation process by December 31, 2015.

**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:

- USDA and CBP developed a strategic plan for the Agricultural Quarantine Inspection (AQI) program that delineates joint mission and program goals with corresponding performance measures for monitoring progress toward those goals. USDA and CBP signed the plan on September 17, 2013.
- CBP also consulted with USDA to develop a strategy and action plan for implementing the forthcoming AQI staffing model. This model assesses the risk of potential fiscal constraints and determines what risk mitigating actions should be taken to ensure that agriculture staffing levels at each port are sufficient. The strategy and action plan establishes clear goals to ensure the model will mature with continuous enhancements and updates as new business transformation initiatives and technology advances are implemented. This will ensure a successful deployment once funding becomes available. As of May 2015, CBP has finalized and approved this strategy and action plan.
- CBP and USDA are collaborating to improve the reliability of AQI data on arrivals, inspections, and interceptions across ports, including reviewing the supervisory review policy and procedures to ensure the data are entered accurately. Specifically, CBP has performed enhancements within the Cargo Enforcement Reporting and Tracking System/

International Trade Data System (ITDS)), a CBP database. The enhancements improve the quality of data captured for agriculture inspections. The automatic interoperability between ITDS/Plant Protection and Quarantine (PPQ) PPQ280 and USDA systems has been completed.

- CBP is working to improve the skill sets of personnel with food oversight responsibilities. CBP, in consultation with USDA, identified agriculture canine supervisors who do not have canine training or experience and created a process to provide them with formal training. Specifically, in September 2013, CBP obtained course content recommendations from USDA for supplemental training for agriculture canine supervisors. Using USDA’s recommendations, CBP developed the course and tested the first iteration of the course in December 2014. The first Agriculture Detector Dog Team Supervisor Training course was held in July 2015. The July 2015 course is being used to train new/incoming detector dog team supervisors.

CBP has also made internal changes to its programs to improve food safety oversight. CBP has taken steps to ensure the agriculture canine program has reliable and meaningful data, and has instituted a timely and consistent review process at CBP field offices, and evaluated the relevance of data collected for the agriculture canine program. In particular, as of July 2014, CBP’s Web-based Canine Tracking System (K9TS) was made live. K9TS replaces the Detector Dog System in the Treasury Enforcement Communications System (TECS). Since K9TS came online, all of the agriculture canine handlers began using the system to enter their activities and canine alert (seizure) information daily. At the conclusion of each month, the handler submits their data to their supervisor for approval. Canine supervisors, field office canine advisors, and headquarters canine program managers have the ability to view handlers’ data and create reports when needed. The data collected is relevant to the agriculture canine program and was defined with input from all levels of agriculture canine personnel from headquarters to field subject matter experts, including advisors, supervisors, and handlers. The TECS Detector Dog System was retired and removed from TECS on August 30, 2014.

**Planned Actions and Key Milestones:** CBP is working toward additional future agricultural system interface deployments for USDA-PPQ 309 (Pest Identification Database), and the PPQ 523 (Emergency Action Notification report), to take action against invasive pests and agricultural concerns. CBP expects to complete these deployments by mid-December 2016. By December 31, 2016, all agricultural modules should be in compliance with the ITDS Presidential Mandate. CBP and USDA agricultural systems will interface data for agriculture program assessment, risk analyses, and risk management. CBP will continue to report on deployment and improvement of AQI data as both agencies work toward modernization, interoperability, and automation of data systems.

**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 Deputy USM (DUSM), Chip Fulghum, DUSM, Chief Financial Officer, and Chief Sustainability Officer

**Progress:** DHS formed the Climate Change Adaptation (CCA) Executive Steering Committee (ESC) in March 2011. The ESC consists of representatives from 17 Components authorized to speak on behalf of their respective offices on climate change issues. The ESC released the *DHS Climate Action Plan Addendum* in October 2014 as required by Executive Order (EO) 13653 to help implement the *President's Climate Action Plan* from June 2013. The ESC has made progress on the following priorities since FY 2014:

- The ESC has supported the Council on Environmental Quality by conducting a federal level exercise on CCA. FEMA and other federal partners conducted exercise events with local leaders and planners throughout 2014 in Texas, Colorado, Alaska, and Virginia to examine climate resilience challenges and opportunities. These exercises were designed to build community capacity to identify and implement risk-driven decision-making strategies that inform resilience initiatives, support efforts to manage risk, and validate capabilities to reduce long-term vulnerability.
- The ESC has promoted appropriate building standards and practices. In January 2015, the President signed EO 13690, which will reduce the risk and cost of future disasters by requiring all federal investments in and affecting floodplains to meet higher flood risk standards. Following its release, FEMA solicited additional input and led eight listening sessions across the country as part of the process seeking public comment on the draft implementing guidelines.
- The ESC worked with several federal partners to ensure that adverse effects of climate change on health are incorporated into the Community Health Resilience Initiative (CHRI), which DHS's Office of Health Affairs (OHA) manages and oversees. In FY 2015, CHRI completed and finalized an online Community Health Resilience Guide and Toolkit to strengthen and enhance community health resilience in the face of disasters, which involved both public and private-sector partners. The CHRI received substantial input from federal stakeholders, including the U.S. Department of Health and Human Services and Centers for Disease Control and Prevention as well as over 200 private sector professionals and organizations working in health related and resilience communities. The CHRI Guide and Toolkit provides tools for communities to better prepare for the health effects of climate change. The CHRI website has been endorsed by the White House and is included in the publicly available Climate Change Resilience Toolkit. The CHRI led to the development of three Disaster Resilience Groups: Pediatric/Children, Geriatric/Elder, and Psychosocial. Each group has generated significant nationwide and Canadian interest with over 100

participants per group. Each group webinar provides two to three speakers presenting on their operational disaster resilience initiatives including the effects of climate change on the respective group populations.

- The ESC created a decision support planning template to inform risk decisions at the operational level for all stakeholders using U.S. Global Change Research Program data. This initiative is ongoing and will continue into FY 2016.
- The ESC assessed the exposure of DHS facilities to flood risk in FY 2014 and FY 2015. OCRSO has developed and implemented a portfolio-level data warehouse which consolidates and integrates DHS’s primary real, mobile and personal property assets by location. The data’s accuracy has been tested and utilized as a key indicator in emergency planning and response. A joint working group of experts is outlining a strategy to integrate FEMA floodplain maps into the system architecture and maximize the geocoded data for mission focused flood risk planning.
- DHS launched a CCA section on its public website. This initiative is ongoing and will continue into FY 2016.

**Planned Actions and Key Milestones:** DHS will advance the following initiatives to implement the DHS Climate Action Plan and manage risks related to climate change:

- DHS will conduct a top down review of the governance structure established in the FY 2011 *Secretary’s Climate Change Adaptation Implementing Guidance* in order to enhance overall governance and oversight. As of August 2015, the ESC and director group leadership has transitioned to the DHS Management Directorate. The amended leadership structure and associated authorities will be codified via the establishment of a DHS Climate Change Directive.
- The reconstituted director group, under the ESC and with the support of DHS USM/OCRSO/ Sustainability and Environmental Programs (SEP), will convene a committee of facility, real property and environmental professionals to address the nexus between EO 13653 and EO 13693 “Planning for Federal Sustainability in the Next Decade.” This committee will focus on the comprehensive planning and reporting relative to greenhouse gas and energy intensity reduction, renewable energy, fleet management, leased real property holdings, and the supply chain.
- SEP will develop a DHS Floodplain Management Directive which establishes departmental policy on implementing EO 11988 and EO 13690.
- FEMA will develop a Climate Adaptation, Preparedness, and Resilience Seminar series and toolkit to help build local community capacity. The toolkit will include references and sources for developing a community-based shared understanding of climate change, exercise strategies and sample materials, and other tools needed to undertake local climate adaptation, preparedness, and resilience exercises. Regionally delivered seminars will educate and train whole community resilience champions on using the climate adaptation, preparedness, and resilience toolkit to enhance and sustain community-based hazard mitigation planning and exercise efforts.
- FEMA will develop a comprehensive preparedness guide (CPG) for climate-informed planning to help communities incorporate future climate conditions into risk assessments, emergency management planning, and resource considerations. The CPG will direct planners to resources where they can learn more about anticipated impacts and highlight best practices in planning for climate change-associated risks. FEMA distributed an early

draft for review by local, state, and federal stakeholders and incorporated their feedback into the draft CPG. FEMA continues to develop the CPG in consultation with stakeholders and will release it by the end of FY 2015.

- A core group of hazard mitigation and public assistance staff from FEMA Region VII will receive integrated mitigation training in October 2015 on screening projects eligible for integrated mitigation funding under the *Stafford Act*. FEMA will also evaluate green infrastructure approaches eligible under the hazard mitigation assistance (HMA) programs that provide natural hazard risk reduction benefits as well as lighten the impacts of climate change. FEMA will determine ways to encourage communities to incorporate climate resilient methods to achieve risk reduction in eligible HMA projects, including potential incentives for the FY 2016 Pre-Disaster Mitigation grant program.
- FEMA will conduct pilots exploring incorporation of sea level rise into FEMA flood maps. Moreover, the Technical Mapping Advisory Council will report on ways to improve the accuracy, quality, and ease of use of the flood insurance rate maps, reporting on relevant climate science and future conditions, and how this information may be incorporated into the mapping program to strengthen NFIP.
- In FY 2016, NPPD will continue to advance the risk climate change presents as a threat multiplier. NPPD will leverage infrastructure exposure screening capability at the local level in an effort to promote decision support and maximize U.S. Global Change Research Program data. NPPD will also work toward the continued development and implementation of an engagement strategy for the broader critical infrastructure community.
- NPPD will work collaboratively with stakeholders to incorporate security and resilience strategies, policies, and best practices into critical infrastructure design and maintenance. In FY 2016, NPPD will expand regional and local partnerships by providing support with building plans that include considerations for climate impacts. Moreover, in conjunction with the Association of Climate Change Officers, NPPD will participate in a certification program to build a cadre of climate change experts to better prepare the agency to advance the mission.
- OHA is currently using results from the U.S. Uniformed Health Services (USUHS) resilience capacity building project, which was completed in August 2015. This includes the incorporation of USUHS project results into various peer support programs and a “stand-alone” Psychological First Aid initiative. In FY 2015, OHA launched the online DHS Resilience Tool Department-wide establishing the benchmark for workforce resilience and provided strategies for improvement. Due to demand, OHA will once again make the online tool available to Department personnel in January 2016.

### 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, cross-departmental opportunities as part of the Secretary's *Unity of Effort* initiative.

**Lead Office and Official:** Office of the CIO, Carlene Iletto, executive director for the Enterprise Business Management Office

**Progress:** DHS continues to enhance its IT practices and is focused on the implementation of the administration's government-wide IT management priorities. The DHS IT Strategic Plan was updated in January 2015 to reflect ever-evolving mission challenges and DHS's coordinated effort to integrate people, processes, technology, information, and governance in a way that fully supports stakeholder needs. The Information Resources Management Strategic Plan and the accompanying DHS Enterprise Roadmap describe the approaches DHS uses to manage its information resources in alignment with the DHS IT Strategic Plan, and ensure that its management is embedded with IT best practices. DHS has made IT progress in several key areas; for example:

- DHS exceeded the goal of reducing the average cost of a help desk ticket from \$90.38 in FY 2013 to an average rate of \$15.79 by August 2015. DHS's current average ticket costs 60 percent less than the federal average.
- DHS implemented a tiered governance structure that is integrated with the budget planning process.
- DHS Management LOBs participated in the JRC and ARB to evaluate high priority, cross-departmental opportunities and develop recommendations for investments as part of the Secretary's *Unity of Effort* initiative.
- DHS has implemented enterprise license agreements, and has shared best practices from its successful program to further Federal Government-wide implementation.
- MGMT/CIO has facilitated DHS Components' successive adoption of agile IT development, designing a consistent process that each Component could adopt without negatively impacting the progress of other Components' adoption efforts. MGMT/CIO, MGMT/PARM, and the Science & Technology Directorate coordinated to draft the DHS Agile Instruction and modified it to address GAO recommendations. This instruction updates the acquisition process to remove redundancies and will streamline and shorten the acquisition path.
- MGMT/CIO is an active member in the planning of the FEMA-led Grant Management Modernization effort and is ensuring that a cross-Component view and supporting best practices are included.
- To address the accuracy and reliability of cost and schedule data on the federal IT Dashboard, DHS deployed the Investment Evaluation, Submission, and Tracking (INVEST) system, an upgrade and merge of two legacy systems (Investment Management System and Next Generation Periodic Reporting System), which allows continuous support of DHS's operational business requirements and gives DHS Headquarters and Components the functionality needed to manage their investment portfolios. The USM directed the Component Acquisition Executives to review and certify key INVEST system data.
- DHS established 21 operational executive steering committees covering 27 programs.
- MGMT/CIO and the Office of the CFO collaborated to incorporate results of IT portfolio reviews into the FY 2016 resource allocation decisions and budget submission.

- MGMT/CIO and MGMT/PARM worked together to streamline and coordinate the oversight and management of the acquisition life cycle process by drafting the Major Acquisitions Integrated Governance and Oversight Concept of Operations.
- MGMT/CIO launched Enterprise Cloud Services Initiative which is designed to leverage the success of the data center consolidation with the federal “Cloud First” mandate and the capabilities and savings being offered by emerging cloud computing technologies.
- To strengthen and provide oversight for IT projects, MGMT/CIO led TechStat accountability sessions. The ICE Student and Exchange Visitor Information System program successfully completed its TechStat action items.

DHS has made significant progress on two key programs outlined in GAO’s high risk list:

- U.S. Citizenship and Immigration Services (USCIS) Transformation has improved its ability to track capability delivery to its operational requirements document. In 2014, Transformation updated key acquisition documents to reflect the decision to rebuild the Electronic Immigration System in the new architecture. In April 2015, the program was granted ADE-2B/re-baseline approval from its FY 2012 Acquisition Program Baseline breach.
- The DHS Human Resources IT (HRIT) portfolio now consolidates, integrates, and modernizes the Department’s HRIT, and DHS is working to address its governance and technical challenges. The program secured a modification to its current development contract that will perform new development and key deliverables for the Performance and Learning Management System (PALMS). It continues to operate within acceptable OMB cost and schedule variance thresholds, and is now fully staffed. In a July 2015 health assessment, the program’s MGMT/CIO rating was upgraded to “3 out of 5.” PALMS successfully implemented the Plateau Learning Management System to CBP in July 2015.

**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:

- DHS initiated a two tiered, top-down and bottom-up approach for the implementation of the *Federal Information Technology Acquisition Reform Act* which should be completed by December 31, 2015. MGMT/CIO is coordinating across the LOBs to complete a gap assessment.
- DHS is currently in the process of vetting the DHS Agile Instruction across the enterprise and expects final approval by the first quarter of FY 2016.
- DHS will continue the Component roll-out of PALMS to FLETC, DHS Headquarters, USCIS, and ICE by the second quarter of FY 2016.
- USCIS Transformation is on track to achieve two key milestones: Immigration Visa Re-Build Deployment by the end of the fourth quarter of FY 2015, and other immigration forms deployment by the first quarter of FY 2016.
- As part of the PortfolioStat benchmarking processes, DHS has identified targets for commodity IT spending for FY 2015 and FY 2016. DHS plans to reduce help desk ticket costs to \$9 per ticket over the next three years.
- MGMT/CIO identified 791 DHS IT systems in the FISMA inventory as of March 18, 2015

and will assess the number of systems that may be duplicative, including performing in-depth analysis as part of our segment architecture initiatives.

DHS can achieve further IT efficiencies by (1) rationalizing applications, (2) moving to enterprise commodity IT services where appropriate, (3) emphasizing agile development methodologies, (4) effectively utilizing the Acquisition Management and Systems Engineering Life Cycle policy and guidance, and (5) integrating mission requirements through the JRC. Over the next year, MGMT/CIO will focus on the adoption of the public cloud infrastructure, cybersecurity effectiveness, and asset management.

## **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>.

## Acronym List

AEER – Air Entry/Exit Re-Engineering	DNDO – Domestic Nuclear Detection Office
ALiM – Acquisition Innovations in Motion	DPIO – Deputy PIO
AoA – Analysis of Alternatives	ECS – Enhanced Cybersecurity Services
APG – Agency Priority Goal	EEIWG – Export Enforcement Intelligence Working Group
ARB – Acquisition Review Board	EO – Executive Order
ATD – Alternatives to Detention	ERO – Enforcement and Removal Operations
BEAP – Border Enforcement Analytics	ESC – Executive Steering Committee
BWS – Balanced Workforce Strategy	ETD – Explosive Trace Detection
BWAT – Balanced Workforce Assessment Tool	FedVTE – Federal Virtual Training Environment
CAP – Cross-Agency Priority	FEVS – Federal Employee Viewpoint Survey
CAE – Component Acquisition Executives	FISMA – Federal Information Security Management Act
CAPSET – Criminal Alien Program Surge Enforcement Team	FLETA – Federal Law Enforcement Training Accreditation
CAP SIS – Consolidated Asset Portfolio and Sustainability Information System	FLETC – Federal Law Enforcement Training Centers
CBP – U.S. Customs and Border Protection	FOUO – For Official Use Only
CBPO – CBP Officers	FPS – Federal Protective Service
CBRN – Chemical, Biological, Radiological, and Nuclear	FSM – Financial Systems Modernization
CCA – Climate Change Adaptation	FTC – Failure to Comply
CDM – Continuous Diagnostics & Mitigation	FY – Fiscal Year
CDS – Consequence Delivery System	FYHSP – Future Years Homeland Security Program
CEP – Civil Enforcement Priorities	GAO – Government Accountability Office
CFATS – Chemical Facility Anti-Terrorism Standards	GPRA – Government Performance and Results Act
CFO – Chief Financial Officer	GPRAMA - GPRA Modernization Act of 2010
CHCO – Chief Human Capital Officer	HCSP – Human Capital Strategic Plan
CHIS – Criminal History Information Sharing	HRIT – Human Resources IT
CIO – Chief Information Officer	HSIN – Homeland Security Information Network
CIP – Critical Infrastructure Protection	IA – Individual Assistance
CISO – Chief Information Security Officer	ICE – U.S. Immigration and Customs Enforcement
COA – Course of Action	IER – Interdiction Effectiveness Rate
COR – Contracting Officer’s Representatives	INVEST – Investment Evaluation, Submission, and Tracking
CRCL – Civil Rights and Civil Liberties	ISC – Interagency Security Committee
CROP – Component Recruitment and Outreach Plan	ISE – Information Sharing Environment
CRR – Cyber Resilience Review	ISSA – Information Sharing Segment Architecture
CS&C – Cybersecurity and Communications	ISSGB – Information Sharing and Safeguarding Governance Board
CSA – Customer Satisfaction Analysis	IT – Information Technology
CSD – Cyber Security Division	JIEP – Joint Industry Engagement Plan
CSET – Cyber Security Evaluation Tool	JRC – Joint Requirements Council
CSOL – Case Status Online	
CSP – Commercial Service Providers	
CVE – Countering Violent Extremism	
DBT – Design Basis Threat	
DHS – U.S. Department of Homeland Security	
DMAG – Deputy’s Management Action Group	

JRIMS – Joint Requirements Integration and Management System  
 JTF – Joint Task Force  
 JTF-E – Joint Task Force-East  
 JTF-I – Joint Task Force-Investigations  
 JTF-W – Joint Task Force-West  
 K9TS – Canine Tracking System  
 KM/DS – Knowledge Management/Decision Support  
 LEP – Limited English Proficiency  
 LOB – Lines of Business  
 LRP – Low Risk Population  
 MIST – Modified Infrastructure Survey Tool  
 MOA – Memorandum of Agreement  
 MS-ISAC – Multi-State Information Sharing and Analysis Center  
 NCCIC – National Cybersecurity and Communications Integration Center  
 NCMEC – National Center for Missing and Exploited Children  
 NFIP – National Flood Insurance Program  
 NGO – Non-governmental Organization  
 NICC – National Infrastructure Coordinating Center  
 NIPP – National Infrastructure Protection Plan  
 NOAA – National Oceanic and Atmospheric Administration  
 NPPD – National Protection and Programs Directorate  
 NSCS – National Customer Service Center  
 NWS – National Weather Service  
 NYULMC – New York University Langone Medical Center  
 OCHCO – Office of the Chief Human Capital Officer  
 OHA – Office of Health Affairs  
 OMB – Office of Management and Budget  
 PA&E – Program Analysis and Evaluation  
 PAAB – Public Assistance Appeals and Audits Branch  
 PALMS – Performance and Learning Management System  
 PARM – Program Accountability and Risk Management  
 PCR – Privacy Compliance Review  
 PIA – Privacy Impact Assessment  
 PIL – Procurement Innovation Laboratory  
 PIO – Performance Improvement Officer  
 PMDF – Performance Measure Definition Form  
 PMO – Program Management Office

PPBE – Planning, Programming, Budgeting, and Execution  
 PPPA – Private-Public Partnership Academy  
 QPR – Quarterly Privacy Review  
 RPEP – Real Property Efficiency Plan  
 RPG – Resource Planning Guidance  
 RPM – Radiation Portal Monitor  
 SAR – Search and Rescue  
 SB&A – Southern Border and Approaches  
 SCAP – Secured Content Automation Protocol  
 SCR – Significant Case Report  
 SEP – Sustainability and Environmental Programs  
 SEPA RTF – Southeastern Pennsylvania Regional Task Force  
 SF – Secure Flight  
 SFHA – Special Flood Hazard Areas  
 SFPD – Secure Flight Passenger Data  
 SLA – Service Level Agreements  
 SLC – Senior Leaders Council  
 SLTT – State, Local, Tribal, and Territorial  
 SMI – Serious Marine Incident  
 SONS – Spill of National Significance  
 SSP – Site Security Plan  
 SSPO – Strategic Sourcing Program Office  
 S&T – Science and Technology Directorate  
 STC – Securing the Cities  
 SWAMP – Software Assurance Marketplace  
 TCC – TSA Contact Center  
 TCO – Transnational Criminals or Criminal Organization  
 THIRA – Threat and Hazard Identification and Risk Assessment  
 TRIP – Traveler Redress Inquiry Program  
 TSA – Transportation Security Administration  
 TSO – Transportation Security Officers  
 TTP – Trusted Traveler Program  
 UASI – Urban Areas Security Initiative  
 UK – United Kingdom  
 UN – United Nations  
 US-CERT – United States Computer Emergency Readiness Team  
 USCG – U.S Coast Guard  
 USM – Under Secretary for Management  
 USSS – U.S. Secret Service  
 WYO – Write-Your-Own  
 USUHS – U.S. Uniformed Health Services



Homeland  
Security



Homeland  
Security