

# FY 2018-2020 Annual Performance Report

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





# About this Report

The U.S. Department of Homeland Security Annual Performance Report for Fiscal Years (FY) 2018-2020 presents the Department's performance measures and applicable results, provides the planned performance targets for FY 2019 and FY 2020, and includes information on the Department's Strategic Review and our Agency Priority Goals. Additionally, this report presents information on other key management initiatives, and a summary of our performance challenges and high-risk areas identified by the DHS Office of the Inspector General and the Government Accountability Office. The report is consolidated to incorporate our annual performance plan and annual performance report.

For FY 2018, the Department's Performance and Accountability Reports consist of the following three reports:

- DHS Agency Financial Report | Publication date: November 15, 2018
- DHS Annual Performance Report | Publication date: March 18, 2019
- DHS Report to our Citizens (Summary of Performance and Financial Information) | Publication date: March 22, 2019

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

## Contact Information

For more information, contact:

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

Information may also be requested by sending an email to [par@hq.dhs.gov](mailto:par@hq.dhs.gov).

## Table of Contents

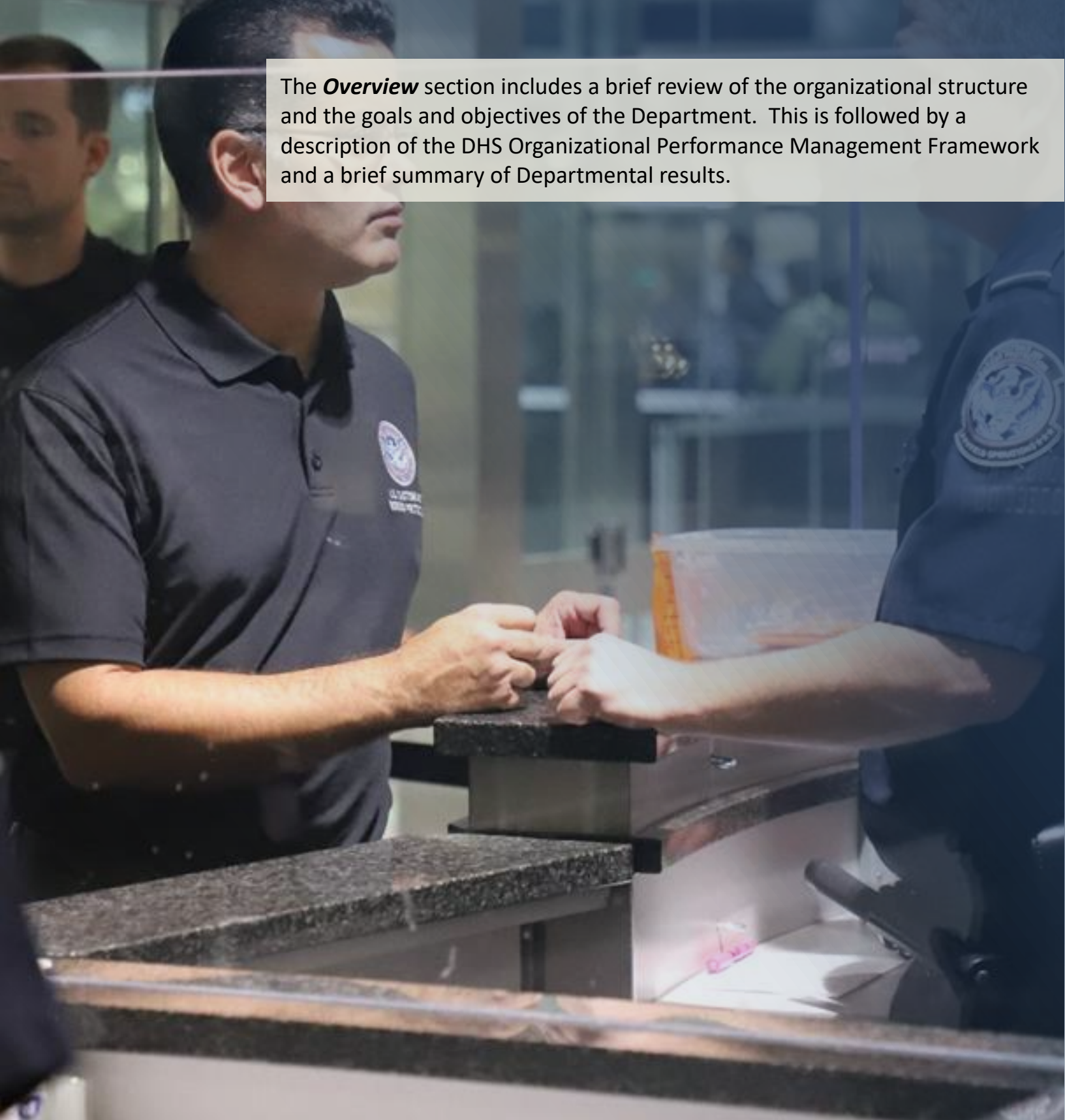
<b>Section 1: Overview.....</b>	<b>2</b>
Introduction.....	3
Organization.....	3
DHS Organizational Performance Management Framework .....	4
Departmental Summary of Results .....	10
<b>Section 2: Performance Results and Plan .....</b>	<b>11</b>
DHS Performance .....	12
<i>Operational Components.....</i>	<i>12</i>
<i>Support Components.....</i>	<i>50</i>
<b>Section 3: Other Information .....</b>	<b>60</b>
Agency Priority Goals (APG).....	60
FY 2018 Strategic Review Results .....	65
<i>Noteworthy Progress Themes .....</i>	<i>65</i>
<i>Focus Areas Themes.....</i>	<i>67</i>
Management Initiatives .....	72
<i>Customer Experience.....</i>	<i>72</i>
<i>Program Management Improvement and Accountability Act (PMIAA).....</i>	<i>82</i>
<i>Regulatory Reform.....</i>	<i>83</i>
<i>Human Capital Operating Plan (HCOP).....</i>	<i>85</i>
Major Management and Performance Challenges and High-Risk Areas – Summary of Progress .....	92
Low-Priority Program Activities.....	124
Acronyms .....	125

Appendix A: Measure Descriptions, Data Collection Methodologies, and Verification and Validation Information

Appendix B: Relevant GAO and OIG Reports

# Section 1: Overview

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





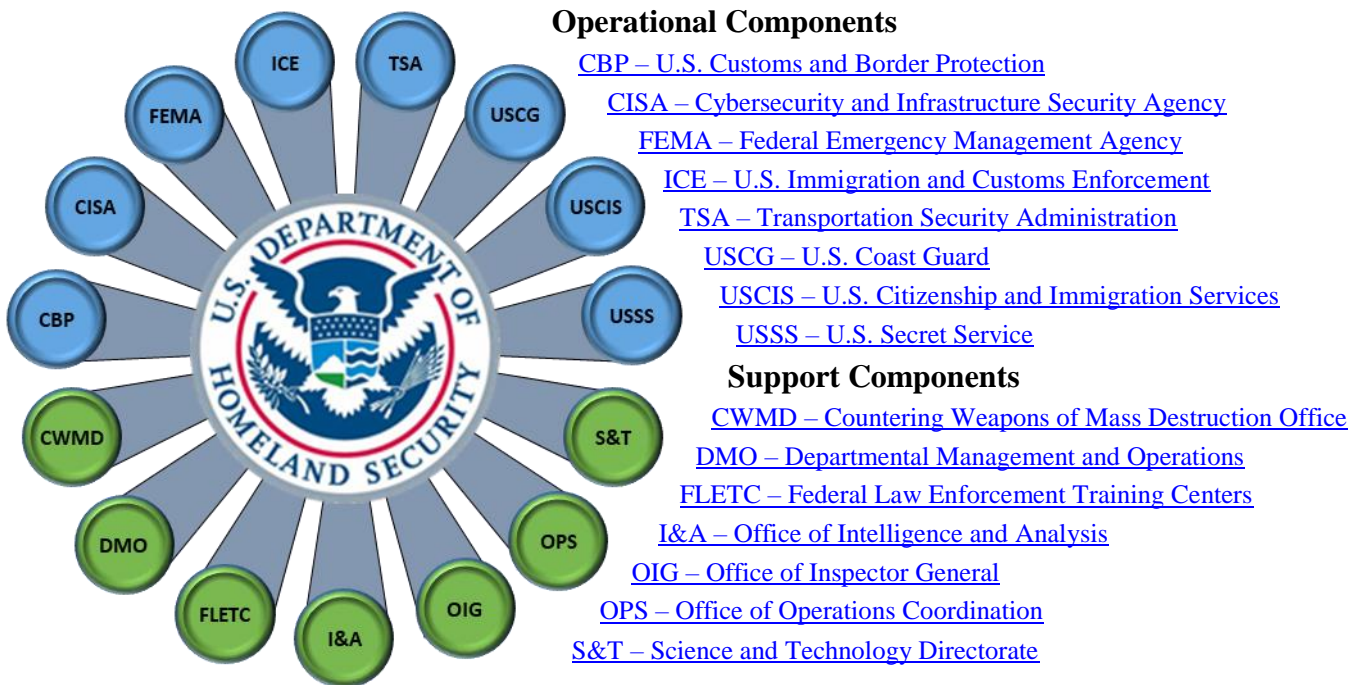
## Introduction

The Department of Homeland Security (DHS) is always seeking ways to communicate the value provided to stakeholders. This report provides a picture of our performance results for FY 2018, along with those planned for FY 2019-2020, aligned to our organizational structure. It satisfies the requirement to publish the Department's FY 2018-2020 Annual Performance Report and Annual Performance Plan. DHS uses our strategic set of measures contained in this report as a means to communicate our progress and the value the Department provides to our stakeholders. Additional performance measure information is also provided in the Overview chapter of each Component's Congressional Budget Justification, which contains both our strategic and management measures. This report may also be found on

our public web site at [Performance & Financial Reports](#), and within the Congressional Budget Justification located at [DHS Budget](#).

## Organization

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



**Figure 1: DHS Operational and Support Components<sup>1</sup>**

<sup>1</sup> The National Protection and Programs Directorate was renamed to Cybersecurity and Infrastructure Security Agency as a result of the enactment of the *Cybersecurity and Infrastructure Security Agency Act of 2018*.

## DHS Organizational Performance Management Framework

DHS has a performance framework that drives performance management and enables the implementation of performance initiatives. As depicted in the following graphic, DHS

leverages our Performance Community to implement key initiatives driven by the original Government Performance and Results Act (GPRA), and signify the enduring foundation of DHS's framework. The Agency Priority Goals, Performance Review, and the Strategic Review are the newer initiatives introduced by the GPRA Modernization Act (GPRAMA).

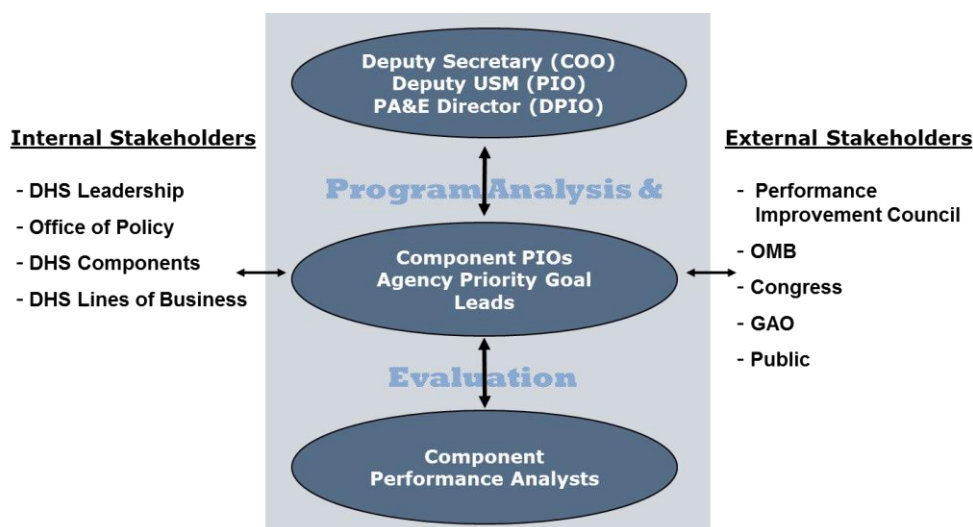


*Figure 2: DHS Performance Management Framework*

### **Performance Community**

The DHS performance community is led by the Chief Operating Officer (COO), the Performance Improvement Officer (PIO), the Deputy PIO (DPIO), and the Assistant Director for Performance Management, all who are supported by performance analysts in the Office of Program Analysis and Evaluation (PA&E) located under the DHS Chief Financial Officer (CFO). In DHS, the COO and PIO are involved in managing performance through a variety of venues. The performance community also includes Component PIOs and Agency Priority Goal

(APG) Leads—the senior leaders driving performance management efforts in their respective Components—interacting with senior DHS leadership on performance management issues. Component performance analysts are the performance measurement experts within their Component who communicate key guidance to program managers, provide advice on measure development concepts, collect and review quarterly and year-end data, coordinate with Component leadership on communicating results internally, and are the primary points of contact within Components on GPRAMA initiatives.



**Figure 3: DHS Organizational Performance Community**

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

### **Managing our Measures**

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

- Feedback provided by senior leadership to mature our ability to describe the value delivered by DHS;
- Suggestions from the Office of Management and Budget (OMB) to achieve greater visibility into program

performance and connection to program resources;

- Recommendations from other external stakeholders such as the Government Accountability Office (GAO) and Congress;
- Suggestions from CFO/PA&E performance analysts working to fill gaps and improve quality; and
- Component leadership and program managers wishing to continually implement measures that are meaningful to their business operations.

While this is a very iterative process, it does follow a continuous improvement process as a means to mature the breadth and scope of our publicly reported set of measures as shown in the next figure. The process begins in the fall where DHS concurrently implements the new measures in the agency performance plan, along with holding discussions regarding gaps and areas for improvement for the following fiscal year. In collaboration with Component programs and CFO/PA&E performance analysts, new measures concepts are developed, as well as modification to existing measures to improve or revise targets to be more in line with expectations. These concepts are then reviewed by Component leadership and submitted to DHS by June 30<sup>th</sup>. Headquarters performance analysts

working in concert with leadership approve changes, which are then submitted to OMB for their review and approval. The results of this process constitute our publicly reported measures associated with our performance budget deliverables, namely our strategic and management set of measures, which are then published in the Department's APR and the Overview Chapters of the Congressional Justification.

#### ***Annual Change Control Process and the PMDF***

To support the measure change process, CFO/PA&E employs a tool known as the Performance Measure Definition Form (PMDF) that provides a structured format to operationally describe every measure publicly reported in the Department's 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. The PMDF is used as a change management tool to propose and review new measures, make changes to existing measures, and to retire measures planned for removal from our strategic and management measure sets. This information is maintained in a Department central data repository, discussed in the next section, and is published annually as Appendix A to our Annual Performance Report.

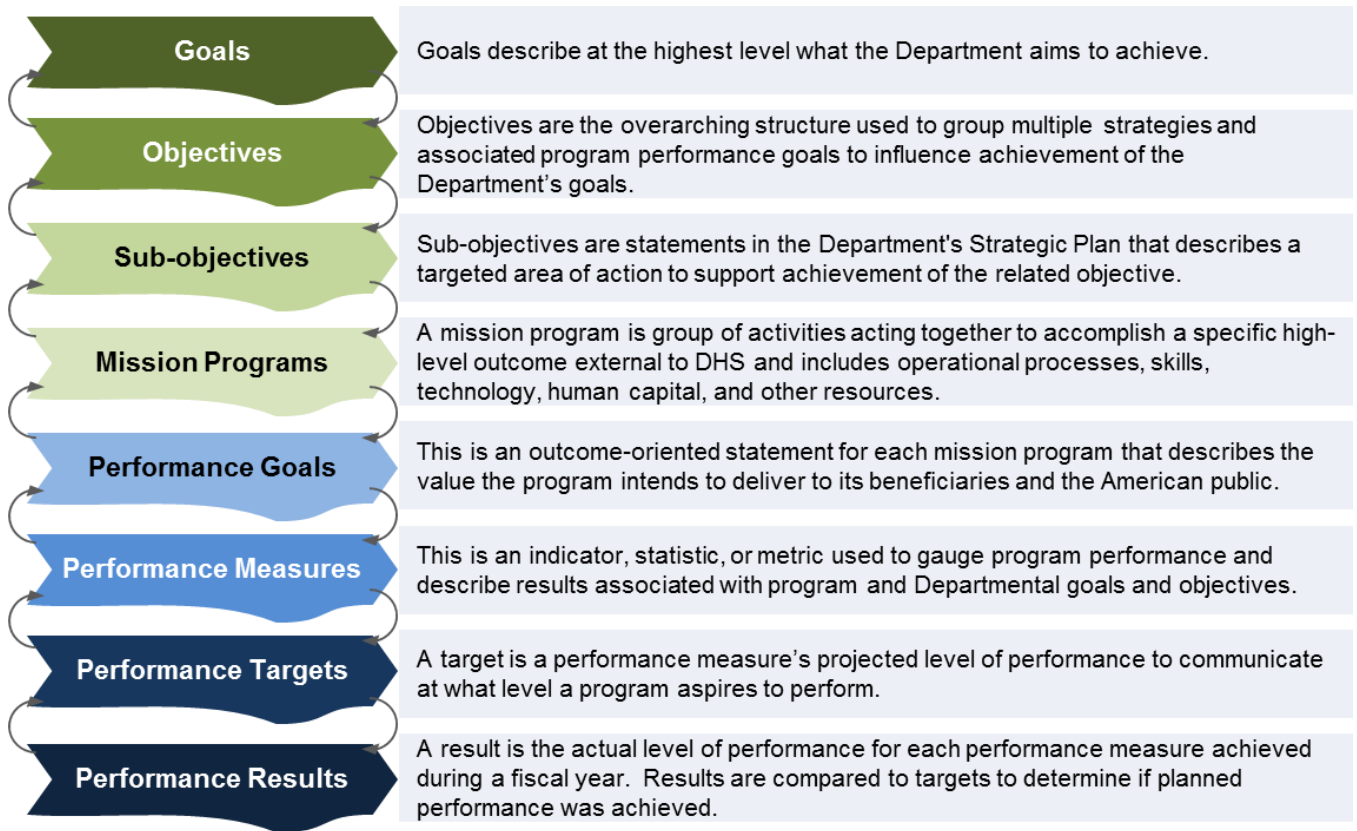


***Figure 4: DHS Annual Measure Improvement Process***

Part of the change process is ensuring alignment to the Department's goals. Figure 5 shows the linkage between the Department's strategic structure, the Department's mission programs, and the

measures used to gauge performance. This approach to measurement ensures that DHS can assess the achievement of the Department's goals.





*Figure 5: DHS Performance Cascade*

## Performance Data Verification and Validation

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

by putting management assurance procedures in place.

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

***Central Information Technology (IT)  
Repository for Performance Measure  
Information***

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

***Performance Measure Checklist for  
Completeness and Reliability***

The Performance Measure Checklist for Completeness and Reliability is a means for Component PIOs to attest to the quality of the information they are providing in our performance and accountability reports. Using the Checklist, Components self-evaluate key controls over GPRAMA performance measure planning and reporting actions at the end of each fiscal year. Components describe their control activities and provide a rating regarding their level of compliance and actions taken for each key control. Components also factor the results of any internal or independent measure assessments into their rating. The Checklist supports the Component Head assurance statements attesting to the completeness and reliability of performance data. Individual Component Head assurance statements serve as the primary basis for the assertion whether

or not the Department has effective controls over financial and performance reporting.

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

CFO/PA&E conducts an assessment of performance measure data for completeness and reliability on a subset of its performance measures annually using an independent review team. This independent review team assesses a select subset of Component GPRAMA measures using the methodology prescribed in the *DHS Performance Measure Verification and Validation Handbook*, documents its findings, makes recommendations for improvement, and may perform a subsequent follow-up review to observe the implementation of recommendations. Corrective actions are required for performance measures that rate low on the scoring factors. The Handbook is made available to all Components to encourage the development and maturation of internal data verification and validation capabilities, increase transparency, and facilitate the review process. The results obtained from the independent assessments are also used to support Component leadership assertions over the reliability of their performance information reported in the Performance Measure Checklist and Component Head Assurance Statement.

***Management Assurance Process for  
GPRAMA Performance Measure  
Information***

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

the Component is taking to correct the measure's reliability.

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

### ***Quarterly Performance Reporting***

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

### ***Performance and Accountability Reporting***

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

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

Combined, these reports comprise our annual performance and accountability reporting requirements. When published, all three

reports are located on our public website at [Performance & Financial Reports](#).

### ***Agency Priority Goals***

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

### ***Performance Reviews***

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

### ***Strategic Reviews***

DHS conducted its fifth annual Strategic Review based on strategic themes and mission programs. Themes are enduring areas of focus for the Department. For each theme, teams were assembled to assess progress. A Headquarters Review Team conducted a cross-cutting review of the Component led teams' assessments and made recommendations to leadership regarding progress ratings. Discussions among senior leaders examined progress made and challenges faced. For a list of our themes and mission programs that rated Noteworthy or were a Focus Area see [Section 3: Other](#)



[Information, FY 2018 Strategic review Results.](#)

## Departmental Summary of Results

A review of the results at the close of FY 2018 demonstrates that 63 percent of the Department's strategic measures met their targets as shown in the table on the next page. Upon further review, 66 percent of measures sustained or improved performance from FY 2017. The FY 2019-2020 performance plan includes a total of 98 measures, representing 22 measures that were retired

from our previous performance plan and the introduction of 21 new measures.

This year's overall results are consistent with historical results. The following chart shows that the measures meeting their target on an annual basis varied between 63 to 68 percent from FY 2011 through FY 2018. Likewise, the percent of measures that maintained or improved over the prior year ranged from 66 to 78 percent. These results are consistent with programs that set ambitious and challenging performance targets as directed by OMB.



## Section 2: Performance Report and Plan

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





## DHS Performance

The DHS Performance section of this report presents information for each Component within the Department that has strategic measures. Each Component begins with an overview to include performance, process, and challenges and risks. Next, a short “success” story from FY 2018 is provided and is followed by a list of contributing mission programs and a description of what they deliver. The final section for each Component is the *Performance Results and Plan* information, presenting measure results and future planned performance. For the performance measures, prior fiscal year results are presented for trend analysis. For those measures that did not meet their current year targets, explanations with corrective action are provided. In addition, changes to measure names and targets from the previous year’s report are identified. To continually

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

For presentation purposes, this report will provide the Operational Components in alphabetical order by followed by the Support Components in alphabetical order. The Department’s Operational Components lead the Department’s frontline activities to protect our Nation. The remaining DHS Support Components provide resources, analysis, equipment, research, policy development, and support to ensure that the frontline organizations have the tools and resources to accomplish the Department’s mission. For more information about the Department’s structure, visit our Web site at <https://www.dhs.gov/organization>.

## Operational Components

### U.S. Customs and Border Protection

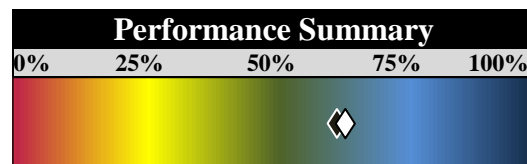
#### Overview

[U.S. Customs and Border Protection \(CBP\)](#) is responsible for securing America’s borders to protect the United States against threats and prevent the illegal entry of inadmissible persons and contraband, while facilitating lawful travel and trade. CBP officers and agents enforce all applicable U.S. laws, including illegal immigration, narcotics smuggling, and illegal importation.

CBPs border security mission is conducted at ports of entry by CBP officers from the Office of Field Operations, along U.S. borders between ports of entry by agents from the U.S. Border Patrol, and from the air and sea by agents from Air and Marine Operations. Also at ports of entry, agriculture specialists are deployed to protect U.S. agriculture from the

introduction of pests or disease from overseas sources.

In FY 2018, there were 11 strategic performance measures used to assess CBP’s efforts. In FY 2018, 64 percent of the measures met their target and 64 percent maintained or improved actual results compared to FY 2017.



◆ - Percent of measures that met their FY 2018 target.

◇ - Percent of measures that maintained or improved actual performance results compared to FY 2017.



## Mission Programs

The mission programs that deliver performance results for CBP are:

- **Border Security Operations:** The Border Security Operations program is charged with securing America's Southwest, Northern, and certain Coastal borders. Through the coordinated use of the Department's operational capabilities and assets of the U.S. Border Patrol, CBP improves operational effectiveness by working across the Department to prevent terrorists and terrorist weapons, illegal aliens, smugglers, narcotics, and other contraband from moving across the U.S. border.
- **Integrated Operations:** The Integrated Operations Program provides: Air and Marine Operations support to the Border Patrol's detection and interdiction roles; international affairs support across all missions; intelligence and information sharing for operations and investigations; and overall operations support for systems, training, firearms, and credentialing.
- **Trade and Travel Operations:** Managed by the Office of Field Operations and the Office of Trade, the Trade and Travel Operations program allows the Department to better intercept potential threats at the ports before they cause harm while expediting legal trade and travel. The program includes a multilayered system of people, technology, intelligence, risk information, targeting, international cooperation, and expanded shipper and traveler vetting that provides greater flexibility and capacity to accomplish these functions prior to arrival at the U.S. border.

## Summary of Progress

**Progress:** The following progress updates were identified through the Strategic Review:

- U.S. Border Patrol developed a Border Security Improvement Plan (BSIP) that included the Southwest Border Capability Roadmaps and requirements related to improving impedance and denial.
- Several projects are under way along the Southern Border to replace primary border barriers and convert vehicle barriers to primary pedestrian barriers.
- Recidivism continues to improve in response to the consistent application of the Border Patrol's Consequence Delivery System, which applies more stringent negative outcomes upon subsequent illegal re-entry attempts.
- CBP established the Northern Border Coordination Center to collect, analyze, and share intelligence-related information with internal and external stakeholders.
- CBP implemented hiring and retention incentives, such as the operational mobility program, to help reduce agent attrition and staff hard-to-fill locations.
- U.S. Border Patrol formulated and began implementation of its Operational Control (OPCON) framework.
- Air and Marine Operations sustained results in countering cross border conventional aircraft incursions and is developing enhanced relationships with intelligence partners through information sharing, such as the Interconnect Service Agreement, to link U.S. Coast Guard, Navy, and Air Force platforms that identify and track any suspicious or illegal activity both on land and sea.
- CBP collected over \$47.2 billion in duties, fees, and taxes, including

increased duties on steel, aluminum, and products from China. With trade and travel projected to continue to grow, DHS and its partners must work to secure and expedite the increasing flows of people and goods to keep our Nation safe and prosperous.

### Did you know?

In FY 2018, CBP processed 35.1 million shipments valued at over \$2.6 trillion. This is about 96,000 shipments every calendar day of the year, all processed through automated systems and vetted for requirements and restrictions of nearly 50 government agencies.

- CBP operationalized 10 [Centers of Excellence and Expertise](#) to improve trade facilitation and enforcement and further strengthen critical agency knowledge on key industry practices.
- A pilot biometric entry/exit process in Orlando, Florida was initiated to collect passenger data prior to departure and is creating a paperless secure platform to identify travelers, which could revolutionize the entry/exit process.

**Challenges and Risks:** The following challenges and risks were identified through the Strategic Review:

- The U.S. is currently encountering illegal immigration at the highest rates since 2007 and is experiencing an unprecedented surge of illegal alien families arriving at our border, along with Unaccompanied Alien Children. A number of dynamics, such as outdated

laws, have created a tremendous pull factor that is spurring this illegal immigration and creating an ongoing humanitarian and security crisis.

- If Border Security Operations does not hire and maintain an adequate number of enforcement and support personnel, then operational control between ports of entry could be diminished.

### Did you know?

In FY 2000, only 2% of the total apprehensions made by the U.S. Border Patrol were citizens of a country other than Mexico (OTM). In FY 2018, OTM's represented nearly 60% of the Border Patrol's total apprehensions primarily from Guatemala, Honduras, and El Salvador.

- If Border Security Operations cannot build more border infrastructure and improve the ability of agents to freely move about the border area, then law enforcement response between ports of entry will remain diminished.
- If Air and Marine is unable to modernize its fleet, then the capability to detect, interdict, and disrupt illegal activity will be degraded.
- The Administration's focus on combating unfair trade practices has accelerated over the last year. The significant growth and expansion of trade remedy programs will continue to place high demand on the trade workforce to continually improve customer service while also strengthening enforcement.



## Border Wall Construction

On January 25, 2017, the President issued Executive Order 13767 which directed DHS to “construct a physical wall.” The impedance and denial capability that the border wall provides has been a consistent operational requirement for the Border Patrol and a lack of this infrastructure was identified as a significant risk in both the FY 2017 and FY 2018 DHS Strategic Reviews. Field commanders have continued to advocate for border wall to impede and/or deny attempted illegal entries while creating additional time to carry out successful law enforcement resolutions.

The border wall is part of an integrated system that will deter and prevent illegal entries, a requirement all along the Southwest Border. The FY 2017

enacted budget included \$341 million to construct approximately 40 miles of replacement wall and close approximately 35 gaps in existing barrier with gates. CBP received its FY 2017 funding in late-May 2017 and immediately started planning for construction. In partnership with the U.S. Army Corps of Engineers, the first contract for design and construction was awarded for approximately two miles of primary border wall in Calexico, California in November 2017 and construction started in February 2018. CBP border wall construction efforts have moved exceptionally quickly for large Federal construction projects, where the process commonly takes two years or more. In some instances, construction of wall began in as little as nine months from funding to building, which is almost a quarter of the time it takes in some parts of the Government.

As of September 30, 2018, approximately 29 of the 40 miles of replacement border wall were completed with completion estimated for May 2019. CBP is also planning and executing the FY 2018 program funded at approximately \$1.375 billion and construction on the first FY 2018 project started in February 2019. CBP has already started execution on FY 2019 funding made available, including releasing requests for industry proposals, for two of the wall construction projects just days after the passage of the FY 2019 appropriations bill.

## Performance Results and Plan

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
<b>Trade and Travel</b>								
Amount of smuggled outbound currency seized at the ports of entry (in millions)								
\$36.9	\$37.7	\$37.6	\$28.9	\$39.0	\$30.0	\$38.7	\$30.0	\$30.0
Number of smuggled outbound weapons seized at the ports of entry (CBP)								
731	411	505	661	421	400	686	400	400
Percent of cargo by value imported to the U.S. by participants in CBP trade partnership programs								
55.2%	53.9%	52.2%	53.0%	53.1%	53.0%	53.3%	53.0%	53.0%
Percent of import revenue successfully collected								
98.73%	99.56%	98.61%	99.06%	99.05%	100%	99.44% <sup>1</sup>	99.0% <sup>2</sup>	99.0%
Percent of imports compliant with U.S. trade laws								
97.66%	97.99%	98.89%	99.18%	99.38%	97.50%	98.72%	97.50%	97.50%
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								
98.00%	99.22%	99.76%	99.28%	99.50%	100%	97.88% <sup>3</sup>	100%	100%

1 – Statistical sampling provides CBP with a high level of confidence that the approach of facilitation and automation of imports yields a high level of compliance, so that the agency can focus resources on higher risk shipments and allegations of fraud. Any discrepancies discovered from the compliance measurement process are addressed through billing and collection, and if broader risks are apparent, further action is taken. Additional enforcement methods such

as audits, targeting, and investigations are employed to find other instances of purposeful non-compliance and fraud, providing CBP with a comprehensive approach to risk management.

2 – FY 2019 target previously published as 100% in the FY 17-19 Annual Performance Report. Component updated targets to be consistent with historical performance and with Congressional reports provided to Congress on actual results.



## FY 2018-2020 Annual Performance Report

3 – 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 (ATS) that is reviewed, scanned, or otherwise examined prior to lading or at arrival at a U.S. 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. The Office of Field Operations will continue to work with the Targeting & Analysis Systems Program Directorate to resolve status tracking problems and information processing errors and with shippers and carriers to rectify logistical and scheduling issues.

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
<b>Border Operations</b>								
Percent of detected conventional aircraft incursions resolved along all borders of the United States								
99.3%	98.8%	99.3%	99.7%	97.9%	98.5%	100%	98.5%	98.5%
Percent of people apprehended multiple times along the Southwest Border								
16%	14%	14%	12.3%	10.5%	≤ 17%	10.8%	≤ 15% <sup>1</sup>	≤ 15%
Percent of recurring border surveillance implemented in remote low risk areas between ports of entry								
---	---	---	---	90.4%	93.0%	99.0%	96.0%	100%
Percent of time the U.S. Border Patrol meets its goal of responding to potential illegal activity in remote, low-risk areas								
---	---	---	---	96.4%	96.0%	92.2% <sup>2</sup>	95.0% <sup>3</sup>	95.0%
Rate of interdiction effectiveness along the Southwest Border between ports of entry								
---	79.3%	81.0%	82.7%	78.9%	81.0%	79.7% <sup>4</sup>	81.0%	81.0%

1 – FY 2019 target previously published as ≤ 17% in the FY 17-19 Annual Performance Report. Component updated target due to the long-term downward trend in the recidivism rate.

2 – This measure missed its target due to manpower prioritization to higher priority events. The Chief of the U.S. Border Patrol has communicated a reprioritization that will improve the level response to potential illegal activity in remote, low-risk areas.

3 – FY 2019 target previously published as 97% in the FY 17-19 Annual Performance Report. Component updated target due to analysis of the situational

awareness requirements needed in these remote areas and challenging environments.

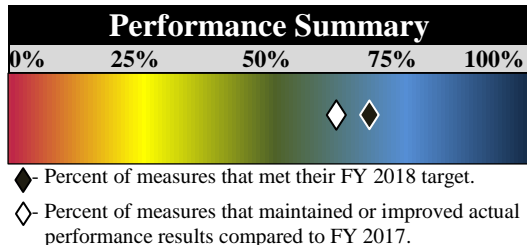
4 – Improvements in situational awareness have increased both the accuracy and the quantity of the known flow of illegal immigrants, the current U.S. Border Patrol staffing is unable to apprehend all border crossings. Implementation of U.S. Border Patrol's Operational Control framework will allow leadership to ensure that Southwest Border commanders focus annual operational planning on efforts that support the framework with the intent of increasing interdiction effectiveness.

## Cybersecurity and Infrastructure Security Agency

### Overview

[Cybersecurity and Infrastructure Security Agency](#) (CISA) leads the national effort to defend critical infrastructure against the threats of today, while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow. CISA's vision is a safe, secure, and resilient infrastructure where the American way of life can thrive. CISA coordinates with critical infrastructure owners and operators, federal building managers, cybersecurity partners, and emergency communications providers.

In FY 2018, there were 16 strategic performance measures used to assess the CISA's efforts. In FY 2018, 69 percent of the measures met their target and 63 percent maintained or improved actual results compared to FY 2017.



### Mission Programs

The mission programs that deliver performance results for CISA are:

- **Cybersecurity:** The Cybersecurity program advances computer security preparedness and the response to cyberattacks and incidents. The program includes activities to secure the federal network, respond to incidents, disseminate actionable information, and collaborate with private-sector partners to secure critical infrastructure. This program supports the implementation of government-wide deployment of hardware and software systems to prevent and detect

incidents, response to incidents at federal and private entities, and collaboration with the private sector to increase the security and resiliency of critical networks. The program also coordinates cybersecurity education for the federal workforce.

#### Did you know?

Continuous Diagnostics and Mitigation (CDM) Dashboards will enhance cybersecurity by providing a dynamic system that focuses on asset-based risk management rather than compliance reporting. CISA is working with agencies to operationalize CDM Dashboard data and incorporate it into existing and new risk mitigation processes to strengthen federal cybersecurity.

- **Emergency Communications:** The Emergency Communications program is responsible for advancing the Nation's interoperable emergency communications capabilities to enable first responders and government officials to continue to communicate in the event of disasters.
- **Federal Protective Service:** The Federal Protective Service protects federal facilities, their occupants, and visitors by providing law enforcement and protective security services. The program provides uniformed law enforcement and armed contract security guard presence, conducts facility security assessments, and designs countermeasures for tenant agencies in order to reduce risks to federal facilities and occupants.
- **Infrastructure Protection:** The Infrastructure Protection program leads and coordinates both regulatory and voluntary national programs and

policies on critical infrastructure security and resilience and develops strong partnerships across government and the private sector. The program conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators and SLTT partners to understand and address risks to critical infrastructure. Additionally, it provides information on emerging threats and hazards and offers tools and training to partners to help them manage risks to critical infrastructure.

### ***Summary of Progress***

***Progress:*** The following progress updates were identified through the Strategic Review:

- Information exchanges between the federal and agency Continuous Diagnostics and Mitigation (CDM) dashboards have been established to provide cybersecurity situational awareness of federal networks.
- The Government Emergency Telecommunications Service (GETS) and Special Routing Arrangement Service ensured the completion of greater than 99 percent of high-priority calls made by national-security and emergency-preparedness personnel using commercial telecommunications infrastructure.
- Implementation of a revised, critical infrastructure post visit (for federal facilities) method, which is based on a nationally recognized, risk-based American National Standards Institute standard.
- Presented results and countermeasure recommendations from Facility

Security Assessments to the Facility Security Committees for consideration.

- The Chemical Facility Anti-Terrorism Standards (CFATS) program implemented an improved risk-tiering methodology to increase the efficiency of determining a facility's risk of release, theft/diversion, or sabotage to chemicals in their possession.
- To enhance CISA leadership oversight of risk mitigation for our national critical functions, DHS has established the National Risk Management Center (NRMC). The NRMC will address both cyber and physical risks to critical infrastructure, focusing resources on our highest national security priorities.

***Challenges and Risks:*** The following challenges and risks were identified through the Strategic Review:

- If governance of federal cybersecurity is not effectively implemented, compliance of directives and understanding of how to leverage tools and services will not occur.
- With respect to emergency communications, the short-term technology mismatch between local exchange carriers may create gaps in service.
- CISA is looking at the Federal Protective Service fee structure to ensure service delivery will be maintained in the outyears.
- CISA also faces delays in the hiring process, which poses challenges and risks to planned staffing levels to support critical infrastructure goals.





## National Level Campaigns Address Nation State Cyber Threats

The Cybersecurity and Infrastructure Security Agency's (CISA) National Cybersecurity and Communications Integration Center (NCCIC) participated in interagency National Level Campaigns addressing cyber-activity and threats from four nation states during 2018.

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

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

### Performance Results and Plan

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
Critical Infrastructure								
Percent of contract security force evaluations conducted at high-risk facilities resulting in no countermeasure-related deficiencies								
97%	97%	97%	98%	83%	85%	87%	Retired Measure <sup>1</sup>	
Percent of high-risk facilities found to have no countermeasure-related deficiencies								
---	---	---	---	---	New Measure <sup>1</sup>		70%	71%
Percent of Critical Infrastructure customers reporting implementation of at least one recommendation following a DHS cybersecurity assessment <sup>2</sup>								
100%	63%	100%	100%	91%	85%	85%	85%	87%
Percent of facilities that are likely to integrate vulnerability assessment or survey information into security and resilience enhancements								
---	---	---	90%	92%	80%	87%	85% <sup>3</sup>	85%
Percent of Facility Security Committee Chairs (or designated officials) satisfied with the level of security provided at federal facilities								
---	---	---	---	77%	79%	80%	80%	81%
Percent of high-risk facilities that receive a facility security assessment in compliance with the Interagency Security Committee (ISC) schedule								
34%	93%	100%	96%	100%	100%	100%	100%	100%
Percent of performance standards implemented by the highest risk chemical facilities and verified by DHS								
46%	78%	93%	97%	93%	95%	91% <sup>4</sup>	Retired Measure <sup>5</sup>	
Average score of initial Site Security Plans (SSPs)								
---	---	---	---	---	New Measure <sup>5</sup>		50	50
Average score of approved Site Security Plans (SSPs)								
---	---	---	---	---	New Measure <sup>5</sup>		70	70
Percent of respondents reporting that DHS critical infrastructure information will inform their decision making on risk mitigation and resilience enhancements								
---	---	---	92%	95%	77%	94%	82% <sup>6</sup>	85%

## FY 2018-2020 Annual Performance Report

1 – This measure is being retired and replaced with “Percent of high-risk facilities found to have no countermeasure-related deficiencies” due to a scope change in the program effort.

2 – Measure name changed from *Percent of customers implementing at least one cybersecurity assessment recommendation to improve critical infrastructure and federal network security*.

3 – FY 2019 target previously published as 80% in the FY 17-19 Annual Performance Report was adjusted to better align with past performance and expected future results.

4 – This measure assesses the percent of DHS verified performance standards implemented by the highest risk chemical facilities to ensure compliance with the Chemical Facility Anti-terrorism Standards (CFATS) regulation. To date, DHS has approved 214 of the 239 Tier 1 and 2 facilities. By the fourth quarter of FY 2018, DHS delivered guidance and requirements to the highest risk chemical facilities, prompting these facilities to include 4,028 security improvements in their security plans to satisfy the risk-based performance standards. Of the 4,028 specific security improvements 3,685 security measures have been implemented. Implementing these performance standards improves the overall security of the highest risk chemical facilities. The revised tiering methodology resulted in a great deal of movement in the tiering of facilities as some enter,

and exit the program, as well as movement within tiers. The impact of the implementation of the new Chemical Security Assessment Tool (CSAT) 2.0 is still being felt as facilities continue to self-report through the tool, develop new site security plans, and implement performance standards based on those plans. In order to improve performance, DHS will continue to prioritize the authorization, inspection, and approval of the highest risk facilities and expects to complete these in a timely fashion. As the tiering of facilities stabilizes in FY 2019, DHS expects a higher percentage of risk-based performance standards will be implemented.

5 – The two measures, “Average score of initial Site Security Plans (SSPs)” and “Average score of approved Site Security Plans (SSPs)” are replacing the retired measure “Percent of performance standards implemented by the highest risk chemical facilities and verified by DHS.” The two new measures will provide better insight to the program’s impact on improving Site Security Plans.

6 – FY 2019 target previously published as 80% in the FY 17-19 Annual Performance Report was adjusted to better align with past performance and expected future results. Due to varying customer feedback ratings, the program is using a conservative target increase and will reassess targets if recent trends persist.

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
Federal Network Security								
Percent of annual risk and vulnerability assessments completed for twenty-three cabinet level agencies and one-third of all non-cabinet level agencies								
---	---	---	42%	35%	40%	53%	Retired Measure <sup>1</sup>	
Percent of incidents detected by the U.S. Computer Emergency Readiness Team for which targeted agencies are notified within 30 minutes								
89.0%	87.2%	96.6%	97.0%	N/A <sup>5</sup>	98.0%	93.4% <sup>2</sup>	Retired Measure <sup>3</sup>	
Average number of hours to notify agency of an incident on their network from earliest detection of potentially malicious activity								
---	---	---	---	---	New Measure <sup>3</sup>		24	24
Percent of incidents detected or blocked by EINSTEIN intrusion detection and prevention systems that are attributed to Nation State activity								
---	---	---	---	---	20%	29%	20%	22%
Percent of participating federal, civilian executive branch agencies for which Continuous Diagnostics and Mitigation (CDM) tools to monitor what is happening on their networks have been made available								
---	---	---	---	0%	95%	96%	Retired Measure <sup>4</sup>	
Percent of significant (critical and high) vulnerabilities identified through a DHS assessment of a federal agency high value asset that are mitigated within 30 days								
---	---	---	---	---	New Measure <sup>5</sup>		45%	50%
Percent of participating federal, civilian executive branch agencies for which Continuous Diagnostics and Mitigation (CDM) capabilities to manage user access and privileges to their networks are being monitored on the DHS managed Federal Dashboard								
---	---	---	---	---	New Measure <sup>6</sup>		42%	63%
Percent of respondents indicating that operational cybersecurity information products provided by DHS are helpful								
---	---	---	---	92%	90%	93%	90%	90%

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
Percent of significant (critical and high) vulnerabilities identified by DHS cyber hygiene scanning of federal networks that are mitigated within the designated timeline								
---	---	---	---	---	80%	52% <sup>7</sup>	70% <sup>8</sup>	75%
Percent of survey respondents that were satisfied or very satisfied with the timeliness and relevance of cyber and infrastructure analysis based products								
---	---	---	93%	93%	92%	96%	94%	96%

1 – DHS has changed its measurement approach to focus on high-value assets, so this measure is being retired in lieu of other existing measures.

2 – This measure assesses the percent of incidents directed at federal agencies and detected by the National Cybersecurity and Communications Integration Center (NCCIC) for which agencies are informed of this malicious activity within 30 minutes. In FY 2018 the NCCIC team met the agency notification requirement of 30 minutes in 171 out of 183 potential incidents for a cumulative average of 93.4%. The FY 2018 target was missed due to analysts spending additional time to complete their review and coordination before notifying agencies. Incident detection and rapid notification are critical elements in reducing the duration and spread of cyber incidents within federal networks. This measure underwent an independent verification and validation in FY 2018 and the program decided to retire and replace this measure to expand the scope of measurement. This measure only covers the amount of time it takes an analyst to create a Remedy ticket and send it to the affected agency. The replacement measure will include the time from the first EINSTEIN alert of the potential incident to agency notification. This is a much more holistic of agency notification procedures that DHS can use to improve response processes and procedures.

3 – The measure “Percent of incidents detected by the U.S. Computer Emergency Readiness Team for which targeted agencies are notified within 30 minutes” is being retired and replaced with “Average number of hours to notify agency of an incident on their network from earliest detection of potentially malicious activity” to more accurately reflect the time between initial activity detection and notification to agency.

4 – The measure “Percent of participating federal, civilian executive branch agencies for which Continuous Diagnostics

and Mitigation (CDM) tools to monitor what is happening on their networks have been made available” is being retired since there is only one contract action remaining which is being tracked and reported through the Agency Priority Goal.

5 – This measure is being added to better reflect progress in protecting high value assets.

6 – This measure is being added to reflect CDM’s growing capability to secure federal networks.

7 – This measure calculates the percent of significant (critical and high) vulnerabilities identified through DHS cyber hygiene scanning that are mitigated within the specified timeline. For critical vulnerabilities the timeline is 15 days and for high vulnerabilities the timeline is 30 days. A key reason this measure did not meet the target is the difference between the required mitigation timeline specified in Binding Operational Directive (BOD) 15-01 and the mitigation timeline defined in the indicator. BOD 15-01 requires agencies to mitigate critical vulnerabilities in 30 days, with no requirement for high vulnerabilities. Identifying and mitigating vulnerabilities on a network in a timely manner is a critical component of an effective cybersecurity program. In order to align the requirements for agency mitigation timelines, DHS is planning on updating BOD 15-01 in FY 2019 in order to require agencies to mitigate critical vulnerabilities in 15 days and high vulnerabilities in 30 days. The communication of this requirement to agencies through the issuance of the BOD will prioritize agency mitigation efforts and will likely lead to improved performance.

8 – FY 2019 target previously published as 90% in the FY 17-19 Annual Performance Report was adjusted based on proposed updates to BOD 15-01 in FY19. The update to BOD 15-01 will place more stringent requirements on agencies and it is anticipated that some agencies may experience difficulties in meeting all the requirements.

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
<b>Man-Made or Natural Incident Preparedness</b>								
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								
---	---	---	55%	55%	57%	50% <sup>1</sup>	Retired Measure <sup>2</sup>	

1 – This measure uses the Threat and Hazard Identification and Risk Assessment (THIRA) and State Preparedness Report (SPR) process, conducted by FEMA on an annual basis, to identify the level of Operational Communications capabilities reported by the 56 States and Territories inclusive of applicable Urban Areas. The measure reflects the level of increase or decrease in those capabilities relative to targets established through the THIRA. All 56 States and Territories

completed State Preparedness Report ratings for the period of January 1, 2017 - December 31 - 2017. Twenty-eight (28) of the 56 States and Territories indicated an overall rating of "4" or "5" within the Operational Communications core capability for calendar year 2017. By ensuring effective emergency communications across the nation, DHS helps to ensure effective emergency response, which ultimately strengthens national preparedness and resilience. To support



## FY 2018-2020 Annual Performance Report

operational communications, DHS will: Continue to fill 11 field vacancies, expected to be filled after one year due to the hiring process, to provide more direct emergency communications support to stakeholders; Conduct national workshops to support states and territories in enhancing their governance and strategic planning processes to strengthen emergency communications; Support data integration into incident communications by working with public safety to develop curriculum for a new communications position (Information Technology Services Unit Leader), complete alpha and beta testing, and conduct a train-the-trainer session; Work with Department of the Interior and states to sign

Memorandum of Understanding allowing non-Federal agencies to access the Federal Enforcement and Incident Response Interoperability Channels; Conduct planned event observations in urban areas focused on data and land mobile radio operability and interoperability.

2 – Due to the change in reporting approach, the measure “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.” A new measure is being developed for implementation in FY20.

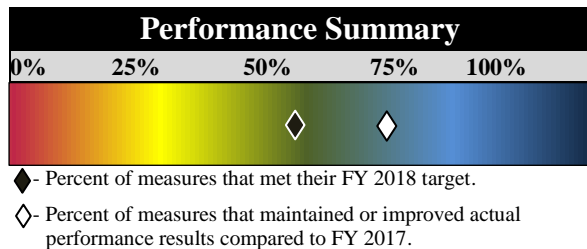
Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
<b>Man-Made or Natural Incident Response</b>								
Percent of calls made by National Security/Emergency Preparedness users during emergency situations that DHS ensured were connected								
96.8%	99.3%	99.3%	99.0%	99.3%	98.0%	99.1%	99.0%	99.0%

## Federal Emergency Management Agency

### Overview

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

In FY 2018, there were 16 strategic performance measures used to assess FEMA's performance. In FY 2018, 56 percent of the measures met their target and 75 percent maintained or improved actual results compared to FY 2017.



### Mission Programs

The mission programs that deliver performance results for FEMA are:

- **Education, Training, and Exercises:** The Education, Training, and Exercises program comprises the U.S. Fire Administration, National Exercise Program and the National Training and Education Division, which includes the Emergency Management Institute and the Center for Domestic Preparedness. These entities provide emergency management, response and recovery training, and exercise coordination to improve the knowledge, skills, and abilities of federal and state, local, tribal, and territorial (SLTT) emergency management personnel.
- **Grants:** FEMA's Grants program leads the Federal Government's financial assistance to state and local jurisdictions

and regional authorities as they prepare for all hazards. The program provides grants to enhance jurisdictions' resiliency to man-made and other major disasters and to enhance their homeland security strategies.

- **Mitigation:** The Mitigation program works to strengthen investments in mitigation nationwide to reduce the Nation's vulnerability to natural disasters or other emergencies, and to facilitate adoption and enforcement of up-to-date design and construction practices through state and local building codes. Developing resilient capacity in communities prior to a disaster supports the development of a culture of preparedness. The program supports activities that result in sound risk management decisions by individuals, the private-sector, and public-sector entities by conducting three core activities: risk analysis, risk reduction, and insurance against flood risk. These areas work together to reduce the loss of life and property, to enable individuals to recover more rapidly from floods and other disasters, and to lessen the financial burden on taxpayers. These investments are implemented at the Headquarters and Regional levels to support communities in mitigation efforts.
- **National Flood Insurance Fund:** The National Flood Insurance Fund aims to reduce the impact of flooding on privately owned property by mapping areas of flood risk, providing flood insurance, encouraging communities to adopt and enforce sound floodplain management regulations, and paying claims. The program also provides technical assistance and monitors communities for compliance with the minimum National Flood Insurance Plan criteria. These actions reduce risk from

flooding, accelerate recovery efforts, and mitigate future flood losses.

- **Preparedness and Protection:** The Preparedness program works to prepare the Nation for disasters of all kinds. Preparedness includes the management and administrative support functions associated with training and national exercise programs. Protection carries out a mandated mission to provide executive agent leadership to guarantee the survival of an enduring constitutional government by ensuring continuity of government, continuity of operations, and national contingency programs.
- **Regional Operations:** The Regional Operations program includes the leadership, management, and mission support functions of the 10 FEMA regions across the Nation. The program works with communities to reduce the impacts of natural disasters; prepare families and individuals for all possible hazards; and support state, local, and tribal partners with technical assistance and grants for projects that aim to reduce risks, improve public safety, and protect the environment.
- **Response and Recovery (including the Disaster Relief Fund PPA):** The Response and Recovery program helps to ready the Nation for catastrophic disasters leveraging resources from various sources including the Disaster Relief Fund (DRF). This includes efforts to coordinate the core federal response capabilities used to save lives, and protect critical infrastructure in communities throughout the Nation that have been overwhelmed by the impact of a major disaster or an emergency. The program also takes the lead among federal agencies, state and local governments, and representatives of non-governmental organizations to support individuals and communities with the goal of reducing losses, improving

recovery operations, and promoting resilience. This program works with residents, emergency management practitioners, organizational and community leaders, and government officials to mature the National Disaster Recovery Framework, enhance logistics and resilient disaster communications, and improve the overall disaster survivor and grantee experience.

### **Summary of Progress**

**Progress:** The following progress updates were identified through the Strategic Review:

- The Center for Domestic Preparedness, the Emergency Management Institute, and the National Domestic Preparedness Consortium trained thousands of state, local, tribal, and territorial first responders and public officials.
- FEMA re-baselined the Threat & Hazard Identification and Risk Assessment (THIRA) and the Stakeholder Preparedness Review (SPR) to common capability targets, striving to improve their usefulness in documenting and closing gaps and demonstrating the impact of grant investments.
- To enhance the effectiveness of Regional Operations, agency leaders have begun to implement FEMA Integration Teams (FIT), temporarily embedding FEMA staff with interested state partners to provide ongoing technical assistance targeted at identified capability gaps.
- Lessons learned from prior-year hurricane and fire events focused agency leaders' attention on developing a scalable, capable incident workforce; a whole-community approach to provide life-sustaining commodities, equipment, and personnel; and a special emphasis on emergency communications as a key enabler for incident command and control.



- FEMA established an Executive Steering Committee to help centralize the management of the Agency's Preparedness, Mitigation, and Disaster Grants.

### Did you know?

In FY 2018, FEMA's grants, subsidies, and contributions were \$16.5 billion to address mitigation efforts and response to disasters.

- The Mitigation program deployed the Hazus Tsunami Model to calculate hazard and disaster impacts which provides information for risk mapping, analysis, and planning.

**Challenges and Risks:** The unprecedented effects of Atlantic hurricanes, West Coast wildfires, and widespread flooding during FY17 presented significant challenges that inform future planning and processes. The following challenges and risks were identified through the Strategic Review:

- Lack of a flexible and scalable incident workforce with the knowledge, skills, and abilities needed to respond to and recover from disasters impacted mobilization to support disaster survivors.

- The unprecedented volume of resource requests and the complexity to support multiple logistics efforts both on the mainland and outside the continental U.S. exposed gaps in logistics coordination.
- If communications are not resilient or are diminished during a catastrophic disaster, then coordination of assets to respond and recover will be hindered.
- Difficulties reported by SLTT partners with respect to navigating complex federal programs intended to assist in disaster recovery hampered efficient mission execution, delaying communities' recovery.
- Lack of prioritized investments in pre-disaster mitigation to prevent additional future losses, especially to infrastructure such as aging levees and dams.
- If the National Flood Insurance program is not effective in selling more flood insurance policies and property owners are not seeking private insurance to cover flood losses, then people will be reliant on individual disaster assistance programs.



## PrepTalks – New Perspectives for Emergency Managers

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

FEMA initiated a partnership to create PrepTalks with the nation's major emergency management organizations, including the International Association of

Emergency Managers, National Emergency Management Association, Naval Postgraduate School Center for Homeland Defense and Security, and the National Homeland Security Consortium. Together, we attract nationally recognized experts to record high quality video presentations for the emergency management community and the public to use anytime for free.

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

**Performance Results and Plan**

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
Man-made or Natural Incident Preparedness								
Percent of adults that took a preparedness action at their workplace, school, home or other community location in the past year								
---	---	---	---	91%	92%	92%	Retired Measure <sup>1</sup>	
Percent of adults that took multiple preparedness actions at their workplace, school, home or other community location in the past year								
---	---	---	---	---	New Measure <sup>2</sup>		48%	49%
Percent of adults that have set aside money for emergencies								
---	---	---	---	---	New Measure <sup>3</sup>		71%	75%
Percent of federal agencies ready to initialize continuity of essential functions and services in the event of a catastrophic disaster								
---	---	96.6%	99.0%	97.2%	98.5%	94.5% <sup>4</sup>	Retired Measure <sup>5</sup>	
Percent of states and territories with a Threat and Hazard Identification and Risk Assessment (THIRA) that meets current DHS guidance								
86%	71%	77%	86%	86%	100%	89% <sup>6</sup>	Retired Measure <sup>7</sup>	
Percent of states and territories that have achieved an intermediate or above proficiency to address their targets established through their THIRA								
---	---	---	66%	70%	70%	70%	Retired Measure <sup>8</sup>	
Percent of the U.S. population directly covered by FEMA connected radio transmission stations								
90%	90%	90%	90%	90%	90%	90%	Retired Measure <sup>9</sup>	
Percent of U.S. population covered by FEMA-connected radio stations with electromagnetic-pulse resilience								
---	---	---	---	---	New Measure <sup>10</sup>		50%	62%
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								
---	---	---	99.8%	99.9%	99.9%	99.8% <sup>11</sup>	99.9%	99.9%
Percent of U.S. population covered by a local-level authority authorized and registered to send alerts and warnings to the public using the Integrated Public Alert and Warning System (IPAWS)								
---	---	---	---	---	New Measure <sup>12</sup>		50%	62%

1 – FEMA is retiring this measure and implementing new measures to support FEMA’s implementation of national preparedness initiatives intended to engage the whole community and ultimately increase the nation’s preparedness.

2 – FEMA is proposing this new measure to communicate that multiple preparedness actions is a best practice.

3 – FEMA’s leadership has made it a priority to help people prepare for disasters by encouraging them to have increased financial preparedness for unexpected events.

4 – This performance measure reflects the number of Category I, II, III, and IV Federal Departments and Agencies (D/As) that acknowledged receipt of continuity readiness alerts and notification within four hours of issuance. For fiscal year 2018, the cumulative performance result was 94.5% and below the annual target. FEMA’s National Continuity Programs division continues to engage with D/As to determine why they do not respond to the test alert messages. FEMA continues to work with D/As to update their contact information to ensure accuracy should a real-world notification be required. The non-responders for this data call are not usually the same D/As from month to month. For FY 2019, FEMA plans to work with D/As to better

understand the barriers to responding to test alert messages in order to ensure greater participation.

5 – This measure is valuable internally as a piece of a larger readiness evaluation process; however, it is limited in its scope and is being removed from this publicly reported set.

6 – In support of the National Preparedness System component “Identifying and Assessing Risk,” FEMA determines the number of states and territories with risk assessments that meet DHS guidance. Jurisdictions that receive preparedness grant funding from FEMA must use the Threat and Hazard Identification and Risk Assessment (THIRA) to identify and assess risk and establish capability targets based upon their risks. In Fiscal Year 2018, 50 out of 56 states and territories completed a THIRA that meets all steps of the current DHS guidance, an increase of two states since 2017 and 10 states since 2014. States and territories had the most difficulty in meeting the following areas of the DHS guidance: including at least one estimated impact and desired outcome for each core capability; and, identifying resources required to achieve the capability targets. This measure is being retired for FY19 because FEMA is implementing a new Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness

## FY 2018-2020 Annual Performance Report

Review (SPR) and corresponding Comprehensive Preparedness Guide 201 methodology. Addressing stakeholder requests for a more intuitive approach to assessing capabilities, FEMA developed a new methodology that is more specific and measureable, using a set of standardized impacts and targets in language commonly used by emergency managers. In the third quarter of Fiscal Year (FY) 2018, FEMA's National Preparedness Assessment Division and Regional Offices rolled out the new methodology with extensive technical assistance across the country for implementation in FY 2019.

7, 8 – FEMA is changing the methodology behind the THIRA and therefore these measures are no longer applicable to the new approach. As the new baseline will not be set until Dec 2019, a new replacement measure cannot yet be recommended.

9 – FEMA is proposing a new measure to address new priorities in hardening the radio transmission systems.

10 – This measure is an improvement from the previous measure for it includes only those radio stations with electromagnetic pulse resilience which supports current actions to harden the radio transmission systems.

11 – The measure is the percent of time the Integrated Public Alert and Warning System (IPAWS) is available for use by federal, state, and local officials for disseminating emergency alerts via cellular phones as Wireless Emergency Alerts messages, radio and TV Emergency Alert System broadcasts, National Oceanic and Atmospheric Administration (NOAA) Weather Radio broadcasts, websites and social media applications. IPAWS operated with 18.47 hours of outage in Fiscal Year 2018. Outages resulted from Managed Trusted Internet Protocols, FEMA Enterprise Service Oriented Architecture system, and Virtual Private Network failures. FEMA is migrating IPAWS to a commercially hosted cloud infrastructure. The program began development and testing of a cloud infrastructure beginning in the fourth quarter of FY18, with full implementation planned in the second quarter of FY20. This migration will improve system reliability by removing dependencies on disparate systems and configuration management discrepancies for certain enterprise network components.

12 – FEMA is proposing a new measure to reflect our ability to send warnings across the relevant population during an emergency.

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
Man-Made or Natural Incident Investments								
Benefit to cost ratio of the hazard mitigation grants								
---	---	---	1.6	1.6	1.4	1.6	1.6	1.6
Number of properties covered with flood insurance (in millions)								
---	---	---	---	---	New Measure <sup>1</sup>		4.5	5.0
Percent of communities in high earthquake, flood, and wind-prone areas adopting disaster-resistant building codes								
57%	61%	63%	68%	67%	64%	67%	65%	66%
Percent of U.S. population (excluding territories) covered by planned mitigation strategies								
76.7%	79.6%	80.8%	81.0%	82.1%	85.0%	90%	85.0%	85.0%
Total national investment in mitigation (in billions)								
---	---	---	---	---	New Measure <sup>2</sup>		\$1.66	\$2.00

1 – This measure will reflect the priority to increase the number of properties covered with flood insurance.

2 – This measure will provide a broad national view of investments in mitigation efforts.

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
Man-Made or Natural Incident Response								
Average number of the incident staff to support small federally-declared disasters								
---	---	---	---	---	New Measure <sup>1</sup>		93	93
Average timeliness of the individual assistance awards of the Individuals and Households program (in days)								
---	---	---	---	---	New Measure <sup>2</sup>		11	9
Operational readiness rating of FEMA’s specialized incident workforce cadres								
---	---	---	61%	60%	80%	62% <sup>3</sup>	68% <sup>4</sup>	70%
Percent of critical federal response teams supported by voice, video, and data connectivity using a fully capable mobile emergency office vehicle								
---	---	---	---	---	New Measure <sup>5</sup>		81%	84%



# FY 2018-2020 Annual Performance Report

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
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								
100%	100%	100%	100%	100%	100%	100%	100%	100%
Percent of Incident Management Assistance Teams establishing joint federal and state response objectives within 18 hours								
100%	100%	100%	100%	100%	100%	100%	Retired Measure <sup>6</sup>	
Percent of incident management planned workforce currently on board								
---	---	---	---	71%	80%	75% <sup>7</sup>	Retired Measure <sup>8</sup>	
Percent of Public Assistance project obligations completed within targeted timeframes								
---	---	---	---	---	New Measure <sup>9</sup>		68%	72%
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								
---	---	---	99.0%	N/A <sup>10</sup>	95.0%	95.0%	95.0%	95.0%
Percent of recovery services through Individual Assistance delivered to disaster survivors gauging the quality of program services, supporting infrastructure, and customer satisfaction following a disaster								
94.5%	91.5%	96.9%	95.3%	95.4%	95.0%	78.3% <sup>11</sup>	Retired Measure <sup>12</sup>	
Percent of applicants satisfied with simplicity of the Individuals and Households Program								
---	---	---	---	---	New Measure <sup>13</sup>		81%	83%
Percent of recovery services through Public Assistance delivered to communities gauging the quality of program services, supporting infrastructure, and customer satisfaction following a disaster								
86.2%	90.9%	92.0%	90.0%	91.0%	93.0%	71.0% <sup>14</sup>	Retired Measure <sup>15</sup>	
Percent of applicants satisfied with simplicity of the Public Assistance process								
---	---	---	---	---	New Measure <sup>16</sup>		82%	84%

1 – This new measure will reflect the program's effort to work with local authorities/communities to build their capability to respond to disasters and over time decrease the amount of federal staff deployed to support disasters.

2 – This new measure will evaluate how quickly disaster survivors receive their first financial assistance allowing the program to assess the effectiveness of a critical, customer facing element.

3 – FEMA measures the Agency's overall operational readiness based on the Cadre Operational Readiness and Deployability (CORDS) Report, which provides Cadre readiness across staffing, equipping, and training metrics. FEMA remains focused the incident workforce as part of FEMA's 2018-2022 Strategic Plan. The Agency is building a scalable and capable incident workforce to ready the nation for catastrophic disasters. Overall force strength increased to 12,096 as the Agency continued to focus on hiring and on-boarding initiatives. As force strength increased, FEMA also qualified 483 more employees to improve the qualified force strength to 7,494. FEMA has continued efforts to align performed tasks with training objectives and revise courses and training materials to more closely support FEMA Qualification System core competencies. In the next fiscal year, FEMA will complete a force structure review and begin implementing the changes to improve the ability to meet force strength and qualification targets.

4 – FY19 target previously published as 80% in the

FY 17-19 Annual Performance Report was adjusted based on three years of past performance.

5 – This new measure captures the need for effective response to a catastrophic incident through the establishment of a communication system to support the response.

6 – This measure has repeatedly demonstrated performance at 100% and this has become a standard operating procedure and this measure is no longer needed.

7 – In FY18, FEMA's overall force strength increased to 12,096, while availability decreased due to increased deployment activity. FEMA is still limited in ability to hire some key members of the incident workforce - Incident Management Cadre of On-Call Response Employees (IM-COREs) due to budgetary constraints on the Disaster Readiness Support, which supports funding for non-deployed IM COREs, Incident Management Assistance Team members, and field leaders. In addition to potentially pursuing changes to staffing that would alleviate constraints on the Disaster Readiness Support budget, FEMA also continues its review of Incident Management (IM) Force Structure. In FY19, FEMA will revise the force structure numbers, which will provide a better understanding of required staffing needs to support disaster operations. FEMA will also work to establish force strength and qualification targets to meet force structure and improve operational readiness. Moreover,

FEMA remains focused on local hiring initiatives and staffing long-term recovery offices, which is directly related to recent events that do not have an impact on force structure but are still related to the Agency's readiness.

8 – Retiring since the program currently tracks this information as part of the composite measure "operational readiness rating of FEMA's specialized incident workforce cadres."

9 – This new measure will make visible how quickly Public Assistance funds are obligated which is a priority of the recovery process.

10 – The program was unable to report data in FY17. See the FY 17-19 Annual Performance Report for more information.

11 – The unprecedented size and scope of the 2017 Hurricanes impacted the IA program throughout FY18. From Hurricane Harvey in August 2017 through the end of FY18, 871,528 applicants received \$2.79 billion in housing assistance. In comparison, in FY17 up to Hurricane Harvey, 51,182 applicants received \$192 million in housing assistance. This large increase in volume, without a comparable increase of staff, resulted in each component of this measure not achieving their targets. The Housing Assistance within 60 days component was impacted the most with 71.6% of applicants receiving housing assistance within 60 days. The Disaster Case Management (DCM) Program was affected with 57% of the States/Territories receiving grants within 120 days compared to 100% in FY17. In addition, limited state/territory experience implementing a DCM program resulted in additional IA technical assistance, causing further delays. FEMA will continue to focus on improving the Individual Assistance (IA) program to ensure that FEMA meets the needs of survivors. In support of the FEMA Strategic Plan, several changes will be made to the IA program in FY19. Examples of changes to be implemented include: the development of a surge playbook to increase contract center staffing during large disasters; replace stand-alone policies with a survivor centric comprehensive document; and develop technology enhancements for the registration and intake process. These changes are intended to improve FEMA's ability to make IA awards in a more accurate and timely manner, while also increasing survivor satisfaction with FEMA's processes.

12 – Retiring as the measure no longer reflects targeted improvements to the strategic vision of the Individual Assistance program.

13 – This new measure gauges disaster survivor and grantee satisfaction of the simplicity of the Individuals and Households program and is directly related to an objective in the new FEMA strategic plan. The insight derived from survey results will help drive improvements for the program.

14 – The Public Assistance (PA) measure assesses the program's ability to delivery initial information and services to communities in a timely manner and in accordance with program regulations. In FY18, the PA program measure achieved a score of 71% due to the performance of the "Request for Public Assistance (RPA) to Kickoff Meeting (KOM) within 21 Days" portion of this composite measure. Only 42% of applicants received a KOM within the set parameter of 21 days; however 65% received a KOM within 30 days and 97% within the fiscal year. FEMA is strategically shifting focus away from this initial timeliness goal in order to ensure applicants have time to identify the scope of their damages and conduct more substantive discussions at these initial meetings to expedite recovery. Learning from the implementation of this measure, FEMA recognizes the need to set different time parameters based on key programmatic criteria such as size and scope of the PA project instead of holding all projects to the same measure. For FY19, FEMA will set timeliness parameters using criteria to group projects by their size and scope and apply review processes that complement the scale of the application. Through this targeted approach, FEMA hopes to see an increase of timeliness of awards as well as an increase in customer satisfaction with the simplicity of the new process.

15 – Retiring as the measure no longer reflects targeted improvements to the strategic vision of the Public Assistance program.

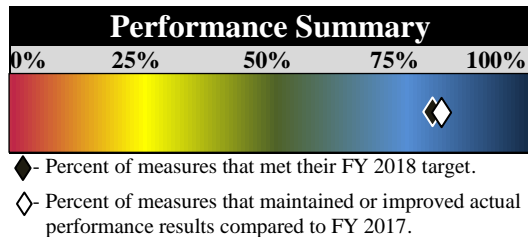
16 – This new measure gauges disaster survivor and grantee satisfaction of the simplicity of the Public Assistance process and is directly related to an objective in the new FEMA strategic plan. The insight derived from survey results will help drive improvements for the program.

## Immigration and Customs Enforcement

### Overview

[U.S. Immigration and Customs Enforcement \(ICE\)](#) is the principal investigative arm of DHS and the second largest investigative agency in the Federal Government. ICE's primary mission is to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration. ICE was created in 2003 through a merger of the investigative and interior enforcement elements of the former U.S. Customs Service and the Immigration and Naturalization Service. ICE now has more than 20,000 employees in more than 400 offices in the United States and 46 foreign countries.

In FY 2018, there were six strategic performance measures used to assess ICE's efforts. In FY 2018, 83 percent of the measures met their target and 83 percent maintained or improved actual results compared to FY 2017.



### Mission Programs

The mission programs that deliver performance results for ICE are:

- **Enforcement and Removal Operations (ERO):** ERO enforces the Nation's immigration laws by identifying and apprehending illegal immigrants, detaining those individuals pending final determination of removability, and removing aliens from the United States. This program carries out its mission through a range of initiatives and activities that focus on

identifying and prioritizing the removal of recent illegal border crossers and individuals who pose a threat to national security or public safety, including, but not limited to, fugitive aliens and aliens convicted of crimes.

- **Homeland Security Investigations (HSI):** The HSI program conducts criminal investigations to protect the United States against terrorism and criminal organizations that threaten public safety and national security. HSI combats transnational criminal enterprises that seek to exploit America's legitimate trade, travel, and financial systems. This program upholds and enforces America's customs and immigration laws at and beyond our Nation's borders.

#### Did you know?

Trade Enforcement Coordination Centers (TECC) merge HSI and CBP resources in major metropolitan areas to investigate shipments threatening national security and public health and safety.

- **Office of the Principal Legal Advisor (OPLA):** OPLA provides a full-range of legal services to ICE. The program provides advice and counsel to ICE personnel on their law enforcement authorities and legal liabilities. The program represents ICE before multiple administrative venues and supports the Department of Justice in the prosecution of ICE cases and in the defense of civil cases against ICE. This program serves as the exclusive DHS representative in removal proceedings before the Department of Justice Executive Office for Immigration Review.



## Summary of Progress

**Progress:** The following progress updates were identified through the Strategic Review:

- Expanded efforts to address all illegal immigrants encountered, prioritized efforts on known threats to national security and public safety, and issued more detainer requests.

### Did you know?

In FY 2018, a six-week nationwide gang operation led by ICE HSI concluded with 1,378 arrests across the United States—the largest gang takedown conducted by HSI to date.

- Increased cooperation with the Department of State to improve repatriation.
- Expanded the 287(g) program to serve as a force multiplier through interaction with state and local law enforcement.
- Integrated intelligence and operations through an interagency assessment and the use of various fusion centers within DHS, the Department of Justice, and the Drug Enforcement Administration.
- Participated in the establishment of the National Vetting Center as a mission center focused on transnational organized crime.
- Doubled criminal prosecutions during FY18 through the Special Assistant U.S Attorney program.
- Defended a greater number of federal lawsuits to protect DHS's enforcement authority relating to family detention, post order bond eligibility and removal authority.
- Pursued a record number of appeals of immigration judge orders in support of immigration enforcement priorities.

**Challenges and Risks:** The following challenges and risks were identified through the Strategic Review:

- Outdated laws and judicial decisions that have occurred over the past few years have curtailed the ability to enforce immigrations laws and maintain and manage detention and removal resources.
- Limitations in other Federal Government Agencies, specifically the Department of Justice's capacity to receive and process illegal immigration cases, are impacting the removal of illegal immigrants residing in the interior of the country.
- If the non-detained docket is not properly managed and continues to grow, then there is a risk that the program will be unable to properly prioritize case management, resulting in delays in enforcement outcomes.
- If cities do not honor ICE detainees, then the effectiveness of arresting interior illegal immigrants is diminished.
- If the Department does not take a holistic approach to combating transnational organized crime, then our Nation will be inadequately prepared to properly identify or prioritize the threat, maximize the impact of the resources we have to counter it, and execute operations.
- If the number of federal cases and class action lawsuits continues at current levels or increases, then the need to recruit, hire, and train new attorneys who specialize in federal litigation and have experience in immigration law increases.



## Enforcement and Removal Operations (ERO)

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

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

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

### Performance Results and Plan

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
Transnational Criminal Organizations								
Percent of significant Homeland Security Investigation cases that result in a disruption or dismantlement								
---	---	---	---	22.9%	15.8%	18.0%	15.9%	16.1%

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
Immigration Enforcement								
Average length of stay in detention of all convicted criminal aliens prior to removal from the United States (in days)								
33.5	37.5	40.3	43.9	48.8	≤ 44.0	47.4 <sup>1</sup>	≤ 44.0	≤ 44.0
Number of convicted criminal illegal immigrants who were returned or were removed from the U.S.								
216,810	177,960	139,368	138,669	127,699	126,000	145,262	151,000	151,000
Number of enforcement-related actions against employers that violate immigration-related employment laws								
4,743	2,191	1,928	1,880	1,730	1,854	6,398 <sup>2</sup>	1,854	1,854
Percent of detention facilities found in compliance with the national detention standards by receiving a final acceptable inspection rating								
100%	100%	100%	100%	100%	100%	100% <sup>3</sup>	100%	100%
Percent of final orders that result in order of removals from the United States								
---	---	---	---	---	New Measure <sup>4</sup>		65%	65%
Total number of illegal immigrants who were returned or removed from the U.S.								
---	---	---	---	---	210,000	256,085	238,000	238,000

1 – Average Length of Stay (ALOS) is impacted by many factors both internal and external to ICE and the detained Average Daily Population (ADP) has risen steadily over the past two fiscal years primarily due to a backlog in adjudication within the judicial system. Additionally, continuing to reduce the number of recalcitrant countries would increase the number of illegal immigrants that could be returned to their country of origin, which would both decrease the ADP

and ALOS. Outside of ICE's control is Executive Office for Immigration Review (EOIR) case processing times. Case type and case backlogs at EOIR are important factors and varies depending on each alien's country of origin. The United States' relationship with other countries and the willingness to accept their own citizens greatly influences the ability of ERO to effectuate removal. Also, cooperating with local embassies, ICE could expedite travel documents for

detained individuals which would accelerate their processing.

2 - HSI greatly surpassed their target for FY 2018. During FY 2018, HSI developed a comprehensive worksite enforcement strategy and conducted a two-part nationwide Notices of Inspection (NOI) surge operation, during which more than 5,000 NOIs were served on businesses throughout the U.S.

3 - ICE inspections during FY 2018 resulted in 100% compliance; however, the DHS Inspector General (IG) conducted a separate [review](#) of the Adelanto ICE Processing Center and found issues and made

recommendations. ICE concurs with the IG's findings and is implementing corrective actions to ensure the Adelanto ICE Processing Center meets required detention standards. ICE reported that it will complete a full inspection of the Adelanto facility and a Special Assessment Review to ensure concerns identified in this report are fully addressed.

4 – This new measure captures the rate at which the Office of the Principal Legal Advisor attorneys secure an enforcement consequence for an illegal alien's violations heard before the Executive Office for Immigration Review.

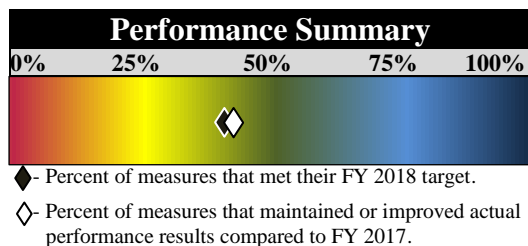
## Transportation Security Administration

### Overview

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

The attacks on September 11, 2001 prompted the creation of TSA, which was charged with the mission to mitigate and prevent similar attacks from happening in the future. Driven by a desire to help our nation, tens of thousands of people joined TSA and committed themselves to strengthening the security of our transportation systems while ensuring the freedom of movement for people and commerce. Today, Transportation Security Officers effectively screen millions of passengers and bags daily, and growing, at nearly 440 airports across the country. TSA is constantly looking for ways to enhance aviation security and improve the passenger experience.

In FY 2018, there were 11 strategic performance measures used to assess TSA's efforts. In FY 2018, 45 percent of the measures met their target and 45 percent maintained or improved actual results compared to FY 2017.



### Mission Programs

The mission programs that deliver performance results for TSA are:

- **Aviation Screening Operations:** The Aviation Screening Operations program applies intelligence-driven, risk-based, layered passenger and baggage screening procedures and

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

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

#### Did you know?

The TSA Freedom of Information Act (FOIA) Branch launched a new version of the electronic FOIA Reading Room in May 2017. Since then, TSA has posted 55,561 pages covering multiple topics. Go to <https://www.tsa.gov/foia/readingroom> to find information on TSA.



## Summary of Progress

**Progress:** The following progress updates were identified through the Strategic Review:

- Enhanced passenger experience occurred at checkpoints through the combined use of trust-based programs (e.g., TSA Pre✓®) and new screening technologies (e.g., Credential Authentication Technology).
- Improved explosive detection capabilities via roll-out of new technology such as Computed Tomography.
- Deployed advanced technologies (e.g., Automated Screening Lanes) and process improvements (e.g., Enhanced Accessible Property Screening) to improve checkpoint security effectiveness.
- Implemented new Federal Air Marshall (FAM) concept of operations to better align flight deployment with passenger risk.
- Implemented the Risk Mitigation Activities for Surface Transportation to better focus time and resources on high-risk surface entities and locations.
- Made process improvements to support recurrent vetting of approximately 20 million credential holders that work within the transportation sector.
- Improved international transportation security by issuing enhanced security requirements and conducting more than more than one hundred airport

assessments and more than 2,000 air carrier inspections.

- TSA worked with 100 percent of last-point-of-departure airports to raise the global aviation security baseline and address security vulnerabilities and gaps.
- Conducted nearly three hundred voluntary assessments for: pipeline; mass transit; bus entities; school districts; and issued guidelines that highlight key vulnerabilities and the means to resolve them.

**Challenges and Risks:** The following challenges and risks were identified through the Strategic Review:

- Continuous improvements to anticipate, identify, analyze, or respond to evolving threats are needed to reduce the likelihood of a terrorist attack on the transportation sectors and to outmatch the evolving threat.
- Improvements are needed to adapt aviation screening security procedures to match emerging threats to reduce the likelihood of terrorist attacks on aviation.
- Improvements are needed to address insider threats to lessen the vulnerability of an attack perpetuated or enabled by transportation insiders.
- Specific improvements need to be made to airport perimeter and access security, passenger rail operations, and identity vetting.



### Improved Intelligence Sharing with Modest Resources

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

TSA's Intelligence & Analysis-led ADIAC team formed a new TSA institution relevant to aviation private sector partners with the development of a full-time aviation industry-government threat intelligence sharing capability that has materially enhanced partner sharing and collaboration. ADIAC industry members are noticing the increased

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

### Performance Results and Plan

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
<b>Transportation Security</b>								
Average number of days for DHS Traveler Redress Inquiry Program (TRIP) redress requests to be closed								
52	62	50	44	50	< 55	37	< 55	< 55
Percent of air carriers operating from domestic airports in compliance with leading security indicators								
98.0%	98.0%	98.0%	98.0%	97.7%	100%	87.0% <sup>1</sup>	100%	100%
Percent of attended interchanges of rail cars containing rail security sensitive materials transiting into or through high-threat urban areas								
---	---	---	---	---	95%	99%	95%	95%
Percent of daily passengers receiving expedited physical screening based on assessed low risk								
---	---	---	46%	55%	50%	54%	50%	50%
Percent of domestic cargo audits that meet screening standards								
---	---	---	98.0%	97.7%	97%	95% <sup>2</sup>	98%	98%
Percent of foreign last point of departure (LPD) airports that take action to address identified vulnerabilities								
---	---	---	---	---	70%	57% <sup>3</sup>	70%	70%
Percent of international cargo audits that meet screening standards								
---	---	---	97.0%	97.6%	97%	88% <sup>4</sup>	98%	98%
Percent of overall compliance of domestic airports with established aviation security indicators								
94.4%	94.0%	95.0%	93.0%	93.9%	100%	91% <sup>5</sup>	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								
69%	78%	80%	71%	74%	77%	67% <sup>6</sup>	79%	81%
Percent of passenger data submissions that successfully undergo Secure Flight watch list matching								
---	---	---	---	100%	100%	100%	100%	100%
Percent of TSA regulated entities inspected per fiscal year by transportation security inspectors								
---	---	---	---	---	90%	98%	90%	90%

1, 4, 5 – Assessing airports and airline vulnerabilities is part of an overall risk reduction process. Compliance with established key security indicators demonstrates the airports and airlines' commitment to ensuring the

safety of the traveling public. While most airports and airlines are diligent in meeting these standards, some are less so due to deficiencies in understanding procedural knowledge and program requirements. The

Security Operations' Compliance office, in conjunction with Global Strategies and Security Policy and Industry Engagement offices, continue to collaborate with both airport and airline partners to share aviation security best practices and offer guidance on improving their security posture.

2 - This measure assesses the percentage rate of domestic audits that meet the screening standards set forth in their standard security program. Due to the nature of the standards there will inherently be violations for a myriad of issues ranging from comprehension of screening requirements to willfully disregard of procedures. The Security Operations' Compliance office, in conjunction with Global Strategies and Security Policy and Industry Engagement offices, continue to collaborate with both airport and airline partners to share aviation security best practices and offer guidance on improving their security posture.

3 – TSA identifies vulnerabilities based on requirements set forth by the International Civil Aviation Organization (ICAO). TSA also identifies best practices beyond the ICAO requirements, in which case, TSA has limited authority to enforce mitigation activities. Through stakeholder engagement and partnerships, TSA seeks to maximize influence regarding efforts to mitigate risk. TSA continues to build influential partnerships as part of ongoing efforts to mitigate vulnerabilities and strengthen the aviation security posture.

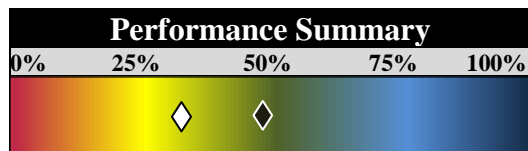
6 – As of the end on FY 2108, 37 of 55 Baseline Assessments for Security Enhancement on Mass Transit Systems have been completed, narrowly missing the target. Resource constraints have limited the ability of the transit systems to maintain or improve their security postures. TSA field personnel have been working with the transit systems by providing best practices and other guidance material to help them improve their respective security postures.

## U.S. Citizenship and Immigration Services

### Overview

[U.S. Citizenship and Immigration Services \(USCIS\)](#) administers the nation's lawful immigration system, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting Americans, securing the homeland, and honoring our values. USCIS is the government agency that oversees lawful immigration to the United States and is funded primarily by immigration and naturalization benefit fees charged to applicants, petitioners, and requestors. USCIS processes more than 8 million citizenship and immigration benefit requests.

In FY 2018, there were six strategic performance measures used to assess USCIS' efforts. In FY 2018, 50 percent of the measures met their target and 33 percent maintained or improved actual results compared to FY 2017.



◆ - Percent of measures that met their FY 2018 target.

◆ - Percent of measures that maintained or improved actual performance results compared to FY 2017.

### Mission Programs

The mission programs that deliver performance results for USCIS are:

- Employment Status Verification:** The electronic employment eligibility verification E-Verify program enables enrolled employers to quickly and easily confirm the work authorization of their newly hired employees. E-Verify is an internet-based system that compares information from an employee's Form I-9, Employment Eligibility Verification, to data available to DHS to confirm employment eligibility within seconds.

- Fraud Prevention and Detection (part of the Fraud Prevention and Detection Account PPA):** The Fraud Prevention and Detection program (fee account) supports activities related to preventing and detecting fraud in the delivery of all immigration benefit types. The program leads DHS efforts to identify threats to national security and public safety, detect and combat immigration benefit fraud, and remove systematic and other vulnerabilities.

#### Did you know?

The USCIS Fraud Detection and National Security (FDNS) Directorate helps fight abuse of the immigration system. FDNS bridges the gap between the immigration adjudication process, law enforcement, and intelligence community. Each day, FDNS officers and analysts work tirelessly to detect fraud and identify security risks.

- Immigration Services (part of the Immigration Examinations Fee Account PPA and the H-1B Nonimmigrant Petitioner Account):** The Immigration Services program (fee account) supports and promotes lawful immigration by processing benefit requests, so that only those eligible for immigration benefits are approved. This includes processing refugee and asylum applications as well as providing assimilation services for lawful immigrants.

### Summary of Progress

**Progress:** The following progress updates were identified through the Strategic Review:

- A multi-year training program was initiated to enhance interviewing skills and increase capacity.



- New methodologies piloted to examine possibilities to realign field office workloads to reduce backlog.
- E-Verify continued to be very successful in matching employees to their government records with nearly 100 percent accuracy.
- Improvements in E-Verify reduced abandoned enrollments by nearly 20 percent and decreased average enrollment time for client companies by nearly 50 percent.
- Established a centralized security check/vetting center to improve timeliness of processing asylum cases.
- Established the Targeted Site Visit and Verification Program for certain nonimmigrant worker visa classifications.
- Operationalized Phase 1 of Continuous Immigration Vetting of benefit applications to screen naturalization applicant data against the Automated Targeting System.

**Challenges and Risks:** The following challenges and risks were identified through the Strategic Review:

- Immigration policies require new and more complex adjudication processes and information technology needs to keep pace to mitigate these complexities.
- Information technology improvements need to be realized to avoid continued delays in administering immigration benefits and to improve productivity.
- If key data providers to the Verification Information System experience significant operational or infrastructure issues, then system availability and performance may be negatively impacted.
- If the Fraud Prevention and Detection program is unable to recruit, timely train, and retain a qualified workforce, then the ability to uphold the security and integrity of the legal immigration system may become compromised.



### USCIS Targets H-1B Visa Fraud and Abuse

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

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

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

**Performance Results and Plan**

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
<b>Immigration Benefits</b>								
Average of processing cycle time (in months) for adjustment of status to permanent resident applications (I-485)								
4.7	6.0	6.4	6.9	9.3	≤ 4.0	11.5 <sup>1</sup>	≤ 4.0	≤ 4.0
Average of processing cycle time (in months) for naturalization applications (N-400)								
4.7	5.5	5.0	5.8	8.6	≤ 5.0	10.4 <sup>2</sup>	≤ 5.0	≤ 5.0
Percent of applications for citizenship and immigration benefits not approved following a potential finding of fraud								
---	---	---	91.3%	91.7%	90%	92.2%	90%	90%
Percent of respondents satisfied with the citizenship and immigration-related support received from the U.S. Citizenship and Immigration Services Contact Center <sup>3</sup>								
87%	86%	88%	85%	84%	85%	83% <sup>4</sup>	85%	85%
Percent of students enrolled in classes under the Citizenship and Integration Grant Program that show educational gains								
---	---	75%	75%	75%	80%	80%	80%	80%
Percent of workers determined to be "Employment Authorized" after an initial mismatch								
0.22%	0.19%	0.17%	0.16%	0.15%	≤ 0.60%	0.16%	≤ 0.50%	≤ 0.40%

1 – While the I-485 cycle time improved during the last half of the fiscal year, the target was nonetheless not met for FY 2018. USCIS expects receipt volumes to continue to be higher than projected. Although the cycle time is above the target, USCIS maintained the accuracy of I-485 decisions. During FY 2019, USCIS will continue to balance workloads, seek process changes that result in increased workload capacity, and leverage overtime and other scheduling options to improve cycle time. In addition, USCIS will execute new hiring strategies and implement additional workplace flexibilities to mitigate hiring and retention issues which have negatively impacted cycle times.

2 – USCIS adjudicated more cases during FY 2018 than any of the previous four fiscal years. The increase in volume was also coupled with the N-400 form becoming more complex, including the addition of 13 new questions on barring naturalization that must be asked and reviewed, which has caused individual adjudications to take longer. USCIS continues to invest in developing process efficiencies and will begin to redirect some staff away from information service

functions to handle case adjudications workload instead, thus increasing production capacity. Although the cycle time is above the target, USCIS has maintained the accuracy of N-400 decisions. Despite the expansion of more than 10 field offices and the opening of three new field offices over the past two years, USCIS continues to face space and related capacity challenges, which combined with the continued high workload demands, will continue to negatively impact cycle time.

3 - Name change from *Percent of customers satisfied with the citizenship and immigration-related support received from the National Customer Service Center* to align with current Administration direction.

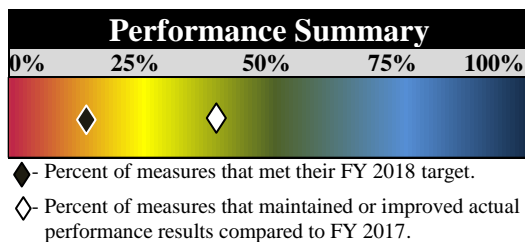
4 – The decrease in respondent satisfaction percentage can primarily be attributed to a transition in vendors for the Tier 1 contract that occurred during last quarter of FY18. With the contract transition and system training completed, along with improved quality of information at Tier 1, USCIS expects respondent satisfaction scores to improve in FY 2019.

## U.S. Coast Guard

### Overview

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

In FY 2018, there were seven strategic performance measures used to assess USCG's efforts. In FY 2018, 14 percent of the measures met their target and 43 percent maintained or improved actual results compared to FY 2017.



### Mission Programs

The mission programs that deliver performance results for USCG are:

- Maritime Law Enforcement:** The Maritime Law Enforcement program preserves America's jurisdictional rights within our maritime borders. The Coast Guard is the lead federal maritime law enforcement agency for enforcing national and international law on the high seas, outer continental shelf, and inward from the U.S. Exclusive Economic Zone to inland navigable waters, including the Great Lakes. The following statutory missions contribute to the Coast Guard's Maritime Law Enforcement program: Drug Interdiction; Migrant

Interdiction; Living Marine Resources; and Other Law Enforcement.

- Maritime Prevention:** The Maritime Prevention program mitigates the risk of human casualties and property losses, minimizes security risks, and protects the marine environment. The following statutory missions contribute to the Coast Guard's Maritime Prevention program: Ports, Waterways, and Coastal Security; Marine Safety; and Marine Environmental Protection.
- Maritime Response:** The Maritime Response program mitigates the consequences of marine casualties and disastrous events. The Coast Guard minimizes loss of life, injury, and property loss by searching for and rescuing persons in distress in the maritime environment. Coast Guard preparedness efforts ensure incident response and recovery resources are fully ready and capable to minimize impact of disasters to people, the environment, and the economy. The following statutory missions contribute to the Coast Guard's Maritime Response program: Search and Rescue and Marine Environmental Protection.

#### Did you know?

The U.S. Coast Guard has bi-lateral agreements with more than 40 nations, including Canada, Mexico, and Russia.

These agreements enable rapid coordination with international partners across a wide spectrum of operational activities such as drug interdiction and oil spill response.

- Maritime Security Operations:** The Maritime Security Operations program encompasses activities to detect, deter, prevent, disrupt, and recover from terrorist attacks and other criminal acts

in the maritime domain. It includes the execution of antiterrorism, response, and select recovery operations. This program conducts the operational element of the Coast Guard's Ports, Waterways, and Coastal Security mission and complements the other two elements: the establishment and oversight of maritime security regimes, and maritime domain awareness.

- **Maritime Transportation System Management:** The Maritime Transportation System Management program ensures a safe, secure, efficient, and environmentally sound waterways system. The U.S. Coast Guard minimizes disruptions to maritime commerce by assessing and mitigating risks to safe navigation and by providing waterways restoration capabilities after extreme weather events, marine accidents, or terrorist incidents. The Coast Guard works in concert with other federal agencies, state and local governments, marine industries, maritime associations, and the international community to optimize balanced use of the Nation's Maritime Transportation System. The following statutory missions contribute to the Coast Guard's Maritime Transportation System Management program: Aids to Navigation and Ice Operations.

### ***Summary of Progress***

***Progress:*** The following progress updates were identified through the Strategic Review:

- Implementation of USCG's Western Hemisphere strategy has more than doubled the number of drug smugglers apprehended since 2014, and nearly tripled the number of cases referred for federal prosecution.
- Advanced maritime safety by conducting nearly 40,000 commercial

vessel inspections and roughly 16,000 marine facility inspections.

- Identified and promoted best practices by conducting more than 3,000 marine casualty investigations and collaborated with the National Transportation Safety Board in response to dozens of major marine casualties, and supporting prevention of similar future incidents in the future.
- The Maritime Response mission program reported saving more than three-quarters of all people identified in imminent danger in the maritime environment, in line with historical performance.
- USCG achieved 89-percent success in keeping high-priority waterways in the Great Lakes and Eastern Seaboard regions open to navigation during an unusually hard-hitting ice season along the East Coast.
- In further support of maritime commerce, USCG met the expectation of keeping aids to navigation available more than 97.5% of the time.
- USCG's domestic icebreaking activities facilitated movement of cargoes valued at more than \$1.5 trillion.
- Maturation of USCG's Risk-Based Maritime Security and Operations Tool has allowed more efficient and effective deployment of assets.
- USCG examined potential operational gaps including threat detection/assessment; defeating waterborne attacks; training operators; planning for a full scope of scenarios; and Maritime Security and Operations platform capability.

***Challenges and Risks:*** The following challenges and risks were identified through the Strategic Review:



- If the flow of illicit narcotics trafficking continues to rise, then the ability to secure borders and approaches decreases.
- TCOs continue to leverage new and existing technologies increasing the risk to U.S. maritime borders, maritime infrastructure, and navigable waterway security.
- Information networks have permeated critical maritime infrastructure, requiring sustained focus on improving the cybersecurity posture.
- The Maritime Response program must maintain organizational capacity and force structure for steady-state, as well as major emergency response and contingency operations.
- USCG must recapitalize aging surface and aviation assets, as well as shore and information technology infrastructure, which improve operational readiness.



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

Recovery efforts continue in response to Hurricanes Harvey, Irma, and Maria and required a complex approach to managing the catastrophic impacts of several major hurricane landfalls in Texas, Florida, U.S. Virgin Islands, and Puerto Rico. The Nationally Declared Disasters were allocated \$156 million for pollution response. The Coast Guard led the response and directed response teams in the affected areas to conduct rapid oil and hazardous material assessments after the storms and provided direct federal assistance to Texas, Florida, Puerto Rico, and the U.S. Virgin Islands. Using the Federal On-Scene Coordinator authority to mitigate hazards, the Coast Guard consulted with federal, state, local, tribal, and

territorial governments to ensure sensitive environmental, cultural, and historical sites, as well as endangered species were protected. 4,215 vessels and related pollutants were removed from the environment over the course of eight months.

### Performance Results and Plan

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
<b>Border Operations</b>								
Migrant interdiction effectiveness in the maritime environment								
---	---	74.8%	79.3%	83.0%	75.0%	72.0% <sup>1</sup>	75.0%	75.0%

1 – This measure reports the percent of detected undocumented migrants of all nationalities who were interdicted by the U.S. Coast Guard and partners via maritime routes. The cumulative migrant interdiction effectiveness for FY 2018 at 72% decreased significantly from FY 2017. The Coast Guard Office Maritime Law Enforcement continues to analyze this performance measure to leverage meaningful policy changes to improve the number of migrants interdicted within the maritime domain. This measure currently includes operations of not only the Coast Guard but also partner agencies and nations that have shared interest in the maritime migration mission. As a result,

considerable effort is being made to improve operations and strategic planning. For example, CG-MLE is continuing to partner with other DHS agencies toward continuing a unified effort in maritime migrant interdiction. Additionally, foreign nations have continued to make a strong effort in the maritime domain, increasing total migrant interdictions in the maritime domain in FY 2018. The Coast Guard anticipates a continuing partnership in effort to increase the overall number of interdictions of migrants in the maritime domain in future years.

# FY 2018-2020 Annual Performance Report

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
<b>Man-Made or Natural Incident Response</b>								
Percent of people in imminent danger saved in the maritime environment								
79.0%	79.0%	80.0%	79.4%	78.8%	80.0%	78.0% <sup>1</sup>	80.0%	80.0%
Three-year average number of serious marine incidents								
---	---	696	688	684	≤ 698	705 <sup>2</sup>	≤ 689 <sup>3</sup>	≤ 644

1 – This is a measure of the percent of people who were in imminent danger on the oceans and other waterways and whose lives were saved by U.S. Coast Guard. Per the U.S. Coast Guard Addendum to the U.S. National Search and Rescue Supplement to the International and Aeronautical Maritime Search and Rescue Manual, this performance measure excludes cases which had greater than 10 lives at risk. The U.S. Coast Guard Office of Search and Rescue Policy continues to analyze this performance measure to leverage meaningful policy changes to improve the number of lives saved within the maritime domain. This measure currently includes maritime deaths that occurred prior to Coast Guard notification. As a result, considerable effort is being made to improve notifications of distress. For example, the USCG Office of Search and Rescue (CG-SAR) is partnering with the National Emergency Number Association to strengthen coordination and understanding between public service answering points and the Coast Guard. Additionally, the recent Cospas-Sarsat implementation of Medium Earth Orbiting Search and Rescue satellites and the USCG continued advocacy for the International Civil Aviation Organization (ICAO) Global Aeronautical Distress and Safety System will provide quicker notification of persons in distress, enhance the

ability to locate the distress event, and get Search and Rescue resources on-scene faster to render assistance. 2 – The three-year average number of serious marine incidents (SMI) did not meet the FY 2018 target. There were 500 U.S. flagged commercial vessels involved in an SMI during FY 2018. Of the 6,176 inspected passenger vessels (largest group of the entire population), only 2.1% were involved in an SMI. SMIs 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. While results did not meet the target, they do fall in line with expected parameters. Significantly, USCG expects this average to fall after a change in reporting criteria for a serious marine incident, which now better reflect a realistic cost structure. Additionally, full implementation for the regulation of Towboat safety and the enhancements to electronic navigation will only further reduce the likelihood of a serious marine incident. 3 – FY19 target previously published as ≤ 698 in the FY 17-19 Annual Performance Report was adjusted based on prior results and future projections factoring a 3-year average.

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
<b>Transportation Security</b>								
Number of breaches at high risk maritime facilities								
---	---	---	---	---	≤ 235	320 <sup>1</sup>	≤ 307 <sup>2</sup>	≤ 307

1 – This measure reports the number of breaches of security incidents at facilities subject to Maritime Transportation Safety Act where no transportation security incident occurred, but established security measures were circumvented, eluded, or violated. The increase is primarily attributed to a policy letter change that occurred in December 2016, clarifying what instances should be classified as breaches of security

required to be reported to the U.S. Coast Guard. No change in procedures/operations are planned going forward. 2 – FY19 target previously published as ≤ 219 in the FY 17-19 Annual Performance Report was adjusted based on prior results and future projections factoring a 3-year average.

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
<b>Waterways and Maritime Resources</b>								
Availability of maritime navigation aids								
98.2%	98.2%	97.7%	97.7%	97.5%	97.5%	97.1% <sup>1</sup>	97.5%	97.5%

# FY 2018-2020 Annual Performance Report

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
Fishing regulation compliance rate								
98.1%	97.5%	97.1%	96.8%	97.1%	97.0%	97.8%	97.0%	97.0%
Interdiction rate of foreign fishing vessels violating U.S. waters								
---	---	---	---	---	18.0%	31.3%	18.0%	18.0%

1 – The primary factor or the decline in the availability of aids to navigation is due to repairs to aids as a result of the 2017 Hurricanes Harvey, Irma, and Maria coupled with the late-2018 aid damage due to Hurricane Florence. This correlates with observed

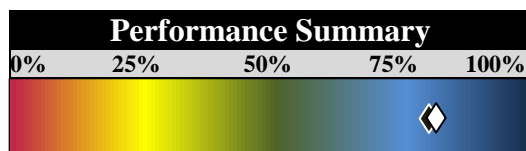
availability in the Mid Atlantic (96.9%), the Southeastern U.S. & Puerto Rico (96.2%), and the Gulf Coast (95.4%) districts. The U.S. Coast Guard is prioritizing ongoing efforts to repair aids to navigation and expects marked improvement in FY 2019.

## U.S. Secret Service

### Overview

[U.S. Secret Service \(USSS\)](#) safeguards the Nation's financial infrastructure and payment systems to preserve the integrity of the economy, and protects national leaders, visiting heads of state and government, designated sites, and National Special Security Events (NSSE). The USSS has grown from a small bureau staffed by a few operatives in 1865, to a law enforcement organization of more than 7,000 employees worldwide. Today, the USSS fights crime on a global scale through its field offices located in the United States, Canada, Mexico, South America, Europe, Africa and Asia. The agency works closely with local, state, and federal law enforcement organizations. These entities are valued partners of the USSS, and they are integral to the agency's investigative and protective endeavors.

In FY 2018, there were 11 strategic performance measures used to assess USSS's efforts. In FY 2018, 82 percent of the measures met their target and 82 percent maintained or improved actual results compared to FY 2017.



◆ - Percent of measures that met their FY 2018 target.  
 ◇ - Percent of measures that maintained or improved actual performance results compared to FY 2017.

### Mission Programs

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

- **Protective Operations:** The Protective Operations program protects the President and Vice President and their families, former Presidents and their spouses, visiting heads of State and Government, and other designated individuals. It also secures the White

House Complex, Vice President's Residence, and other designated places; and designs, coordinates, and implements operational security plans for designated National Special Security Events. The program investigates, evaluates, disseminates, and maintains information concerning known, potential, or perceived threats to protectees, locations, and National Special Security Events. The program is staffed by Special Agents, Uniformed Division Officers, and administrative, professional, and technical personnel that work closely with the military and with federal, state, county, local, and international law enforcement organizations to ensure mission success. This enables the Department to facilitate continuity of government and overall homeland security.

### Did you know?

The Secret Service provides free computer forensic training at the National Computer Forensics Institute (NCFI) to over 1,000 individuals each year from local, state, and federal law enforcement agencies nationwide. Students are also provided critical tools such as hardware, software, and licenses necessary to conduct these investigations for their home agencies.

- **Field Operations:** The Field Operations program supports the daily operations of the domestic and international field offices. The program is staffed by Special Agents, Uniformed Division Officers, Technical Law Enforcement, and administrative, professional, and technical personnel. Program personnel divide their time between conducting criminal investigations of



financial crimes, cybercrimes, counterfeit currency, protective intelligence, and performing protection responsibilities. This enables the Department to protect the United States economy and continuity of government by investigating threats to financial payment systems, threats to leadership and locations, and events with symbolic and practical significance to United States citizens in physical space and cyberspace.

### ***Summary of Progress***

**Progress:** The following progress updates were identified through the Strategic Review:

- Contributed to national security by safeguarding the current and former presidents of the United States, designated family members, and other foreign dignitaries.
- Successfully led the protective security for several NSSEs by coordinating effectively with law enforcement partners and intelligence agencies to safeguard millions of people.
- Improved investigative, logistical, and analytical support to field operations by developing and deploying the Global Investigative Operations Center.
- Initiated and applied web-based reporting advancements (e.g., Incident Based Reporting) to improve coordination within the USSS.

- Safeguarded the integrity of the U.S. financial system by investigating thousands of criminal cases, most of which were directly related to financial/cyber financial crimes.

***Challenges and Risks:*** The following challenges and risks were identified through the Strategic Review:

- If potential security gaps for multi-stage or multi-actor attacks are not addressed, then the program will not be able to mitigate the vulnerability and threat exposure of key leadership, places, and events.
- Managing ongoing challenges of hiring, training, and retaining personnel.
- If defensive measures do not continue to adapt to new adversarial capabilities, then the vulnerability and threat exposure of key leadership, places, and events will increase.
- If cyber and technological capabilities do not adapt to adversaries' evolving capabilities, then the Field Operations Program's ability to detect, deter, and investigate evolving financial crimes will be degraded.

Training for Field Operations staff must be maintained to ensure capability to respond to current and emerging threats.



### Security at the Historic Singapore Summit

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

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

### Performance Results and Plan

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
Leaders, National Security Events, and Financial Systems								
Amount of cyber-financial crime loss prevented (in billions)								
---	---	---	---	---	New Measure <sup>1</sup>		\$4.50	\$3.50
Amount of dollar loss prevented by Secret Service cyber investigations (in millions)								
\$1,119	\$384	\$589	\$558	\$3,145	\$600	\$5,181 <sup>2</sup>	Retired Measure <sup>3</sup>	
Financial crimes loss prevented through a criminal investigation (in billions)								
\$4.20	\$3.04	\$1.47	\$2.42	\$3.55	\$1.90	\$0.41 <sup>4</sup>	Retired Measure <sup>5</sup>	
Number of cyber mitigation responses								
---	---	---	157	253	390	271 <sup>6</sup>	225 <sup>7</sup>	240
Number of financial accounts recovered (in millions)								
3.90	0.29	0.93	0.51	27.18	0.50	5.7	0.50	0.50
Number of law enforcement individuals trained in cybercrime and cyber forensics both domestically and overseas								
1,517	1,533	2,070	1,906	1,968	2,000	2,773	2,500 <sup>8</sup>	2,800
Percent of currency identified as counterfeit								
0.0072%	0.0068%	0.0058%	0.0057%	0.0093%	<0.0088%	0.0064%	<0.0088%	<0.0090%
Percent of National Center for Missing and Exploited Children (NCMEC) examinations requested that are conducted								
100%	100%	100%	100%	100%	100%	100%	100%	100%
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								
100%	100%	100%	100%	100%	100%	100%	100%	100%
Percent of days with incident-free protection at the White House Complex and Vice President's Residence <sup>9</sup>								
100%	100%	100%	99.7%	100%	100%	100%	100%	100%
Terabytes of data forensically analyzed for criminal investigations								
4,002	4,902	6,052	3,334	5,019	5,000	8,862	5,100	5,600

1, 3, 5 – The new measure “Amount of cyber financial crime loss prevented (in billions)” is replacing two measures “Amount of dollar loss prevented by Secret Service cyber investigations (in millions)” and “Financial crimes loss prevented through a criminal investigation (in billions)” to better represent the overall cyber financial crime efforts by USSS.

2 – The USSS maintains Electronic Crimes Task Forces that focus on identifying and locating domestic and transnational cybercriminals connected to cyber-intrusions, bank fraud, data breaches, and other computer-related crimes. This measure reflects USSS’ efforts to reduce financial losses to the public from cybercrimes. The USSS closed two very large cases in the first quarter of FY 2018 which greatly impacted the results of the measure (one relating to tax fraud and the other a significant network intrusion into a major retailer). This year’s result of \$5.2 billion is the largest reported for this measure, greatly exceeding the target of \$650 million. The year-to-year results for this performance measure are highly variable based upon the cases closed in a particular reporting period.

4 – The Criminal Investigations program prevented \$407 million dollars in financial losses. A larger number of cases were committed through cyber means than anticipated (results for the cyber loss prevented measure are much higher than anticipated). As technology advances and cyber-crime becomes ever more pervasive, the distinction between traditional financial crime and cyber financial crime becomes arbitrary. As such, the USSS is combining measures for future reporting as annotated in Notes 1, 3, and 5.

6 – The USSS did not meet its target for this measure, although up from FY 2017, by responding to 271 organizations that suspected a malicious network intrusion in FY 2018. The main factors that resulted in lower than anticipated measure of performance involves specialized agent training and overall Secret Service staffing levels. On average, 48 Network Intrusion Responder (NITRO) agents must be trained each year to offset the attrition rate of agents in the program (due to out of program transfers, resignations/retirements, and promotions). In FY 2016, there were 0 agents trained due to increased protective staffing for the presidential campaign, and the effect of the Continuing Resolution on our ability to process procurements related to NITRO training. The number of NITRO agents dropped from 193 in FY 2016 to 134 in FY 2018 which greatly reduced the ability to respond to cyber incidents. Based on the current staffing projections, the USSS is adjusting targets accordingly.

7 – FY19 target previously published as 400 in the FY 17-19 Annual Performance Report was adjusted based on current performance trends.

8 – FY19 target previously published as 2,000 in the FY 17-19 Annual Performance Report was adjusted based on current performance trends.

9 – Previous measure name: *Percent of total protection activities that are incident-free at the White House Complex, Vice President’s Residence, and other protected facilities.*

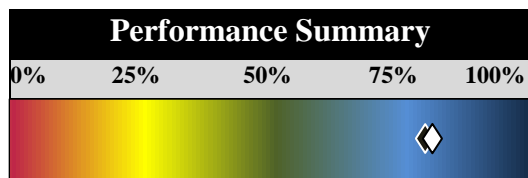
## Support Components

### Analysis and Operations

#### Overview

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

In FY 2018, there were six strategic performance measures used to assess Analysis and Operations' efforts. In FY 2018, 83 percent of the measures met their target and 83 percent maintained or improved actual results compared to FY 2017.



◆- Percent of measures that met their FY 2018 target.

◇- Percent of measures that maintained or improved actual performance results compared to FY 2017.

#### Mission Programs

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

- **Analysis and Operations:** The A&O program analyzes and shares domestic threat and hazard information through the activities of I&A and OPS. These two offices work together to improve

intelligence, information sharing, and coordination with stakeholders. These offices also develop protective measures and countermeasures to protect the homeland.

#### Did you know?

The DHS Office of Intelligence and Analysis hosts Specialized Analytic Seminars that bring together a diverse range of federal, state, and local subject-matter experts to address specialized-threat topic areas (e.g., cybersecurity, narcotics, transnational organized crime, gangs, privacy, and civil rights, and civil liberties) to enhance the analytic capabilities of state and local intelligence analysts.

#### Summary of Progress

**Progress:** The following progress updates were identified through the Strategic Review:

- The OPS program provided 100 percent timely responses and a high-level of customer service to federal, state, and local law enforcement partners through the Special Events Working Group in a year with increasing volume requests.
- Members of the Special Events Program team continued to leverage available resources within the Federal Government community to enhance the process and procedures related to short notice event assessments.
- OPS continued to refine their Special Event Assessment Rating (SEAR) methodology to stay ahead of evolving threats.



- The program partnered several federal agencies to ensure the safety and security of attendees and facilities at the highest risk events (e.g., the Super Bowl, Rose Parade and Bowl, Indy 500).

**Challenges and Risks:** The following challenges and risks were identified through the Strategic Review:

- The increasing number of ad hoc events submissions is adversely impacting the Special Events Program's ability to provide timely support to its state and local partners. Front-end planning will aid OPS' adjudication efforts and will mitigate negative impacts to special events coordination.



### The Public-Private Analytic Exchange Program Celebrating Seven Years!

The DHS Office of Intelligence and Analysis (I&A) Private Sector Engagement (PSE) team facilitates the Public-Private Analytic Exchange Program (AEP), now in its seventh year, on behalf of the Office of the Director of National Intelligence. The AEP brings together analysts from the public and private sector, for six months, to work on topic-focused teams to create unclassified deliverables of national and homeland security interest. Additionally, it builds and strengthens partner relationships by connecting analysts that would not ordinarily work together.

The 2018 teams were comprised of analysts from 38 private sector companies—including some Fortune 500 companies—and 24 government agencies. DHS participation, included analysts from U.S. Customs and Border Protection, Immigration and Customs Enforcement, I&A, Cybersecurity and Infrastructure Security Agency, and the Science and Technology Directorate. Of the 100 participants for the 2018 rotation, 47 work in government and 53 work in private sector. It is notable to mention that AEP had representation from 9 of the 16 critical

infrastructure sectors, including commercial facilities, communications, and critical manufacturing.

These analytic deliverables are shared with over 10,000 recipients via the DHS Homeland Security Information Network-Critical Infrastructure/Intelligence, FBI's Domestic Security Alliance Council Portal, association partners, and the AEP participant network.

### Performance Results and Plan

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
<b>Mission Support</b>								
Number of intelligence reports shared with the intelligence community (I&A)								
---	---	---	---	3,602	2,730	5,270	2,784	2,839
Percent of Intelligence and Analysis finished intelligence reports incorporating DHS and state/local originated data (I&A)								
---	---	---	---	62%	80%	60% <sup>1</sup>	60% <sup>2</sup>	60%
Percent of intelligence reports rated "satisfactory" or higher in customer feedback that enable customers to manage risks to cyberspace (I&A)								
94%	94%	93%	84%	90%	95%	95%	95%	95%
Percent of intelligence reports rated "satisfactory" or higher in customer feedback that enable customers to understand the threat (I&A)								
93%	95%	95%	95%	94%	95%	99%	95%	95%
Percent of National Operations Center incident reports and situational awareness products produced and disseminated to the homeland security enterprise within targeted timeframes (OPS)								
---	---	---	---	98%	90%	99%	90%	90%

## FY 2018-2020 Annual Performance Report

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
Percent of risk assessments for federal security support of large public/community special events completed within the targeted time frame (OPS)								
---	---	---	---	99.4%	98%	100%	98%	99%

1 – This measure reflects the impact that DHS's Office of Intelligence & Analysis (I&A) provides to the U.S. Intelligence Community (IC) by disseminating finished intelligence reports with information harnessing DHS and state, local, tribal, and territorial data that is unique. It provides an indication of the value that DHS raw intelligence reporting is providing to the IC. In FY 2018, 60% of the disseminated intelligence analysis produced by I&A included information originating from DHS collected intelligence or information that is directly attributable to state and local governments. While I&A didn't meet its annual target of 80%, I&A is

committed to using DHS and state and local information in its disseminated intelligence and determined to include information that is not traditionally available to the IC. The results also indicate that DHS and state and local information remains relevant to I&A's analysis when communicating its assessments to its customers nationwide.

2 – FY19 target previously published as 80% in the FY 17-19 Annual Performance Report was adjusted based on two years of past performance.

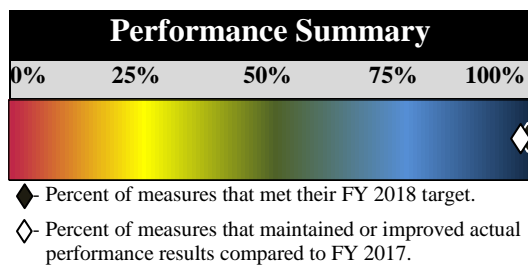
## Countering Weapons of Mass Destruction Office

### Overview

Countering Weapons of Mass Destruction (CWMD) Office was created on December 7<sup>th</sup> of 2017 to elevate and focus the CWMD missions within DHS and to provide a focal point for the interagency. The CWMD Office was formed primarily by consolidating the Domestic Nuclear Detection Office and a majority of the Office of Health Affairs, as well as other relevant DHS elements.

The danger from hostile state and non-state actors who are trying to acquire nuclear, chemical, radiological, and biological weapons is increasing. CWMD's objective is to support the President's National Security Strategy and lead the Department's efforts to develop and enhance CWMD programs and capabilities that defend against WMD, and combat bio-threats and pandemics. CWMD will give our frontline defenders—including homeland security, law enforcement, and intelligence professionals—the tools and resources to stop WMD terrorist acts before they take place. CWMD serves as the Department's representative at domestic, interagency, and international venues related to CWMD strategy, policy, planning, investment, acquisition, and joint operational matters.

In FY 2018, there were five strategic performance measures used to assess CWMD's efforts. In FY 2018, 100 percent of the measures met their target and 100 percent maintained or improved actual results compared to FY 2017.



### Mission Programs:

The mission programs that deliver performance results for CWMD are:

- Capability and Operational Support:** The Capability and Operational Support program analyzes sensor data, defines requirements, provides test and evaluation capabilities, and procures chemical/biological and radiological/nuclear detection equipment that can be carried, worn, or easily moved to support operational end-users. The Program manages and supports national biosurveillance and detection capabilities, coordination, and preparedness for biological and chemical events to help communities build capabilities to prepare, respond, and recover.
- Capability Building:** The Capability Building program supports projects and activities that provide chemical, biological, radiological, nuclear, and medical support, as well as readiness activities, in support of interagency partners, DHS Components, state and local first responders, and international partners. The program pursues this by establishing, maintaining, and supporting projects and activities to defend against chemical, biological, radiological, nuclear, and other health security threats.

### Summary of Progress

The CWMD office stood up its new organization, while simultaneously continuing to advance the Department's capability prevent and protect against chemical, biological, radiological, and nuclear threats, whether terrorist based or naturally occurring.

**Progress:** The following progress areas are highlighted:

- Initiation of the BioDetection-21 program developing the next generation of bio-detection approaches.
- The Threat Response Operation program is under way to improve chemical detection capabilities.

**Challenges and Risks:** The following challenge is highlighted:

- Moving forward, CWMD's biggest challenge will be working through the merger process to ensure the operational aspects of CWMD and employee engagement are enhanced.

### Performance Results and Plan

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
Weapons of Mass Destruction								
Average time (in hours) to initiate a BioWatch National Conference Call to discuss the detection of a biological agent of concern and assess the risk to public health with federal, state, and local partners								
---	---	---	---	2.0	≤ 3.0	1.9	Retired Measure <sup>1</sup>	
Number of people covered by Securing the Cities program preventive radiological and nuclear (rad/nuc) detection capabilities (in millions)								
---	23.0	23.0	37.0	37.0	46.0	46.0	Retired Measure <sup>2</sup>	
Percent of cargo conveyances that pass through radiation portal monitors upon entering the nation via land border and international rail ports of entry (CWMD)								
FOUO	FOUO	FOUO	FOUO	FOUO	FOUO	FOUO <sup>3</sup>	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 <sup>3</sup>	FOUO	FOUO
Percent of top 25 special events integrating biodetection monitoring								
---	---	---	---	---	New Measure		60%	65%
Time between laboratory receipt of BioWatch detector samples to completion of screening for known biological micro-organisms of interest (in hours)								
---	---	---	---	5.0	≤ 7.0	5.0	Retired Measure <sup>4</sup>	

1 – This measure is being retired as it does not align with new CWMD strategic priorities. Once the BioDetection-21 program, currently in technical demonstration phases, is fully tested and validated in its intended operational environment it will serve as the Nation's preeminent biodetection capability. The program will also develop a measure to assess ongoing performance once operational.

2 – Under the CWMD reorganization and re-prioritization, the Securing the Cities program is being realigned to co-exist with other detection capabilities and will no longer exist as a stand-alone program.

3 – These measure met their targets for FY 2018.

4 – This measure is being retired as it does not align with new CWMD strategic priorities. See Note 1 for more detail.

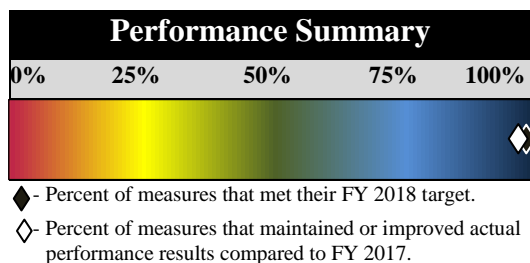


## Federal Law Enforcement Training Centers

### Overview

The [Federal Law Enforcement Training Centers \(FLETC\)](#) provide career-long training to law enforcement professionals to help them fulfill their responsibilities safely and proficiently. FLETC trains those who protect the homeland, and therefore, its training audience includes federal, state, local, and tribal departments throughout the U.S. FLETC's impact extends outside our Nation's borders through international training and capacity-building activities funded by the State Department. Over the past 48 years, FLETC has grown into the Nation's largest provider of law enforcement training. Under a collaborative training model, FLETC's federal partner organizations deliver training unique to their missions, while FLETC provides training in areas common to all law enforcement officers, such as firearms, driving, tactics, investigations, and legal training. Partner agencies realize quantitative and qualitative benefits from this model, including the efficiencies inherent in shared services, higher quality training, and improved interoperability.

In FY 2018, there were two strategic performance measures used to assess FLETC's efforts. In FY 2018, 100 percent of the measures met their target and 100 percent maintained or improved actual results compared to FY 2017.



### Mission Programs

The mission program that delivers performance results for FLETC is:

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

#### Did you know?

In FY 2018, FLETC provided training to more than 70,000 officers and agents from more than 90 federal law enforcement agencies and from state, local, and tribal agencies across the country, and engaged in law enforcement training and capacity-building in support of U.S. Government interests abroad.

### Summary of Progress

FLETC trains those who protect the homeland, and therefore, its training audience also includes federal, state, local, and tribal departments throughout the U.S. FLETC's impact extends outside our Nation's borders through international training and capacity-building activities funded by the State Department.

**Progress:** FLETC is a perennial top performer as evidenced by their steady performance in growing and maintaining a

strong network of training partners and continuing to receive top satisfaction ratings for the training conducted by FLETC.

**Challenges and Risks:** Moving forward, FLETC's biggest challenge will be managing

the influx of new training requirements due to the personnel required to support Border Security, Immigration Enforcement, and Interior Enforcement.



### FLETC Partner Organization Liaison Officer

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

During FY 2018, FLETC fully implemented an effort to integrate partner relations into a single point-of-contact charged with ensuring its federal Partner Organizations (POs) have access to the information they need to achieve their training goals in support of their operational missions. Through this focused approach, the PO Liaison Officer facilitated improvement to communication

mechanisms such as the FLETC PO website and orientation program, newly minted monthly meetings among PO and FLETC leadership, and instituted monthly open-dialogue sessions among small groups of partners to share information and discuss topics of mutual interest. In FY 2018, the FLETC PO Liaison Officer worked with federal POs on more than 900 questions and issues, ranging from simple inquiries about FLETC procedures to complex matters that impact the full enterprise.

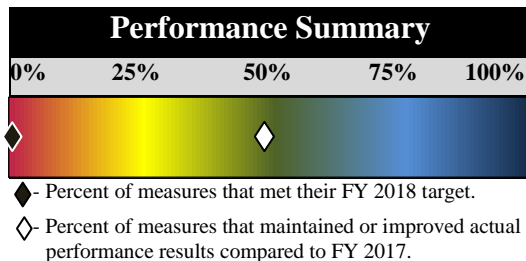
### Performance Results and Plan

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
Mission Support								
Number of federal law enforcement training programs and/or academies accredited or re-accredited through the Federal Law Enforcement Training Accreditation process (FLETC)								
97	107	114	119	129	128	141	Retired Measure	
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)								
100%	91%	98%	95%	97%	90%	98%	90%	90%

## Science and Technology Directorate

### Overview

[Science and Technology Directorate \(S&T\)](#) is the primary research and development arm of the Department. It provides federal, state, and local officials with the technology and capabilities to protect the homeland. Technology and threats evolve rapidly in today's ever-changing environment. S&T monitors those threats and capitalizes on technological advancements at a rapid pace, bridging capability gaps, and developing solutions. S&T's mission is to deliver effective and innovative insight, methods, and solutions for the critical needs of the Homeland Security Enterprise. In FY 2018, there were two strategic performance measures used to assess S&T's efforts. In FY 2018, 0 percent of the measures met their target and 50 percent maintained or improved actual results compared to FY 2017.



### Mission Programs

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

- Acquisition and Operations Analysis:** The Acquisition and Operations Analysis program provides expert assistance to entities across the homeland security enterprise to ensure that the transition, acquisition, and deployment of technologies, information, and procedures improve the efficiency and effectiveness of operational capabilities. This program assists in testing and evaluation, standards development, requirements

analysis, systems engineering, and supporting technology transition.

- Laboratory Facilities:** The Laboratory Facilities program provides the Nation with a coordinated enduring network of science, technology, and engineering laboratories, organizations, and institutions. This network delivers the knowledge, technology, and resources required to secure our homeland.

### Did you know?

S&T oversees a coordinated network of five DHS laboratories and as many as 13 Department of Energy national laboratories that are vital to the national homeland security mission.

- Research, Development, and Innovation:** The Research, Development, and Innovation program provides state-of-the-art solutions to meet the needs of DHS Components and the first responder community. This includes customer-focused and output-oriented Research, Development, Test, and Evaluation (RDT&E) programs that balance risk, cost, impact, and time to delivery.
- University Programs:** University Programs supports critical homeland security-related research and education at U.S. colleges and universities to address high-priority DHS-related issues and to enhance homeland security capabilities over the long term. University Programs includes DHS Centers of Excellence and Minority Serving Institutions, creating a consortium of universities generating groundbreaking ideas for new technologies and critical knowledge for the homeland security enterprise.

## Summary of Progress

Across all DHS mission areas, S&T helps integrate innovative technology into everyday use. S&T works directly with operators in the field to understand their unique needs and challenges.

**Progress:** DHS's Research and Development activities have an important impact on the departmental missions:

- The advanced technologies, knowledge products, technical analyses, laboratories, and university-based research contribute to the effectiveness and efficiency of DHS operations.
- S&T has contributed to the success of CBP and other DHS Operational Components by developing and evaluating alternative technologies and Concepts of Operation for Biometric Entry/Exit, Global Entry, Modified Egress, as well as enhancing the performance of core Face Recognition capabilities.
- From wireless emergency alert improvements to thermal sensor

warning for fire safety to mitigating threats from Vehicle Improvised Explosive Devices, S&T has made significant progress improving technology and processes to make the nation safer.

### Challenges and Risks:

- For all research elements, the greatest challenge in the results and outcomes of research and development programs is the uncertainty of the practicality of the results that will be delivered and the ongoing funding to support the work in light of this uncertainty.
- The management controls and planning processes instituted in the research elements make S&T a strong steward for government funding; however, funding fluctuations can disrupt research efforts and the potential to deliver needed capabilities to the operational elements within the Department. These fluctuations can also strain the organization's ability to retain top-level expertise and talent.



### Android Team Awareness Kit (ATAK)

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

In 2018, S&T has deployed ATAK to support public safety through several multi-agency coordinated and cooperative operations in which all DHS Component and Homeland Security Enterprise participants benefited from improved situational awareness. These events included Super Bowl LII, the NBA All-Star game, U.S. Border Patrol's San Diego,

California Sector field experiment, and a marijuana-growing sting operation. At each of these events, ATAK was successfully utilized to improve situational awareness through capabilities such as full-motion video dissemination, blue force tracking of law enforcement agents, and other geographic information. This information was available to various mobile and fixed operations centers, as well as operators in the field via mobile devices with the ATAK application. ATAK technology enables personnel from multiple agencies to track response assets, identify hazards, locate people needing rescue, coordinate interagency response, and share video feeds of operations while also maintaining tactical awareness of weather, critical infrastructure, and other important information.

-- Statement by Homeland Security Intelligence (HSI) Special Agent/Special Response Team (SRT) member.

**"ATAK is like having the connectivity of a command center at your fingertips."**



**Performance Results and Plan**

Prior Results					FY 2018		Performance Plan	
FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	Target	Result	FY 2019	FY 2020
Mission Support								
Percent of planned cybersecurity products and services transitioned to government, commercial and open sources								
89%	93%	60%	73%	71%	80%	78% <sup>1</sup>	Retired Measure <sup>2</sup>	
Percent of Apex technologies or knowledge products transitioned to customers for planned improvements in the Homeland Security Enterprise								
---	---	82%	100%	83%	80%	67% <sup>3</sup>	80%	80%

1 – The result of this measure consists of the Cyber Security Division (CSD) completion of planned transitions of cybersecurity products and/or services, which means cybersecurity research and development efforts have resulted in deployable security solutions. In FY 2018, CSD completed seven of nine planned transitions: a Cyber.gov study and published baseline document to CISA; test results for a technology solution to the Cyber Apex Review Team for operational consideration; completion of additional open source module development for law enforcement forensics; reference materials for the forensic acquisition and analysis of 20 commercially available drones to Cyber Forensics Working Group member agencies; data set/test cases to Software Assurance Marketplace; and report on Safety Instrumented Systems released through the Automation Federation website. Two planned transitions were not completed due to delays by a customer's internal processes and delay in awarding agreements. As part of S&T's revitalization efforts, S&T plans to increasingly focus on engagement with its customers, which will help bring leadership focus to the achievement of transitions planned for a fiscal year.

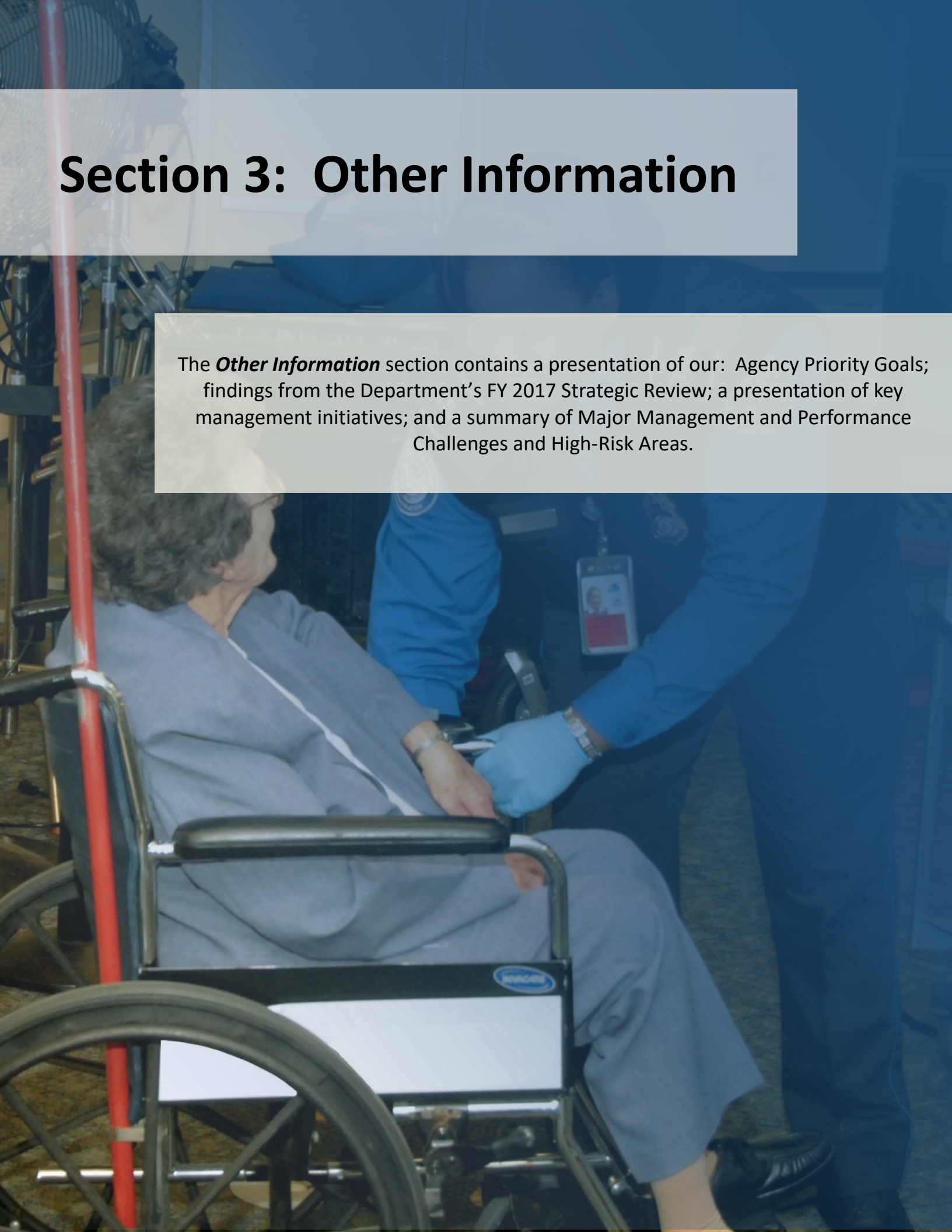
2 – The FY 2019 President's Budget for S&T transfers cybersecurity research and development funding from S&T to CISA. Since some of the programs for which

this measure would obtain data may not exist in FY 2019, S&T is retiring this measure.

3 – This measure tracks transitions of high priority and high value research and development (R&D) projects known as Apex programs. A successful transition is the ownership and operation of a technology or knowledge product by a customer within the Homeland Security Enterprise. In FY 2018, S&T completed six of nine planned transitions: a passenger screening algorithm to TSA; a Cyber.gov study and published baseline document to CISA; test results for a technology solution to the Cyber Apex Review Team for operational consideration; published recommendations to prepare public safety organizations and federal law enforcement agencies with jamming incidents; and an analysis of advanced analytic applications. These indicate high priority and high value R&D projects are being delivered to improve homeland security operations. Three planned transitions were not completed due to delays by customers' internal processes and operational priorities delaying contract award. As part of S&T's revitalization efforts, S&T plans to increasingly focus on engagement with its customers, which will help highlight leadership focus to the achievement of planned transitions throughout a fiscal year.

## Section 3: Other Information

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



## Agency Priority Goals (APG)

### Agency Priority Goal 1: Enhance Southern Border Security

**Impact and Goal Statement:** Improve security along the Southwest Border of the U.S. between ports of entry

- By September 30, 2019, DHS will implement the Operational Control (OPCON) framework between ports of entry in 100% of U.S. Border Patrol Sectors along the Southwest Border as the means to enhance security

#### Measures:

Measure Name	FY 2018 Target	FY 2018 Result
<b>Key Measure:</b> % of Southern Border sectors that have implemented the operational control framework	N/A*	N/A*
% of the Southern Border sectors with which the U.S. Border Patrol has coordinated to determine how OPCON standards apply to the sectors' areas of responsibility	50%	50%
Rate of interdiction effectiveness along the Southwest Border between ports of entry	81%	79.69%
% of time the U.S. Border Patrol reaches a detection site in a timely manner to assess the nature of detected activity in remote, low-risk areas of the Southern Border	96%	88.7%
% of U.S. Border Patrol agent workforce who are trained and certified to perform enforcement actions	94%	96%

Miles of Southern Border with additional pedestrian wall	74	20
----------------------------------------------------------	----	----

\*Key measure begins reporting in FY19

**Progress Updates:** In FY18, the U.S. Border Patrol made significant strides in advancing the Agency Priority Goal to improve the security along the Southwest Border through the following key efforts:

- USBP Planning Division presented briefings and training to all nine Southwest Border sector and station personnel on the OPCON framework and obtained feedback from the field on gaps and requirements
- Conducted two pilots at the Brown Field Station in San Diego Sector (SDC) and Laredo South Station in Laredo Sector (LRT)
  - The Pilots enabled USBP Planning Division to gather preliminary data in two sectors with distinct threat and resource environments, enhancing understanding of the range of OPCON baseline scores
  - The team also applied the framework to Imperial Beach Station in SDC and Laredo North Station in LRT which provided a more comprehensive picture of the sectors, with more data to inform analysis
  - As a result of the pilots each element (Situational Awareness, Impedance and Denial, and Law Enforcement Resolution) of the OPCON framework is now assessed using a set of measures that support each of the mission tasks in each element
- Trained two personnel from all 20 USBP sectors to ensure sectors are prepared when the OPCON framework



is being implemented in their respective sectors

- Began working with CBP Office of Information Technology to identify solutions to automate the OPCON framework rather than having to do a manual data pull for measures
- Coordinated with the USBP Geospatial Information Systems team to create an application where each station can code their area of responsibility to be able to perform a detailed map analysis for OPCON measures requiring location information
- All FY19 Sector Master Concepts of Operations (CONOPs) were submitted and approved
  - Master CONOPs are USBP Sector plans that outline specific actions to target identified, traceable capability gaps
  - The Sectors identify an appropriate end state with the non-materiel/materiel strategies, and measureable outputs
  - The outputs are then directly associated to individual measures in the OPCON Strategic Framework
- Logic models that outline each CONOP's target capability gaps, objectives, strategies for solutions, and tactical measures were completed
  - The logic models take a plan and dissolve it into its four basic parts and displaying a direct line of effort from: capability gap; objective; strategy; output
  - The logic models will be the basis of the quarterly CONOPs reporting
- Established linkages between CONOP measures and Strategic OPCON Framework measures to help identify activities that make the biggest impact

on the overall OPCON score; and to enable sectors to determine how to apply those measures directly in their CONOPs

#### **Next Steps:**

- As the OPCON Framework is introduced in FY19, the evaluation of the CONOPs that will occur concurrently will enable the USBP to see direct impacts of operations on identified measures. For example, as RGV Sector deploys 14 Mobile Remote Video Surveillance System to border zones in FY19 to fill detection, identification, and classification gaps, observed changes in two of the measures in the OPCON framework will be seen: Surveillance Capability Score and Average Time from Detect to Identify
- The team is on target for completing OPCON implementation for all Southwest Border line stations in all nine sectors by the end of FY19, which includes carrying out CONOPs that aim to improve capabilities for the three elements of OPCON
- The USBP Planning Division will finalize FY19 Sector CONOPs reporting procedures, and execute quarterly progress update protocols

### ***Agency Priority Goal 2: Strengthen Federal Cyber Security***

**Impact and Goal Statement:** Strengthen the defense of the federal network through the increased dissemination of cyber threat and vulnerability information in near real time to federal agencies

- By September 30, 2019, Federal agencies will mitigate 70% of significant (critical and high) vulnerabilities identified through DHS



scanning of their networks within a designated timeline

#### Measures:

Measure Name	FY 2018 Target	FY 2018 Result
<b>Key Measure:</b> Percent of significant (critical and high) vulnerabilities identified by DHS cyber hygiene scanning of federal networks that are mitigated within the designated timeline	80%	52%
Percent of participating federal, civilian executive branch agencies with an active Continuous Diagnostics and Mitigation (CDM) data feed into the DHS managed Federal Dashboard	50%	88%
Percent of participating federal, civilian, executive branch agencies for which CDM capabilities to manage user access and privileges to their networks are being monitored on the DHS managed Federal Dashboard	21%	0%
Percent of participating federal, civilian executive branch agencies for which CDM tools to monitor what is happening on their networks have been made available	95%	96%
Percent of incidents detected or blocked by EINSTEIN intrusion detection and prevention systems that are attributed to Nation State Activity	20%	29%
Percent of significant (critical and high) vulnerabilities identified through a DHS assessment of a federal agency high value asset (HVA) that are mitigated within 30 days	68%	32%

#### Progress Updates:

##### *Cyber Hygiene Scanning*

- The severity level of a particular vulnerability was reevaluated in the 4<sup>th</sup> quarter, causing a spike in reporting in the 4<sup>th</sup> quarter, which required manual correction of the data
- Migration of the cyber hygiene scanning capability to a cloud environment caused some initial disruption due to agencies having difficulty recognizing the scans, preventing data from being included in the result. The program is taking steps to mitigate the issue, such as establishing dedicated IP addresses so agencies can easily identify the scanning activity

##### *CDM Deployment*

- Phase 1 (Asset Management) completed all but two exchanges for CFO Act agencies, meeting all FY18 Phase 1 milestones
- Progress on Phase 2 (Identity & Access Management) exchanges gained momentum with the contract protest withdrawal of the DEFEND E contract (6 agencies) in the 4<sup>th</sup> quarter
- Phase 3 (Network Security Management) tools and services are now available to all CFO Act agencies, with only non-CFO Act Phase 3 exchanges remaining

##### *High Value Assets*

- Federal Network Resilience (FNR) prioritized delivery of guidance to, and direct engagement with, agencies with the largest number of unmitigated vulnerabilities to improve the mitigation rate in the 4<sup>th</sup> quarter
- FNR also escalated those agencies' mitigation status to their leadership to coordinate an effective response

**Next Steps:**

*Cyber Hygiene Scanning*

- A revision to BOD 15-01 to address the mitigation timeline requirements is planned
- NCATS analysts are working to identify the biggest factors affecting vulnerability mitigation in order to make recommendations to improve the mitigation rate

*CDM Deployment*

- The CDM program office will continue to work with the integrators of all DEFEND groups on Phase 2 exchange timelines
- Five agencies are expected to complete Phase 2 by Q2, FY19
- DEFEND F is expected to be awarded in Q3, FY19
- The measure, “Percent of DHS endpoints identified with high and

critical vulnerabilities relating to hardware and software that are patched within 30 days,” is estimated to begin reporting in Q2, FY19

*High Value Assets*

- FNR will continue to support agencies through targeted mitigation guidance and escalation of mitigation priorities to agency leadership
- Mandatory involvement of agency-designated Senior Accountable Officials of Risk Management (SAORMs), per BOD 18-02, will bring increased visibility, prioritization, and resources to agencies’ mitigation efforts
- FNR is establishing an HVA interagency Community of Interest (COI) to identify and promote HVA best practices and foster a whole-of-government approach to reducing systemic risk

## FY 2018 Strategic Review Results

DHS conducted this fifth annual review of progress last winter and spring of FY 2018 to coincide with the schedule agreed upon by the Office of Management and Budget (OMB). Because DHS is in a transition year with the strategic plan, the Strategic Review used Themes as a framework of common functions to conduct the assessment. Within each Theme, the Strategic Review focused on the associated mission programs. A mission program is a group of activities acting together to accomplish a specific high-level outcome external to DHS and includes operational processes, skills, technology, human capital, and other resources.

The motivation to move to a focus on mission programs included:

- The mission programs reflect the operational Programs, Projects, and Activities (PPA) that represents the majority of the DHS total budget authority.
- Issuance of the Program Management Improvement and Accountability Act (PMIAA) and soon to be released implementing guidance from OMB.
- Desire to more strongly leverage the performance management logic model.

DHS determined the progress ratings listed below in cross-cutting Headquarters Review and discussions with senior leadership. Noteworthy progress requires a combination of programs exceeding expectations, to include:

- Mission programs working effectively.
- Notable impact delivered to stakeholders.
- Performance measures gauge relevant activities and value.
- Risks are known and managed.

Focus areas are ones that, due to a variety of factors, including external pressures not completely controlled by the Department, continued focus is needed to enhance progress in the future. The criteria for Focus Area include:

- Mission programs face challenges in execution.
- Strategies and actions lack impact of significant magnitude.
- Significant performance measurement gaps exist.
- Risk environment has excessive uncertainty and/or known risks exceed current mitigation strategies.

The progress findings for the FY 2018 strategic review were:

### *Noteworthy Progress Themes*

- Trade and Travel.
- Leaders, National Security Events and Financial Systems.

### *Focus Areas Themes*

- Border Operations.
- Immigration Benefits.
- Man-Made or Natural Incident Response.
- Man-Made or Natural Incident Investments.

### **Noteworthy Progress Themes**

For each Noteworthy Progress Theme, a brief narrative enumerating their progress is detailed.

#### **Theme: Trade and Travel**

##### **Overview and Impact**

Lawful trade and travel is not only a critical component of national security, but also of the Nation's economic prosperity. This continues to be made clear by the steady increase in both international business and tourist travelers who choose to visit the

United States. With respect to trade and travel:

- CBP processes more than \$2 trillion in imports and nearly 30 million cargo containers annually. With trade and travel projected to continue to grow, DHS and its partners must work to secure and expedite the increasing flows of people and goods to keep our Nation safe and prosperous.
- CBP has operationalized 10 Centers of Excellence and Expertise to improve trade facilitation and enforcement and further strengthen critical agency knowledge on key industry practices.
- Numerous innovations in both the trade and travel are supporting higher traffic volume, faster processing, and shorter wait times with increases in both trade and travel volumes.
- The Automated Commercial Environment system improvements resulted in nearly \$30M in processing efficiencies and more than \$50M savings for industry.
- Implemented Automated Targeting Rules to assist in identifying the illegal movement of fentanyl and opioids.
- Initiated a pilot biometric entry/exit process in Orlando, Florida to collect passenger data prior to departure and is creating a paperless secure platform to identify travelers which could revolutionize the entry/exit process.

***Theme: Leaders, National Security Events, and Financial Systems***

***Overview and Impact***

The USSS protects national leaders, visiting heads of state and government, designated sites, and National Special Security Events. The USSS fights crime on a global scale through its field offices located in the United

States, Canada, Mexico, South America, Europe, Africa, and Asia.

The USSS has grown from a small bureau staffed by a few operatives in 1865, to a law enforcement organization of more than 7,000 employees worldwide. The USSS continues to provide superior services to include:

- Successfully executed the third largest ever year of foreign and domestic protective stops.
- Protected a number of significant events and locations, including the White House Complex, reducing the likelihood of an incident by seizing more than 13,000 weapons at screening checkpoints.
- Successfully led the protective security for NSSEs by coordinating effectively with law enforcement partners and intelligence agencies to safeguard millions of people at highly visible events such as the United Nations General Assembly and the State of the Union.
- Improved investigative, logistical, and analytical support to field operations by developing and deploying the Global Investigative Operations Center.
- Initiated and applied web-based reporting advancements (e.g., Incident Based Reporting) to improve coordination within the USSS.
- Applied knowledge from USSS-conducted cyber-crime and cyber-forensics training resulted in more than 5,000 terabytes of analyzed data.
- Safeguarded the integrity of the U.S. financial system by investigating nearly 3,000 criminal cases, 60 percent of which were directly related to financial/cyber-crimes.



## **Focus Areas Themes**

For each Focus Area Theme, a brief narrative is provided followed by a summary of planned corrective actions.

### **Theme: Border Operations**

#### ***Overview and Challenges***

The U.S. Border Patrol has the opportunity to improve Southern Border security and protect the Nation by articulating a framework to advance operational control of the border. Some of the challenges include:

- This framework relies on the interconnectedness of the three elements of Operational Control (OPCON): 1) Situational Awareness; 2) Impedance and Denial; and 3) Law Enforcement Response and Resolution.
- CBP's implementation and refinement of the OPCON framework is in its early stages. The effort requires significant change that will link tactical prioritization, operational planning, and data analysis to strategic outcomes with the intent of clearly articulating organizational effectiveness.
- CBP's Integrated Operations (Air and Marine Operations) also faces challenges affecting its ability to consistently fill requests for air support. The demand for air support exceeds capacity, creating a need to improve prioritization of requests, as well as data collection and analysis to guide decisions.
- Critical to U.S. Border Patrol and integrated operations, staffing shortfalls, compounded with retention issues, are unlikely to change significantly in the near-term, straining the ability to execute border-operations missions effectively.

#### ***Corrective Action***

Border Security Operations will be taking the following steps to address some of the

significant challenges identified during the FY 2018 Strategic Review:

- Improve security along the Southwest Border between ports of entry by the end of FY 2019 through the implementation of the OPCON framework as communicated in the DHS Agency Priority Goal: Enhance Southern Border Security.
- Implementation of the OPCON framework includes development of sector-specific Master Concepts of Operation (CONOPS) that are based on each sector's unique terrain, threats, flow, and resources. The CONOPS seek to improve OPCON by executing plans for operations that address capability gaps associated with one or more of the three elements of OPCON, then data is analyzed to determine the operation's influence on U.S. Border Patrol effectiveness.
- Address staffing issues through targeted hiring efforts intended to mitigate a shortfall from the authorized and funded levels.
- Increase emphasis on building more law enforcement engagement with international partners in Mexico and Canada (supporting Situational Awareness and Law Enforcement Response).
- Ongoing focus on planning related to impedance and denial through the repair and replacement of existing physical barriers and new construction as funded.
- Once OPCON is implemented along the Southern Border, USBP plans to expand the framework to the Northern Border and Coastal sectors.

Integrated Operations (Air and Marine) will be taking the following steps to address some of the significant challenges identified during the FY 2018 Strategic Review:

- Develop a Flight Hour Executive Council Charter to oversee implementation of flight hour prioritization processes to meet emerging threats.
- Continue to work with U.S. Border Patrol and other partners to share and improve situational awareness.
- Develop a Capability Analysis Report quantifying current and future gaps in air domain awareness capability.
- Continue to seek initiatives to address retention and hiring challenges.
- Pursue alternative fleet modernization programs such as Vertical Lift (VL), Air Interdiction, Light Enforcement Aircraft and Helicopters, and Air Domain Awareness.
- Assess and develop enhanced performance measures to communicate the effectiveness and value of AMO operations, gauge effectiveness of alternative approaches, and to identify opportunities for improvement.

### ***Theme: Immigration Benefits***

#### ***Overview and Challenges***

U.S. Citizenship and Immigration Services (USCIS) is facing many challenges to include:

- The potential for changing policies, judicial decisions, and new mandatory in-person interview requirements may pose significant challenges to the program's ability to manage and process the more than 2 million cases that are in the backlog.
- Processing times for the most requested immigration benefits have increased dramatically over the past three years due to a variety of factors including increased complexity and demand.
- Applicant reaction to backlog and policy changes has cascading effects on multiple offices and other agencies.

For example, the workload for the Citizenship and Immigration Services Ombudsman has nearly doubled.

#### ***Corrective Action***

USCIS has taken or will be taking the following steps to address some of the significant challenges identified during the FY 2018 Strategic Review:

- Reduce the backlog by utilizing a six-year forecasting model to increase the number of adjudications officers in the near term, and achieve sustained officer productivity over the six-year period in order to manage moderately increasing workloads.
- Published a final rule in the Federal Register to increase the premium processing fee effective October 1, 2018. USCIS will hire additional staff and make investments in information technology systems with the premium funds that are generated by the fee increase.
- Complete the FY 2019/2020 Immigration Examinations Fee Account fee review to determine whether adjustments to the current fee schedule are needed.
- Increase the authorization level for Asylum operations and resume the use of "Last In, First Out" policy to eliminate the backlog for Form I-589, Application for Asylum and Withholding of Removal.
- Deploy Refugee Affairs Division staff to border sites (for credible and reasonable fear cases) and asylum offices to provide additional adjudication, supervisory, and support personnel to adjudicate and process the Asylum Division workload.
- Implement an eProcessing initiative to move USCIS from a paper based environment to a digital environment where filing, adjudication,

communication, and determinations are all electronic. Digital processing of all forms is targeted for December 2020.

- Coordinate with directorates and program offices to review their respective performance measures, their indicators of progress for the strategic objectives, and the associated targets, particularly those that assess current processing times, and recommend modifications as warranted.
- Pilot new methodologies to realign field office workloads while building capacity to increase interviews through process re-engineering and enhanced interview training.

### ***Theme: Man-Made or Natural Incident Response***

#### ***Overview and Challenges***

The Federal Emergency Management Agency (FEMA) was significantly impacted in FY 2018 from the 2017 hurricane season. Disasters challenged emergency communications capabilities due in part to the need to expand scope and build contingency networks in Puerto Rico. Some of the challenges include:

- The unprecedented hurricane season highlighted the need for a scalable/capable incident workforce; whole community approach for life-sustaining commodities, equipment, and personnel; and the vital importance of emergency communications in establishing command and control.
- The response and recovery mission areas face growing challenges as program strategies do not yield desired impacts during intense demand for services.
- State, local, tribal, and territorial governments find FEMA's disaster assistance programs, funded through the Disaster Relief Fund, difficult to

navigate, which can delay a community's recovery timeline.

#### ***Corrective Action***

The Response and Recovery and Preparedness and Protection programs will be taking the following steps to address some of the significant challenges identified during the FY 2018 Strategic Review:

#### ***Workforce Actions***

- Implement the National Qualification System by providing jurisdictions with the technology and technical assistance necessary to support the qualification and growth of the national disaster workforce.
- Improve the recruitment and retention of the incident workforce by reviewing and revising staffing needs, increasing career progression opportunities and streamlining the on-boarding and orientation processes.
- Mature partnerships with other Federal agencies to more effectively integrate the DHS Surge Capacity Force volunteers and FEMA Corps teams into disaster operations.

#### ***Logistics Actions***

- Increase commodity stock and facility size to avoid transportation delays and extended supply chain risks in order to fully prepare locations and territories outside of the Continental U.S. (OCONUS) for future disasters.
- Restructure Incident Support Base Teams to increase the capacity and capability to deploy staging management teams within 12-18 hours.
- Improve transportation capabilities by expanding OCONUS transportation contracts to include catastrophic level intra- and inter-island support, cross-dock support, and on-island trucking.

### *Emergency Communications Actions*

- Coordinate with and support the 10 Regional Emergency Communications Coordination Working Groups in ensuring effective operational communications and continuity plans across all levels of government.
- Institute a program of national-level exercises that includes government agencies and infrastructure providers to increase the scope and complexity of exercises to permit refinement, testing, and exercising of communication plans and procedures.

### *Recovery Actions*

- Streamline the housing inspection and awards process, in order to align inspection efforts across federal agencies and increase timeliness of recovery assistance awards.
- Improve integration between Individual Assistance service delivery channels to provide survivors clear and easy access to the full range of FEMA assistance.
- Expand and integrate the use of outcome-driven recovery (e.g. Section 428 Alternative Procedures) into the overall delivery of Public Assistance.
- Simplify and streamline the Public Assistance disaster closeout process by reducing the current backlog, assessing current procedures, and addressing systematic issues that impede closeout.

## ***Theme: Man-Made or Natural Incident Investments***

### ***Overview and Challenges***

The Grants Program, via the Grant Programs Directorate, provided financial assistance and technical support to state, local, tribal, and territorial (SLTT) partners to build operational capabilities to implement preparedness strategies. However, as cited by GAO and the DHS OIG, management execution challenges exist for preparedness

grants that limit the program from providing the greatest benefit to taxpayers.

In addition, while the National Flood Insurance Fund paid \$4.2B in claims to more than 83,000 families, the overall program is not sustainable without congressionally approved changes.

### ***Corrective Action***

The Response and Recovery, Mitigation, and Grants Programs will be taking the following steps to address some of the significant challenges identified during the FY 2018 Strategic Review:

- Establish a Grants Management Executive Steering Group to provide executive-level leadership for the consistent implementation and administration of grants.
- Leverage internal and external partnerships to establish simplified and standardized grants management training opportunities.
- Establish a single, holistic grants management information technology platform through its Grants Management Modernization initiative.
- Continue to invest in our Enterprise Data & Analytics Modernization Initiative to provide consistent data management and an integrated, modern, and cost-effective enterprise data analysis and reporting environment.
- Continue to invest in our Financial Systems Modernization effort to acquire a financial system with business intelligence and analytics capabilities that can help the program spend its resources efficiently and effectively.

The National Flood Insurance Program will be taking the following steps to address some of the significant challenges identified during the FY 2018 Strategic Review.

- Expand the number of properties covered by flood insurance and work closely with the insurance industry, realtors, mortgage lenders, community leaders, and Congress to increase insurance purchases.
- Transform the program into a simpler, customer-focused insurance program that policyholders value and trust.
- Increase the public's knowledge of risk and encourage adequate coverage so

individuals, communities, and businesses can reduce their losses from all hazards.

- Launch a new website to increase the public's awareness and understanding of flood insurance.
- Conduct an affordability study that will serve to influence conversations on flood risk with Congress.
- Enhance the Reinsurance program for increased sound financial management.



## Management Initiatives

### Customer Experience

The President's Management Agenda includes a focus on improving the customer experience with federal services. Below are DHS's major high impact service provider organizations efforts and successes in FY 2018 and next steps and challenges moving forward.

#### ***International Travel (CBP)***

In 2018, CBP continued its long-standing efforts to aggressively identify innovative ways to increase security while also improving the international travel experience to and from the United States in the air, land, and sea border environment – welcoming more than one million international travelers a day.

#### ***Progress***

In furtherance of the national goal CBP established in 2015 to provide a best-in-class international arrival experience while maintaining the highest standards of national security, CBP has been working to make improvements in three key areas:

- Improve upfront screening to reduce traveler processing times
- Increase traveler communications and expedited processing programs to improve transparency and the traveler's experience
- Identify, customize, and scale new technologies to effectively address traveler needs better

**Improve upfront screening to reduce traveler-processing times:** CBP's 2016 Innovation Strategy set a goal to create a unified CBP arrivals process that uses the latest technology to enhance frontline risk assessment capabilities, streamline processes, and augment operational efficiency without sacrificing CBP's ability to enforce the law.

In furtherance of this goal, CBP has continued to work with private sector stakeholders to improve the pre-arrival data (APIS data) that CBP receives on passengers. This APIS data powers customer-centric processing tools that CBP has deployed in recent years, including the Automated Passport Control (APC) Kiosks, the Mobile Passport Control (MPC) Smart Phone Application, and the deployment of facial comparison technology. While these customer-processing tools are mainly used in the air environment, CBP is also enhancing operations at land and sea ports.

In recent years, CBP has improved the pre-arrival data it receives from cruise passengers. Since the summer of 2017, CBP trialed facial recognition technology through partnerships with several cruise lines in Bayonne, NJ and Miami, Florida. These trials have shown a decrease in passenger clearance times and have led to multiple sessions between CBP and the cruise industry to discuss additional facial recognition trials, automating paper forms, and implementing Smart Queuing.

While CBP currently receives APIS data from sea and air carriers, it does not currently require APIS data from bus and rail operators. Over the past few months, CBP has started working with private sector stakeholders, passengers, and front line CBP Officers to design a system that can collect APIS data from bus and rail operators. This new system and data collection will provide land ports greater visibility into who is coming to the border prior to passenger arrival, and will allow CBP to maximize safety and improve the customer experience by expediting border screening time.

Lastly, CBP developed a new secondary system, Unified Secondary, which combines the functionality of existing processing systems into a more robust inspection system that optimizes secondary operations, which results in fewer secondary referrals and quicker adjudications for passengers.

**Increase traveler communications and expedited processing programs to improve transparency and the traveler's experience:**

To increase transparency for travelers, CBP stood up the Traveler Communications Center (TCC), a 24/7 customer facing contact center to address admissibility questions or issues that international travelers encounter. On average, the TCC handles over 6,000 traveler connections per week. The TCC team conducted customer-facing research to understand current customer challenges. From that research, the team identified over 60 "pain points" and worked to identify improvement opportunities to address those pain points. The TCC developed a future state customer-centric design that incorporates best-in-class technology, standards, and processes for customer-centric contact centers.

CBP continued to expand the Global Entry (GE) program through targeted outreach campaigns that have grown the program to over 5.8M members. In total, over 8M members are enrolled in CBP Trusted Traveler Programs (Global Entry, Nexus, SENTRI), which provide expedited entry to the United States for members. During the summer of 2017, CBP unveiled Enrollment on Arrival, which allows conditionally approved GE applicants to enroll when they arrive at participating CBP airports instead of waiting to schedule an interview. This option has been more convenient for passengers and has allowed CBP to expand the number of interviews it is able to grant to potential GE members. Enrollment on Arrival has now been scaled to 47 major international airports, with over 70,000 enrollments in FY18 alone.

Modified Egress (ME) eliminates the traditional egress checkpoint passengers encounter when leaving the CBP Federal Inspection Services (FIS) at airports, a frequent source of negative feedback from travelers, airlines, and airports. ME has expanded to 18 airports since the beginning of

the pilot in 2015. Since ME implementation at Dallas Fort Worth Airport (DFW), the average transit time for passengers, from baggage claim through the FIS exit, has decreased from 10 minutes to 26.4 seconds. Miami International Airport (MIA) reported that: "Misconnects in Miami have dropped 27% due to no egress lines which has saved airlines millions." CBP is improving its officer roving operations to make sure enforcement is not compromised in favor of faster end-to-end processing times.

**Identify, customize, and scale new technologies to more effectively address traveler needs:**

CBP continues to work with stakeholders in the air, land, and sea environments to identify new opportunities to deploy facial comparison technology. This effort meets congressional and presidential mandates to biometrically confirm passengers entering and exiting the United States. CBP is also looking for opportunities to integrate facial comparison technology into its existing passenger processing programs, such as GE. CBP piloted facial recognition for U.S. GE applicants entering the Orlando Airport (MCO) and has expanded the pilot to 10 additional airports by the end of 2018.

CBP is also developing biometric submission kiosks, a new tool that helps streamline the enrollment of trusted travelers by allowing applicants to submit their biometrics and biographic information ahead of their interviews. This tool reduces wait times and improves the interview experience. These kiosks are currently going through development cycles based on user testing and changing requirements.

CBP is looking at ways to improve how CBP and passengers interact with their checked luggage at airports. In May of 2018, CBP finalized policy guidance for International to International baggage transfers, whereby passengers arriving to the United States from a foreign country and immediately transferring to another foreign country now have their bags transferred directly to their

connecting flight without having to claim them in the CBP FIS and then recheck them. This allows passengers to avoid waiting for their bags at the baggage carousel before rechecking them with the airline, which was a time-consuming and inefficient process. CBP is also working with several private sector stakeholders on baggage transfer solutions for international passengers arriving and staying in the United States.

### ***Challenges and Next Steps***

Over the last decade, CBP has transformed from paper-based clearance processes that required significant amounts of officer time to a paperless process leveraging self-service technologies like kiosks and smart phone applications. While CBP has received high marks from the traveling public for these improvements, the agency continues to see strong year over year growth in passenger volumes. On top of these increased passenger volumes, the agency is integrating facial comparison technology in entry and exit processing to meet the Biometric Entry/Exit mandate. CBP is doing all this with virtually the same size workforce it had 10 years ago.

As with any multi-year organizational transformation, there are risks associated with budget allocations, resource prioritization, systems integration processes that require alignment from multiple offices within CBP and across the broader DHS family, as well as significant contributions from private sector stakeholders. Setbacks in any of these areas could cause delays in the agency's agenda. On top of that, passenger volumes are out of CBP's control; and CBP's success in improving the customer experience is contributing to these ever-increasing passenger volumes.

There are additional challenges making sure our work force has bought into these changes. CBP leadership is working hard on this by conducting workforce listening sessions to gain feedback from front line officers, developing communications to inform the

workforce of changes, creating new training programs, and working to adapt CBP's hiring processes to adapt to the changing times.

Over the next few years, CBP will continue to aggressively develop, test, and implement new solutions to expand our business transformation initiatives. As facial comparison technology continues to be implemented across the agency, options to improve the value proposition for members of Global Entry are being considered, so the program maintains its status as the premier program for border crossers.

CBP is also looking to improve communication with our industry stakeholders. The changes CBP is making to our entry and exit processes impact airlines, airports, sea carriers, bus companies, rail companies and anyone who crosses the border. CBP also realizes that many of these initiatives, like modified egress, biometric entry/exit, and the expansion of bus and rail APIS, require strong buy-in from industry. That is why CBP is convening regular sessions with our stakeholders across the air, land, and sea environments, to co-create on solutions that will not only achieve CBP's security objectives, but will also be able to integrate with our partners' processes.

Lastly, CBP will continue our focus on travelers. CBP is working to improve our customers' ability to get their travel related questions answered with quick and straightforward answers via the TCC and is also implementing improvements in the enrollment process for programs like Global Entry. CBP will continue to solicit feedback from travelers via CBP's Customer Service Survey, and will continue to integrate opportunities to improve the customer experience, as the program did with Modified Egress.

## Emergency and Disaster Relief (FEMA)

FEMA helps to ready the Nation for catastrophic disasters and coordinates the core federal response capabilities used to save lives and protect critical infrastructure in communities throughout the Nation that have been overwhelmed by the impact of a major disaster or an emergency. When a national disaster has been formally declared, FEMA works with all those affected using a customer centric approach to ensure needs are met. The breadth of FEMA's customer base includes residents, emergency management practitioners, organizational and community leaders, and government officials. Progress and challenges and next steps are highlighted below.

### Progress

**FEMA Integration Teams:** In July 2017, FEMA Administrator Brock Long announced his intent to enhance the Agency's customer service, and the efficiency of its program delivery, by embedding FEMA staff with its state, local, tribal, and territorial (SLTT) partners via the FEMA Integration Team (FIT) program. FEMA solicited input on the FIT concept from internal and external stakeholders and received more than 500 comments. Based on the feedback, FEMA developed a phased, scalable, and tailored approach to the FIT program. The FIT program, as outlined in Objective 2.2 of the [FEMA Strategic Plan](#), ensures FEMA is planning, training, exercising, and executing with our SLTT partners every day. Better integrating FEMA operations with emergency management partners will build shared capabilities and capacity, resulting in more effective disaster response and recovery operations and a more prepared and resilient nation.

In April 2018, FEMA established the first FIT in [North Carolina](#). The effects of the team were seen immediately in the coordinated

response efforts to Tropical Storm Alberto and more recently during Hurricane Florence. FIT staff worked to establish immediate incident response and coordination support working alongside North Carolina staff. Based on this joint response, North Carolina emergency management staff were able to leverage FEMA technical expertise to further develop disaster management capabilities at the state level. At the end of Fiscal Year 2018, FEMA established the FIT program in a total of eight states with the goal of achieving 34 teams across the nation in the next year.

**Improvements in Service Delivery for Hurricane Florence:** In September 2018, as [Hurricane Florence](#) made landfall over the Carolinas, FEMA worked to coordinate the response and recovery efforts. Building upon the lessons learned from the 2017 hurricane season, and in support of improving the grantee and survivor experience under Objective 3.1 of the FEMA Strategic Plan, FEMA implemented several service delivery improvements. Specifically:

- [Simplified Transitional Sheltering Assistance \(TSA\)](#): FEMA issued disaster-specific policy that implements revisions to the TSA activation timeline, initial eligibility criteria, as well as continued eligibility directly linked to the Individuals and Households Program eligibility. Revisions also limited the need for state and tribal governments to submit extension requests.
- [Inspections Triage](#): FEMA added damage self-assessment questions to the survivor registration process, which enabled FEMA to prioritize resources and in-person inspections for those reporting the most damage.
- [Individual Assistance Delegations of Authority](#): FEMA made changes to internal processes authorizing field leadership, who have the greatest situational awareness and

understanding of need, to activate and extend FEMA Individual Assistance programs.

- **Increased Fraud Controls:** FEMA implemented increased controls to better protect survivor information and minimize fraudulent applications through added password protection and verification for survivors.

### **National Flood Insurance Program Customer Experience Improvements:**

FEMA began a Customer Experience Transformation project in 2015 to improve the National Flood Insurance Program (NFIP). As part of this customer-focused approach, FEMA conducted surveys and interviews with NFIP policyholders, advocacy groups, program partners and others, which resulted in a five-year plan to implement 40 transformational initiatives to improve customer experience. To date, FEMA completed 23 of the 40 initiatives including:

- **Appeals Journey Redesign:** In order to reduce and simplify steps in the claims and appeals process, FEMA accelerated the processing and transparency of claims by establishing standard operating procedures for claims processing and a case management tracker for transparency of claims throughout the process.
- **Claims Guidance Simplification:** FEMA clarified underwriting and claims guidance by incorporating feedback from loan executives, industry stakeholders, and regional insurance specialists. This new guidance helps NFIP better meet stakeholder expectations and better understand and apply program requirements to service policyholders.

### **Challenges and Next Steps**

On October 5, 2018 President Trump signed the Disaster Recovery Reform Act of 2018 (DRRA) into law as part of the Federal Aviation Administration Reauthorization Act

of 2018. FEMA worked closely with Congress over the past year as they considered, and ultimately passed, important reforms to federal disaster programs. These reforms acknowledge the shared responsibility of disaster response and recovery, aim to reduce the complexity of FEMA, and build the nation's capacity for the next catastrophic event. Over the next year, FEMA will work to implement the provisions of this new law to ensure enhanced service delivery for all of FEMA's customers.

Highlights from the DRRA include:

- **Greater investment in mitigation, before a disaster:** Authorizing the National Public Infrastructure Pre-Disaster Hazard Mitigation Grant Program, funded through the Disaster Relief Fund, as a six percent set-aside from disaster expenses.
- **Reducing risk from future disasters after fire:** Providing hazard mitigation grant funding in areas that received Fire Management Assistance Grants as a result of wildfire. The DRRA adds fourteen new mitigation project types associated with wildfires and windstorms.
- **Increasing state capacity to manage disaster recovery:** Allowing for higher rates of reimbursement to SLTT partners for their administrative costs when implementing public assistance (12 percent) and hazard mitigation projects (15 percent). Additionally, the legislation provides flexibility for states, tribes, and territories to administer their own post-disaster housing missions, while encouraging the development of disaster housing strategies.
- **Providing greater flexibility to survivors with disabilities:** Increasing the amount of assistance available to individuals and households affected by disasters. This includes allowing



repairs that increase accessibility for people with disabilities, without counting those repairs against their maximum disaster assistance grant award.

- **Retaining skilled response and recovery personnel:** Authorizing FEMA to provide the opportunity to certain types of temporary employees who have been with the Agency for three continuous years in order to compete for full-time, permanent positions within the Agency. This will allow the agency to retain and promote talented and experienced emergency managers.

### ***Domestic Aviation Travel (TSA)***

The Transportation Security Administration (TSA) performs domestic security operations at the nation's airports, screening about two million domestic travelers a day. TSA has taken several steps to improve the travelers' experience maintaining a strong security posture. Several examples are provided below.

#### ***Progress***

**TSA Website:** Each month, tsa.gov gets more than 7.5 million page views, making it one of the most-visited Department of Homeland Security websites. TSA designed a new layout for the [What Can I Bring?](#) tool to make it easy for passengers to determine whether items are allowed in carry-on or checked bags. TSA developed a new [online web form](#) to request surface transportation training materials, which simplified and streamlined the user experience. TSA developed a series of successful one-minute [TSA Cares videos](#) on tsa.gov to clarify screening procedures and policies for travelers with disabilities and medical conditions.

During fiscal year 2018, TSA also deployed an enhanced version of the free downloadable MyTSA mobile app with new features to

check flight delay information, current weather conditions, graphs predicting how busy airport checkpoints will be based on historical throughput data, and a live chat option with AskTSA for any travel-related questions.

#### **Traveler Redress Inquiry Program**

**(TRIP):** In FY 2018, The Transportation Security Redress Branch, along with support from interagency partners, developed a 3 x 5 inch, front/back information card that provides a quick list of traveling challenges that can be remedied by applying to the DHS Traveler Redress Inquiry Program (DHS TRIP) as well as DHS TRIP contact information. This card serves as a valuable resource for front-line Transportation Security Administration (TSA) and U.S. Customs and Border Protection (CBP) airport officers, CBP border officers, and U.S. Department of State (DOS) embassy personnel to educate both the internal USG stakeholders and the external traveling public with which they interact regarding DHS TRIP. The DHS TRIP Information Card has been well-received by our USG partners working in airports, border crossings, and embassies.

**TSA Customer Service Branch (CSB):** In 2018, CSB participated in several roundtables with other government agencies to share best practices for metrics related to the customer experience. The CSB staff developed a bi-monthly newsletter for Customer Support Quality Improvement Managers in the field responsible for dealing directly with customers outlining trends in customer complaints and best practices for resolution and held quarterly Video Teleconferences providing training on dealing with difficult customers and plain language responses. Through the work of CSB, TSA was able to increase the response rate of complaints sent to the field to 98% within 60 days up from 30% in previous years.

**Multicultural Branch:** In FY 2018, TSA saw a twofold growth in the TSA Multicultural Coalition (Coalition) through

direct engagement driven by the Multicultural Branch (MB). Engagements included speaking to and attending the Pakistani-American Chamber of Commerce and Business Council conference, Sikh American Legal Defense and Education Fund's *Know Your Rights* events, Gathering of Nations Powwow, and the Southern Comfort Transgender Conference. In addition, MB hosted multiple conference calls with Coalition members to share information about TSA programs for travelers. MB also shares information regularly with Coalition organizations and the communities they represent, through the *Know Before You Go* publications, holiday travel tips, and coordinating TSA presence at regional and local Coalition organization events with field TSA colleagues and hosting TSA's 16<sup>th</sup> Annual Coalition conference. Other engagements included sharing information with participants in U.S. Department of Justice's Muslim Arab, Sikh, South Asian and Hindu (MASSAH) community meetings, and Department of State's Hajj briefing for Hajj travelers and travel agents/planners. MB partnered with Training & Development to develop Passenger Support Specialist (PSS) training; training on screening transgender travelers, and training on Civil Rights and Liberties requirements for all public facing programs at TSA. In addition, MB worked with Strategic Communication & Public Affairs on an AskTSA video on hair pat-downs.

**Disability Branch:** In FY 2018, TSA's Disability Branch drove robust outreach and engagement activities with the Disability and Medical Conditions Coalition, which consists of 400 national, regional, state, and local disability organizations and advocacy groups. Engagements included speaking at the biannual Open Doors Organization conference, issuing holiday travel tips and a monthly *What to Expect* publication, sponsoring booths at conferences, and hosting the 16<sup>th</sup> annual Coalition conference. Also,

this year, the Disability Branch partnered with Security Operations to launch a new Passenger Support Specialist (PSS) identifier as well as an "American Sign Language" nametag for officers to wear to make it easier for travelers to identify officers who can provide specialized assistance at the checkpoint. Moreover, the Disability Branch and Security Operations convened listening sessions with Coalition members to discuss proposed procedures changes. The Disability Branch partnered with Strategic Communications and Public Affairs to develop and launch *TSA Cares* videos using Coalition members, which are posted to tsa.gov, and are designed to help travelers better understand how to prepare for security screening. The Branch partnered with Training & Development, and Coalition members, to develop PSS training, which will be available online for the workforce in FY 2019.

**TSA Tort Claims Process:** TSA screens millions of passengers and bags each year; occasionally TSA will damage a passenger's personal belongings. To assist with filing a claim with the Agency, information can be found on the TSA user friendly public website. Passengers may submit a claim by email, fax, or USPS. TSA has continued to train transportation security officers on actions that may lead to claims, promoted efficient baggage tracking, lost and found systems, and other procedural changes to assist in reducing claims and keep the public's trust. This work has resulted in a 50 percent reduction in tort claims over the last six years.

#### ***Challenge and Next Steps***

The TRIP case management system has reached the end of its useful life expectancy and is subject to slowdowns and failures, leading to decreased programmatic performance. The Transportation Security Redress Branch will continue to work with TSA IT to determine a viable technology solution for the program's complex requirements, while also coordinating with

TSA IT on a weekly basis on the status of all ongoing system problems in an effort to get them resolved quickly.

CSB is facing: 1) a significantly increased passenger complaints workload, which must be processed by limited staff within the 180-day statutory deadline, and 2) limited availability of funds to engage in more proactive measures to stem the complaints volume (*e.g.*, workforce training, public booth, and speaking events).

In FY 2018, the Disability Branch received 1,387 complaints as compared to 862 referrals in FY 2017 and 573 referrals in FY 2016. The increased passenger complaints activity exceeds the estimated 4-8 percent increased passenger volume at the checkpoints each year. This trend is expected to continue as passengers become more aware of their federally-mandated civil rights in TSA's security screening activities, including the right to file discrimination complaints.

### ***Immigration Benefits (USCIS)***

USCIS processes more than 8 million citizenship and immigration benefit requests annually. Through a variety of forums, USCIS communicates information about the immigration benefit request process to help applicants successfully navigate. At USCIS, commitment to Customer Experience (CX) drives the design and development of programs and compels transparency with applicants and the public.

#### ***Progress***

**Public Engagement Efforts:** USCIS holds a variety of external stakeholder events to share information and obtain feedback on USCIS programs and policies. During FY 2018, USCIS held 3,528 engagements across USCIS and the country, with a total of 142,285 applicants and individuals reached through a combination of in-person meetings, teleconferences, webinars, trainings, and other outreach activities. From June 2018 to September 2018, USCIS hosted over 1,000

activities for more than 30,000 individuals. Key efforts involve promoting USCIS priorities such as online filing, immigration scams, and immigration fraud. Public engagement had a major role promoting USCIS' transition to online filing. Numerous training sessions were hosted for Community Relations Officers and USCIS staff participated in external and internal presentations in the field (Miami, Boston, Dallas, San Francisco), held four national stakeholder webinars on online filing, presented online filing on a quarterly webinar with the Institute of Museum and Library Services (IMLS), and presented a webinar for recipients of the Citizenship and Assimilation grants. USCIS continue to lead the USCIS immigration scams working group, hosting monthly meetings with USCIS colleagues from the Fraud Detection and National Security Directorate, Office of Policy and Strategy, Office of the Chief Counsel, and others to discuss and take action on relevant topics in the immigration scams and fraud arena.

Additionally in FY 2018, public engagement coordinated the development of USCIS' External Disability Access Plan, a DHS requirement. This was an agency-wide effort involving numerous working meetings with most USCIS directorates and program offices to develop a robust action plan. The action plan is under concurrence and will be submitted to DHS in early FY 2019.

**Citizenship Outreach:** Under its formal partnership with IMLS, USCIS continued its efforts to provide immigration and citizenship information for public libraries across the United States and worked on expanding awareness within the museum community. The partnership expands the availability of information about the citizenship and naturalization process for immigrants by equipping libraries and museums with information on available USCIS resources that they can share within their communities. In FY 2018, USCIS program offices

collaborated with IMLS to conduct three national webinars for libraries and museums on citizenship and immigration-related topics. More than 311 library and museum representatives participated. In addition, USCIS participated in 16 national or state-level conferences for libraries and museums. To date, USCIS has 11,171 subscribers registered to receive information specific to libraries and museum. In FY 2018, there were approximately 5.4 million unique visitors to the Citizenship Resource Center, which is a dedicated online portal for the public with information and resources on citizenship and the naturalization process. In FY 2018, the online Citizenship Resource Center received an overall American Customer Satisfaction Index score of 86 out of 100. The Citizenship Resource Center continues to outperform all benchmark categories and is the top performer within DHS according to ForeSee. USCIS continuously looks to incorporate feedback from usability audit reviews of the site, update and provide new content for the three main audiences of the site (applicants/learners, educators, and organizations), and implement industry best practices when possible.

**myUSCIS:** USCIS is leveraging technology to design various electronic tools that give applicants faster and easier access to immigration information. The flagship of this suite of tools is [myUSCIS](#), an online portal designed to help applicants navigate the immigration process. It includes an Explore My Options tool, Civics Practice Test, Naturalization Class Locator, and Find a Doctor (for required immigration physicals), all of which are accessible from any mobile device without a need for an account. In addition, myUSCIS continues to serve as the portal for all online filings. USCIS currently offers online filing for Form I-90, Application to Replace Permanent Resident Card; Form N-336, Request for a Hearing on a Decision in Naturalization Proceedings (Under Section

336 of the INA); Form N-400, Application for Naturalization; and Form N-565, Application for Replacement Naturalization/Citizenship Document. In FY 2018, online filings accounted for approximately 40 percent of all filings, and [myUSCIS](#) saw nearly 31 million online visits—a 90 percent increase from FY 2017.

**USCIS eProcessing Initiative:** The eProcessing initiative is an agency-wide priority to move USCIS from a paper-based environment to a digital environment where filing, communication, and adjudication are all completed on an electronic platform. As part of eProcessing, USCIS will adapt existing systems to use as enterprise services and develop micro-services, which are a functional, reusable IT services that can be accessed across all agency product lines and operations, as needed. This approach enables USCIS to erect functionally-aligned services at the agency level that all case management systems will rely on. The developed enterprise micro-services include intake, payment, accounts, case management, content management, risk and fraud, person-centric data, scheduling, correspondence, and appeals.

USCIS continues to expand the product lines digitally processed through the Electronic Immigration System (ELIS), which to date has ingested over 10 million cases, and currently processes about 40 percent of the agency's annual workload. This system supports intake, processing, and adjudication of applications, petitions, and requests filed through both paper and online channels. Over the past year, USCIS continued to make system enhancements designed to increase productivity, and enhance the reliability, security, and overall capability and efficiency of ELIS. During 2018, USCIS added intake, processing, and adjudication functionality for Form N-336 and Form N-565 to ELIS, enhanced streamlined processing capabilities for certain existing product lines, and



introduced several new efficiencies intended to align with the eProcessing initiative.

### ***Challenges and Next Steps***

**Promoting Awareness of Online Tools and Services:** With the priority to direct applicants to online filing and online self-help tools, USCIS has begun a robust promotion plan to help familiarize our stakeholders and applicants with the new opportunities to file online or request services online. During FY 2018, USCIS hosted 14 national and local engagements with nearly 1,400 participants focused specifically on online services, including stakeholder engagements in each of the four USCIS regions. In addition, community relations officers have shared information about USCIS' online tools and resources during hundreds of outreach events with thousands of stakeholders and members of the public. The plan also involves using social media, redesigning the look and feel of web pages to promote increased use of online tools, and launching an updated virtual assistant to help online visitors.

USCIS recognizes the diversity of those served. In order to meet the various needs of our applicants, USCIS has implemented strategies to seek stakeholder and applicant input through ongoing research and engagement. This includes user-research and testing for public-facing online tools, as well as in-language resources and outreach efforts. Additionally, providing resources to immigrant communities to help build digital literacy is crucial for transitioning from a paper-based to a digital-based operation.

**myUSCIS:** In FY 2019, USCIS will continue integrating new forms and product lines into the online experience. This will include Form N-600, Application for Certificate of Citizenship; Form N-600K, Application for Citizenship and Issuance of Certificate Under Section 322; Form I-539, Application to Extend/Change Nonimmigrant Status; and Form I-130, Petition for Alien Relative. The myUSCIS team works closely with external

stakeholders to conduct ethnographic research on the immigrant journey to better identify the diverse needs within the applicant experience. In addition, myUSCIS hosts voluntary interviews and surveys to collect research data on process gaps and process improvement opportunities intended to improve the online applicant experience and to inform agency policy and procedures.

The myUSCIS team uses the agile methodology to develop new products. A key component of this approach is engaging in quantitative and qualitative research with end users so that USCIS develops meaningful products and solutions. Leveraging technology from GSA, USCIS is working to add a recruiting tool to the myUSCIS site to solicit feedback and volunteers for moderated and unmoderated surveys. The unmoderated surveys can provide real-time transaction-level measures. As the applicant uses a product, USCIS can receive valuable feedback and insight. USCIS is currently awarding an omni-channel survey contract that will potentially allow the measurement of an applicant's perspective after a single transaction, a journey, or a series of transactions and journeys with USCIS.

The agency is taking measureable steps to implement a robust CX program that complies with the requirements of Office of Management and Budget (OMB) [Circular A-11, Section 280](#). The Circular includes three requirements: Maturity Self-Assessment; Development of a Customer Service Action Plan; and Implementation of Customer Experience Measures.

**Maturity Self-Assessment:** Led by the Office of Citizenship and Applicant Information Services (CAIS), External Affairs Directorate, USCIS is working with partners across the agency to execute the maturity self-assessment. These partners represent key management and operational functions within the agency. CAIS is developing internal policies and procedures, including



standardized rules of engagement for conducting the annual assessment.

**Development of an Action Plan:** USCIS is on target to meet OMB's deadline of June 30, 2019, for the service action plan and will use the results of the maturity self-assessment to develop an action plan that addresses the primary components outlined in A-11, Part 280, as well as any other gaps and deficiencies identified. Specifically, the plan will capture:

- Organization/Accountability;
- CX Program Maturity;
- CX Data Collection and Metrics; and
- CX Delivery Improvement.

The plan will also address the core CX functions, to include Measurement, Governance and Strategy, Culture and Organization, Customer Understanding, and Service Design.

**Implementation of CX Measures:**

USCIS is complying with OMB's requirement to report CX performance measurement data quarterly. Currently, USCIS manually administers a survey via telephone to a statistically valid sample size of callers contacting the USCIS Contact Center toll-free number.

By late FY 2019, USCIS will transform the process through the implementation of an automated omni-channel survey tool that will eliminate the need for the manual telephone survey. The tool will be integrated across all public-facing channels within the [USCIS Contact Center](#) to include the toll-free phone number, e-mail, and live chat. It will also include two digital channels: the [myUSCIS](#) website and the interactive virtual assistant "Emma" [within](#) the [USCIS website](#). In addition to significantly expanding the sample size and channels, the tool will transform how USCIS measures the applicant experience by enabling the agency to assess survey feedback real-time across multiple touchpoints. It will also enable USCIS to review and analyze trends and issues at a strategic level.

## **Program Management Improvement and Accountability Act (PMIAA)**

### **Overview**

On December 14, 2016, the Program Management Improvement Accountability Act (PMIAA), Pub. L. No. 114-264, was signed into law. The Act aims to improve Program and Project Management (P/PM) practices within the Federal Government, requires Government-wide standards and policies for program management, and establishes a new interagency council to improve P/PM practices among agencies. The Act establishes a new role: the Program Management Improvement Officer (PMIO). The responsibility of PMIOs is to implement program management policies established by their respective agencies and develop strategies to enhance the role of program management and managers within their departments. Additionally, the PMIAA requires that agencies conduct annual portfolio reviews of programs in coordination with the Office of Management and Budget (OMB) to ensure major programs are being managed effectively, and that OMB conduct reviews of areas identified by the Government Accountability Office (GAO) as "high risk." The Act complements implementation of the Presidents Management Agenda and the broader Administration goal of ensuring taxpayer dollars are providing critical federal services to citizens efficiently and cost-effectively.

### **Progress**

PARM has created an internal Integrated Program Team (IPT) that is in the process of building the DHS draft PMIAA Implementation Plan. The IPT held a kick off meeting in October 2018 and has created a high level outline based on OMB guidance. The IPT is used this outline to create the first draft of the Implementation Plan.

PARM also met with the Office of Program Analysis and Evaluation (PA&E) in September 2018 to discuss ideas for integrating the Strategic Review (SR) with the Portfolio Review as directed by PMIAA. As a result, PARM provided a series of analytic questions for consideration during the SR Assessment Teams discussions of evidence of progress made during the past fiscal year. PARM also suggested the use of “one-pagers” for the major acquisition programs to be used as evidentiary data.

The IPT had the first version of the DRAFT PMIAA Implementation Plan completed by late October. It was reviewed and finalized and submitted to OMB as required in November 2018.

### ***Next Steps***

The IPT will continue to work with stakeholders on defining and coordinating PMIAA requirements and establish a high-level plan of action and milestones (POA&M). The IPT will also coordinate with the DHS OCFO Office of PA&E to fully integrate acquisition program oversight and governance with the FY19 DHS Strategic Review. Staff supporting the PMIO will also continue to coordinate with those leading the Strategic Review effort to consider the results from the review and connections between operational progress and the program management for our major acquisitions.

## **Regulatory Reform**

DHS remains committed to regulatory reform as identified in *Executive Order (EO) 13771, Reducing Regulation and Controlling Regulatory Costs*. Regulatory components throughout DHS continue to review their regulatory and related stock, analyze the impacts and costs of that stock, identify possible deregulatory actions, and develop deregulatory actions.

Section 4 of *EO 13777* specifies that agencies should measure their progress in performing

regulatory reform tasks. Specifically, the executive order states that agencies should incorporate performance indicators into their annual performance plans; those performance indicators should measure progress toward the goals of: 1) improving implementation of regulatory reform initiatives and policies, and 2) identifying regulations for repeal, replacement, or modification. DHS has implemented these requirements.

### ***Progress***

DHS’s regulatory reform progress in FY18 was notable. DHS issued a total of 13 deregulatory actions and realized a present value cost savings of -\$163.5 million (7% discount rate). In addition, in FY18, DHS issued no new significant regulations imposing costs. Of the 25 agencies that OMB ranked for deregulatory activity in FY18, DHS had the sixth highest number of deregulatory actions, and DHS was in the top half of agencies with the highest monetized cost savings. DHS hopes to make continued good progress this coming fiscal year in identifying and issuing deregulatory actions.

In accordance with the Office of Management and Budget *Memorandum M-17-23:*

*Guidance on Regulatory Reform*

*Accountability under Executive Order 13777: Enforcing the Regulatory Reform Agenda*, below is the planned performance targets for FY19 and FY20 for regulatory reform.

### **1. Evaluations**

Number of evaluations to identify potential EO 13771 deregulatory actions that included opportunity for public input and/or peer review	FY19 Target	FY20 Target
	3	5

### **Description and Data Collection**

**Methodology:** This indicator represents the number of evaluations DHS will issue in the given FY *and* for which DHS will seek public input or peer review. The evaluations are used to identify potential *EO 13771*

deregulatory actions. These evaluations include proposed rules and regulatory impact analyses that publish during the FY, and exclude interim final rules, final rules, and collections of information. DHS has a centralized regulatory clearance process managed by the Office of the General Counsel (OGC). Evaluations will be tracked through the internal DHS regulatory tracking system, through the internal OMB tracking system, as well as based on publication in the Federal Register.

## 2. Deregulatory Actions Recommended

Number of EO 13771 deregulatory actions recommended by the Regulatory Reform Task Force to the agency head, consistent with applicable law	FY19 Target	FY20 Target
	14	10

### Description and Data Collection

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

## 3. Deregulatory Actions Recommended & Issued

Number of EO 13771 deregulatory actions issued that address recommendations by the Regulatory Reform Task Force	FY19 Target	FY20 Target
	8	4

### Description and Data Collection

**Methodology:** This indicator represents the number of EO 13771 deregulatory actions that DHS issues in a given fiscal year based on recommendations that the Regulatory Reform Task Force made to the Secretary. These *EO 13771* deregulatory actions include

proposed rules, interim final rules, final rules, collections of information, and guidance documents that publish in the given fiscal year. DHS has a centralized regulatory clearance process managed by OGC. All regulatory and deregulatory actions are tracked through the internal DHS regulatory tracking system, through the internal OMB tracking system, as well as based on publication in the Federal Register.

## 4. Regulatory Actions Issued & Deregulatory Actions Issued

Number of EO 13771 regulatory actions and, separately, EO 13771 deregulatory actions issued	FY19 Target	FY20 Target
	11 / 8	11 / 4

### Description and Data Collection

**Methodology:** This indicator contains two parts.

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

DHS has a centralized regulatory clearance process managed by OGC. All regulatory and deregulatory actions are tracked through the internal DHS regulatory tracking system,

through the internal OMB tracking system, as well as based on publication in the Federal Register.

### 5. Total Incremental Cost

Total incremental cost of all EO 13771 regulatory actions and EO 13771 deregulatory actions (including costs or cost savings carried over from previous fiscal years)	FY19 Target	FY20 Target
	\$0	\$0

#### Description and Data Collection

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

#### Challenges and Next Steps

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

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

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

In addition, DHS continues to work on regulatory actions required by statutes, such as those required by the *Implementing*

*Recommendations of the 9/11 Commission Act of 2007 and the Sandy Recovery Improvement Act of 2013.*

The need for DHS to prioritize regulatory actions that flow from these immigration Executive Orders and to fulfill existing statutory mandates poses a challenge for DHS regulatory components also concurrently prioritizing regulatory reform.

### Human Capital Operating Plan (HCOP)

The Office of the Chief Human Capital Officer (OCHCO) continues to meet personnel challenges to support the dynamic mission of the Department. In FY 2018, OCHCO sustained a progressive pace in human capital processes and solutions. OCHCO maintained success in the areas of mission critical skill gaps closure, leadership accountability, and human resources developmental training. OCHCO also made accomplishments in the area of recruiting to ensure talented individuals from all aspects of the population fill mission critical occupations as well as other job opportunities.

The Human Capital Operational Plan (HCOP) serves as the guiding document to unify the DHS human capital community's efforts to achieve DHS's human capital goals through Department-wide programs and initiatives. The Human Capital Leadership Council – consisting of the DHS Chief Human Capital Officer, chief human capital officers from each of the DHS Components, and OCHCO executives – has continued the practice of developing and implementing the annual HCOP which executes the Secretary's human capital objectives, highlighted in blue, and addresses regulatory requirements under 5 CFR Part 250, Subpart B – Strategic Human Capital Management.



***Promote a culture of leadership and empower employees to execute their missions***

The Secretary designated FY 2018 as DHS Leadership Year in an effort to elevate a culture of leadership excellence and evolve leadership practices that increase morale and deliver mission results. DHS Components have documented nearly 300 initiatives and activities to integrate Leadership Year principles and ideals into future improvements beyond the close of the year. All DHS organizations have made considerable progress in developing, promoting, and integrating Leadership Year key principles into practice. At the Department level, Leadership Year has been supported by a dynamic strategy, robust infrastructure, and several high-visibility, high-impact products and opportunities. Some events included senior leader videos, a bi-weekly Leaders Digest, Component commitments, and initiatives that promoted the value of leaders at all levels. Components also built products and programs that implemented and supplemented Department-wide initiatives.

Additionally, Leadership Year has become integrated in sustainable ways to support ongoing organizational productivity. For instance, the new Countering Weapons of Mass Destruction (CWMD) office is using Leadership Year strategies as the foundation of their organization development and change management strategies as they move into a new organizational structure for FY 2019.

***Enhance recruiting efforts and streamline personnel hiring practices***

DHS has the largest law enforcement population in the Federal Government. Women occupy approximately eight percent of law enforcement positions in DHS, compared to approximately 16 percent in the rest of the federal sector. The Department is committed to hiring talented individuals from underrepresented groups and fill vacancies in our mission critical occupations. Based on a

comprehensive data analysis of the Department's current and future hiring requirements, the need to attract more women into our law enforcement positions, and in support of Executive Orders (EO) 13767 and 13768, OCHCO led the planning effort for a recruiting and hiring event to fill hundreds of critical law enforcement vacancies across the Department.

DHS held the Joint Law Enforcement Recruitment and Hiring event, specifically targeting women, from June 26 – 27, 2018, in Arlington, Texas. Nearly 2,000 highly qualified individuals attended the event. As a result of the event, job opportunity announcements posted, and marketing efforts, the Department issued 759 tentative job offers to fill critical vacancies across the Department. The hiring event supported the EO hiring surge and provided the Department with additional resources, tools, and personnel to carry out the critical work of securing our borders, enforcing our immigration laws, and ensuring that individuals who pose a threat to national security or public safety cannot enter or remain in our country. The Department also shortened the time-to-hire at the event by using direct hire and other special hiring authorities, having human resources staff work directly with hiring managers, and bringing candidates through the security process with personnel security specialists on site.

DHS continued to be more strategic in tracking how it uses its recruitment, outreach, and marketing resources by relying upon a standardized method of collecting Component data on thousands of recruitment activities. The Recruiting, Outreach, and Marketing Matrix (ROMM) allows DHS to track attendance, locations, recruiting costs, target audience, and marketing focus, helping to maximize recruiting return on investment. In FY 2018, OCHCO developed requirements to automate and streamline this data collection method and began the design and development phases of the system. In FY



2019, OCHCO will finalize the initial phase of requirements gathering on ROMM automation and pilot the ROMM with the majority of DHS Components. Ultimately, the ROMM will provide real-time data analytics, hiring and recruitment forecasts, talent workforce gaps, and best practices to allow the Department to hire the workforce of the future.

DHS increased its cybersecurity workforce planning and analysis efforts to gain better insight into cybersecurity work to meet mission needs and meet statutory mandates Cybersecurity Workforce Assessment Act - P.L. 113-246, and Federal Cybersecurity Workforce Assessment Act of 2015 - P.L. 114-113). During FY 2018, DHS made great progress in identifying and coding cybersecurity positions and employees according to the National Initiative for Cybersecurity Education Workforce Framework's new three digit, role-based coding structure required by P.L. 114-113. In April 2018, Components completed coding of both vacant and encumbered positions, establishing a new baseline of over 10,000 civilian federal positions. In addition, DHS refined its processes for validating DHS-wide cybersecurity workforce planning data, in compliance with recommendations from the Government Accountability Office (GAO-18-175).

DHS also deployed a process for analyzing data to surface work roles of critical need, and provided the Office of Personnel Management with an initial set of critical needs, which will be the focus for gap closure efforts in FY 2019.

Lastly, DHS continues to finalize the design of a new cybersecurity personnel system, using authority granted to the Department through P.L. No. 113-277. In FY 2018, OCHCO crafted several foundational design elements of the new personnel system and addressed key policy decisions with the DHS Office of the General Counsel, Component cybersecurity and human capital staff, and

OPM, with whom Congress asked DHS to coordinate implementation. DHS also began planning for initial launch, which is scheduled for late FY 2019.

### ***Improving Personnel Training, Professional Development, and Education Opportunities***

OCHCO implemented multiple initiatives to enhance the effectiveness, return on investment, and return on expectation in the training, professional growth, and development of its people.

OCHCO facilitated improved employee engagement through Department-wide activities including: the launch of "DHS Leadership Year," designed to reinforce a culture of leadership excellence; a "listening tour" by senior officials to hear how to most effectively support the workforce; sharing of best practices and new ideas through the Employee Engagement Steering Committee (EESC); and a continued structured, rigorous approach to Component-level employee engagement action planning.

The 2018 FEVS results were overall positive, with the Employee Engagement Index holding steady and the Global Satisfaction and New IQ Indices increasing by one percentage point. OCHCO worked extensively with the EESC to develop Employee Engagement Action Plans targeting Component and sub-Component issues.

As a result of the preliminary data analysis and information gathered through the listening tours, during FY 2019 DHS leadership will host an all-executives forum and work with the Operational Components on implementing the engagement elements of the President's Management Agenda, to include identifying and working intensively with the Components and offices with lower scores to increase their employee engagement and morale percentages.

OCHCO continues to develop the data visualization of mission-critical training and leader development metrics across all Components, allowing organizations across

the Department to view and access training, reducing redundancies and increasing consistency in outcomes. Continuing this review cycle and projected DHS Mission Training and Leadership data calls, OCHCO will further the Department's unity of effort. The reviews and data calls will also contribute to the Department's ability to respond to requests quickly, demonstrating DHS's commitment to training and development. This sends a positive message that DHS is effectively using data to drive decisions. Through the implementation of the DHS wide Mandatory Training (MT) application and review process, OCHCO reviewed and approved six of eleven MT courses to ensure MT criteria were met. These efforts have significantly improved MT training quality and overall effectiveness while decreasing duplicative efforts DHS-wide. These actions minimize employee loss of productivity and save DHS-wide financial resources. OCHCO also successfully reviewed the current and projected future use of mobile learning technology and developed a DHS Mobile Learning Technology Strategy Report to support the Workforce Development Strategy. Additionally, the DHS Leader Development Program delivered a study that assessed the value of the significant investment that the Department makes in the Senior Executive Service Candidate Development Program (SES CDP), a targeted executive succession program. OCHCO defined effectiveness as whether graduates perform higher than non-graduate peers. In all categories, supervisors rated graduates' performance higher than non-graduate peers' performance. Differences were greater in SES positions, suggesting that the SES CDP's benefit is best realized at its intended level. These results indicate that supervisors consider SES CDP graduates among the best performers they supervise much more often than individuals who did not participate in the SES CDP. This study is important not only to assess the viability of the Leader Development Program in meeting

its objective, but further indicates DHS will benefit from selecting executives from the graduate pool.

### ***Retain and Reward Exceptional Performers***

In an effort to retain and reward exceptional performers, the Department continues to research and consider available solutions to address pay parity concerns. A review of uniformity across pay compensation levels available for law enforcement officers (LEO) revealed that pay parity is not an overwhelming issue. The pay parity study revealed that employees are concerned with other equity issues such as work/life balance, staffing levels in remote duty stations, special law enforcement retirement coverage, and accounting for uncontrollable overtime work. Where pay parity concerns do exist, OCHCO provided study findings to the Secretary, continued pursuing legislative proposals for law enforcement availability pay, and explored options for the Federal Protective Service retirement parity. Additionally, the Department has recommended special salary rates and compensation to attract and retain personnel in mission critical occupations (MCOs) and submitted a request to the Office of Personnel Management (OPM) for Special Salary Rates (SSR) and compensation for U.S. Customs and Border Protection pilots.

Employee performance management and appraisal are important in the Department's strategy to create a culture of superior organizational performance. Successful accomplishment of individual employee performance in support of the DHS mission is a worthy goal of both managers and employees, and creating and implementing meaningful performance feedback is an ongoing priority of the Department. OCHCO has benchmarked current employee recognition programs across the Department. The intent is to strengthen and mobilize programs and to communicate and reward employee performance. Components identified programs and mechanisms and

OCHCO created the DHS Plan to Maximize Employee Performance. OPM's "Coach for Success and Difficult Conversations" is available for managers across the Department through Component learning management systems. Other performance feedback mechanisms include the DHS-wide Employee Performance Management Program, the DHS Mentoring Program, Secretary's Awards Program, and specific Component awards programs.

***Enhance career paths and develop greater cross-Component opportunities for career advancement***

The Joint Duty Program provides the DHS workforce with opportunities to 1) enhance operations and mission execution; 2) support unity of effort; and 3) enhance leadership and professional development opportunities. The pilot began in May 2017, with the assignment of Joint Duty Program participants in the DHS Joint Task Force elements. Program success led to the continued phased expansion during FY 2018 throughout DHS and across the Federal Government. Program growth continues with enhanced marketing and process improvement.

DHS is also analyzing and recommending career pathing for law enforcement positions within the 1800 job series. For the 0201 human resources job series, DHS is analyzing, recommending, and creating career pathing with online resources, assessment tools, and skill-building opportunities. Through the establishment of these career paths, DHS can offer more career mobility options, further retention of personnel, and maximize unity of effort across the Department.

OCHCO continues to build a strong relationship with all of the Department of Defense (DOD) Senior Service Schools. Through an inter-agency agreement with DOD, the Department selects 30 employees to attend both in-residence and distance learning graduate degree programs that focus on

strategic and operational security planning. This inter-agency partnership, which includes the presence of DHS faculty at the schools, ensures the DHS mission is represented in the curricula at the DOD Senior Service Schools and the Command and Staff programs. In addition, DHS participates in various strategic leader development programs sponsored by the Departments of State and Defense, the Director of National Intelligence, the Massachusetts National Guard, and the Center for Homeland Defense and Security, providing another 90 development opportunities.

OCHCO launched the DHS HR Academy to strengthen the professionalism of the Department's HR cadre and to provide a developmental path for new HR hires. The academy will provide a range of developmental experiences, from internships, rotations, and classroom training, to on-line training opportunities in both foundational and specialized HR topics, as well as coaching and mentoring.

***Develop programs to enhance employee health, fitness, readiness, and resilience***

DHS employees stand ready on the front line of the Nation's security. The Department's work is challenging, and many of its employees work long hours in remote locations as they execute the five core homeland security missions. The Department's goal is to support employees and their families with practical assistance for everyday issues as well as provide support during times of crises and unexpected emergencies.

The Employee and Family Readiness Program (EFR) was established in January 2018 and is one of the Secretary's key priorities. The goal of the EFR Program is to ensure employees and their families have the resources to manage day-to-day stressors while being fully prepared to manage emergency events or unexpected crises.

The governing body is the Employee and Family Readiness Council (EFRC), which is comprised

of members from each of the Operational Components. In 2018, the EFRC drafted a Strategic Plan for full program implementation by the end of FY 2019. Key goals of the plan are to establish, in cooperation with the Components, an overarching resilience and family readiness policy that sets standards for a minimum level of services available to employees and their family members and to develop guidelines by which Components are to develop and implement EFR initiatives.

Benchmarking of Component programs was completed in 2018, as was an EFRC prioritized ranking of wellness and resilience programs of greatest importance to the DHS workforce. In addition, the EFR Program identified metrics for program success.

The EFR Council (EFRC) has ranked 18 family resilience issues by priority and is systematically addressing these items.

- The top five items are:
  - General Stress
  - Dependent Care (child care)
  - Personal Relationship Issues (couples)
  - Mental Illness
  - Financial Concerns

**FY 2019 Actions:**

- **General Stress:** Deliver Mindfulness-based Stress Reduction training
- **Dependent Care:** Develop a DHS-wide approach and recommendation
- **Personal Relationships:** Expand CBP's "Building Stronger Bonds" relationship training to all of DHS
- **Mental Illness:** Public-facing DHS.gov website tools and information for employees and families to:
  - Manage stress
  - Improve mental health and physical well-being
  - Find professional help

- **Financial Concerns:** Yearlong campaign – "Invest in Your Financial Health"

As an organization, the Department has a duty to ensure employees and their families have the right resources, at the right time, to enhance their wellness and increase resilience. Taking care of our workforce and their families is vital to operational readiness and mission accomplishment. A well and resilient workforce is a ready workforce.

***Support HR operational effectiveness using information technology***

In support of meeting the Secretary's human capital objectives, the Department continues to strengthen its Human Resources Information Technology (HRIT) program using a cyclical portfolio analysis process and adds Strategic Improvement Opportunity (SIO) initiatives to fill gaps in the portfolio. The Human Capital Segment Architecture Blueprint update uses a two-year cycle to review and analyze the DHS HRIT portfolio to identify capability gaps in IT solutions and addresses these gaps by setting technical and business requirements to acquire effective solutions. These initiatives include improving policy, processes and governance, connecting IT systems DHS currently uses to make the systems more effective, as well as acquiring new automation capabilities. As a result of OCHCO's work to support the Human Capital Segment Architecture's Department-wide requirements are more clearly defined and provide the foundation for more efficient and effective human capital operations.

In FY 2018, OCHCO completed four SIO initiatives: capturing and making available position management data for analytics; aligning positions to manpower models for mission critical positions; semi-automating employee relations reporting; and semi-automating labor relations reporting. In FY 2019, OCHCO will begin implementation of automation capabilities for position management, talent development and training,

employee performance management, employee relations, and labor relations. Additionally, OCHCO will complete several data interchanges, various staffing solution

upgrades, and begin migrating the final Component to the DHS-wide time and attendance solution.



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

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

OIG's 2018 Major Management and Performance Challenges report focused on highlighting persistent management and performance challenges that hamper the Department's efforts to accomplish the homeland security mission efficiently and effectively. The Senior Official Performing the Duties of the Inspector General (SOPDIG) stated the Department continues to strive to act as a single, focused organization while establishing strong internal controls and incorporating management fundamentals. The SOPDIG identified challenges in four broad areas:

- Unified Effort, Internal Controls, and Management Fundamentals;
- Oversight and Management of the Homeland Security Mission;
- Acquisition Program Management; and
- Cybersecurity.

The SOPDIG stated that overcoming these challenges demand unified action and that the Department has taken steps to achieve this unity. However, the challenges persist.

Additional details can be found in the OIG's

report "Major Management and Performance Challenges Facing the Department of Homeland Security," OIG-19-01, dated November 9, 2018, located at:

<https://www.oig.dhs.gov/sites/default/files/assets/2018-11/OIG-19-01-Nov18.pdf>

The Department's management response letter to the SOPDIG's draft report emphasized that DHS senior leadership continues to maintain a culture where everyone understands and believes that audits make the Department stronger and recognized that the OIG's report provides valuable insights. However, the Department expressed concern that the report did not seem to equitably balance the challenges the Department faces with the progress made in addressing those challenges. For example, senior leadership believes that OIG's original characterization of internal controls could leave readers of the report with a mistaken impression about DHS efforts and success achieved in implementing effective internal control and incorporating management fundamentals in programs and operations across Components. Based on management's feedback, OIG updated its report as the SOPDIG deemed appropriate. A full copy of the Department's response was included in an Appendix to the OIG's final report.

The most recent report, GAO "High Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others" (GAO-17-317), found at:

<http://www.gao.gov/assets/690/682765.pdf>

was published on February 15, 2017. The report included two areas in which DHS is the lead federal agency, and eight government-wide areas with significant DHS equities, seen in the following table.

Scope	Issue Area	Year Issue First Added to GAO's High Risk List
DHS-specific	Strengthening DHS Management Functions	2003
	National Flood Insurance Program	2006
Government-wide	Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructures and Protecting the Privacy of Personally Identifiable Information	1997
	Strategic Human Capital Management	2001
	Managing Federal Real Property	2003
	Ensuring the Effective Protection of Technologies Critical to U.S. National Security Interests	2007
	Improving Federal Oversight of Food Safety	2007
	Limiting the Federal Government's Fiscal Exposure by Better Managing Climate Change Risks	2013
	Improving the Management of IT Acquisitions and Operations	2015
	Government-wide Personnel Security Clearance Process	2018

DHS carries out multiple complex and highly diverse missions that range from aviation and border security, to emergency response, cybersecurity analysis, and chemical facility inspection. All are focused on securing our Nation from the many threats we face. The Department continually strives to improve the efficiency and effectiveness of all its programs and operations, however, the areas identified above merit a higher level of focus

and attention. It is important to note that overcoming challenges in these areas requires long-term strategies for ensuring stable operations, sustained management attention, and resources; which the Department is providing.

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

## GAO High-Risk – Status Update

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

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

In response to this high-risk designation, DHS biannually publishes the *Integrated Strategy for High Risk Management (Integrated Strategy)*. The *Integrated Strategy* outlines the Department's framework to systematically strengthen and integrate its management functions, while simultaneously addressing the High-Risk List designation by GAO. First issued in 2011, the biannual *Integrated Strategy* has been commended by GAO as a best practice and is now required by statute.<sup>2</sup>

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

<sup>2</sup> National Defense Authorization Act for Fiscal Year 2017, Public Law 114-328 § 1903 (December 23, 2016), page 675.

refocusing by GAO is a reflection of the considerable progress DHS has made in transforming original Component agencies into a single cohesive department.

**Lead Office and Official:** Immediate Office of the Under Secretary for Management (USM), Janene Corrado, Deputy Chief of Staff

**Progress:** In the 2017 GAO High-Risk Report, GAO commended the Department’s top leadership for demonstrating exemplary commitment and support for addressing the high-risk designation on DHS management functions.<sup>3</sup> GAO also cited the frequent engagement with top DHS leaders as a model for senior-level engagement that helps to ensure a common understanding of the remaining work needed to address the high-risk designation.<sup>4</sup>

In September 2018, DHS published its fifteenth *Integrated Strategy* (see <https://www.dhs.gov/publication/dhs-integrated-strategy>), which outlines the Department’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 performance measures that support implementation of the action plans for the 30 high-risk outcomes. The 30 GAO outcomes reflect desired end-states of maturation for several of DHS’s management functions.

Since 2010, DHS has intensified its focus on strengthening its management foundation in several ways, including:

- 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;
- Strengthening the DHS Chief Information Officer’s (CIO) ability to improve the management, acquisition and oversight of the Department’s IT resources by, among other means, ensuring the DHS CIO has direct access to the Secretary, as well as to the USM who is the third highest official at the Department and who also functions as the DHS Chief Acquisition Officer; and
- Sustaining key reforms implemented under the Unity of Effort initiative, such as maturing the joint requirements process and solidifying a transparent and comprehensive Planning, Programming, Budgeting, and Execution (PPBE) system.

Collectively, these efforts aim to strengthen all elements of the PPBE process, including strategy development, planning and joint requirements, which will ensure that the total budget is spent effectively and efficiently.

Making major strides during the past two years, the Department has:

- Earned a “Fully Addressed” or “Mostly Addressed” rating on 21 of the 30 (70 percent) GAO outcomes, a significant improvement compared to 47 percent (14 of 30) in 2015 and 26 percent (8 of 31) in 2013.
- Met three of the five (60 percent) criteria for list removal (leadership commitment, a framework to monitor progress, and corrective action plans), making DHS among the few

<sup>3</sup> GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: February 15, 2017), page 354.

<sup>4</sup> *Ibid.*, page 356

agencies on the High-Risk List to have met at least three of GAO's criteria; and partially met the two remaining criteria (capacity [i.e., resources] and demonstrated progress).

- Received a sixth consecutive unmodified (i.e., clean) audit opinion on all five financial statements in November 2018. This success is a confirmation of the Department's ongoing commitment to sound financial management practices, with its first unmodified audit opinion in December 2013. These successes led to GAO assessing the associated outcomes as "Fully Addressed."
- Received a downgrade to DHS's property, plant and equipment (PP&E) material weakness in FY 2017. A material weakness is a control gap that increases the risk of an error in financial data and keeps DHS from getting a clean audit opinion on internal control. In reducing the PP&E material weakness, DHS demonstrates that its procedures and controls to properly and timely account for DHS-owned assets and record them into the financial system are effective and solid.
- Continued to conduct annual cycles of strategic human capital planning and implementation, contributing to the advancement of two additional GAO outcomes to a "Fully Addressed" status since GAO published its 2017 High-Risk Series report.
- Continued focus on employee engagement by sustaining improvements seen in the 2016 and 2017 Federal Employee Viewpoint Survey (FEVS) where DHS improved more than any other agency in the "very large agency" category. In 2018, DHS also achieved increases in two engagement-related indices on the FEVS—the Global Satisfaction Index increased from 55 percent in 2017 to 56 percent in 2018, and the New Inclusion Quotient increased from 52 percent in 2017 to 53 percent in 2018.
- Made significant progress in reforming its acquisition process by implementing governance structures, updating policies and processes, standardizing and professionalizing the DHS acquisition leadership and workforce and overseeing the Department's major acquisitions in an integrated manner.
- Piloted leading-edge agile processes to achieve improvements in acquisition program performance and leveraged lessons learned to institutionalize policy and process enhancements.

**Planned Actions and Key Milestones:** DHS will continue to implement the *Integrated Strategy* and other efforts that contribute to strong and efficient management functions. During FY 2019, DHS expects to accomplish the following:

- Sustain progress on GAO outcomes and the five criteria for High-Risk List removal;
- Earn a "Fully Addressed" or "Mostly Addressed" on additional GAO outcomes, including for all IT and human capital management outcomes, which collectively constitute nearly half of the GAO outcomes;
- Continue positive momentum and sustain progress on increasing employee engagement across the Department by building on the DHS Leadership Year initiative and other engagement efforts;
- Establish data interchanges to enable enterprise-wide reporting and analytics of DHS training data;
- Demonstrate continued improvement in the performance of acquisition programs and related processes;

- Obtain the seventh consecutive clean audit opinion on financial statements and downgrade one of two remaining material weaknesses in internal controls; and
- Modernize the U.S. Coast Guard (USCG) Financial System. This is a key financial management priority for DHS, and supports the goal of a clean internal control opinion. USCG cross-services the Transportation Security Administration (TSA) and the Domestic Nuclear Detection Office (DNDO) portion of the Countering Weapons of Mass Destruction (CWMD) Office, in addition to itself. Previously, DHS transitioned the DNDO portion of CWMD to a modern platform and expects to complete the work to transition TSA to that same platform by the end of FY 2019. TSA will go-live in FY 2020 and USCG in FY 2021.

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

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

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

Congress reauthorized NFIP for five more years in the *Biggert-Waters Flood Insurance Reform Act of 2012* (BW-12) which mandated certain premium rate increases to begin transitioning the program where approximately 20 percent of policies were discounted or 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 (which maintains a subset of discounted policies); set limits on premium rate increases for certain policyholders; and applied an annual surcharge to all policyholders.

However, the NFIP is not designed to be self-sufficient, as any insurance program that takes all comers without the ability to underwrite for concentration risk will end up in the financial position that the program currently finds itself. The NFIP is developing a sound financial framework to enhance and bring clarity the NFIP's solvency within its statutory limitations.



**Lead Office and Official:** FEMA Federal Insurance and Mitigation Administration (FIMA), David Maurstad, Deputy Associate Administrator for Federal Insurance and Mitigation

**Progress:** FEMA continued implementing (1) annual premium rate increases in accordance with BW-12 and HFIAA, including (2) applying new surcharges and (3) releasing new rates and mapping standards. Further, FEMA is (4) transforming the NFIP to improve the experience of NFIP policyholders.

- To advance the agency’s initiative to replace the NFIP’s legacy mainframe solution, the FEMA Insurance Systems Program Management Office (PMO) coordinated with FEMA’s Office of the Chief Procurement Officer and Office of the Chief Information Officer to develop the System Engineering Life Cycle and Acquisition artifacts necessary to garner approval for a DHS Acquisition Decision Memorandum (ADM) for the “Analyze/Select” Phase (ADE-2A/2B), completed in the first quarter of FY 2017. This ADM gave the PMO permission to proceed to the “Obtain” phase and begin obtaining the target solution, with Initial Operating Capability (IOC) to be delivered in Q2 FY 2018, and Full Operating Capability (FOC) to be delivered by FY 2020.
- FEMA published the NFIP Rate Guidance Issue in bulletins to WYO insurers in April and October 2018, allowing the mandated six months required for consultation and notice of changes impacting their IT systems and operational processing procedures.
- FEMA integrated the following requirements into its ongoing program and reporting processes:
  - Set 25 percent annual premium rate increases for businesses, mandated under BW-12, which took effect in April 2016.
  - Set the annual premium rate increases, as required by HFIAA, at an average rate between 5-15 percent per risk class, without exceeding the 18 percent cap on annual premium rate increases for any individual policy.
  - Applied a preferred risk premium rate for the first year to policies on properties that are newly mapped into a special flood hazard area, with increases of 18 percent per year until the rate reaches full risk rate.
- FEMA expedited flood insurance reform and implemented program changes through policy and by leveraging existing processes to release program updates every six months. Specifically, FEMA released mapping standards by publishing them on [www.FEMA.gov](http://www.FEMA.gov) in May and November 2017, allowing the mandated time required for public comment.

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

of 2019. FEMA will continue to track and monitor progress on implementation of the concept of operations and how they relate to GAO recommendations for effectiveness.

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

FEMA is redesigning the premium rating structure and is planning to announce new rates to policyholders that will reflect the risk of structures by reflecting the local hazard and the exposure of the structure including the replacement cost. FEMA is also redesigning the insurance product to better meet survivor’s needs and provide choice to policyholders. The rate and product changes are intending to support FEMA’s goal to close the insurance gap and FIMA’s goal to increase flood insurance coverage.

Additionally, FEMA is developing a sound financial framework for the NFIP including the National Flood Insurance Fund, the Reserve Fund, repayable borrowing, Reinsurance and catastrophe bonds, and appropriations.

Reinsurance and similar risk transfer mechanisms allow FEMA to diversify the tools it uses to manage the financial consequences of its catastrophic flood risk. Prior to establishing the reinsurance program, the NFIP and the U.S. Treasury bore all of the policyholders’ risk. Investments made through the NFIP reserve fund and the purchase of reinsurance for 2017 and 2018 helped improve the soundness of the NFIP’s financial framework, but they do not allow the NFIP to repay borrowings or service the debt should interest rates rise or to pay future catastrophic losses. The current statutory language enables the NFIP’s Reinsurance Program to explore a range of reinsurance and Insurance Linked Securities mechanisms. FEMA continues working to expand the NFIP Reinsurance Program.

In 2017, the NFIP transferred \$1.042 billion of its financial risk to the private reinsurance market for the 2017 calendar year. FEMA recovered \$1.042 billion from the private reinsurers following Hurricane Harvey. Continuing this risk management practice, in January 2018, FEMA secured \$1.46 billion in reinsurance from 28 reinsurance companies to cover qualifying flood losses in excess of \$4 billion dollars per event occurring in calendar year 2018. To complement the NFIP’s existing traditional reinsurance coverage, FEMA recently completed an additional reinsurance placement. For the first time, this transaction secures reinsurance coverage from the capital markets. By engaging both the traditional reinsurance markets and the capital markets, the NFIP can reduce risk transfer costs, access greater market capacity, and further diversify its reinsurance partners.

Effective August 1, 2018, for a period of three years, this placement transfers \$500 million in NFIP flood risk to capital markets investors. The agreement is structured to cover, for a given flood event, losses between \$5 billion and \$10 billion. Combined with the January 2018 traditional reinsurance placement, FEMA has transferred \$1.96 billion of the NFIP's flood risk for the 2018 hurricane season to the private sector. The NFIP's reinsurance purchases represent significant steps toward involving the private sector in bearing a meaningful portion of NFIP flood risk.

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

- IOC, which includes establishing the Pivot infrastructure (hosting environment, development tools, cybersecurity, etc.), the Pivot Analytics and Reporting Tool (PART), establishing a data migration plan, delivering near-real time claims information, and establishing an appeals tracker. The PART tool was placed into production in October 2017, and the remaining functions are being released in Q2 FY 2018, on or ahead of schedule. The program is currently on track to decommission the legacy system ahead of the approved FOC date of FY 2020.

Planned Actions and Milestones for new rates include:

- Announcing new rates in April 2019; and
- Implementing new rates to the first group of policy holders in April 2020.

**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. Safeguarding federal computer systems and 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:** Cybersecurity and Infrastructure Security Agency (CISA) Office of Cybersecurity and Communications (CS&C) Lilian Colon, Senior Cybersecurity Strategist, Strategy Coordination & Management

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

awareness of cyber threats and vulnerabilities while providing a security baseline for federal civilian agencies.

DHS's National Cybersecurity Assessment and Technical Services (NCATS) team continues to increase its cyber hygiene scanning activities, which ensure that federal agencies are aware of vulnerabilities in their internet-facing systems. Throughout FY 2018, the NCATS team has detected 95,264 new vulnerabilities on federal networks, including 7,725 rated critical or high, and provided the affected agencies with details and mitigation strategies. Under the Federal Information Security Modernization Act of 2014, DHS released its first binding operational directive (BOD) in May 2015, which requires agencies to quickly patch their most critical cyber vulnerabilities based on the results of NCATS cyber hygiene scans. Nearly three years after the BOD's issuance, federal agencies continue to patch their most critical vulnerabilities and do so in a timely manner. At the time the BOD was issued, federal agencies took on a median time of 32 days to patch critical vulnerabilities identified in cyber hygiene scans. Today, federal agencies take a median time of 21 days to patch critical vulnerabilities. In addition, a general reduction in time to patch non-critical vulnerabilities also followed the issuance of the BOD. Similar outcomes are expected to result from agencies' increased visibility into their assets and vulnerabilities as Continuous Diagnostics and Mitigation (CDM) Phase 1 tools are installed. The Department has developed an FY 2018-2019 Agency Priority Goal, which will measure agencies' use of NCATS vulnerability assessment results to ensure quick patch management related to the most significant vulnerabilities.

In FY 2018 the NCATS team completed 29 Risk and Vulnerability Assessments (RVAs) at federal agencies, of which 25 were conducted on high-value asset systems. Through Q1 of FY 2019, NCATS has scheduled 9 RVAs on Federal high-value assets. RVA services include, among other things, penetration testing, wireless discovery and identification, database scanning, web application scanning and testing, and social engineering. Each RVA that is conducted on Federal High-Value-Assets also receive a Security Architecture Review (SAR), which is conducted by DHS' Federal Network Resilience division. A SAR includes in-depth document reviews and interviews based on analysis of strengths and weaknesses of security controls supporting network and system architectures and components that compromise HVAs based on Federal requirements, specifications, and risk management strategies. Significantly, DHS currently provides agencies with actionable risk mitigation information based on cyber hygiene scans, RVAs, and SARs focused on high-value assets, and has already met the June 2018 deadline for this requirement.

DHS also strengthened the effectiveness of its partnerships with the private sector and other federal agencies in securing cyber critical infrastructure. For example, DHS has made efforts to provide CDM to other federal agencies. As of December 31, 2016, DHS had provided CDM Phase 1 and Phase 2 tools to 100 percent of participating agencies. Since then, agencies have deployed tools and their agency-level dashboards to monitor and manage their security. DHS CDM Federal Dashboard 3.0 received its authority to operate in August 2017, and became operational in October 2017. During Q1 FY 2018, DHS was successful in establishing Information Exchanges between several Agency Dashboards and the Federal Dashboard. Throughout FY 2018, DHS continued to establish information exchanges, achieving 21 of 23 agencies completed by the end of FY 2018. The estimated completion for the remaining two Chief Financial Officer (CFO) Act agencies' Information Exchanges is Q1 FY 2019. Establishment of data exchanges for the non-CFO Act agencies will continue throughout FY 2019.

DHS also continues to provide EINSTEIN intrusion detection and prevention services to federal agencies. EINSTEIN 3 Accelerated (E3A), which actively blocks known malicious traffic, is currently being deployed through the primary internet service providers serving the Federal Government. As of September 26, 2018, 250 federal, civilian executive branch Department and Agency entities were brought on to E3A services, representing approximately 2.089 million users, or 95 percent of the total user population. The National Cybersecurity and Communications Integration Center (NCCIC) has improved public-private sector partnerships by improving information sharing so they can block threats before penetrating networks or otherwise detect intrusions sooner. NCCIC continues its dissemination of alerts, warnings, and bulletins. In addition, it implemented the Automated Indicator Sharing (AIS) capability in accordance with the Cybersecurity Information Sharing Act of 2015. From March 2016 to February 2018, NCCIC had shared approximately 3,727,000 unique indicators through the AIS capability. As of February 2018, 165 non-federal entities—including several information sharing and analysis organizations, managed security services providers and commercial threat feeds—are connected to the AIS capability and 77 components across 33 federal agencies are connected. Four organizations are actively sharing into the AIS capability, including six non-federal information sharing and analysis organizations or security providers, which share on behalf of their membership.

DHS delivered the National Cyber Incident Response Plan to the White House on January 18, 2017, as required by the National Cybersecurity Protection Act of 2014 and Presidential Policy Directive 41. During Q4 FY 2018, NCCIC provided 13 incident response and recovery team onsite deployments, as of September 2018, it provided a total of 52 of these onsite deployments for FY 2018.

In the past, GAO reported that DHS's National Cybersecurity Protection System (NCPS) was partially, but not fully, meeting its stated system objectives of detecting intrusions, preventing intrusions, analyzing malicious content, and sharing information. GAO has also reported that DHS also had not developed metrics for measuring the performance of NCPS, recommending DHS take action to enhance NCPS's capabilities, among other things. As of October 2018, NCPS continues to enhance its intrusion detection capabilities. NCPS recently transitioned a non-signature based detection capability from a pilot to an operational capability. This capability enhances NCPS's current intrusion detection capability to include functionality that would detect deviations from normal network behavior baselines. Additionally, CISA, specifically CS&C, began reporting on a new Government Performance and Results of the Modernization Act measure focused on the extent to which the NCPS intrusion detection and prevention capabilities detect or prevent nation state threat activity. The measure also is included as a supporting measure in the aforementioned Agency Priority Goal (APG) for FY 2019, which focuses on federal cybersecurity outcomes. Finally, CISA and OMB submitted the Report on the Effectiveness of NCPS and CDM to congress in December 2017. The report included operational metrics for NCPS representing deployment and adoption at Federal Departments and Agencies, activity levels, and typical use cases. Informed by the measurement concepts identified in the Report on the Effectiveness of NCPS and CDM and the FY 2018 DHS Strategic Review, CISA continued to develop and refine additional NCPS performance measures for inclusion in the FY 2019 publicly reported measure set and for internal CISA collection to assess program effectiveness. On October 1, 2018, CISA updated the applicable DHS Annual Performance Goals (APG) and publicly reported measures that will focus on quality and effectiveness of NCPS capabilities and will be reported quarterly in FY 2019.



DHS creates a culture of compliance by integrating privacy protections into its cybersecurity programs from the outset. With the DHS Privacy Office being the first statutorily mandated privacy office in the federal government, it serves a unique role as both an advisor and oversight body for the department. DHS deploys a layered approach to privacy oversight for the Department's cybersecurity activities, starting with the Chief Privacy Officer, and extending through CISA's Component Privacy Officer and dedicated privacy staff across the Department. Additionally, as part of its privacy compliance responsibilities, DHS conducts Privacy Impact Assessments, (or "PIAs") which are designed to identify privacy issues early in the program or system development process and build appropriate privacy protections into programs or systems from the beginning. The issue identification and privacy protections specifically related to the Department's EINSTEIN, CDM, and other cybersecurity programs and initiatives are discussed more fully in PIA documentation available at <https://www.dhs.gov/privacy-documents-national-protection-and-programs-directorate-nppd>. As discussed in these PIAs, DHS has processes in place to implement data minimization to ensure data collection is limited to information determined to be necessary to understanding cyber threats. DHS further facilitates the implementation of appropriate privacy requirements through oversight activities such as Privacy Compliance Reviews and CISA's Privacy Oversight Reviews. These reviews provide structured opportunities to verify that PII is being handled appropriately and that privacy oversight mechanisms are operating effectively.

Moving forward, to further protect the Federal Government's information systems and to collaboratively protect non-federal entities, DHS will increase its E3A coverage in accordance with the *Cybersecurity Act of 2015*, and support for agencies through the procurement and deployment of CDM capabilities. The Department is also planning to increase the volume of cyber threat indicators and defensive measures shared through the AIS capability while analyzing the relative value of those indicators. Additionally, DHS will continue to implement the requirements of Presidential Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."

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

**Planned Actions and Key Milestones:** To further protect the Federal Government's information systems and to collaboratively protect non-federal entities, DHS will increase its E3A coverage, in accordance with the *Cybersecurity Act of 2015*. DHS is also planning to continue supporting agencies through the procurement and deployment of CDM capabilities, and increase the volume of cyber threat indicators and defensive measures shared through AIS capability while analyzing the relative value of those indicators.

During FY 2019, DHS expects to make important progress in reinforcing DHS's role in protecting the Federal Government's information systems and the Nation's cyber critical infrastructures. Specifically, DHS plans to:

- Continue to provide agencies with actionable risk mitigation information based on cyber hygiene scans and RVAs focused on high-value assets; and
- Continue to establish and improve active agency CDM data information exchanges with the Federal Dashboard with participating Federal Agencies.

GAO High-Risk Area: Strategic Human Capital Management (Government-wide)
<p><b>GAO Overview:</b> Addressing national challenges requires a high-performing federal workforce able to safeguard the homeland against national threats and emergencies. However, current budget and long-term fiscal pressures, declining levels of federal employee satisfaction, the changing nature of federal work, and a potential increase 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 resources 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 past 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.</p>
<p><b>Lead Office and Official:</b> Management Directorate, Office of the Chief Human Capital Officer (OCHCO), Roland Edwards, Deputy Chief Human Capital Officer</p>
<p><b>Progress:</b> Regarding Human Capital Management (HCM), DHS continues to demonstrate substantial progress by sustaining a “Fully Addressed” or “Mostly Addressed” rating on six of seven HCM outcomes on the <i>Integrated Strategy</i> referenced in the “Strengthening DHS Management Functions” update, with two of those advancing to Fully Addressed since June 2017. GAO favorably recognized the Department’s structured workforce planning for mission critical occupations, enhanced employee engagement activities, improvements in enterprise leader development, and human capital strategic planning activities.</p> <p>The Department will continue to focus on improving employee morale, as measured by the Employee Engagement Index of the Federal Employee Viewpoint Survey. In 2016 and 2017, the Department’s employee engagement scores improved more than any other agency in the “very large agency” category. The Department’s overall employee engagement score held steady in 2018, while several individual Components experienced increases. FEMA and U.S. Immigration and Customs Enforcement (ICE) increased employee engagement scores by two and one percentage points respectively, while the U.S. Secret Service and TSA saw the largest increases of six and three percentage points respectively. In addition, DHS as a whole achieved increases in two other engagement-related indices—the Global Satisfaction Index increased from 55 percent in 2017 to 56 percent in 2018, and the New Inclusion Quotient (IQ) Index increased from 52 percent in 2017 to 53 percent in 2018.</p> <p>The emphasis on leadership engagement at all levels continues, most recently through the Leadership Year initiative and the DHS Leadership Survey pilot. Leadership Year promotes a culture of leadership excellence through cross-Component initiatives that increase capabilities and improve transparent, inclusive practices in leaders at all levels. Finally, the Department continues to play an important role in the Office of Personnel Management’s (OPM) efforts to address this area by identifying and formally documenting human capital requirements for high priority missions. These efforts include utilizing innovative approaches to attract and retain talent to address skills gaps in key disciplines such as those for cybersecurity professionals and border and immigration security officers.</p> <p>To sustain and build on the progress made in this area, DHS continues to implement and enhance workforce planning processes, particularly those supporting the Department’s priority mission critical occupations (MCOs). In May 2018, the DHS OCHCO met with each Component to review workforce plans for priority MCOs. Workforce plan trackers, highlighting key findings from each workforce planning step, along with updated environmental scans and action plans,</p>

were collected as part of the mid-year review process. The review of Component submissions revealed continued progress in documenting DHS priority MCO workforce requirements, resources, and skill gaps, along with clear strategies in the action plans to close them. On May 31, 2018, the DHS Chief Human Capital Officer approved the biennial revalidation of the MCO list, which includes 13 civilian occupations whose functions most closely support the core functions of the Department. The FY 2018 MCO list included three significant changes from previous lists:

- Identification of the 1811, Criminal Investigator, series as a DHS-wide MCO for all Components;
- Establishment of a mission critical function (MCF) list to identify core organizations and functions throughout the Department requiring special attention for resourcing and hiring; and
- Identification of positions requiring cybersecurity expertise, regardless of Component or occupational code as a workforce subset requiring special emphasis.

The OCHCO Data Analytics Division has updated the human capital dashboard to support these efforts and enhance leadership's ability to monitor the key performance indicators associated with the Department's human capital goals and priorities. Additional accomplishments include:

- Adding webTA (i.e., time and attendance) data to the Analytics Intelligence System (AXIS) database—which supports enterprise human capital reporting—to identify DHS-wide onboard staffing, along with work hours, leave, and other non-available time down to the person level;
- Refining the administrative leave monthly report to improve management visibility and cost controls, which enables DHS to better manage administrative leave throughout the Department;
- Continuing production of a monthly health metrics report on priority MCOs; and
- Leveraging state of the art data visualization tools to develop placemats that highlight key aspects of the DHS workforce, including views that detail the hiring plans supporting implementation of the Executive Orders requiring additional U.S. Border Patrol (USBP) and ICE agents.

The Department is sustaining its progress through continued implementation of the Component Recruitment and Outreach Plan (CROP) to assess recruiting, outreach, and marketing strategies and activities. The FY 2018 CROP template was revised to reflect changes in the identified DHS Priority MCOs, include sections highlighting efforts around law enforcement and cyber recruitment, and incorporate increased accountability for targeted recruitment. DHS—through the Strategic Recruitment, Diversity & Inclusion division within the DHS OCHCO—implemented the Recruiting, Outreach, and Marketing Matrix (ROMM) to identify target audiences, monitor attendance and funds spent at key recruiting events, and analyze marketing campaigns focused on recruiting. The Department leveraged data from the ROMM to develop a recruiting placemat that provides a closer look at active military/veteran/transitioning service member, law enforcement, and cyber recruitment efforts. In partnership with the DHS Office of Academic Engagement, OCHCO is identifying collaborations with colleges and universities, where potential strategic relationships exist for both academic and recruiting purposes. Through this partnership, OCHCO is coordinating and providing guidance on several outreach and recruitment approaches to augment the hiring buildup necessitated by Executive Orders 13767 and 13768, which mandate the hiring of 5,000 USBP agents and 10,000 ICE agents, respectively.

In June 2018, the Department conducted a joint hiring event in Arlington, Texas in support of the Executive Orders and in coordination with Components throughout DHS. Prior to the event, DHS conducted 12 webinars, including offerings in the evening to accommodate interested applicants nationwide; in total, there were approximately 9,000 webinar participants. Utilizing innovative approaches to market the event and interact with prospective candidates, DHS staff met with almost 2,000 applicants over the two-day event, which resulted in over 125 interviews. Separately, with women making up only 8 percent of law enforcement positions at DHS, the event focused heavily on attracting female applicants and resulted in over 9,000 women applying for law enforcement positions across the Department. This joint hiring event concept is a best practice for the Department and will be utilized moving forward. The action plan that follows describes the near-term actions DHS is taking to further sustain this outcome, as well as historical actions that led to a “Fully Addressed” rating.

DHS leadership continues to engage directly with employees. Beginning October 1, 2017, DHS launched a year-long effort to highlight the importance of leadership at all levels, and a culture of leadership excellence. This effort, DHS Leadership Year, featured Component- and DHS-level initiatives that promote awareness of leadership roles and responsibilities, provided resources for supervisory and non-supervisory leaders, and increased transparency and access to leader development opportunities. A new Leadership Excellence Award has been established, which was presented at the Secretary’s Awards ceremony on November 7, 2018 in conjunction with the Senior Leader Forum, and is one of many ways in which the principles and practices highlighted during Leadership Year will continue to be represented into the future. In February 2018, the Department launched an innovative pilot survey in two Components, U.S. Citizenship and Immigration Services and TSA. The Leadership Survey is designed to foster employee engagement by providing upward feedback from employees to their leaders. This innovative survey is intended to empower employees and improve leadership culture, with the goal of creating a culture of leadership excellence to drive effective, high-performing workplaces. In 2019, DHS will evaluate the survey results to determine the advisability and feasibility of rolling the Leadership Survey out to the entire Department.

The Department also implemented Performance and Learning Management System (PALMS) capabilities in select Components, based on a business case analysis, in order to enhance the accessibility and comparability of DHS training data. While PALMS serves a majority of DHS, it is not the sole enterprise solution for learning management. The Department has awarded a one year extension (expires May 2019), with a one year option (expires May 2020), for PALMS to allow time for the selection and implementation of follow on talent development and training capabilities for DHS. In addition, the Department is building data interchanges between the four learning management solutions and the Human Capital Enterprise Information Environment to create a central repository for the Department’s training data, which allows for enterprise-wide reporting and data analytics. The estimated completion date for the data interchanges is June 30, 2019.

**Planned Actions and Key Milestones:** To sustain a GAO assessment of “Fully Addressed” for five of the seven outcomes and continue progressing toward a “Fully Addressed” assessment for the remaining two outcomes, the Department-wide human capital community and its key stakeholders will, in FY 2019 and beyond:

- Continue to sustain progress on increasing employee engagement across the Department through building on the DHS Leadership Year initiative and other engagement programs and activities;

- Establish data interchanges to enable enterprise-wide reporting and analytics of DHS training data;
- Continue to implement annual operational plans and data-driven performance reviews, to include continual monitoring and evaluation of the human capital dashboard;
- Continue to employ Department-wide and Component-specific recruitment strategies, which is key to sustaining progress in skill gap closure;
- Update annual CROPs, with a focus on targeted recruitment for Priority MCOs;
- Continue to apply the five-step workforce planning framework for the department's priority MCOs, which consist of occupations most impactful to DHS's overall mission areas;
- DHS will also continue to track all cyber recruitment, outreach, and marketing for all components due to the critical need across the enterprise;
- Improve training quality and consistency implementing enterprise training metrics, and sharing information among Components on common training offerings;
- Continue to implement the Joint Duty Assignment Program to provide cross-Component rotational experiences to develop DHS leaders with broad departmental perspectives;
- Conduct annual recruitment planning sessions to prioritize events and ensure alignment with workforce planning and diversity analysis, to meet or exceed hiring goals; and
- Continue to work through the DHS Employee Engagement Steering Committee to improve Component engagement action planning processes, share and spread best practices, and keep DHS leadership apprised of issues and challenges related to employee engagement.

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

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

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

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

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



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

*Federal Real Property Management:* Following the DHS Real Property Resource/Funding Requirements Assessment Study (Assessment Study) in FY 2017, DHS required the submission of a real property exhibit to provide senior Department officials with visibility into real property requirements at the Departmental level. OCRSO through the Office of Program Analysis and Evaluation (PA&E) within the Office of the Chief Financial Officer (OCFO) will institutionalize this as an annual budget exhibit through the 2021 Resource Allocation Plan (RAP) providing reliable budget projections for the real property lifecycle and ensuring alignment of planning with budget in support of mission and increased resilience.

DHS, through its real property program, was one of the first Departments to adopt a Workspace Standard for office space in 2014. This standard is consistent with the DHS Real Property Efficiency Plan which requires conformance with the standard for major reconfigurations and new requirements, subject to available funding. The DHS Workspace Standard for office and related spaces (conference rooms, break rooms, file rooms, etc.) set the DHS standard utilization ceiling at 150 SF/per person. In 2019, DHS intends to replace this standard with more inclusive planning guidance expanding from office into mission spaces and associated utilization targets.

In 2018, DHS launched a Field Efficiencies Program Management Office (FE-PMO) to implement a unified cross component planning process and identify opportunities for consolidations along common and/or similar mission functions with compatible mission support requirements, anchor locations, or future mission needs. The FE-PMO is staffed with 5 regional coordinators aligned with GSA regions. These headquarters employees are responsible for regional outreach and coordination of cross Component activities while also serving as a DHS advocate with the respective GSA Regions.

In 2017, DHS also stood up a resilience framework tiger team to develop a roadmap to formalize a Department-wide process that integrates the activities for incorporating resilience into our critical infrastructure. This effort provides a holistic framework to ensure sustained resilience of mission essential functions and assets, and related supporting critical infrastructure assets during all phases of mission operations (normal operations, disruptive event, response, and recovery/reconstitution). This effort has been integrated and coordinated with the Office of Operations/Continuity, FE-PMO, and Real Property efforts. The Deputy Under Secretary for Management signed the Resilience Framework on August 13, 2018.

The Department, in coordination with GSA, is in the process of revising our consolidation plans for the National Capital Region (NCR), which contains the largest geographic concentration of DHS office space. DHS in coordination with GSA will provide an amendment to the St. Elizabeths' master plan to address funding reduction in FY 2017 and FY 2018 that have caused misalignments with certain commercial lease expirations. In addition, GSA has encountered challenges with the renovation of historic buildings on the St. Elizabeths campus that necessitates a revaluation of the development plan going forward.

*Protection of Facilities:* FPS leads efforts within a complex operating environment to protect and secure federal facilities from increasingly dangerous and unpredictable physical and cyber

threats. FPS continues to develop national-level policies, operational initiatives, capabilities and programs that are grounded in the seamless integration of law enforcement, security, and intelligence activities. These efforts are instrumental for threat detection and deterrence while enhancing security and promoting facility and infrastructure resilience. For example:

- With GSA, FPS is the co-Sector-Specific Agency for the Government Facilities Sector (GFS), one of the 16 critical infrastructure sectors identified in the 2013 Presidential Policy Directive 21 on Critical Infrastructure Security. In this capacity, FPS uses institutional knowledge and specialized expertise about federal facility security and infrastructure resilience to issue briefings, notifications, and alerts to members of the GFS.
- Between FY 2017 and FY 2019, FPS provided information to GFS member agencies on topics relevant to facility security and infrastructure resilience, including:
  - In July 2017, FPS coordinated a briefing on the Cybersecurity Framework developed by the National Institute of Standards and Technology, which focuses on getting organizations to use business drivers to guide cybersecurity activities and consider cybersecurity risks as part of a broader risk management process.
  - In March 2018, the GFS issued a compilation of reference topics on facility security protection relevant to federal facilities.
  - In June 2017, FPS and GSA led a GFS Government Coordinating Council meeting to cover lessons learned from the Washington Navy Yard shooting; an overview of training programs and resources available from the DHS Office of Infrastructure Protection; and main objectives and protection tactics employed by FPS's Active Threat Program.
  - In July 2018, FPS coordinated with the DHS Office of Cyber Security and Communications to host a webinar on Cyber Supply Chain Risk Management. The webinar covered supply chain risks mitigation tools and strategies for federal departments and agencies.
  - In October 2018, FPS presented a webinar to the GFS on federal facility screening operations. FPS shared lessons learned after implementing an alternative random screening program across its facility portfolio and methods and steps the agency took to mitigate future impact to employees and visitors while maintaining an effective security posture.
- FPS and GSA finalized an update to their 2006 memorandum of agreement (MOA) in September 2018. The revised MOA identifies, defines, and addresses roles, responsibilities, and operational relationships between FPS and GSA concerning the protection of federally-owned, leased, or operated buildings, grounds, and property under the jurisdiction, custody, or control of GSA. The MOA provides guidance on how FPS and GSA should coordinate facility management with security and law enforcement efforts to the extent that both FPS and GSA are able to carry out their respective responsibilities.
- FPS continues to develop strategies for effecting cybersecurity in facility safety and security control systems. FPS has led the effort to incorporate cyber security controls in the recent release of the *ISC's Risk Management Process: Appendix B: Countermeasures*. FPS is currently working toward implementation of interim operating capability for the Federal Facilities Control System Strategy. Implementation of the strategy includes

assessment activities, stakeholder engagement and education, and protective intelligence information sharing relevant to cyber threats (actors, incidents). In FY 2018, FPS piloted a Cyber Security Assessment process for Federal facilities. Based on this pilot, FPS developed policies, procedures, and deliverables for assessing the cyber security of building safety and security control systems.

FPS applies the national standards and strategies to develop or improve and implement operational policies and procedures across the mission areas. GAO has issued recommendations to FPS pertaining to risk assessment and the protective security officer (PSO) program. FPS's efforts have resulted in the closure of remaining risk assessment recommendations in FY 2017. For the few PSO-related recommendations that remain, FPS is actively working to address their closure through efforts that cut across various aspects of the PSO program to ensure that requirements for PSOs are clearly defined, communicated, and monitored, including the following:

- FPS has established a working group to review performance data nationwide to identify trends and monitor, review, and improve FPS's screening process. FPS uses collaborative analyses and evaluation of covert testing, prohibited items, and other PSO oversight data to mitigate trends and systematically assess and improve security at federal facilities.
- FPS has established training guidelines to ensure that PSOs are providing high quality protective security services at federal facilities nationwide. FPS has developed standardized lesson plans for basic and refresher PSO training courses and established minimum requirements that proposed training instructors from vendor companies must meet in order to train PSOs. FPS has also developed procedures for certifying PSO training certifications and monitoring training to ensure that training requirements are met.
- FPS's PSO Program continues to develop systems that will automate aspects of the program to include tracking PSO identify, time on post, as well as management of the training and certification data, further facilitating the management and oversight of PSOs.

FPS has established a defensible standard for engaging PSOs throughout the portfolio, which enables an FPS Inspector to proactively interact with PSOs, involving them as key team players within the FPS operational environment and encouraging positive working relationships to improve operational readiness.

**Planned Actions and Key Milestones:** DHS continues to improve the management, oversight, and physical security of our inventory. Specific initiatives include:

- The FE-PMO is on schedule to establish integrated real property mission support plans for all major metropolitan regions with a significant concentration of DHS assets and activities by FY 2022. The regional plans will focus on increased utilization of DHS assets in support of improved efficiency.
- DHS continues to work with GSA to develop a revised enhanced plan that will ultimately reduce the number of locations in the NCR from more than 50 to 8 or fewer. DHS is pursuing contingency housing plans to address critical lease replacements that do not have flexibilities for extensions. The DHS goal remains to improve the efficiency of our NCR portfolio by optimizing the use of federal property, using long-term commercial leases when necessary, and supporting the Unity of Effort initiative.

- FPS is in the process of enhancing the capabilities of its Modified Infrastructure Survey Tool, FPS's facility protection tool, to incorporate the constantly changing environment. For example, in FY 2017, FPS implemented a cyber-physical question set to its assessment process, a mechanism to track countermeasure implementation status, a threat module aligned with the Interagency Security Committee's (ISC) design basis threat, a risk analysis profile, a consequence scoring algorithm, and several other features to enhance the capabilities of the organization and continue to improve upon the efficiency of the FPS protective mission.

**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 the ongoing challenges of balancing national security concerns and economic interests in the area of emerging technologies are multiform and shifting.

GAO notes the role of the Export Enforcement Coordination Center (E2C2) as a platform for improving coordination and de-confliction for U.S. Export Control efforts. The E2C2 is managed by a Director, from DHS ICE's Homeland Security Investigations and two Deputy Directors from the Federal Bureau of Investigation (FBI) and the Commerce Department. The E2C2 serves as a conduit among the Federal Export Enforcement Agencies, Licensing Agencies, and the Intelligence Community for the exchange of information related to potential U.S. export control violations. The E2C2 primary function is to de-conflict potential enforcement actions and intelligence among the participating U.S. Government Agencies.

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

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

**Progress:** To improve the coordination of intelligence among the various agencies involved in export controls, DHS ICE HSI has made efforts to improve the operation of the E2C2 by establishing the Export Enforcement Intelligence Cell Working Group (EEICWG). Since August 2017, the EEICWG has been de-conflicting information among the interagency group, to include HSI, Commerce's Bureau of Industry and Security, Department of Defense, and other U.S. Government Agencies. Although staffing at the E2C2 remains an issue, and at this time is primarily performing de-confliction rather than intelligence analysis activities, DHS ICE HSI is committed to working with E2C2 partner agencies to fully staff the intelligence cell.

CBP has made the improvements to management and oversight of FMS noted by GAO, and has requested that the related recommendation be closed. As of May 1, 2018, CBP and the Defense Security Cooperation Agency completed the integration of the electronic sharing of the Letter of Offer and Acceptance data for FMS cases, allowing for a centralized process for tracking FMS

shipments and enhancing the FMS export data validation and decrementation process. Any associated amendments or modifications for FMS cases issued after 2004 may be returned to the entity that provided the documentation while CBP will retain all information regarding any import or export shipments against the FMS cases including the decrementation of the cases. On August 13, 2018, the President signed the Foreign Investment Risk Review Modernization Act (FIRRMA), a significant statutory reform of the authorities of the Committee on Foreign Investment in the United States (CFIUS). FIRRMA expands CFIUS authority to cover a range of foreign investments not previously within its jurisdiction, and singles out critical technology as an area of focus.

FIRRMA defines critical technology to include any items currently controlled under existing export control regimes, as well as technology the export control agencies determine should receive additional protection pursuant to the Export Control Reform Act of 2018 (ECRA). The ECRA expands the current U.S. export control authority to include “emerging and foundational technologies” and establishes a formal process for the heads of Federal agencies to identify those technologies. Candidate technologies include cutting-edge, dual-use technologies such as robotics, semiconductors, nanotechnology, quantum computing, and artificial intelligence.

FIRRMA expands CFIUS jurisdiction to include certain non-controlling investments in U.S. businesses with access to critical infrastructure, critical technology, and sensitive personal data of U.S. citizens, and, pursuant to regulations which took effect November 10, 2018, will require mandatory, short-form declarations of any such investments in which a foreign government holds a “substantial interest.” Under the prior statutory regime, CFIUS could review only those foreign investments that conferred control over an existing U.S. business to a foreign person, and most filings were made on a voluntary basis by parties seeking safe harbor for their transactions following CFIUS review.

FIRRMA also expands CFIUS jurisdiction to cover new categories of real estate transactions involving foreign purchases or leases of real estate that will form part of, or be in proximity to, airports, maritime ports, and sensitive national security sites such as military bases. Finally, FIRRMA gives CFIUS the discretion to require declarations of foreign investments in any U.S. business that produces, designs, tests, manufactures, fabricates, or develops critical technology. CFIUS has prescribed such regulations under a pilot program that took effect on November 10, 2018.

**Planned Actions and Key Milestones:** As the Department’s primary point of contact to CFIUS, PLCY is taking a number of steps to ensure the Department has deep interagency coordination for the protection of critical technology under this new regulatory regime:

- First, PLCY will work with the Office of the General Counsel (OGC) and other relevant Components to represent the Department in FIRRMA regulation drafting sessions hosted by the Department of the Treasury. Key Department equities in drafting the regulations include articulating the scope of the definition of critical infrastructure and the application of real estate provisions to airports and seaports, as well as delineating the nexus between “critical technology” now under CFIUS review authority and “emerging and foundational technologies” potentially subject to the ECRA.
- Second, pursuant to a memorandum signed by the Acting Deputy Secretary on October 12, 2018, PLCY will convene a FIRRMA Implementation Task Force with representatives from every Component to develop resource recommendations pertaining to CFIUS, including staffing levels, physical space requirements, and an appropriate



<p>budget request. The task force will present its final resourcing recommendations to the Deputy's Management Action Group (DMAG) during FY 2019, Q2. Once PLCY receives DMAG concurrence with its recommendations, PLCY will work with PA&amp;E within OCFO to prepare a departmental CFIUS budget request for FY 2021, along with possible reprogramming requests of prior year funds as appropriate. Concurrently, PLCY will work with OGC and the Management Directorate to revise the Department's delegation, directive, and instruction governing CFIUS functions consistent with the DMAG-approved recommendations.</p> <ul style="list-style-type: none"> <li>• Finally, PLCY will work with the Science and Technology Directorate and relevant Components to review, and assess the need to update, existing departmental directives and instructions relating to export controls to ensure compliance with both FIRRMA and the ECRA.</li> </ul>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p><b>GAO High-Risk Area:</b> Improving Federal Oversight of Food Safety (Government-wide)</p> <p><b>Overview:</b> 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.</p> <p>GAO has also emphasized the need to develop a government-wide performance plan for food safety. P.L. 115-43, Securing our Agriculture and Food Act, as well as Homeland Security Presidential Directive Nine (HSPD-9) outline oversight requirements for DHS; the latter articulates Assistant Secretary for Health Affairs responsibilities in coordinating efforts of the Department of Homeland Security related to food, agriculture, and veterinary defense against terrorism, and for other purposes. 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.</p> <p><b>Lead Office and Official:</b> CBP, Office of Field Operations, Mikel Tookes, Deputy Executive Director, Agriculture Programs and Trade Liaison</p> <p><b>Progress:</b> CBP has undertaken several initiatives with the U.S. Department of Agriculture (USDA) to improve federal food safety oversight. For example:</p> <ul style="list-style-type: none"> <li>• In January 2018 CBP, Office of Field Operations, Agriculture Programs and Trade Liaison realigned and issued a new strategic plan for 2017-2020. The plan included a new mission and vision statement and updated long and short term goals to: operationalize our partnerships, champion innovation, shape the leaders of tomorrow, and modernize data operations.</li> <li>• In December 2013, DHS and USDA issued its 2014-2019 joint strategic plan for the Agricultural Quarantine Inspection (AQI) program and identified performance measures</li> </ul>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

to monitor progress towards program goals. DHS and USDA developed performance measures for many aspects of the AQI program including interagency coordination, identification of high priority pests, and pest and animal disease training.

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

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

**Planned Actions and Key Milestones:** CBP will continue to report on deployment and improvement of AQI data as both agencies work toward modernization, integration, and automation of data systems. However, USDA must have the capability to interface with all CBP systems in order for system-to-system interoperability and integration to be successful. CBP has completed all agriculture modules in the International Trade Data System (ITDS) and Cargo Enforcement Reporting and Tracking System and are awaiting USDA completion of their interface system, Agriculture Risk Management (ARM). CBP and the APHIS, Plant Protection and Quarantine, Quarantine Policy, Analysis Support Staff meet weekly to discuss the APHIS Participating Government Agencies Message Sets for CBP's Automated Commercial Environment (ACE) and the interface between the CBP systems and ARM. CBP and APHIS also meet regularly on the Border Interagency Executive Council that includes representatives

from all federal agencies that have a role in importing, exporting, or border management. Additionally, CBP and APHIS meet on the ITDS Board for the single-window development through ACE. As a result of the aforementioned efforts and CBP's dedication to food safety, CBP has successfully met the intent and fully implemented all of the CBP assigned recommendations associated with this High Risk Issue area.

**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 NFIP, 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 Under Secretary for Management (USM), Chip Fulghum, Deputy USM and Chief Sustainability Officer

**Progress:** In FY 2018, DHS made significant advancements in addressing mission-related resilience efforts outlined in the DHS Climate Action Plan and Climate Resilience Directive 023-03. The natural disasters of 2017 and 2018 further highlighted the focus on mission resilience and underscored the need to reduce the impact on the Department's mission-capability.

Operational resilience to support critical infrastructure continues to be a cornerstone of many of the Department's programs, policies, and activities. OCRSO's Sustainability and Environmental Programs (SEP) continues to lead the Department's resilience efforts. In FY 2018, a Resilience Tiger Team championed by the DHS SEP Executive Director, was established. The Tiger Team, consisting of DHS Components, Program Offices and the Department of Energy (DOE), developed the Department's first ever Resilience Framework. The Framework, signed by the USM on August 13, 2018, defined a systematic approach to measure and plan for resilience and incorporate it into our critical infrastructure in the areas of energy and water, facilities, information and communication technology, and transportation. This Framework ensures sustained resilience and readiness of our mission essential functions supporting critical infrastructure assets during all phases of mission operations (normal operations, disruptive event, response, and recovery and reconstitution).

In FY 2018, DHS also signed a Memorandum of Understanding (MOU) with DOE. The MOU outlined three areas of support:

- Development of resilience framework;
- Development of an assessment tool; and
- Execution of pilot projects to support incorporation of resilience within our critical infrastructure.

In FY 2018, SEP hosted a “Leadership in Resilience” summit. The Summit brought together DHS, DOE, DOD, and White House Council on Environmental Quality (CEQ) Senior Leadership and the environmental, logistics, continuity of operations, energy, and facility management communities and served as a platform to:

- Present the DHS Resilience Framework;
- Improve mission readiness; and
- Foster inter- and intra-agency relationships.

**Planned Actions and Key Milestones:** During FY 2019, DHS plans to advance the following initiatives:

- Development of Component Plans for Resilience for all DHS Components and Headquarters; and
- Furtherance of a DHS enterprise system for governance and oversight of infrastructure management which includes the incorporation of the Department’s largest utility consumer data and expansion of current analytical capabilities.

#### **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* (FITARA), 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 Joint Requirements Council (JRC) to evaluate high priority, and cross-Departmental opportunities.

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

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

- Updated existing departmental policies and procedures to promote compliance with FITARA transparency and risk management reporting and review requirements.
- Developed IT maturity model and expanded the IT internal control program, which is a joint effort by the DHS CIO and the Chief Financial Officer (CFO), to assist in the monitoring and management of the IT internal controls for the Department and jointly support Components in efforts to strengthen IT general controls, systems security, and IT internal controls environments (see charts following this section). The DHS CIO and CFO will sign a commitment letter to track progress towards continued improvements and enhanced sustainability.
- Continued to employ mature enterprise-wide governance processes, including program reviews, IT Acquisition Reviews, and CIO approval of acquisition plans and reprogramming requests. OCIO is a key contributor to the DHS JRC process and reviews.
- Partnered with the OCFO for the third year to conduct an in-depth review of DHS IT infrastructure. In FY 2018, OCIO and OCFO conducted the next annual IT Infrastructure Assessment and refined performance measures for end user, network, and server assets, with additional emphasis on collecting information on approximately 700 DHS systems to inform planning for cloud migration and reducing reliance on DHS data centers. The results of this study informed the FY 2020-2024 budget formulation cycle, the DHS Cloud planning, and enterprise data center-related target goals. OCIO and OCFO have initiated the FY 2019 IT Infrastructure Assessments to continue this work and to add focus on continuity and disaster recovery capabilities.
- Continued to update the IT Federal Dashboard, which has resulted in approximately 200 Program Health Assessments in the calendar year.
- Established a more robust relationship between the OCIO community and the acquisition community. OCIO leadership sit on the Acquisition Review Board and play an important role in informing the USM while making acquisition decisions on IT programs. As a result, cyber maturity has increased in the past year with more focus on threat assessments, with the Chief Information Security Officer and Chief Technology Officer playing critical roles.
- Continued the DHS Headquarters Agile Acquisition Working Group to bring together representatives from OCIO, PARM, JRC, Office of the Chief Procurement Officer (OCPO), OCFO, and S&T through the IT Program Management Center of Excellence and completed 10 of 18 specific action plans to streamline acquisition for all future DHS IT investments with the remainder scheduled for completion by Q2 FY 2019.
- Ensured that a minimum of 80 percent of DHS's major IT software delivery acquisitions deliver usable functionality every 6-12 months (100 percent as of December 2017 and continuing to monitor monthly). The Investment Evaluation, Submission and Tracking (INVEST) system collects information from OCIO compliance analysts to indicate the CIO certification of incremental development for appropriate software development projects and reports DHS Agile Core Metrics to support the CIO's certification requirement.
- Addressed the lack of sufficient program management capabilities for major high-priority IT investments, by developing a number of IT-focused support and oversight capabilities.



- Continued optimizing data center hosting across the Department resulting in the consolidation of 47 data centers and generating cost savings or avoidance. DHS Components continue to migrate to private “as-a-service” offerings or other cloud options, and/or strategically-sourced enterprise contract vehicles. This effort is accelerating with IT modernizations to migrate or develop over 130 systems to public cloud service providers and additional efforts to reduce the square footage in one enterprise data center by Q2 FY 2019 and eliminating a second enterprise data center by FY 2021.
- Completed the DHS Software Centralization Overview as of December 8, 2017, the associated DHS Software Optimization Model on April 23, 2018, and the DHS Enterprise Software Asset Management Framework, on August 30, 2018. These documents demonstrate how DHS is leveraging the arrival of CDM asset-based security capabilities to implement software asset and risk management framework, policy and processes continually across the DHS network environment to achieve compliance with the Megabyte Act of 2016 and OMB Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing. As a result, GAO determined that DHS is fully compliant with the Megabyte Act, has closed all open software licensing audit recommendations, and recommended that DHS receive an “A” for software licensing on the upcoming FITARA scorecard. DHS will continue implementation of its CDM asset-based security management framework and optimization model during FY 2019.
- Assisted with the transition of current DHS Mobility Managed Service(s) to Next Generation Mobility Managed Service(s) in accordance with OMB Category Management Policies Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops (15-1) and Mobile Devices and Services (16-3). The IT Mobility Sub-Category Management Working Group completed requirements analysis in February 2018 and identified a target for an end-to-end, automated, fully managed service to centrally manage, accurately track, and report on all fixed and mobile telecommunications voice, data, and assets to reduce expenses and control costs throughout the telecommunications lifecycle. The DHS CIO Product and Services Delivery Management Mobility team is currently working with the DHS Enterprise Infrastructure Solutions (EIS) Working Group to convert the extensive next generation Mobility requirements document to EIS format for solicitation in FY 2019.

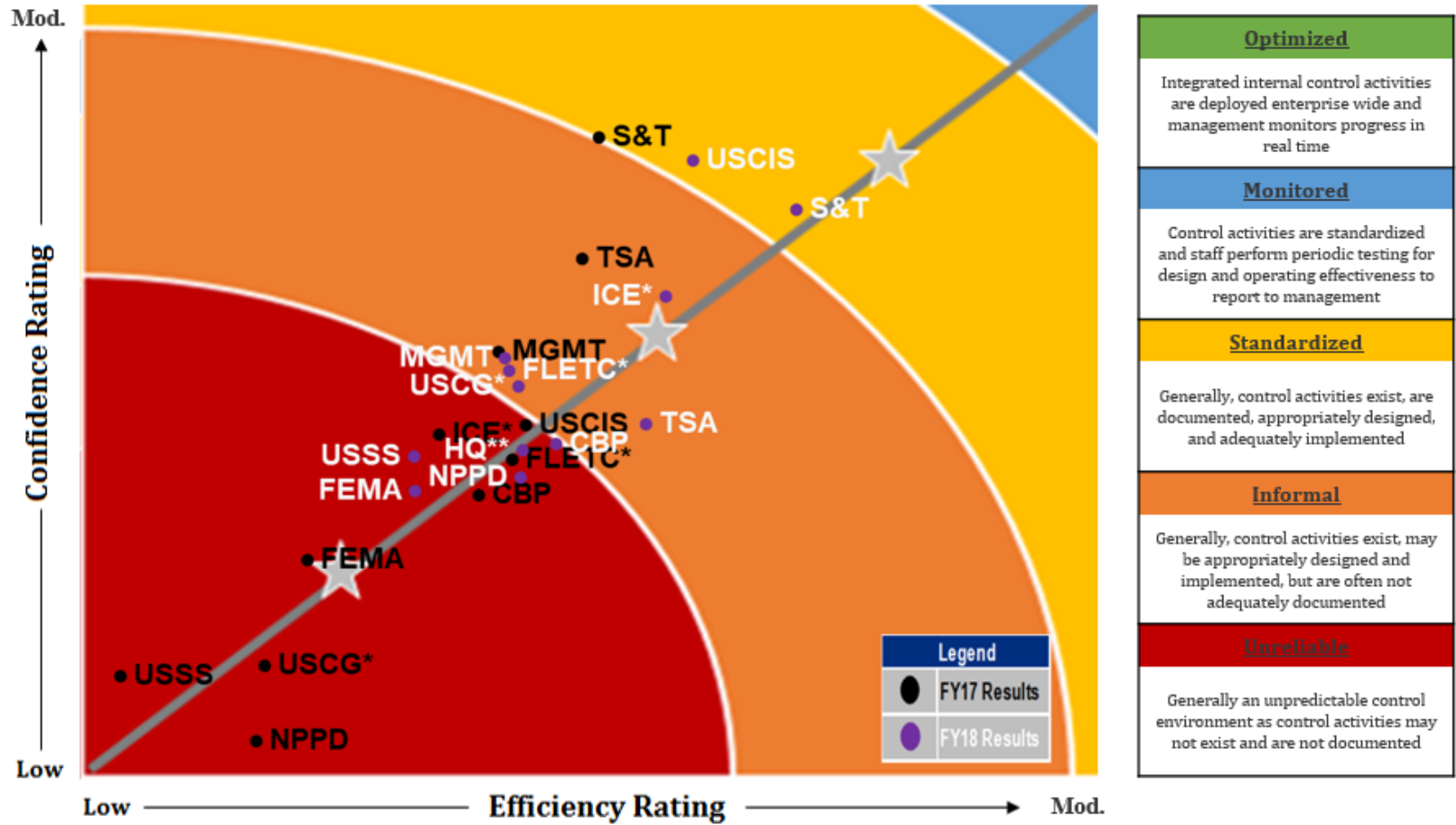
**Planned Actions and Key Milestones:** DHS will continue to implement OMB initiatives to improve IT management, reduce duplication and costs, and improve services to the public with ongoing in-person TechStat reviews of IT programs, monthly reporting to the Federal IT Dashboard, and leveraging strategic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

- Implementing a new personnel system that will enable DHS to better compete with industry on recruiting and retaining cybersecurity professionals. DHS is also a leading voice in OPM's efforts to address mission critical skills gaps.
- Submitting an IT Competency Models and Gap Analysis Report to GAO for IT roles (GS-2210s: Enterprise Architecture, Information Security, IT Program Management, and Policy and Planning), as well as the IT Acquisition Cadre.

- Utilizing a range of available evaluation metrics, measures, and tools, including operational assessments, to monitor and report on the status of the Digital Transformation Program. The program has made significant strides having reduced technical debt and other risks, and transitioned to a cloud environment.
- Continuing to outline the key processes, practices, and steps to be undertaken as a part of a comprehensive centralization plan and management adoption framework and utilize an agile methodology and the concept of progressive elaboration so that as more detailed information becomes available the plan for software licenses may continuously and constantly be modified.
- In accordance with OMB Category Management Policies Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops (15-1) and Mobile Devices and Services (16-3), the IT Mobility Sub-Category Management Working Group, continuing to identify Component Mobility related requirements and priorities; validate the delivery of transition activities to satisfy those requirements; and drive the planning, execution, monitoring and tracking of the Component transition to the Next Generation Mobility Managed Service(s).
- The Information Technology Asset Management and Refresh Directive (138-03), issued on March 30, 2018, will be utilized to provide input into the FY 2021-2025 DHS budget formulation review and decision process.
- Continuing to utilize the Open Source Community of Practice (COP) to include representatives from all major DHS components to collaborate and determine existing Open Source repository implementations across DHS.
- Continuing to collaborate with the COP and will partner with other agencies to compare and combine existing best practices and tools into a consolidated DHS Open Source repository strategy, and will commence a pilot implementation of Open Source software into a shared repository.



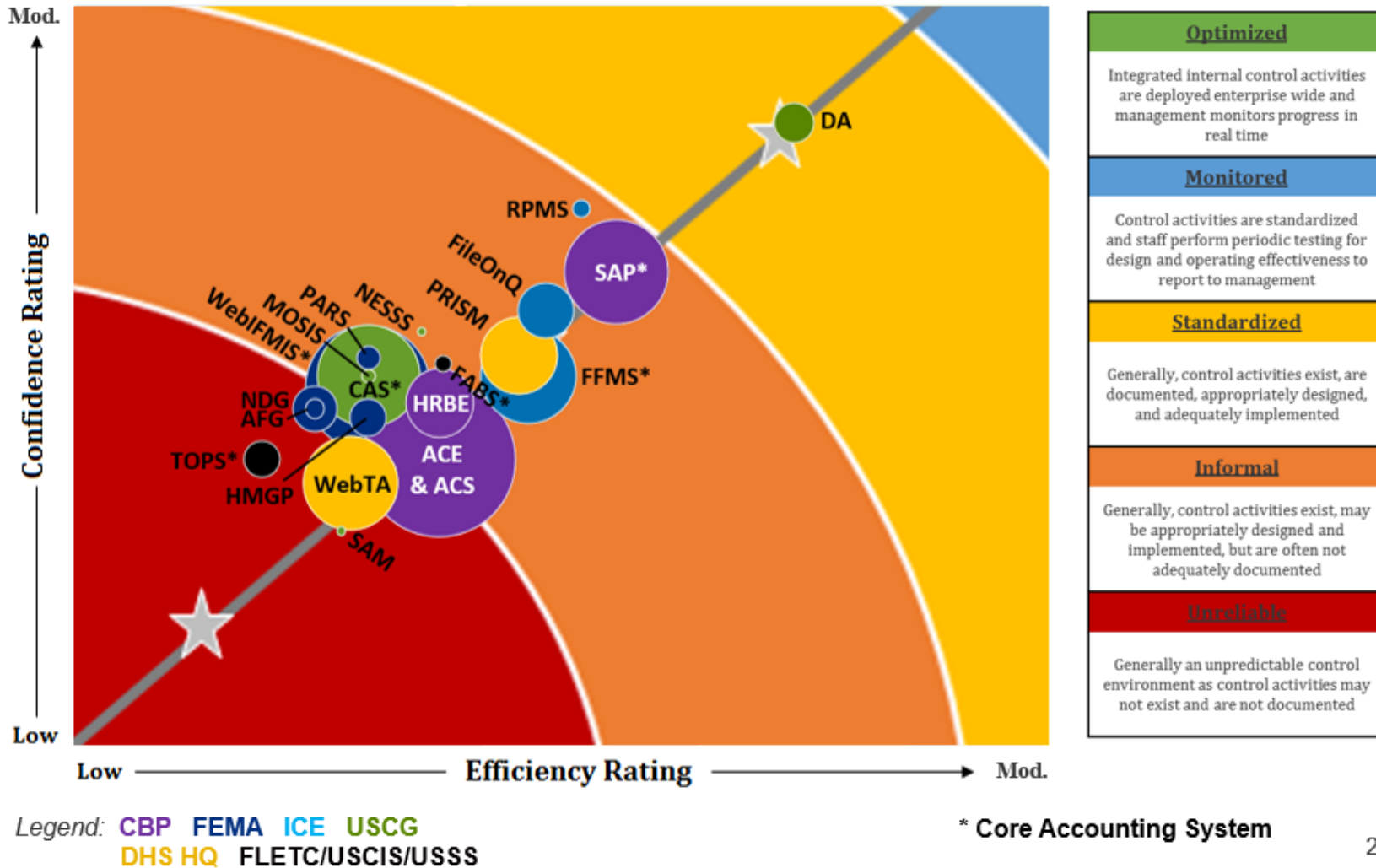
# Internal Controls Maturity Model Information Technology – As of 9/30/2018



\*Financial Service Providers  
\*\*HQ placement provided in FY18, whereas it was not provided in prior years.



# Internal Controls Maturity Model – IT High Impact Systems – As of 9/30/2018



**GAO High-Risk Area: Government-wide Personnel Security Clearance Process**

**Overview:** In January 2018, GAO added the government-wide personnel security clearance process to the High Risk List. A high-quality and timely government-wide personnel security clearance process is essential to minimize the risks of unauthorized disclosures of classified information, and to help ensure that information about individuals with a criminal history, or other questionable behaviors, is identified and assessed. As of October 1, 2015, the latest date for which data is available, approximately 4.2 million government and contractor employees, at nearly 80 executive branch agencies, were eligible to hold a personnel security clearance.

DHS has been aggressive with its efforts to mitigate impediments to the current clearance process. DHS has issued internal guidance through policy memoranda in order to streamline the personnel security process, and to instill consistency across the enterprise. DHS is a very active member in government-wide personnel security reform efforts, with representation and input on numerous inter-governmental working groups. This includes Trusted Workforce 2.0, which is a high-level management working group dedicated to re-thinking personnel vetting processes across the federal government. DHS is also involved in the Performance Accountability Council (PAC) PMO, the arm of the PAC mandated to create governmental enterprise technical solutions for the personnel security process, and Office of the Director of National Intelligence's (ODNI) Continuous Evaluation (CE) working group.

DHS is actively involved on many fronts to address the high-risk areas of timeliness and backlog of investigations, reform initiatives, and the quality of background investigations. DHS is engaged with OPM, ODNI, and our contract background investigation vendors to prioritize DHS cases, and increase timeliness wherever possible. DHS is an active participant in government-wide reform initiatives and efforts regarding the quality of background investigations. For example, DHS uses the ODNI Quality Assessment Reporting Tool to report on the quality of investigations, and ensures that all adjudicators and background investigators are trained in accordance with national standards promulgated by OPM and ODNI.

In addition to those efforts, the DHS Chief Security Officer (CSO) established the Personnel Security Operations Task Force (PSOTF) to support reforms efforts across the Department. The PSOTF's charter is to identify Departmental improvements to the personnel security posture by evaluating enterprise-wide personnel security processes, procedures, best practices, and organizational structures. The PSOTF consists of personnel security representatives from all DHS Components and employs Lean Six Sigma – Continual Process Improvements techniques to evaluate personnel security processes and procedures within DHS, and benchmark against other federal agencies. DHS is working diligently to address and lessen the impact of the systemic problems afflicting the governmental personnel security process.

**Lead Office and Official:** Management Directorate, Office of the CSO, Richard D. McComb, CSO

**Progress:** DHS is actively working on reducing the length of time to onboard federal and contractor personnel. DHS is collaborating both internally and externally with our federal partners to transform the personnel security process. Initiatives include:

- Since 2017, DHS has issued multiple policy memoranda to clarify reciprocity guidance, and further streamline and standardize personnel security procedures across the Department. Examples include Departmental guidance on expediting entry on duty for contractors with active security clearances; polygraph reciprocity; guidance on



streamlining personnel security procedures for internal and external transfers; and, in compliance with ODNI standards, DHS-specific mitigation strategies to address the investigative backlog. These measures show through metrics that DHS tracks and provides to senior leadership. On average, DHS on-boards both contractors and federal applicants over 87 percent of the time based on preliminary, risk-based assessments, prior to completion of the full background investigation. For example, in September 2018, DHS cleared contractors to begin work in an average of 15 days in over 94 percent of cases. For federal employee applicants during this same period, DHS cleared applicants to begin work in an average of 43 days in over 86 percent of cases.

- In September 2018, the PSOTF finalized their report containing recommendations to further improve the Department's personnel security clearance process. While the final report is still pre-decisional, tentative initiatives include increased coordination with the OCPO to standardize contractor security requirements in contracts; seeking department-wide delegated investigative authority; and establishing a DHS personnel security surge force across the Department to support high impact efforts or workload surges impacting specific Components. The next step is for the PSOTF to prioritize the list of recommendations, and establish an estimated completion date for each.
- DHS is currently collaborating with industry partners in a series of Acquisition Innovation Roundtables (AIRs) designed to increase transparency, consistency of application, and increased communication across the Department including enhancing DHS's public-facing website and notifications to industry.
- DHS remains closely engaged with industry through organizations such as the Industrial Security Working Group who hosts annual Personnel Security Forums. These events provide a venue for DHS to socialize the latest personnel security policies, procedures, and initiatives.
- DHS continues to collaborate with ODNI to utilize their CE system, and is in compliance with ODNI policy on CE requirements for national security positions. DHS has exceeded ODNI requirements for CE of five percent of the Top Secret population in both FY 2017 and FY 2018.
- DHS is actively engaged with the Human Resources Information Technology (HRIT) effort, which will streamline and eliminate manual and redundant processes surrounding the hand-off between security and human resources for on-boarding.

**Planned Actions and Key Milestones:** DHS has documented the estimated completion times for the various efforts it is currently undertaking. It should be noted that some of these efforts depend on future funding. Initiatives include:

- DHS expects the HRIT initiative to be completed in the second quarter of FY 2019, and will continue to look for areas to gain efficiencies between security and human resources for onboarding. The expected result of HRIT implementation is a more efficient and timely onboarding processing between security and human resources by eliminating duplicative and manual processes.
- DHS is developing a more effective communication through the Application Lifecycle Management initiative, which will also provide systematic and more expeditious notifications to industry when their staff clear the personnel security process enabling industry partners to commence work on DHS contracts.

- DHS is focusing on developing relationships with industry partners, in part through continued AIRs. The next AIR will focus on improving security language in contracts and visibility into the personnel security process. Engagements will continue in the first quarter of FY 2019. To date, AIR working groups have resulted in an open dialogue between federal staff and industry partners. One result is the update to formatting of information found on the public-facing website, providing information for industry to better serve DHS mission areas.
- DHS will begin implementing recommendations stemming from the PSOTF, starting in the first quarter of FY 2019. One example is a personnel security manual to standardize fitness determinations and facilitate reciprocity, clarify department-wide personnel security operating processes, and to increase consistency and validity of metrics.
- DHS will continue to partner with ODNI on CE efforts, including the ODNI CE unclassified system once it is functional. The estimated timeframe for initial operating capability is the first quarter of FY 2019. DHS is currently working with the ODNI on system-to-system access and integration.
- DHS will remain engaged with the PAC and the Department of Defense regarding information technology shared services for personnel security processing, and any recommendations coming from Trusted Workforce 2.0 efforts.

## Low-Priority Program Activities

The President's Budget identifies the lower-priority program activities, as required under the *GPRA Modernization Act*, 31 U.S.C.

1115(b)(10). The public can access the volume at:  
<http://www.whitehouse.gov/omb/budget>

## Acronyms

ADE – Acquisition Decision Event  
 AIS – Automated Indicator Sharing  
 ALOS – Average Length of Stay  
 APG – Agency Priority Goal  
 AQI – Agricultural Quarantine Inspection  
 ARB – Acquisition Review Board  
 ARM – Agriculture Risk Management  
 ATS – Automated Targeting System  
 A&O – Analysis and Operations  
 BASE – Baseline Assessment for Security Enhancement  
 BOD – Binding Operational Directive  
 CA-Plan – Climate Action Plan  
 CBP – U.S. Customs and Border Protection  
 CDM – Continuous Diagnosis Mitigation  
 CERTS – Cargo Enforcement Reporting and Tracking System  
 CFATS – Chemical Facility Anti-terrorism Standards  
 CFO – Chief Financial Officer  
 CHCO – Chief Human Capital Office  
 CIO – Chief Information Officer  
 CIP – Critical Infrastructure Protection  
 CISA – Cybersecurity and Infrastructure Security Agency  
 CISR – Critical Infrastructure Security and Resilience  
 COO – Chief Operating Officer  
 CROPs – Component Recruitment and Outreach Plans  
 CSD – Cyber Security Division  
 CSAT – Chemical Security Assessment Tool  
 CS&C – Office of Cybersecurity and Communications  
 CTHA – Continued Temporary Housing Assistance  
 CTO – Chief Technology Office  
 C-TPAT – Customs-Trade Partnership Against Terrorism

DEFEND – Dynamic Emerging Federal Enterprise Network Defense  
 DHS – U.S. Department of Homeland Security  
 DMO – Departmental Management and Operations  
 DNDO – Domestic Nuclear Detection Office  
 DOS – Department of State  
 DPIO – Deputy Performance Improvement Officer  
 E2C2 – Export Enforcement Coordination Center  
 EAB – Enterprise Architecture Board  
 EEI – Employee Engagement Index  
 EEIWG – Export Enforcement Intelligence Working Group  
 EITSB – Enterprise IT Services Board  
 EO – Executive Order  
 ERO – Enforcement and Removal Operations  
 ESC – Enterprise Computing Services  
 EXD – Explosives Division  
 FAC-P/PM – Federal Acquisition Certification for Program and Project Managers  
 FEMA – Federal Emergency Management Agency  
 FEVS – Federal Employee Viewpoint Survey  
 FIMA – Federal Insurance and Mitigation Administration  
 FLETC – Federal Law Enforcement Training Centers  
 FMS – Foreign Military Sales  
 FPS – Federal Protective Service  
 FSA – Facility Security Assessment  
 FY – Fiscal Year  
 FYHSP – Future Years Homeland Security Program  
 GAO – Government Accountability Office  
 GCC – Government Coordinating Council  
 GFS – Government Facility Sector

## FY 2018-2020 Annual Performance Report

GPRA – Government Performance and Results Act  
GPRAMA – GPRA Modernization Act  
HCOP – Human Capital Operating Plan  
HME – Homemade Explosives  
HOMECORT – Homeland Criminal Organization Target  
HPRDS – Human Portable Rad/Nuc Systems  
HQ – Headquarters  
HRM – Human Resource Management  
HSI – Homeland Security Investigations  
HVA – High Value Assets  
IC – Intelligence Community  
ICE – U.S. Immigration and Customs Enforcement  
IEFA – Immigration Examination Fee Account  
IPT – Integrated Project Team  
IRS – Internal Revenue Service  
ISC – Interagency Security Committee  
ISP – Internet Service Provider  
IT – Information Technology  
ITDS – International Trade Data System  
I&A – Office of Intelligence and Analysis  
JIOCC – Joint Intelligence and Operation Coordination Centers  
JOA – Joint Operating Areas  
JTF – Joint Task Force  
LEO – Law Enforcement Officer  
MCO – Mission Critical Occupation  
MEXUS – Mexico-US Joint Contingency Plan  
MFR – Modular Firing Range  
MT – Mandatory Training  
MS-13 – Mara Salvatrucha drug cartel/gang  
NCATS – National Cybersecurity Assessment and Technical Services  
NCCIC – National Cybersecurity and Communications Integration Center  
NCEPP – National Cyber Exercise and Planning Program  
NCMEC – National Center for Missing and Exploited Children

NCPS – National Cybersecurity Protection System  
NFIP – National Flood Insurance Program  
NIST – National Institute of Standards and Technology  
NOC – National Operations Center  
NTAG – National Targeting and Analysis Group  
NSSE – National Special Security Event  
OCHCO – Office of the Chief Human Capital Officer  
OCPO – Office of the Chief Procurement Officer  
OCRSO – Office of the Chief Readiness Support Officer  
OEWG – Organizational Effectiveness Working Group  
OGC – Office of the General Counsel  
OHA – Office of Health Affairs  
OIG – Office of Inspector General  
OMB – Office of Management and Budget  
OPCON – Operational Control  
OPLA – Office of the Principal Legal Advisor  
OPM – Office of Personnel Management  
OPMAT – Operations Matador  
OPS – Office of Operations Coordination  
PARM – Program Accountability and Risk Management  
PA&E – Office of Program Analysis and Evaluation  
PCoE – Protection Center of Excellence  
PIO – Performance Improvement Officer  
PMDf – Performance Measure Definition Form  
PMCO – Priority Mission Critical Occupation  
PPA – Program, Project, and Activity  
PTI – Priority Trade Issue  
RFID – Radio Frequency Identification  
RIG – Regional Integration Group  
RPM – Radiation Portal Monitors  
RVA – Risk and Vulnerability Assessments  
SBA – Small Business Administration  
STT – Sample Tracking Tool



S&T – Science and Technology Directorate  
TCO – Transnational Criminal Organizations  
THIRA – Threat and Hazard Identification  
and Risk Assessment  
TRIP – Traveler Redress Inquiry Program  
TSA – Transportation Security  
Administration  
USCG – U.S. Coast Guard

USCIS – U.S. Citizenship and Immigration  
Services  
USDA – U.S. Department of Agriculture  
USM – Under Secretary for Management  
USSS – U.S. Secret Service  
VBIED – Vehicle-Borne Improvised  
Explosive Device  
WDP – Workforce Development Plan  
WYO – Write-Your-Own





Homeland  
Security



Homeland  
Security