Annual Performance Report

Fiscal Years 2017-2019

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

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

We are DHS

About this Report

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

For FY 2017-2019, the Department is using the alternative approach—as identified in the Office of Management and Budget's Circular A-136—to produce its Performance and Accountability Reports, which consists of the following three reports:

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

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

Contact Information

For more information, contact:

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

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

Table of Contents

Introduction

This Appendix provides, in tabular format, a detailed listing of all performance measures in the Annual Performance Report with their respective measure description, scope of data, data source, data collection methodology, reliability index, and explanation of data reliability check. Performance measures and their related data are listed alphabetically by Component.

Performance Data Verification and Validation Process

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

DHS implemented a multi-pronged approach to effectively mitigate risks and reinforce processes that enhance the Department's ability to report complete and reliable data for performance measure reporting in support of the Government Performance and Results Act (GPRA) Modernization Act (GPRAMA) of 2010. This approach consists of the: 1) an annual change control process that uses a tool called the Performance Measure Definition Form (PMDF); 2) a central information technology repository for performance measure information; 3) the Performance Measure Checklist for Completeness and Reliability; and 3) annual assessments of the completeness and reliability of a sample of our performance measures by an independent review team.

Performance Measure Definition Form (PMDF)

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

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

Central Information Technology Repository for Performance Measure Information

All of DHS's approved measures are maintained in the FYHSP system, which is a Department-wide IT system accessible to all relevant parties in DHS. The system is a modular database which allows for the management of the Department's performance plan and the capturing of performance results on a quarterly basis. The FYSHP 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 is used to populate the Department's business intelligence tools to provide real-time information.

Performance Measure Checklist for Completeness and Reliability

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

Independent Assessment of the Completeness and Reliability of Performance Measure Data

CFO, PA&E conducts an assessment of performance measure data for completeness and reliability on a subset of its performance measures annually using an independent review team. This independent review team assesses selected Component GPRAMA measures using the methodology prescribed in the *DHS Performance Measure Verification and Validation Handbook*, documents their findings, makes recommendations for improvement, and may perform a subsequent follow-up review to observe the implementation of recommendations. Corrective actions are required for performance measures determined 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 its 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 attesting to the completeness and reliability of performance measure information in our Performance and Accountability Reports. Any unreliable measures and corrective actions are specifically reported in the Annual Performance Report.

Measure Descriptions, Data Collection Methodologies, and Verification and Validation Information

Analysis and Operations

Performance Measure	Number of intelligence reports shared with the intelligence community
Program	Analysis and Operations
Description	This measure reflects the DHS contribution of raw, unevaluated intelligence, to the intelligence community and the federal government so as to share the unique information obtained from intelligence officers in the field. This intelligence is only that which has been aligned to relevant Homeland Security Intelligence Priorities driven by the Homeland Security Intelligence Council. The measure counts the number of unique intelligence reports that the DHS Office of Intelligence and Analysis has disseminated.
Scope of Data	The measure reflects all Office of Intelligence and Analysis intelligence information reports that are tagged with the relevant Homeland Security priority codes and are available to the entire Intelligence Community. The Department uses an annual process to refine the topics of concern to the enterprise and to create a hierarchy of those priority intelligence requirements and codes by which incoming information can be cataloged and retrieved for analysis later.
Data Source	The intelligence information reports are stored and available in the official federal intelligence repository named Chrome. It is accessed through the HUMINT Online Tasking and Reporting (HOT-R) system. These systems are also the same ones used by the rest of the intelligence community to access all intelligence reporting.
Data Collection Methodology	Intelligence officers in the field gather information through their interactions with sources and then they prepare a report that is considered to be raw, unevaluated information. These intelligence reports are cataloged and tagged to priorities as they are entered into the system the HOT-R system. There is significant training and a review process before reports are made permanent in the system. Once made permanent, they are available to other intelligence officers across the federal government. Reports are run to count the number of unique intelligence reports that the Office of Intelligence and Analysis has disseminated.
Reliability Index	Reliable
Explanation of Data Reliability Check	The repositories are designated as the official repositories for the collection reports across the intelligence community and the data are reviewed at least monthly by Office of Intelligence and Analysis performance and operational analysts for completeness and accuracy. In the event that inaccurate data is reported, processes are in place to adjudicate any issues and correct the record to ensure accuracy.

Performance Measure	Percent of Intelligence and Analysis finished intelligence reports incorporating DHS and state/local originated data
Program	Analysis and Operations
Description	This measure gauges the impact that DHS provides to the intelligence community by disseminating in finished intelligence reports information harnessing DHS and state, local, tribal, and territorial data that is unique. The measures provides an indication of the value that DHS Intelligence is providing to the larger intelligence community through its ability to collect and leverage unique data to support analytical judgements and reduce potential overlap with analysis from other agencies. The measure reflects intelligence that may have been produced solely by DHS or in a partnership with other agencies.
Scope of Data	Information that is used to calculate this result is based on all DHS and state, local, tribal, and territorial (SLTT) unique information cited in Intelligence and Analysis (I&A) finished intelligence reports. A finished intelligence report is a product of analytical judgement applied to address an intelligence question where the analytic conclusions have been drafted, reviewed, and disseminated outside of I&A.
Data Source	Analysts begin their analysis in the System for Analytic Review and Approval (SARA) system, and then the finished analytical production and reports are stored in an internal system named HELIX. All analytic products must include sources and metadata associated with those sources.

Performance Measure	Percent of intelligence reports rated "satisfactory" or higher in customer feedback that enable customers to manage risks to cyberspace
Program	Analysis and Operations
Description	This measure gauges the extent to which the DHS Intelligence Enterprise (DHS IE) is satisfying their customers' needs related to understanding the threat. This measure encompasses reports produced by all DHS component intelligence programs and provided to federal, state, and local customers.
Scope of Data	The scope of this measure is all feedback received from customer satisfaction surveys returned to the DHS IE member (U.S. Coast Guard, Transportation Security Administration, etc.) that originated the intelligence report. For this performance measure "intelligence report" is defined per Component.
Data Source	The data source for this performance measure will be customer feedback surveys fielded by the DHS IE.
Data Collection Methodology	Members of the DHS IE will attach an electronic survey instrument to each intelligence product disseminated to customers. The recipient of the intelligence completes and then returns the survey to the issuer. The DHS Intelligence Enterprise will provide Intelligence and Analysis (I&A) with the survey results on the second Friday following the end of each quarter. Upon receipt of the data, I&A will average the data across the Intelligence Enterprise for each of DHS mission area and report the total. For this measure, customer satisfaction is defined as responsiveness of the product and its value in helping the customer manage risks to cyberspace. Customers rate their satisfaction on a five point scale from: very satisfied, somewhat satisfied, neither satisfied nor dissatisfied, somewhat dissatisfied, or very dissatisfied. Responses "very satisfied" and "somewhat satisfied" will be considered to have met the criteria for "satisfactory."
Reliability Index	Reliable
Explanation of Data Reliability Check	Individuals within the DHS IE are responsible for collecting, storing, and reporting data generated by the source above. I&A Performance Management & Evaluation (PME) personnel are responsible for aggregating the data from the DHS IE and reporting the results quarterly. Once the survey responses are received and aggregated, I&A PME staff review the results for consistency and look for any anomalous trends that would signal a data integrity problem. Any issues are researched and if any erroneous data is found, it is corrected or removed from the overall calculation.

Performance Measure	Percent of intelligence reports rated "satisfactory" or higher in customer feedback that enable customers to understand the threat
Program	Analysis and Operations
Description	This measure gauges the extent to which the DHS Intelligence Enterprise (DHS IE) is satisfying their customers' needs related to anticipating emerging threats. This measure encompasses reports produced by all DHS component intelligence programs and provided to federal, state, and local customers.
Scope of Data	The scope of this measure is all feedback received from customer satisfaction surveys returned to the DHS IE member (U.S. Coast Guard, Transportation Security Administration, etc.) that originated the intelligence report. For this performance measure "intelligence report" is defined per Component.
Data Source	The data source for this performance measure will be customer feedback surveys fielded by the DHS IE.
Data Collection Methodology	Members of the DHS IE will attach an electronic survey instrument to each intelligence product disseminated to customers. The recipient of the intelligence completes and then returns the survey to the issuer. The DHS IE will provide Intelligence and Analysis (I&A) with the survey results on the second Friday following the end of each quarter. Upon receipt of the data, I&A will average the data across the Intelligence Enterprise for each of DHS mission area and report the total. For this measure, customer satisfaction is defined as responsiveness of the product and its value in helping the customer anticipate emerging threats. Customers rate their satisfaction on a five point scale from: very satisfied, somewhat satisfied, neither satisfied nor dissatisfied, somewhat dissatisfied, or very dissatisfied. Responses "very satisfied" and "somewhat satisfied" will be considered to have met the criteria for "satisfactory."
Reliability Index	Reliable
Explanation of Data Reliability Check	Individuals within the DHS IE are responsible for collecting, storing, and reporting data generated by the source above. I&A Performance Management & Evaluation (PME) personnel are responsible for aggregating the data from the DHS IE and reporting the results quarterly. Once the survey responses are received and aggregated, I&A PME staff review the results for consistency and look for any anomalous trends that would signal a data integrity problem. Any issues are researched and if any erroneous data is found, it is corrected or removed from the overall calculation.

Performance Measure	Percent of National Operations Center Incident Reports and Situational Awareness Products produced and disseminated to the homeland security enterprise within targeted timeframes
Program	Analysis and Operations
Description	This measure evaluates percent of Situational Awareness (SA) Products disseminated within targeted timeframes. These products serve as the basis for senior leader decision-making and SA across the homeland security enterprise. To augment SA, facilitate coordination, and provide decision support, the National Operations Center (NOC) utilizes a web-based DHS Common Operating Picture (COP). The COP can be accessed through various Briefing Display Systems within the NOC, or through any computer using the Homeland Security Information Network (HSIN). HSIN allows only authorized users to manipulate information on the COP. The NOC Watch Team creates a geographically located icon on the COP and an overall written situation summary to provide SA on the event to decision makers and the Homeland Security Enterprise. The targeted timeframe to create and display information on the COP is within 30 minutes of the Senior Watch Officer determining that an incident requires posting to the COP.

Scope of Data	This measure includes all Incident Reports and situational awareness products at the "monitor" or "higher" incident level as determined by the Senior Watch Officer. The NOC Standard and Operating Procedures (SOP) promulgate the type of report and timeline requirements for incident reporting. Type of reportable events can include initial breaking, pre-planned, weather, and current reports updates. Incident reports are at the Monitored, Awareness, Guarded (Phase 1), Concern (Phase 2), or Urgent (Phase 3) level.
Data Source	Primary source for the required data is the Phase Notification Log which is an electronic data base with controlled access on the DHS shared network drive. During an event, a designated desk position on the NOC Watch Team captures and manually enters the data into the electronic data base which provides the detailed report timing information.
Data Collection Methodology	The data for this measure will include the creation of an icon and summary on the DHS Common Operating Picture (COP) for all "monitored" and "higher" level Homeland Security situations. The targeted timeframe for this measure starts when the Senior Watch Officer announces designation of an incident at the "monitored" or higher level. The time stops when the incident has been added to the COP, thus informing the Homeland Security Enterprise. The Notification Log (monitored and higher) will be used to provide the times for this measure as it maintains a detailed incident timeline summary. The manually captured data is entered into the notification log for management review.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data is entered into the program as the incident/event is being reported. Data in the system is reviewed by the Knowledge Management Officer desk supervisor and Operations Officer to ensure standardization is maintained.

Performance Measure	Percent of risk assessments for federal security support of large public/community special events completed within the targeted time frame
Program	Analysis and Operations
Description	This measure indicates the percent of Special Event Assessment Ratings (SEAR) completed within the targeted timeframe. State and local authorities voluntarily submit events taking place within their jurisdictions to the National Special Events Data Call. These events are assessed using the SEAR methodology, resulting in the National Special Events List, providing a SEAR that defines 5 levels of risk, with SEAR 1 being the highest. SEAR levels are used by federal agencies as criteria to determine their level of support to state and local events. The list is the primary federal awareness mechanism for special events occurring across the nation.
Scope of Data	This measure includes all events submitted for review in the SEAR process. Events are collected one of two ways; either during the National Special Events Data Call period, or on an ad hoc basis throughout the calendar year. Submitted events receive a final adjudication by either November 25th for events submitted to the annual data call, or 5 business days for submitted short-notice events.
Data Source	The Homeland Security Information Network Special Events Working Group Community of Interest (HSIN COI). It is accessible on HTTPS://hsin.dhs.gov. Users must be nominated and provided access to the COI to view the material. It is available in Microsoft EXCEL format upon request.
Data Collection Methodology	This measure is currently tracked utilizing the Homeland Security Information Network Special Events Working Group Community of Interest (HSIN SWEG COI). The HSIN COI sends a notification email to the Special Events Program when a new item is received, the date of this email establishes the start time for the assessment. The new event is then adjudicated with the proper SEAR rating by the Special Events Program; the corresponding SEAR rating is then entered into the SEWG COI. The date the adjudicated SEAR rating is entered into the SEWG COI represents the end time for the measure.
Reliability Index	Reliable

Explanation of Data Reliability Check	The Special Events Program (SEP) manages the adjudication of submitted events, and provides a weekly report summarizing adjudicated events. The SEP has a full time program analyst responsible for event database management.

Countering Weapons of Mass Destruction Office

Performance Measure	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
Program	Chemical and Biological Readiness
Description	This measure calculates the time in hours between a BioWatch Actionable Result (BAR) Declaration and the BioWatch National Conference Call (BWNCC) with federal, state, and local partners. A BAR is declared when positive laboratory test results detects a biological agent present within a geographical area or within an indoor facility. The BioWatch National Conference Call is a formal procedure initiated by DHS to notify federal, state, and local resources. During an incident where a BAR is declared, the correlation between the time it takes to inform and coordinate between federal, state, and local jurisdictional resources will impact the number of lives to be saved by the coordinated response. In most cases, the highest effect would be detecting and locating hostile use of chemical, biological, radiological, or nuclear materials.
Scope of Data	Any incident that is formally defined as a BioWatch Actionable Result (BAR) Declaration that is documented by the completion of the BAR Declaration Form is included in this measure.
Data Source	The data source is the National Conference Call Initiation spreadsheet and the original BAR Data Forms. Both of these forms are maintained by the OHA Desk at the DHS National Operations Center.
Data Collection Methodology	The BioWatch Program Office issues guidance to each of the BioWatch jurisdictions with outlined expectations and requirements for activities to determine if a BAR has been detected. To make this determination, the lab must run collected samples from BioWatch collectors in indoor and outdoor field locations through two verification panels and a positive result occur on both tests. A BAR is declared after the jurisdictional laboratory director (or designee) determines that the results are valid and not the results of artifact or contamination and meet the predetermined algorithm constituting a positive result. Laboratory Directors have the option to hold a conference call with OHA and CDC to review the molecular biology results prior to making a BAR declaration. If the decision is to move forward with the findings, the Lab Director initiates the formal BAR Declaration process by completing and distributing the BAR Data Form to the OHA desk at the DHS National Operations Center.
Reliability Index	Reliable
Explanation of Data Reliability Check	The Program Manager will double check the validity of the summary results recorded on the National Conference Call Initiation spreadsheet against the original BAR Declaration Forms to confirm that the calculations are accurate

Performance Measure	Number of people covered by Securing the Cities program preventive radiological and nuclear (rad/nuc) detection capabilities (in millions)
Program	Securing the Cities
Description	The Securing The Cities (STC) program provides financial assistance to state, local, and tribal organizations to develop a robust regional radiological/nuclear detection program. For the STC program to count the population as covered by a robust radiological/nuclear detection capability, the region must demonstrate that 10% or more of its standing law enforcement are trained and equipped to conduct primary screening and patrolling as part of their daily routine duties and there are equipped and trained personnel to conduct secondary screening and alarm adjudication. In addition, the region must conduct at least one multi-jurisdictional exercise a year, and allow the exchange of information among regional partners and with federal agencies, and mutually assist each other in performing the radiological/nuclear detection mission. If the measure is met, the entire population from the statistical area is counted as covered.
Scope of Data	The measure includes data for the rad/nuc detection capability coverage within STC regions and the population data (Resident Population) for the applicable regions. The population data range is calculated using the U.S. Census Bureau Population of Combined Statistical Areas in the United States and Puerto Rico 2010 (as defined in February 2013). Census numbers are rounded to the nearest 500,000. The rad/nuc detection capability coverage within STC regions will calculate the percentage of standing law enforcement trained and equipped to conduct primary screening and patrolling as part of their daily routine duties and personnel trained and equipped to conduct secondary screening and alarm adjudication.
Data Source	Data for this measure are collected from the STC program, and population data will be sourced from the U.S. Census Bureau information from the 2010 census (Resident Population) which provides the Population of Combined Statistical Areas. The measure includes all communities and capabilities within the supported STC-eligible highest-risk metropolitan regions that exist to protect the population of the United States against the possession, transportation, or use of nuclear or other radioactive material outside of regulatory control.
Data Collection Methodology	Quarterly reports required of the STC grant recipients provide the operational, deployed capabilities, indicating the coverage of rad/nuc detection capabilities. Additionally, regional Multi-Year Training and Exercise Programs validate the status of readiness to include information exchange and regional coordination between State, local, county, tribal, and Federal agencies. The program threshold of 10% or greater of law enforcement personnel trained and equipped to cover the population provides the minimum detection architecture when deployed in 24 hour “steady state” operations creating a random, overlapping, mobile detection network. Achievement of the 10% training criterion is determined by reviewing the training numbers included in the quarterly reporting by the recipient. Population data are based on the U.S. Census Bureau 2010 census data (Resident Population). Census numbers are rounded to the nearest 500,000.
Reliability Index	Reliable
Explanation of Data Reliability Check	Programmatic completion with the quarterly reporting mechanisms; major training and exercise performance outlined within the program to validate the overall capability readiness; and long-term sustainment plans to maintain the program's capabilities are the key indicators of the population's security against nuclear or other radioactive material outside of regulatory control.

Performance Measure	Percent of cargo conveyances that pass through radiation portal monitors upon entering the nation via land border and international rail ports of entry
Program	Large Scale Detection Systems
Description	This measure gauges the proportion of cargo scanned by radiation detection equipment deployed to the Nation's land border crossing ports of entry and international rail ports of entry. It is expressed in terms of the percent of cargo conveyances scanned by radiation portal monitors (RPM) which enter the Nation through land ports of entry and by international rail. The Domestic Nuclear Detection Office (DNDO) procures and/or installs RPMs at ports of entry, and the U.S. Customs and Border Protection (CBP) conducts the cargo scanning using RPMs to prevent nuclear and other radioactive materials that are out of regulatory control from entering the country via cargo conveyances.
Scope of Data	The measure is based on the total number of cargo conveyances entering the Nation through CBP land ports of entry and railroad cars entering through international rail ports of entry. The portion of cargo conveyances that are scanned using RPMs is reported.
Data Source	This data is jointly managed, reviewed, and provided by the CBP and DNDO Radiation Detection Equipment (RDE) Integrated Product Acquisition and Deployment Directorate. Bi-weekly progress reports of completed RPM installations are provided by the installation agent, the Pacific Northwest National Laboratory (PNNL), to CBP and DNDO. Baseline land border cargo data are maintained by CBP, and baseline rail cargo data are maintained by the Department of Transportation, Bureau of Transportation Statistics, and are published in their on-line database. They maintain monthly and annual data on the amount of cargo arriving at U.S. land border and rail crossing sites. Current detector coverage is tabulated by the DNDO Product Acquisition and Deployment Directorate (PADD) on the Land Border Cargo Analysis spreadsheet.
Data Collection Methodology	Bi-weekly progress reports are provided to CBP and DNDO by PNNL and represent the number of RPM installations completed to date. DNDO calculates the percent of conveyances passing through RPMs, using baseline cargo data from 2013 and the number of deployed RPMs, to determine the percent of scanned conveyances and rail containers out of the total entering through U.S. land and rail ports of entry.
Reliability Index	Reliable
Explanation of Data Reliability Check	Portal monitor installation and system availability information is monitored and verified by CBP and DNDO, and validated by annual system recalibrations in the field. Data generated by the Department of Transportation is integrated and reviewed by DNDO PADD.

Performance Measure	Percent of containerized cargo conveyances that pass through radiation portal monitors at sea ports of entry
Program	Large Scale Detection Systems
Description	This measure gauges the amount of containerized cargo scanned by the radiation detection equipment deployed to the Nation's sea ports of entry. It is expressed in terms of the percent of containerized cargo conveyances that are scanned by radiation portal monitors (RPM) entering the nation through sea ports of entry. The Domestic Nuclear Detection Office (DNDO) procures and/or installs RPMs at sea ports of entry and the U.S. Customs and Border Protection (CBP) conducts the cargo scanning using the RPMs to prevent nuclear and other radioactive materials that are out of regulatory control from entering into the country via cargo containers at sea ports of entry.
Scope of Data	The measure is based on the total number of containerized cargo entering the Nation through CBP sea ports of entry. It identifies the portion that is scanned using RPMs. This measure does not include roll-on/ roll-off (for example, vehicles) and bulk cargo.

Data Source	Sea port cargo data for conveyances entering the U.S. is provided by CBP through their Operations Management Reporting (OMR) database. Bi-weekly reports of RPM installations are provided by the installation agent, the Pacific Northwest National Laboratory (PNNL). These reports represent the number of RPM installations completed to date. The DNDO Product Acquisition and Deployment Directorate (PADD) calculates the percent coverage from that data using the Sea Port Cargo Analysis spreadsheet.
Data Collection Methodology	Sea port cargo data for containerized cargo entering the United States is provided by CBP. Additionally, PNNL provides CBP and DNDO bi-weekly reports indicating RPM installations completed. The percent of containerized cargo passing through RPMs is calculated by DNDO, based on the number of deployed RPMs and the OMR baseline (FY 2013) containerized cargo data for sea ports. The number of containers scanned is divided by the total number of containers incoming. DNDO PADD calculates the final percent coverage from that data using the Sea Port Cargo Analysis spreadsheet.
Reliability Index	Reliable
Explanation of Data Reliability Check	Portal monitor installation and system availability information is monitored and verified by DNDO and CBP, and validated by annual system recalibrations in the field. Data generated by the Department of Transportation is integrated and reviewed by DNDO PADD.

Performance Measure	Time between laboratory receipt of BioWatch detector samples to completion of screening for known biological micro-organisms of interest (in hours)
Program	Chemical and Biological Readiness
Description	This measure reflects how quickly BioWatch laboratories are completing the screening tests of field samples from BioWatch detectors to determine if known biological microorganisms of interest are present. This screening may potentially consist of two steps. The first step is to determine if a potentially harmful biological agent exists in the sample. If a positive results is found, then the sample testing moves to the second set of panel tests to confirm the results, and is then followed by reporting by the local laboratory representative if a confirmed result is found. This measure will be determined and recorded daily at each operational laboratory. The system-wide average will be calculated to determine if degradation in the ability to generate results within the required time frame is occurring across the program. This measure gauges the ability to determine if a known biological agent of interest has been confirmed and notify the proper authorities.
Scope of Data	The scope of this measure includes all samples taken from BioWatch detectors in the field and delivered to designated BioWatch laboratories that have been authorized to support the BioWatch program. This measure includes the time to run the initial tests along with the time to run the confirmation tests for those samples where the second test was required.
Data Source	Each BioWatch laboratory captures the times to complete the initial tests and if needed the confirmation tests on a daily basis on a spreadsheet is known as the Sample Management System. The results for tests run on each sample are recorded and transmitted in the Laboratory Response Network Results Messenger system managed by the Centers for Disease Control. If a confirmation test is positive for a known biological micro-organism of interest, a BAR Data Form is produced.

Data Collection Methodology	Samples that are collected in the field and provided to authorized laboratories, who then test them for the presence of known biological micro-organisms of interest. Identification of known biological micro-organisms of interest is the laboratory process by which samples are tested for multiple pieces of DNA. The BioWatch program manages the development of the standard operating procedure and the format for the excel spreadsheet to allow the laboratories to capture time of receipt and time to run the tests for each sample as needed. The time from receipt of the sample to completion of the initial screening test, and completion of the confirmation test if needed, is recorded by lab technicians on the Sample Management System spreadsheet. Reports to calculate this measure are then run and the average time is calculated.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data reliability of the process is overseen by quality assurance staff of the BioWatch program. These individuals verify if the data provided by the BioWatch Quality Assurance program contractor complies with the standards of reporting and analysis established in their contract. Staff from the BioWatch program also perform periodic site visits to the laboratories for first-hand observation of procedures to ensure compliance with program policies, protocols, and procedures.

Customs and Border Protection

Performance Measure	Amount of smuggled outbound currency seized at the ports of entry (in millions)
Program	Trade and Travel Operations
Description	This measure provides the total dollar amount of all currency in millions seized during outbound inspection of exiting passengers and vehicles, both privately-owned and commercial.
Scope of Data	All outbound-related currency seizures are included in this measure. This covers both the southwest and northern borders and includes all modes (land, air, and sea).
Data Source	All currency seizures are entered into the Seized Assets and Case Tracking System (SEACATS), which is a subsystem of TECS, the principal system of record used by CBP. Currency seizure information is accessed in report format through the BorderStat reporting tool.
Data Collection Methodology	All CBP officers effecting outbound currency seizures enter seizure data into TECS via the SEACATS, using the proper codes to denote the seizure was made at exit during outbound operations. The SEACATS analyzes all seizure data and allows extracts of seized currency data for the different categories of currency violations such as undeclared or illicit currency, negotiable instruments (travelers checks, promissory notes, money orders) in bearer form.
Reliability Index	Reliable
Explanation of Data Reliability Check	CBP Officers enter information into TECS via SEACATS for each currency seizure performed. A first line supervisor must review the information and verify/approve it before it can be extracted and included in daily, monthly and annual reporting. A validation check is also conducted when the data is extracted from TECS and reported via BorderStat.

Performance Measure	Number of smuggled outbound weapons seized at the ports of entry
Program	Trade and Travel Operations
Description	This measure provides the total number of illegal weapons seized during outbound inspection of exiting passengers and vehicles, both privately-owned and commercial. Weapons are defined as pistols, rifle-shotgun combinations, rifles, revolvers, shotguns, disguised weapons, machine guns, submachine guns or machine pistols. Seizing weapons being smuggled for criminal purposes strengthens our border security by preventing the movement of assault weapons and ammunition.
Scope of Data	All outbound-related seizures of weapons being smuggled for criminal purposes are included in this measure. This covers both the southwest and northern borders and includes all modes of transportation (land, air, and sea). This measure excludes temporary seizures from legitimate exporters due to improper documentation or administrative errors.
Data Source	All weapons seizures are entered into the Seized Assets and Case Tracking System (SEACATS), which is a subsystem of TECS, the principal system of record used by CBP. Weapons seizure information is accessed in report format through the BorderStat reporting tool.
Data Collection Methodology	All CBP officers effecting outbound weapons seizures enter seizure data into TECS via the SEACATS subsystem. The SEACATS subsystem analyzes all seizure data and extracts weapons seized data.
Reliability Index	Reliable
Explanation of Data Reliability Check	CBP Officers enter information into TECS via SEACATS for each weapons seizure performed. A first line supervisor must review the information and approve it before it can be extracted and included in daily, monthly and annual reporting. A validation check is also conducted when the data is extracted from TECS and reported via BorderStat at CBP Office of Field Operations Headquarters.

Performance Measure	Percent of cargo by value imported to the U.S. by participants in CBP trade partnership programs
Program	Trade and Travel Operations
Description	This measure describes the percent of all cargo that is imported from CBP trade partnership programs based on the value compared to total value of all imports. Partnership programs include both Customs-Trade Partnership Against Terrorism (C-TPAT) and Importer Self Assessment (ISA). CBP works with the trade community through these voluntary public-private partnership programs, wherein some members of the trade community adopt tighter security measures throughout their international supply chain and in return are afforded benefits. A variety of trade actors are included in these partnership programs, such as importers, carriers, brokers, consolidators/third party logistic providers, Marine Port Authority and Terminal Operators, and foreign manufacturers.
Scope of Data	This measure includes all imported cargo and is a comparison of the value of cargo that is imported from trade partnership programs to the total value of all imports.
Data Source	Import data is stored in the Automated Targeting System (ATS) and the Automated Commercial Environment (ACE). Information is transmitted by the relevant broker under a unique entry number including individual lines with a Harmonized Tariff Schedule of the US number and line value.
Data Collection Methodology	Importers, or brokers acting on their behalf, submit data electronically, which is captured by ATS and ACE Automated Commercial System (ACS). The Office of International Trade (OT) pulls this data from their systems of record (ATS and ACE) once a month. After the line value data is extracted, the measure is calculated by dividing the import value associated with ISA or C-TPAT importers by the total value of all imports.
Reliability Index	Reliable

Explanation of Data Reliability Check	Monthly internal monitoring of process and data quality issues is conducted at both the field level and HQ level. As part of our analytical process, the data used for this measure is compared to other known reliable data sets and measures in ACE Reports and the Trend Analysis and Analytical Selectivity Program.

Performance Measure	Percent of detected conventional aircraft incursions resolved along all borders of the United States
Program	Border Security Operations
Description	The measure represents the percent of conventional aircraft detected visually or by sensor technology, suspected of illegal cross border activity, which are brought to a successful resolution. Resolution of the incursion is accomplished by the Air and Marine Operations Center (AMOC) working with federal, state, and local partners. The incursion is considered resolved when one of the following has occurred: 1) law enforcement action has been taken for criminal violations; 2) appropriate regulatory or administrative action has been taken for non-criminal violations; or 3) the aircraft did not land or otherwise display unlawful conduct while in the United States, was continuously visually or electronically monitored while over the United States, and has exited U.S. airspace and no longer a threat to national security.
Scope of Data	The scope of this measure includes all airspace incursions by conventional aircraft along all borders of the United States. The scope of data excludes reporting of unconventional aircraft, such as ultra-light aircraft or small unmanned aircraft systems.
Data Source	Data is stored in the Tasking Operations Management Information System (TOMIS) and the CBP Border Enforcement Management System (BEMS) Data Warehouse.
Data Collection Methodology	Airspace incursions are identified by the Air and Marine Operations Center (AMOC). After an incursion is established, this information is transmitted to the appropriate air branch for air response. The results are then entered into and tracked in the Air and Marine Operations system of record, and summarized on a monthly basis. In calculating the incursion percentage, the total number of resolved incursions represents the numerator, while the total number of detected incursions represents the denominator.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data is routinely reconciled by a comparison of information in the systems manually by contractor and program staff on a monthly and/or quarterly basis.

Performance Measure	Percent of import revenue successfully collected
Program	Trade and Travel Operations
Description	This measure estimates the collected duties, taxes, and fees (called net undercollection of revenue) expressed as a percent of all collectable revenue due from commercial imports to the United States directed by trade laws, regulations, and agreements. The total collectable revenue is total collected revenue plus the estimated net undercollected revenue based on trade violations. The revenue gap is a calculation of uncollected duties (the difference between estimated undercollection and overpayment) based on statistical sampling.
Scope of Data	This measure is part of the annual Trade Compliance Measurement (TCM) program. The program involves taking a statistical sample (about 65,000 import entry lines) from a given population of imports. This population covers consumption and Anti-Dumping/Countervailing Duty (AD/CVD) entry types, excluding informal entries (value <$2k). This data will be produced monthly, aggregated year-to-date, and then presented as an annual figure.
Data Source	The targeting feature of the program resides in the Automated Targeting System (ATS) with User Defined Rules (UDR) and the review findings are recorded in the Automated Commercial Environment (ACE) using the Validation Activity (VA) functionality.

Data Collection Methodology	At the start of each fiscal year, an analysis of import data is conducted to help design a statistical survey program, which is implemented with UDRs in the ATS. Entry Summary line transactions are identified by ATS, which opens a VA in ACE. Each Field Office must review the identified entry summary line transaction for compliance and record the findings with a Validation Activity Determination (VAD). VAD data is extracted monthly by HQ analysts and statistics are compiled monthly and annually by the resident statistician within the Trade Analysis and Measures Division.
Reliability Index	Reliable
Explanation of Data Reliability Check	Processes and data quality are monitored monthly at both the field and HQ levels. This responsibility is shared between HQ and field locations, where multiple levels of checks are conducted, and any found problems are quickly addressed. HQ also hosts quarterly conference calls with field locations to openly discuss any issues, and provides reports to field locations when remediation action is needed. This oversight is documented and provided as evidence of program control to outside independent auditors each year.

Performance Measure	Percent of imports compliant with U.S. trade laws
Program	Trade and Travel Operations
Description	This measure reports the percent of imports that are compliant with U.S. trade laws including customs revenue laws. Ensuring that all imports are compliant and free of major discrepancies allows for lawful trade into the U.S.
Scope of Data	The measure is part of the annual Trade Compliance Measurement (TCM) program. The program involves taking a statistical sample (about 65,000 import entry lines) from a given population of imports. This Major Transactional Discrepancy compliance rate (MTD) measure covers the population consumption and Anti-dumping and Countervailing Duty entry types, excluding informal entries. Recorded discrepancies are considered to be significant or major if they reach certain thresholds, such as: the value of imports, amount of revenue loss, etc. Examples of these thresholds include: a discrepancy in value with a revenue loss greater than $1,000, a clerical error that results in a revenue loss greater than $1,000, an IPR violation, and a country of origin discrepancy with value greater than 33rd percentile or revenue loss greater than $1,000.
Data Source	Data resides in the Automated Targeting System (ATS) with User Defined Rules (UDR) and the review findings are recorded in the Automated Commercial Environment (ACE) using the Validation Activity (VA) functionality.
Data Collection Methodology	At the start of each fiscal year, based on previous year imports, risk, volume, value, and compliance history, a stratified random sampling methodology is used to select import entry summary lines, which is implemented with UDRs in the ATS. Entry Summary line transactions are identified by ATS, which opens a VA in ACE. Each Field Office must review the identified entry summary line transaction for compliance and record the findings with a Validation Activity Determination (VAD). VAD data is extracted monthly by HQ analysts and statistics are compiled monthly and annually by the resident statistician within the Trade Analysis and Measures Division.
Reliability Index	Reliable
Explanation of Data Reliability Check	Monthly internal monitoring of process and data quality issues are conducted at both the field level and HQ level. This is treated as a shared responsibility of both HQ and field locations, where multiple levels of checks are conducted, and any found problems are quickly addressed. HQ also hosts quarterly conference calls with field locations to openly discuss these issues, and provides reports to field locations when remediation action is needed. This oversight is documented and provided as evidence of program control to outside independent auditors each year.

Performance Measure	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
Program	Trade and Travel Operations
Description	This measure gauges the percent of international cargo coming to the United States via air, land, and sea identified as potentially high-risk using the Automated Targeting System (ATS) that is assessed or scanned prior to lading or at arrival at a U.S. port of entry. Assessing, resolving, and when necessary scanning potentially high-risk cargo prior to lading or at arrival at the ports of entry ensures the safety of the U.S. public and minimizes the impact to the trade through the effective use of risk-focused targeting.
Scope of Data	This measure includes cargo in the land, sea, and air environments destined for a U.S. port of entry. Cargo is identified as potentially high-risk by CBP's Automated Targeting System (ATS) using a risk-focused security index scoring algorithm. Shipments are flagged as potentially high-risk if they have an ATS security index score of 190 or above on either bill or entry. The National Targeting Center - Cargo works with the Targeting and Analysis Systems Program Office (TASPO), Office of Information Technology to determine the final status of all identified potentially high-risk cargo.
Data Source	CBP's Automated Targeting System (ATS) contains the requisite data to determine the total amount of cargo that was scored 190 or above by either bill or entry.
Data Collection Methodology	Electronic manifest data is provided to CBP by shippers and brokers and loaded into CBP's ATS database. The ATS screening algorithms are applied to this data and the results are provided electronically to the Cargo Enforcement Reporting and Tracking System (CERTS), including entry status data for all modes of cargo identified as high-risk. Based on this information, the percent of cargo reviewed, scanned, and resolved is calculated by taking all cargo shipments with a score of 190 or above that have been reviewed/examined/mitigated (determined from CERTS) and dividing this by the total number of cargo shipments with a score of 190 or above.
Reliability Index	Reliable
Explanation of Data Reliability Check	CBP Officers review and examine the ATS information on potentially high-risk cargo, resolve or mitigate security concerns, determine those cases where further examination is required, and record the findings of this review/examination process in the ATS 4 CERTS module, annotating all methods and tools they required to complete the examination. For land border ports of entry, they also enter findings into the ACE system, which is mandatory for land ports to allow the truck and cargo to be released from CBP. Supervisors periodically extract high threat examination findings data from the CERTS module for review and validation of the data entered by CBP Officers. Anomalies in the findings data are identified and immediate corrective actions are taken to ensure data integrity.

Performance Measure	Percent of people apprehended multiple times along the Southwest border
Program	Border Security Operations
Description	This measure examines the percent of deportable individuals who have been apprehended multiple times by the U.S. Border Patrol. This measure identifies the percentage of people apprehended multiple times along the Southwest border over the previous twelve months. Effective and efficient application of consequences for illegal border crossers should, over time, reduce overall recidivism.
Scope of Data	Apprehensions of deportable illegal aliens that have or receive a Fingerprint Identification Number (FIN), who are apprehended multiple times within the previous twelve months are used in calculating this measure. The apprehensions occur within the nine sectors of the Southwest Border. Fingerprints are not taken and FINs are not generated for individuals under age 14, over age 86, and some humanitarian cases are not included in calculating the percentage of people apprehended multiple times along the Southwest border.

Data Source	Apprehension data is entered into the e3 Processing system by Border Patrol Agents at the Station level. Data input can be made by any agent who knows the details of the apprehension. The e3 system continuously updates the Enforcement Integrated Database (EID), with the apprehension information. All data entered in the e3 system resides in the EID, the official system of record for this data, which is under the purview of the Border Patrol Headquarters Statistics and Data Integrity unit. The physical database is owned and maintained by Immigrations and Customs Enforcement's (ICE) Office of Chief Information Officer (OCIO).
Data Collection Methodology	Apprehension data is entered into the e3 system by Border Patrol Agents at the Station level. Data input can be made by any agent who knows the details of the apprehension. The e3 system continuously updates the EID with the apprehension data. This data can be reviewed at the station, sector or Headquarters level in a variety of reporting formats. Calculation of this measure is as follows: The number of individuals that have been apprehended multiple times, divided by the total number of individuals apprehended during the same time period and geographic parameter.
Reliability Index	Reliable
Explanation of Data Reliability Check	All apprehension data entered into e3 Processing is subject to review by supervisors at multiple levels. Data reliability tools are built into the system; for example, data input not conforming to appropriate expectations is reviewed for accuracy and flagged for re-entry. The EID continuously updates to compile all apprehension data. This data can then be extracted into summary reports, and these summaries are available for review and analysis at station, sector, and Headquarters levels. At the Headquarters level, the Statistics and Data Integrity Unit conducts monthly Data Quality reports as well as weekly miscellaneous checks. When discrepancies are found, they are referred back to the apprehending Sector/Station for review and correction.

Performance Measure	Percent of recurring border surveillance implemented in remote low risk areas between ports of entry
Program	Border Security Operations
Description	This measure represents the percentage of remote low risk areas along the land border that are covered by recurring surveillance that can detect possible illicit activity. Low risk areas are geographically remote parts of the border that also have historically had low levels of illegal activity. Recurring surveillance is achieved through geospatial capabilities that monitor these areas for potential illicit activity and provide information to CBP Office of Intelligence analysts who review the information and determine if a response is needed. The measure demonstrates the Border Patrol's ability to maintain awareness of illicit activity without needing to have agents directly located in these remote areas.
Scope of Data	This measure includes the entire southern and northern land borders (excluding Alaska) that have been determined by CBP's U.S. Border Patrol Sector Chiefs to be low flow/low risk areas. Each Sector Chief can change the designation for any mile within their area of responsibility. A "covered border mile" is defined as one mile of the border where CBP has the capability of deploying geospatial intelligence (GEOINT) capabilities if intelligence reports or risk analyses require GEOINT surveillance. This measure does not include the maritime domain.
Data Source	The data will be collected by CBP Office of Intelligence in the National Technical Collections Branch. The data is based on measurements from maps. The miles covered and required to be covered are currently stored in the CBP Shared Server. That data is reported to U.S. Border Patrol enterprise Geospatial Information Services office for reporting.

Data Collection Methodology	As U.S. Border Patrol (USBP) coverage capability increases, USBP changes the designation of border miles from "proposed GEOINT collection area" to "active GEOINT collection area." Sector Chiefs report which miles of the border are low risk to CBP's Office of Intelligence (OI), who then works to deploy GEOINT capabilities in those areas. CBP OI maintains an excel spreadsheet in OI's National Technical Collections Branch (NTCB) by a Collections Manager, which is updated as OI adds designated miles of the border that are covered by GEOINT capabilities. The NTCB Branch Chief reviews the spreadsheet for accuracy. After approval the spreadsheet is saved to the CBP Shared Server. The NTCB Collections Manager then emails the new miles to a Geospatial Information Services (GIS) analyst who updates the GIS map. The Branch Chief of the NTCB uses these maps in their monthly report to the Border Patrol Chief. The USBP liaison will report this information quarterly.
Reliability Index	Reliable
Explanation of Data Reliability Check	A Collections Manager inputs the data, which is reviewed for accuracy by the Branch Chief.

Performance Measure	Percent of time the U.S. Border Patrol meets its goal of responding to potential illegal activity in remote, low-risk areas
Program	Border Security Operations
Description	In order to ensure an effective response, the U.S. Border Patrol (USBP) aims to respond to potentially illicit activity in remote low risk areas within 24 hours. This measure gauges U.S. Border Patrol's ability to meet that goal and ensure potential illegal activity is responded to and properly assessed
Scope of Data	This measure encompasses all geospatial intelligence-informed reports of potential illicit activity in remote low risk areas. This measure includes all miles of the southern and northern land border (excluding Alaska) that have been determined by each USBP sector to be low flow and low risk areas. This measure does not include the maritime domain. A response is defined as when a USBP sector receives an e-mail notification from an analyst and deploys USBP Agents to investigate the detected activity.
Data Source	The data source is mined from e-mail notifications and individual Field Information Reports (FIR) which are stored in CBP Intelligence Reporting System – Next Generation (IRS-NG) and maintained by CBP Office of Information Technology.
Data Collection Methodology	When the collection platform detects potential illicit activity the Office of Intelligence sends an e-mail notification to the appropriate USBP Sector. The Sector then deploys Border Patrol Agents to respond. The clock officially starts on the response when the e-mail notification is sent and is recorded by the responding sector. The arrival time of the Agents at the coordinates provided in the notification is recorded as the response time in the FIRSs. The measure will be reported quarterly by USBP Sectors to USBP Headquarters.
Reliability Index	Reliable
Explanation of Data Reliability Check	The responding Agent drafts the Field Information Reports (FIR), which is then reviewed by a supervisor. The Patrol Agent In Charge must review and give final approval on all FIRs submitted. All FIRs must be submitted within 72 hours of notification.

Performance Measure	Rate of interdiction effectiveness along the Southwest Border between ports of entry
Program	Border Security Operations
Description	This measure reports the percent of detected illegal entrants who were apprehended or turned back after illegally entering the United States between the ports of entry on the Southwest border. The Border Patrol achieves this desired strategic outcome by maximizing the apprehension of detected illegal entrants or, confirming that illegal entrants return to the country from which they entered; and by minimizing the number of persons who evade apprehension and can no longer be pursued.
Scope of Data	The scope includes all areas of the Southwest border that are generally at or below the northern most checkpoint within a given area of responsibility, and applies the following data filters: In Border Zones: Includes all Apprehensions, Got Aways (GA), and Turn Backs (TB). In Non-Border Zones: Includes apprehended subjects who have been identified as being in the US illegally for 30 days or less, does not include GA and TB. Definitions: Apprehension: A deportable subject who, after making an illegal entry, is taken into custody and receives a consequence. Gotaway: A subject who, after making an illegal entry, is not turned back or apprehended and is no longer being actively pursued by Border Patrol agents. Turn Back: A subject who, after making an illegal entry into the US, returns to the country from which he/she entered, not resulting in an apprehension or GA.
Data Source	Apprehension, gotaway, and turnback data is captured by Border Patrol agents at the station level into the following systems. Apprehensions are entered into the e3 Processing (e3) system. All data entered via e3 resides in the Enforcement Integrated Database (EID), the official system of record for this data, which is under the purview of the Border Patrol Headquarters Statistics and Data Integrity (SDI) Unit. The physical database is owned and maintained by Immigrations and Customs Enforcement (ICE). Gotaways and Turnbacks are entered into the CBP Enforcement Tracking System 1 (BPETS1), which resides with Office of Border Patrol. BPETS1 is under the purview of and is owned by the Enforcement Systems Unit.
Data Collection Methodology	Apprehension data is entered into e3 by Border Patrol agents (BPAs) at the station level as part of the standardized processing procedure. BPAs use standard definitions for determining when to report a subject as a GA or TB. Some subjects can be observed directly as evading apprehension or turning back; others are acknowledged as GAs or TBs after BPAs follow evidence that indicate entries have occurred, such as foot sign, sensor activations, interviews with apprehended subjects, camera views, communication between and among stations and sectors, and other information. Data input into the BPETS1 system occurs at the station level. The e3 Processing application and BPETS1 are used continuously to document apprehension, GA, and TB data. Calculation of the measure is done by the HQ SDI Unit and is: (Apprehensions + TB)/Total Entries. Total entries is the sum of Apprehensions, TBs, and GAs.
Reliability Index	Reliable
Explanation of Data Reliability Check	Patrol Agents in Charge ensure all agents are aware of and utilize proper definitions for apprehensions, GAs and TBs at their respective stations. They also ensure the necessary communication takes place between and among sectors and stations to ensure accurate documentation of subjects who may have crossed more than one station's area of responsibility. In addition to station level safeguards, the HQ Statistics and Data Integrity (SDI) Unit validates data integrity by utilizing various data quality reports. Data issues are corrected at the headquarters level, or forwarded to the original inputting station for correction. All statistical information requested from within DHS, USBP, or external sources are routed through the centralized HQ office within USBP. The SDI Unit coordinates with these entities to ensure accurate data analysis and output.

Federal Emergency Management Agency

Performance Measure	Benefit to cost ratio of the Hazard Mitigation Grants
Program	Grants
Description	This measure reports the estimated annual benefit to cost ratio of grants provided by the FEMA Hazard Mitigation Assistance program to lessen the impact of disasters. A value greater than one indicates more benefit was reaped than cost expended. The program works with state, tribal, territorial, and local (STTL) governments engage in hazard mitigation planning to identify natural hazards that impact them, identify strategies and activities to reduce any losses from those hazards, and establish a coordinated approach to implementing the plan. These plans are the basis for STTL grant requests. Once grants are provided, program staff evaluate the benefit to cost ratio of the implementation of the plan to ensure that taxpayer dollars are spent effectively.
Scope of Data	The scope of this measure includes all grants on an annual basis provided by the FEMA HMA program.
Data Source	The systems primarily used for the data collection includes FEMA's Enterprise Data Warehouse (EDW) which consolidates data from Hazard Mitigation Grant Program - National Emergency Management Information System (HMGP-NEMIS) and Mitigation Electronic Grants Management System (MT- eGrants) systems. Data is collected and consolidated into an Excel spreadsheet where the calculations for aggregate BCR will be performed.
Data Collection Methodology	The total project cost and the benefits are calculated by the applicant for each of the projects. The estimated benefits are derived based on benefit-cost analysis methodologies developed by FEMA and has been in use for the past 10 years. To determine the cost effectiveness of a HMA project, FEMA utilizes a BCR, which is derived from the project's total net benefits divided by its total project cost. Each sub-grant obligation and total project cost is captured in the HMGP-NEMIS or MT-eGrants system by FEMA HMA staff. Quarterly reports will be generated utilizing FEMA's EDW which will be utilized for the data reporting.
Reliability Index	Reliable
Explanation of Data Reliability Check	Each sub-grant obligation and total project cost is captured in the HMGP-NEMIS or MT-eGrants system. This information is electronically consolidated in FEMA's Enterprise Data Warehouse (EDW). FEMA HMA staff download relevant data from the EDW, and after making the calculations for an aggregate BCR generate Quarterly excel based reports. These calculations go through a series of staff reviews before being reported on FEMA's performance system of record – the Performance Hub.

Performance Measure	Operational readiness rating of FEMA's specialized incident workforce cadres
Program	Response and Recovery
Description	This measure gauges the overall readiness of 23 cadres in the Incident Management Workforce (IMW) by examining staffing, training, and equipping variables of qualified personnel. The IMW are the primary first responders that provide services to disaster survivors immediately after an event and support Response and Recovery operations. The ability to gauge readiness provides key information for ensuring that qualified and equipped personnel are available to respond to a disaster examining the below variables: 1. Staffing Category Variable: % of Force Structure currently on board; % of force strength available; % of force strength deployed 2. Training Category Variable: % of force strength qualified; % of qualified personnel currently available; % of all trainees who have completed their qualification sheets but still need to demonstrate performance. 3. 3. Equipping Category Variable: Percent of Reservists 1-1-1* ready * The Reservist has a laptop, RSA token, and a phone

Scope of Data	The results are based on all available data and not a sample of data. The data included in this performance measure are an aggregate of measures of staffing, training, and equipping readiness categories.
Data Source	The data source is the Cadre Operational Readiness and Deployability Status (CORDS) Report that measures the overall readiness of the incident management workforce for all 23 cadres. The Response Directorate's Incident Management Workforce Division (IWMD) pulls this data bi-weekly from the Deployment Tracking System.
Data Collection Methodology	IWMD pulls data from the Deployment Tracking System. The CORDS report algorithm measures 3 readiness categories and assigns an overall Cadre Readiness metric called its Deployability Rating (D-Rating of 1-5) to each cadre and the organization as a whole. The D-Rating applies a weight to each individual factor used to determine the final score: 50% Staffing, 35% Training, 15% Equipping. This weighting recognizes staffing as the critical element of an expeditionary workforce. Training and Equipping are instrumental to success and efficiency, but in an emergency, having people on-hand and available is most important. The formula for measuring the D-Rating is: [(Force Strength * .5) + (Availability of Force Strength * .15) + (Inverse of Deployed * .35)] *.5 = Staffing [(Qualified &Available * .35) + (Trainees with Academics Complete * .15) + (Qualified Force Strength * .5)] * .35 = Training (Equipment Ready * .15) = Equipping Staffing + Training + Equipping = Weighted Average
Reliability Index	Reliable
Explanation of Data Reliability Check	IWMD conducts quality assurance/quality management reviews of DTS data to ensure the system accurately reflects deployment and qualifications related data reflected in the system is accurate. If deployment or qualifications data is incorrect, IWMD works with the Cadre or Program Office to change the data based upon internal data management processes. Once verified, reliable data will be made in the system immediately.

Performance Measure	Percent of adults that took a preparedness action at their workplace, school, home or other community location in the past year
Program	Preparedness and Protection
Description	This measure represents the percent of adults responding to a survey who took a preparedness action at their workplace, school, home, or community, including drills. Improving the public's knowledge and ability to take effective protective actions for hazards is a key objective of preparing the public. Research indicates that drills and exercises are an effective method for increasing both knowledge and the ability to act quickly and effectively in emergency situations. Research indicates that, in addition to preparing those that are direct participants, drills and exercises provide a visible action that promotes discussion and motivates others to take action.
Scope of Data	As part of the national survey, a total of about 5,000 or more telephone interviews are conducted yearly on individual and household preparedness. The survey contacts individuals throughout the United States. Results include adults who answer in the affirmative that they have taken any preparedness actions, which include seeking information on preparing for disasters, talking with others in the community about preparedness, attending a preparedness meeting/training, practicing a drill/exercise, developing a household emergency plan, or storing supplies specifically for a disaster in their workplace, school, home or another community location in the past year.
Data Source	The data source for this measure is the Computer Assisted Telephone Interviewing (CATI) system.

Data Collection Methodology	The measure calculates the percent of adults surveyed via landline or cellular phone who responded affirmatively to the question regarding whether they have taken any preparedness actions. Survey data is collected using a Computer Assisted Telephone Interviewing (CATI) system and results from the survey are analyzed in SPSS and SAS. When processing the data from the random digit dialing surveys, results are weighted to correct for unequal probabilities of selection. The sample data are also post-stratified according to geography, age, gender, and race to account for potential biases such as over- and under-representation of certain population segments. This will adjust the sample's demographic distributions to match the distribution derived from the latest available Current Population Survey estimates.
Reliability Index	Reliable
Explanation of Data Reliability Check	There is currently no way to independently verify the accuracy of participants' responses or the responses recorded by survey administrator. But, each programmed survey instrument goes through a rigorous quality control process. When the instrument is in the field, this rigorous quality assurance process continues. The overall process includes, but is not limited to, program testing, a pre-test and cognitive testing to determine the effectiveness of the survey and questions, monitoring of in-progress calls, recording of all interviews, and the production of tabulations of every question and variables to detect any missing data or errors. Additional quality measures include the checking of survey skip patterns and data accuracy and consistency checks.

Performance Measure	Percent of communities in high earthquake, flood, and wind-prone areas adopting disaster-resistant building codes
Program	Mitigation
Description	This measure assesses the number of communities adopting building codes containing provisions that adequately address earthquake, flood, and wind hazards. FEMA works with code adoption and enforcement organizations to support community implementation of disaster resistant building codes, defined as being in compliance with the National Flood Insurance Program regulations, equivalent to the National Earthquake Hazards Reduction Program recommended provisions, and in compliance with the provisions of the International Codes as designated by the International Codes Council. FEMA also works with the Insurance Services Office (ISO) Building Code Effectiveness Grading Schedule (BCEGS) data to track the number of high-risk communities subject to flood, wind, earthquake, and combined perils that have adopted disaster resistant building codes over time.
Scope of Data	The scope of this measure includes all communities in high earthquake, flood, and wind-prone areas as determined by ISO through their BCEGS database.
Data Source	The source of data for this measure is ISO's BCEGS database which tracks the number of communities subject to flood, wind, earthquake, and combined perils and those communities that have adopted disaster-resistant building codes. ISO provides data on building codes adopted by participating jurisdictions from the BCEGS questionnaire. The BCEGS data includes building code data from 44 of the 50 states. The six states not included are Kansas and the five Bureau states (Hawaii, Idaho, Louisiana, Mississippi, and Washington).The BCEGS database is updated daily to include the latest surveys taken. ISO surveys each participating jurisdiction every 5 years.
Data Collection Methodology	The Mitigation program receives data from ISO through their BCEGS database which provides the number of communities subject to flood, wind, earthquake, and combined perils and those communities that have adopted disaster-resistant building codes. This data is used to calculate the percent of communities in high earthquake, flood, and wind-prone areas adopting disaster-resistant building codes.
Reliability Index	Reliable

Explanation of Data Reliability Check	FEMA relies on ISO to manage the completeness and reliability of the data provided thought their BCEGS database to the program; however, the data are reviewed by FEMA's Mitigation program to ensure results are consistent over time. If significant fluctuations in quarterly and annual results occur, the program will work with ISO to address issues with data reliability.

Performance Measure	Percent of federal agencies ready to initialize continuity of essential functions and services in the event of a catastrophic disaster
Program	Preparedness and Protection
Description	This measure assesses the percent of federal agencies ready to respond immediately to a continuity of operations event. This measure encompasses Category I through IV Federal agencies that respond to Department and Agency (D/A) monthly notification tests and real-world incidents within four hours.
Scope of Data	The scope of this measure includes Category I, II, III, IV Departments and Agencies (D/As), as defined by HSPD-20/NSPD-51.
Data Source	The D/As determine which individuals and entities (i.e. Emergency Operations Centers) within their agency will receive the alert and provide their contact information to the National Continuity Programs Directorate (NCP). NCP maintains a hard copy roster in Microsoft Word that contains the contact data; NCP uses this roster to update the FEMA Emergency Notification System (ENS) and verify test results and D/A contact information. The ENS stores the D/A contact data within its database and uses that contact data to conduct drills and real world notifications. The ENS compiles notification results.
Data Collection Methodology	The FEMA ENS stores the D/A contact data within its database and uses that contact data to notify Category I through IV agencies during drills and real world notifications. The system tracks whether each D/A was successfully contacted and whether the notification was acknowledged. NCP receives this information from the system in a Qualifications and Exception report. NCP reviews the report and compares it to the D/A roster that NCP maintains to determine the percent of Category I through IV D/As that were successfully notified.
Reliability Index	Reliable
Explanation of Data Reliability Check	NCP reviews each ENS Qualification and Exception report to determine which agencies were successfully notified and acknowledged alert receipt. On a quarterly basis, NCP asks all Federal executive branch D/As to review their listed points-of-contact and contact information and update, if needed. On a quarterly basis, NCP briefs the results of tests and real world events to the Continuity Advisory Group, an Assistant Secretary-level forum attended by the National Security Council Staff, to inform leadership on results.

Performance Measure	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
Program	Response and Recovery
Description	This measure reflects FEMA's role in effectively responding to any threat or hazard, with an emphasis on saving and sustaining lives within 72 hours, in support of state, local, tribal, and territorial governments. "Actions necessary to stabilize an incident" are defined as those functions that must be initiated immediately following an incident in order to ensure the best outcomes for survivors. These actions include establishing joint federal/state incident objectives and interoperable communications between FEMA-supported incident sites, deploying urban search and rescue resources, rapidly activating response coordination centers, and issuing timely alerts, warnings, operations orders, and situation reports.

Scope of Data	The scope of this measure includes all incidents—defined as all significant events, exercises, or activities—that require execution of the critical response functions. These functions must be performed within established timeframes and include: (1) Incident Management Assistance Teams (IMATs) establishing joint federal/state incident objectives; (2) disaster communication capabilities linking FEMA-supported incident sites; (3) national Urban Search and Rescue (US&R) resources arriving on-scene; (4) response coordination centers activating to directed levels; (5) watch centers transmitting operations orders and situation reports; and (6) the FEMA Operations Center issuing alerts, warnings, and notifications.
Data Source	National and Regional IMAT deployment data are submitted to the National Watch Center (NWC), which provides it to the Field Operations Support Branch for management and tracking. The Disaster Emergency Communications Division manages a database of Mobile Emergency Response Support-related deployment and response data. FEMA's US&R Branch manages deployment and response data associated with the National US&R Response System. National US&R statuses are updated every two hours during deployment, which is captured through National Response Coordination Center (NRCC) and NWC reporting and is tracked by the US&R Branch. Situation reports and operations orders are tracked by both the National and Regionals watch centers, electronically and on paper. NRCC and Regional Response Coordination Centers (RRCC) data are tracked through the manual comparison of operations orders and NRCC/RRCC activation logs. FEMA Operations Center data are managed and tracked through the Emergency Notification System.
Data Collection Methodology	For each quarter, FEMA tracks when an incident requires one or more of the six activities described above and whether or not the activity is accomplished in the time required. Each activity is scored quarterly based on percent of times completed within required timeframe (i.e. if the NRCC is activated 5 times in one quarter and activates to the directed level 4 of those times, the activity is scored as 80%). These six activity-level scores are then equally averaged for a total composite score each quarter.
Reliability Index	Reliable
Explanation of Data Reliability Check	Each supporting activity mentioned above is responsible for reporting on the timeliness of the response for each incident requiring FEMA assistance. For each incident a score is determined based on the data collection methodology. Each quarter the sum of these scores is additive and divided by the number of incidents occurring during the quarter, resulting in an equally weighted average.

Performance Measure	Percent of Incident Management Assistance Teams establishing joint federal and state response objectives within 18 hours
Program	Response and Recovery
Description	This measure gauges the percent of time that Incident Management Assistance Teams (IMATs) have deployed and have established initial joint federal and state response objectives within 18 hours of a request from a state or jurisdiction. IMATs rapidly deploy to an incident, provide leadership for federal assistance, and coordinate and integrate inter-jurisdictional response in support of an affected state or territory.
Scope of Data	FEMA is responsible for three National and thirteen Regional Incident Management Assistance Teams (IMATs). The scope of this measure includes all significant activities or events that require the deployment of one or more IMATs. This measure is restricted to IMATs that are deployed within the continental United States.
Data Source	IMAT notification and arrival times are tracked by the National Watch Center (NWC) and the National Response Coordination Center (NRCC). The NWC maintains this information on a shared drive.

Data Collection Methodology	The teams are notified of deployment and FEMA's NWC documents the notification. Once the team arrives on scene, the team chief contacts the NRCC to update their status in the NWC shared drive. This tool is used during declared disasters and for other emergency incidents or exercises. FEMAs Response staff at HQ extract data from the database related to on-scene arrival times of any (or all) teams deployed to one or more incidents and compares to when teams were notified of deployment for corresponding incidents. This data is analyzed by comparing team arrival times to the times teams were initially notified of deployment. The data is based on the total number of actual real-world or exercise deployments, rather than a specific number of deployments throughout the year.
Reliability Index	Reliable
Explanation of Data Reliability Check	FEMA's NWC database is used as the system of record to report and archive data for historical reference. Program personnel review the data after each deployment to ensure accuracy of data entered. Any anomalies are researched against other data records to confirm time of notification.

Performance Measure	Percent of incident management planned workforce currently on board
Program	Response and Recovery
Description	This measures tracks FEMA's progress towards achieving an optimal incident management force strength. FEMA's Incident Management Force Structure establishes the total number of personnel required, by position and employee type, for FEMA to respond to a variety of concurrent events and scenarios. It is updated every three years.
Scope of Data	The scope of this measure includes planned workforce employees within the Cadres (23 total) positions. The Cadre positions include represented are Acquisition, Alternate Dispute Resolution, Disaster Emergency Communications, Training, Disability Integration, Disaster Survivor Assistance, External Affairs, Environmental and Historic Preservation, Equal Rights, Federal Coordinating Officer, Financial Management, Hazard Mitigation, Human Resources, Individual Assistance, Information Technology, Logistics, National Disaster Recovery, Office of Chief Counsel, Operations, Public Assistance, Planning, Safety and Security.
Data Source	Data for this measure is maintained in the Deployment Tracking System.
Data Collection Methodology	This data is available at any time in the Deployment Tracking System, which is integrated with FEMA's Human Capital systems to ensure real-time tracking on employee on-boarding, promotions, organizational alignment, and separations. FEMA, in coordination with the Office of Policy & Program Analysis has developed a dashboard to assist in the assessment of the data at any given point in time.
Reliability Index	Reliable
Explanation of Data Reliability Check	The System of record for this measure (DTS) is regularly updated and monitored by the Field Operations Division, and results reviewed for quality by senior managers in the Office of Response and Recovery.

Performance Measure	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
Program	Disaster Relief Fund
Description	FEMA commits to helping survivors recover from federally declared disasters and the Office of Response and Recovery (ORR) is instrumental to fulfilling this commitment. The Individual Assistance (IA) Program is integral to improving the clarity of and access to actionable information, streamlining and simplifying processes and policies to ensure that survivors receive disaster assistance quickly and conveniently. FEMA-ORR developed the Recovery Services IA Measure to report on how well FEMA is delivering on this commitment. The Recovery Services IA Measure is a composite measure comprised of five weighted performance indicators to produce a percentage reflecting FEMA's role in delivering quality services to disaster survivors. The weighting of this composite measure is as follows: Providing temporary housing assistance–35%; Disaster Case Management–20%; Availability of Grant Management and Registration Systems–25%; Call Center Response Time–10%; and Organization Staffing–10%.
Scope of Data	Each of the three indicators reflect data collected in a fiscal year for all federally declared disasters within the fiscal year. The data are reported quarterly against an annual target and includes all data collected for the year, meaning there is no sampling done of the data.
Data Source	Several data sources provide data for this measure. Data for the number of days for the Request for Public Assistance to the kickoff meeting come from the Emergency Management Mission Integrated Environment (EMMIE). Information on EMMIE availability comes from the Office of the Chief Information Officer Operational Report and Organizational fill information comes from the Recovery Human Capital Report.
Data Collection Methodology	All data are collected, recorded, collated, and analyzed by the Recovery Performance Management Team. All data are checked for quality including completeness, potential errors, and by conducting a peer review. Once data are validated, the data are grouped into the two categories, and weighted to determine the composite score for the measure. Weighting is as follows: program services is 73 percent, and supporting infrastructure is 27 percent. Program services encompass the percent of time that kickoff meetings occur within 21 days of a request for public assistance. Supporting infrastructure encompasses the percent of time that the Public Assistance grants management system (EMMIE) is available. The organizational fill of FEMA's Public Assistance organization is determined by PFT available positions vs. PFT filled positions at Headquarters.
Reliability Index	Reliable
Explanation of Data Reliability Check	Each data source for the measure is reliable and the Recovery Reporting and Analytics Division (RRAD) implements appropriate quality controls to ensure data consistency. The data for the Housing Assistance within 60 Days component come from the NEMIS database. This data set is checked by SMEs before and after analysis. The human resources data are pulled by a human resources analyst. Before the individual sends the data for analysis, the Executive Officer of the IA Division checks to ensure correctness. A specialist from the Recovery Technology and Programs Division pulls the system uptime information and sends it to RRAD for analysis. Disaster Case Management data are collected quarterly by Community Service Program SMEs. Finally, all data are reviewed and submitted to RRAD staff and compared to previous quarter and are shared with IA leadership and program SMEs for review and concurrence before the final results are submitted to the Office of Policy and Program Analysis.

Performance Measure	Percent of recovery services through Public Assistance delivered to communities gauging the quality of program services, supporting infrastructure, and customer satisfaction following a disaster
Program	Disaster Relief Fund
Description	FEMA makes a commitment to helping communities recover from federally declared disasters and the Office of Response and Recovery (ORR) is instrumental to fulfilling this commitment. Supporting and ensuring our citizens have quality assistance after a disaster is critical to facilitating a community's recovery. The Public Assistance (PA) Program is integral to improving the clarity of and access to actionable information, streamlining and simplifying processes, and policies to ensure that survivors receive disaster assistance quickly and conveniently. ORR developed this measure to report on how well FEMA is meeting this commitment. The measure is a composite measure comprised of three weighted performance indicators to produce a percentage reflecting FEMA's role in delivering quality services to communities. The weighting is as follows: Timely Kick-Off Meetings – 41%; Availability of Grant Management – 32%; and, Organization Staffing – 27%.
Scope of Data	The scope of this measure includes all federally-declared disasters within the United States and its territories.
Data Source	Several data sources provide data for this measure. Data for the number of days for the Request for Public Assistance to the kickoff meeting come from the Emergency Management Mission Integrated Environment (EMMIE). Information on EMMIE availability comes from the Office of the Chief Information Officer Operational Report and Organizational fill information comes from the Recovery Human Capital Report.
Data Collection Methodology	All data are collected, recorded, collated, and analyzed by the Recovery Performance Management Team. Once data are validated, the data is grouped into three categories, and weighted to determine the composite score for the measure. Weighting is as follows: program services are 50 percent, supporting infrastructure is 25 percent, and customer satisfaction is 25 percent. Program services encompass the percent of time that kickoff meetings occur within 60 days of a request for public assistance. Supporting infrastructure encompasses the percent of time that the Public Assistance grants management system (EMMIE) is available and the organizational fill of FEMA's Public Assistance organization. Customer satisfaction information expresses the percent of grantees and sub-grantees who expressed satisfaction after receiving a Public Assistance grant in the previous quarter.
Reliability Index	Reliable
Explanation of Data Reliability Check	Each source of data of the composite measure is reliable and Recovery Reporting and Analytics Division (RRAD) has implemented appropriate quality controls to ensure data consistency. The data for the RPA to Kickoff measure come from the EMMIE database. The data are checked by SMEs before and after they are analyzed. For the human resources data, a human resources analyst from the ORR Business Management Division pulls the data. Before the data set is sent to RRAD for analysis, it is checked by the Executive Officer of the Public Assistance Division to ensure the numbers are correct. Finally, a systems specialist from the Recovery Technology and Programs Division pulls the system uptime information and sends to RRAD for analysis. RRAD compares all numbers to previous quarter and sends them to the programs for confirmation. Finally, the results are shared with PA leadership for review and concurrence before the final results are submitted to FEMA's Office of Policy and Program Analysis.

Performance Measure	Percent of shipments for required life-sustaining commodities (meals, water, tarps, plastic sheeting, cots, blankets, and generators) and key initial response resources delivered by the agreed upon date
Program	Response and Recovery
Description	This measurement evaluates the percent of shipments from FEMA Distribution Centers or logistics partners that arrive at the specified location by the validated and agreed upon delivery date.
Scope of Data	The parameters used to define what data is included in this performance measure are comparison of requested materials, date to be delivered, arrival status, and quantity received. All shipments resulting in a valid shipment will be measured. The "agreed upon date" is the established date that both supplier (logistics) and customer (operations) have determined best meets the need of the situation.
Data Source	FEMA is shifting from manual record-keeping systems to an automated Logistics Supply Chain Management System (LSCMS). Both systems are used to report Receipt information from state sites to FEMA. As FEMA strives to integrate the LSCMS Request and Order systems, there may be some errors in recording the Required Delivery Date (RDD) on the Request into the Order system. Data responsibilities are shared by several FEMA and external groups: The NRCC Resource Support Section (RSS) verifies and validates the information and orders the assets. FEMA partners/Distribution Centers/Incident Support Bases (ISBs) fulfill the order and dispatch the shipments; FEMA HQ/field sites/states receive the shipments and verify time received and condition of the shipment. FEMA Logistics Management directorate owns the reporting database through the LSCMS/Total Asset Visibility (TAV) Program.
Data Collection Methodology	Requests for disaster assets are entered into LSCMS by supply chain managers at FEMA HQ or regional staff. When shipments are received at designated locations (either FEMA or state sites), the receipt is recorded in LSCMS by FEMA staff (state representatives report data to FEMA). FEMA analysts extract Tier I (life-saving/life-sustaining resources) and Tier II (key operational resources) data from LSCMS: (1) the number of shipments in an order meeting the RDD. For each tier, FEMA staff tabulates the percent of shipments arriving by the RDD.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data is first checked for accuracy and completeness by the Logistics Management Center (LMC) within the Logistics Operations Division. The specific role within the LMC to conduct this comprehensive review and analysis is the LMC Chief. As a double-check, the Transportation Management Branch (TMB) within the Distribution Management Division verifies any shipment where there is a question against the actual Bill of Lading (BOL), which is the contract between FEMA and the Transportation Service Provider, and is signed and dated by the driver and the customer upon delivery. By comparing the date the BOL was signed against the reported receiving date within LSCMS, the TMB provides the double check to ensure data is accurate. The TMB also maintains a daily log of all orders throughout the year which is used to clarify any questions or discrepancies.

Performance Measure	Percent of states and territories that have achieved an intermediate or above proficiency to address their targets established through their THIRA
Program	Preparedness and Protection
Description	This measure assesses the percentage of state and territorial State Preparedness Report (SPR) ratings at or above the 3.0 threshold (on a five-point scale) when averaging across the planning, organization, equipment, training, and exercise (POETE) elements rated by grantees for each core capability. The measure is calculated by averaging SPR POETE ratings for each core capability that a state or territory has identified as high-priority. If a state's or territory's average SPR rating for its high-priority core capability POETE elements is 3.0 or higher, it is counted toward the measure. To increase the rating for one POETE element of a core capability by one point, a state/territory would have to increase capability by as much as 20 percent.
Scope of Data	The scope of this measure includes all 50 states and six territories.
Data Source	States and territories assess their current core capability levels relative to their own capability targets annually through the State Preparedness Report (SPR). This annual self-assessment provides detailed data on the number of states and territories whose capability levels increase or decrease each year. SPR data used in this measure are a self-assessed rating for each POETE solution area and a priority (high, medium, or low) for each core capability. The data are collected using Microsoft Excel from the official states' and territories' responses to the annual SPR capability assessment that is submitted to the National Preparedness Assessment Division (FEMA\NPD\NPAD). The analysis is done using Excel.
Data Collection Methodology	For each core capability, states and territories assess their preparedness levels in each of the five solution areas—planning, organization, equipment, training, and exercises (POETE). They use a five-point scale for each assessment, where level one indicates little-to-no capability, and level five indicates that they have all or nearly all of the capability required to meet their target. The data are obtained from state and territory SPRs submitted to FEMA each year. The Excel based data analysis tool will extract SPR data into a raw data worksheet. NPAD will calculate the measure from the raw data.
Reliability Index	Reliable
Explanation of Data Reliability Check	States and territories receive substantial technical assistance (TA) on conducting the THIRA and submitting their capability levels estimates through the SPR. TA takes the form of published guidance (Comprehensive Preparedness Guide (CPG) 201: THIRA Guide, Second Edition), workshop sessions in the FEMA Regions, and just-in-time instruction during the assessment period. SPR submissions are routed through the Homeland Security Grant Program State Administrative Agency to ensure it represents all preparedness stakeholders in the jurisdiction. The Regional Federal Preparedness Coordinator and/or his or her staff review all state, territorial, and other eligible grantee THIRA submissions in their area of responsibility. The review ensures that the submitted THIRAs are developed in alignment with CPG 201.

Performance Measure	Percent of states and territories with a Threat and Hazard Identification and Risk Assessment (THIRA) that meets current DHS guidance
Program	Preparedness and Protection
Description	This measure quantifies the percentage of states and territories that develop a THIRA in accordance with the DHS guidance. The Homeland Security Grant Program (HSGP)/Urban Areas Security Initiative (UASI) grant guidance requires the development and maintenance of a THIRA. Developing and maintaining an understanding of risks faced by communities and the Nation is an essential component of the National Preparedness System. THIRA guidance provides a common and consistent approach for identifying and assessing risks and their associated impacts. This common approach enables the whole community to maintain a baseline understanding of the risks that they face, facilitating efforts to identify capability and resource gaps, focus capability improvements, and inform the community of actions they can take to manage their risks.
Scope of Data	The scope of this measure includes all 50 states and six territories.
Data Source	Grantees will be required to develop and submit a THIRA to PrepCAST no later than December 31 annually. The regions will review the THIRAs received and submit to headquarters via e-mail verification that the THIRAs meet current guidance; National Preparedness Assessment Division will be reviewing the results to use in the annual National Preparedness Report (NPR).
Data Collection Methodology	Grantees will be required to develop and submit a THIRA to their FEMA region no later than December 31 annually as part of the HSGP/UASI grant guidance. The regions will review the THIRAs received and submit to headquarters verification that the THIRAs meet current guidance. Headquarters then calculates the percent of states and territories that completed all steps of the THIRA guidance and obtained regional review and verification. As THIRAs are submitted to FEMA at the end of the calendar year, there is a data lag for this measure - the activities occurring during calendar prior year will be analyzed during the current year and will be reported as end of year results at the close of current fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	The FEMA Regional Federal Preparedness Coordinators (FPCs) will review all state and territorial THIRA submissions to ensure that the submitted THIRAs meet current DHS guidance.

Performance Measure	Percent of the U.S. population directly covered by FEMA connected radio transmission stations
Program	Preparedness and Protection
Description	This measure tracks the percentage of U.S. residents that will be capable of receiving an emergency alert message from a broadcast station that is connected and enhanced by FEMA to provide resilient, last resort capability for the President to address the American people. Executive Order 13407 requires the Integrated Public Alert Warning System (IPAWS) to implement a capability to alert and warn the American people in all hazards and "to ensure that under all conditions the President can communicate with the American people."
Scope of Data	The population in the Continental United States as well as Alaska, Hawaii, and the 6 U.S. territories.
Data Source	For population data, the source of data in the most recent U.S. Census bureau data. The source of data for radio locations, transmission data, contour maps, frequency propagation tools, and population coverage is provided by the Federal Communications Commission (FCC).

Data Collection Methodology	An accounting of the Continental United States, Hawaii, Alaska, and the 6 U.S. territories population that can receive alert and warning messages directly from an initial delivery system is developed as follows: Service contours for stations participating in the Primary Entry Point program are calculated using standard FCC methodology. Reference signal levels follow recommendations of Primary Entry Point Administrative Council (PEPAC): AM signal level: 0.5 mV/m, FCC M3 ground conductivity data; FM signal level 50 dBu, USGS 3 second terrain data. Station power and antenna specifications used are extracted from the FCC's online data resource. Served population is based on the most current US Census data aggregated into one kilometer tiles. The calculation of the population that can receive alert and warning messages is then divided by the total population to determine the percent of the U.S. population directly covered by FEMA connected radio transmission stations.
Reliability Index	Reliable
Explanation of Data Reliability Check	The program office uses standard Federal Communications Commission accepted means and methods to calculate the amount of the population reached. Calculations are verified by a broadcast engineer within the program office.

Performance Measure	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
Program	Preparedness and Protection
Description	EO 13407 states "It is the policy of the United States to have an effective, reliable, integrated, flexible, and comprehensive system to alert and warn the American people in situations of war, terrorist attack, natural disaster, or other hazards to public safety and well-being (public alert and warning system), taking appropriate account of the functions, capabilities, and needs of the private sector and of all levels of government in our Federal system, and to ensure that under all conditions the President can communicate with the American people." The IPAWS infrastructure provides alert and warning message collection and dissemination so that United States residents will receive authenticated emergency alert messages over as many communications paths as possible.
Scope of Data	The data range covers the Continental United States (CONUS) as well as Alaska, Hawaii, and the 6 U.S. territories (OCONUS) Census population data and available audience reach measures.
Data Source	US Census bureau data for population. Initially based on 2000 census statistics, to be updated with 2010 census inputs as received; FCC radio station location and transmission data; Radio frequency propagation tools; OCIO server up time reports; test and exercise reports.
Data Collection Methodology	This is a composite of three metrics. The percent of time the Emergency Alert System (EAS) server is up and running: National Continuity Programs will receive reports from FEMA Office if the Chief Information Officer on server up time daily. This second metric is a result of a twice-weekly test of the IPAWS OPEN system: twice a week, IPAWS will send out a test message from the primary FEMA Operations Center (FOC) and the Alternate FEMA Operations Center (AFOC) systems to the FEMA Primary Entry Point (PEP) Stations. The final metric will be the results of a survey of PEP Station broadcasters as to whether the television and radio broadcasters received the weekly test and whether their systems operated as required.
Reliability Index	Reliable

Explanation of Data Reliability Check	FEMA can verify the availability and operability of the EAS server and PEP Stations. There are some vulnerabilities, such as the physical equipment at each PEP Station which is susceptible to local events. The remainder of the system is dependent upon numerous large and small national and local private sector partners who rebroadcast the EAS messages to the American people through a variety of communications technologies. NCP verifies the operability of the entire system with occasional tests. The first nationwide test of FEMA PEP Station to AM, FM, Satellite Radio, Digital, Analog, Cable, and Satellite TV will be November 2011.

Performance Measure	Percent of U.S. population (excluding territories) covered by planned mitigation strategies
Program	Mitigation
Description	This is a point in time metric that determines the percent of U.S. population (excluding territories) covered by approved or approvable local Hazard Mitigation Plans. The population of each community with approved or approvable local Hazard Mitigation Plans is used to calculate the percentage of the national population. The FEMA Mitigation program gathers and analyzes critical data to aid in future mitigation efforts and enable communities to be better informed and protected. FEMA Mitigation helps communities reduce risk through sound land-use planning principles (such as planned mitigation strategies), floodplain management practices, and financial assistance.
Scope of Data	The scope of this measure includes all Unites States jurisdictions excluding territories.
Data Source	Data are derived from Regional Reports and are entered into a Microsoft Excel spreadsheet, which is maintained on redundant network drives. A Headquarters master spreadsheet is populated monthly by FEMA Regional Risk Analysis staff that record, report, and store the names and locations of the jurisdictions that have received FEMA approval of mitigation plans.
Data Collection Methodology	FEMA regional staff review each mitigation plan based on the regulations found in 44 CFR Part 201. Plans are not approved until they demonstrate that the affected jurisdiction(s) engaged in a planning process, identified and evaluated their risks from natural hazards, create overarching goals, and evaluate a range of specific actions that would reduce their risk, including a mitigation strategy that describes how the plan will be implemented. Data on the approved plans is stored by FEMA Headquarters (HQ) Risk Analysis Division in a Microsoft Excel spreadsheet. The percent is calculated by dividing the population of jurisdictions with approved, or approvable, plans by the total population in the United States (excluding territories).
Reliability Index	Reliable
Explanation of Data Reliability Check	FEMA utilizes an iterative validation process for its Mitigation Plan approval inventory. The FEMA Regions house the approved plans and approval records, and the master spreadsheet is kept at FEMA HQ. Each Region produces monthly reports on approved plans, which are then sent to FEMA HQ and compiled into a master All Regions Plan Approval Inventory. The Inventory is matched to Federal Information Processing Standard and Community Identification Database codes to jurisdictions and utilizes Census data to match populations for each jurisdiction. The information is sent back to the Regions for validation and updating each month.

Federal Law Enforcement Training Centers

Performance Measure	Number of Federal law enforcement training programs and/or academies accredited or re-accredited through the Federal Law Enforcement Training Accreditation process
Program	Law Enforcement Training
Description	This performance measure reflects the cumulative number of federal law enforcement training programs and/or academies accredited or re-accredited through the Federal Law Enforcement Training Accreditation (FLETA) process. Accreditation ensures that training and services provided meet professional training standards for law enforcement. Re-accreditation is conducted every five years to remain current. The results of this measure provide on-going opportunities for improvements in federal law enforcement training programs and academies.
Scope of Data	The scope of this measure includes all federal law enforcement training programs and academies that have ever applied for accreditation/re-accreditation through the Federal Law Enforcement Training Accreditation's Office of Accreditation. The FLETA Office of Accreditation's applicant/customer base extends potentially to all federal agencies with a law enforcement role.
Data Source	The source of the data is the FLETA Office of Accreditation applicant tracking database in Microsoft Access which is used to track and maintain the status of all accreditations/re-accreditations.
Data Collection Methodology	As accreditations/re-accreditations are finalized, the results are provided to the FLETA Office of Accreditation. Program personnel update the FLETA Office of Accreditation applicant tracking database and generate a report from the database to tabulate the number of federal law enforcement training programs that have a current accreditation or re-accreditation.
Reliability Index	Reliable
Explanation of Data Reliability Check	The FLETA Office of Accreditation verifies the data through quarterly reviews of the applicant tracking database. Program personnel generate a report and provide it to the Federal Law Enforcement Training Accreditation Board for review and discussion at regularly scheduled meetings. No known integrity problems exist.

Performance 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
Program	Law Enforcement Training
Description	This performance measure reflects the satisfaction of Partner Organizations (POs) that Federal Law Enforcement Training Centers' (FLETC) training programs address the right skills needed for their officers/agents to perform their law enforcement duties such as the prevention of the introduction of high-consequence weapons of mass destruction, terrorism and other criminal activity against the U.S. and our citizens. The results of the measure provide on-going opportunities for improvements that are incorporated into FLETC training curricula, processes and procedures.
Scope of Data	This measure includes the results from all Partner Organizations (POs) that respond to the Partner Organization Satisfaction Survey Statements 1 and 2, respectively: "The FLETC's basic training programs and courses of instruction address the right skills needed for my officers/agents to perform their law enforcement duties," and "The FLETC's advanced training programs and courses of instruction address the right skills needed for my officers/agents to perform their law enforcement duties." FLETC collaborates with more than 85 Partner Organizations, both internal and external to the Department of Homeland Security.

Data Source	The source of the data is the FLETC Partner Organization Satisfaction Survey administered via a web-based survey program (Vovici), which tabulates and calculates the survey results. The PO representative from each Partner Organization provides responses to the survey through Vovici and saves the responses online when the survey is completed.
Data Collection Methodology	The FLETC POs are surveyed using the PO Satisfaction Survey. Data are collected from mid-May through June. The measure uses an average of survey Statements 1 and 2. Statement 1 begins "The FLETC's basic" and Statement 2 begins "FLETC's advanced." Each statement ends with "training programs and courses of instruction address the right skills needed for my officers/agents to perform their law enforcement duties." The survey uses a modified six-point Likert scale. Program personnel import the survey data as saved by survey respondents from Vovici into the Statistical Package for the Social Sciences to generate descriptive statistics and then into Excel to generate data charts and tables. The percent is calculated as the average of the number of POs that responded "Strongly Agree" or "Agree" to Statements 1 and 2 divided by the number of POs that responded to each of the respective statements. POs that responded "Not Applicable" to either Statement were excluded from the calculations.
Reliability Index	Reliable
Explanation of Data Reliability Check	The survey was developed using contemporary survey methods comparable to those used by the military services and other major training organizations. Following release of the survey summary report, FLETC leaders conduct verbal sessions with Partner Organization key representatives to confirm and discuss their responses. Throughout the year other formal and informal inputs are solicited from the Partner Organization representatives by FLETC staff and used to validate the survey results. No known integrity problems exist.

Immigration and Customs Enforcement

Performance Measure	Average length of stay in detention of all convicted criminal aliens prior to removal from the United States (in days)
Program	Enforcement and Removal Operations (ERO)
Description	This measure provides an indicator of efficiencies achieved in working to drive down the average length of stay for convicted criminals in ICE's detention facilities. Decreases in the average length of stay can significantly reduce the overall costs associated with maintaining an alien population prior to removal.
Scope of Data	The scope of this measure includes all criminal aliens who were detained within ICE's detention facilities or while in ICE custody in federal, state, and local jails during the fiscal year awaiting due process.
Data Source	Data is maintained in the Alien Removal Module of the ENFORCE database. This database is maintained at headquarters and the data entry occurs at Enforcement and Removal Operations (ERO) Field Offices throughout the country. Tools in the Integrated Decision Support System are used to query the Alien Removal Module and produce reports to calculate the final results for this measure.

Data Collection Methodology	Enforcement and Removal Operations field offices are responsible for the entry and maintenance of data regarding the detention of illegal aliens in ICE Custody. The length of stay for an alien's detention stay is calculated by counting the number of days between the alien's initial book in date into ICE Custody and their final book out date. If an alien is booked in and out of ICE custody on the same day, the alien's length of stay is 0 days. The Average Length of Stay (ALOS) is the sum of the length of stay for all applicable detention stays divided by the number of detention stays using only detention stays that have concluded within a given fiscal year. Aliens that are initially booked into the Department of Health and Human Services, Office of Refugee and Resettlement, Mexican Interior Repatriation Program, or transport facilities, and U.S. Marshals Service Prisoners are excluded from ICE's ALOS. All other detention facilities, including hold rooms, are included in the ALOS count.
Reliability Index	Reliable
Explanation of Data Reliability Check	Headquarters staff validate the completeness and accuracy of the data entered by field offices into the Alien Removal Module through trend analysis to look for aberrations and unusual patterns. Data is analyzed on a weekly basis and compared to statistics from prior months and the previous year. An additional reliability check occurs when data is cross - referenced between field office detention facility reports of the number of removals, and data entered into the database. The Statistical Tracking unit checks for consistency of the results or measuring instrument through validation, back-end testing, or reproducibility of the data through alternative methodology. Depending upon the degree of consistency between two measures of the same measure allows the statistician to determine whether the data is considered reliable and or stable. Any inaccuracies will need to be sent to the Unit Chief, who will make the necessary corrections to the tasking query.

Performance Measure	Number of convicted criminal illegal immigrants who were returned or were removed from the U.S.
Program	Enforcement and Removal Operations (ERO)
Description	This measure includes both the return and removal of illegal immigrants who have a prior criminal conviction from the United States by ICE Enforcement and Removal Operations (ERO). Criminal convictions can range in seriousness from misdemeanors to felonies. This measure reflects the program's efforts to ensure convicted criminal illegal immigrants do not remain in the United States and thus make the nation safer for legal citizens.
Scope of Data	All returns and removals of illegal immigrants who have had a prior criminal conviction are included in this measure. All non-criminal immigration violators are excluded from the count. An immigration violator is only considered a convicted criminal if he or she has also been convicted of a crime.
Data Source	Data is maintained in the Alien Removal Module of the ENFORCE database. This database is maintained at headquarters and the data entry occurs at Enforcement and Removal Operations (ERO) Field Offices throughout the country. Tools in the Integrated Decision Support System (IIDS) are used to query the Alien Removal Module and produce reports to calculate the final results for this measure. The IIDS data warehouse is maintained by ERO's Statistical Tracking Unit (STU).

Data Collection Methodology	Enforcement and Removals Operations field offices are responsible for the entry and maintenance of data regarding the removal and return of illegal immigrants. When an illegal immigrant is removed and/or returned from the United States, case officers in the field will indicate in the database the case disposition and date the removal/return occurred in the database. Officers track the status of administrative processes and/or court cases and indicate when actual removals occur in the Alien Removal Module of the ENFORCE database. Reports generated from the Alien Removal Module using IIDS determine the number of convicted illegal immigrants returned/removed from the country during the specified time.
Reliability Index	Reliable
Explanation of Data Reliability Check	Headquarters staff validate the completeness and accuracy of the data entered by field offices into the Alien Removal Module through trend analysis to look for aberrations and unusual patterns. Data is analyzed on a weekly basis and compared to statistics from prior months and the previous year. An additional reliability check occurs when data is cross - referenced between field office detention facility reports of the number of removals, and data entered into the database. The Statistical Tracking unit checks for consistency of the results or measuring instrument through validation, back-end testing or reproducibility of the data through alternative methodology. Depending upon the degree of consistency between two measures of the same measure allows the statistician to determine whether the data is considered reliable and or stable. Any inaccuracies will need to be sent to the Unit Chief, who will make the necessary corrections to the tasking query.

Performance Measure	Number of enforcement-related actions against employers that violate immigration-related employment laws
Program	Homeland Security Investigations (HSI)
Description	This measure is a cumulative result of enforcement-related actions against employers that hire illegal labor. Enforcement-related actions include criminal arrests, audits, and final orders of fines of employers related to worksite enforcement. This measure demonstrates the impact of worksite enforcement operations to ensure that employers do not violate immigration-related employment laws.
Scope of Data	This measure includes employers that have been audited, sanctioned, fined, arrested, or otherwise brought into compliance with the law. For the purpose of this measure, "audit" is defined as an administrative examination by ICE personnel of employer organizations. "Sanction" is defined as a detriment, loss of reward, or coercive intervention as a means of enforcing immigration law.
Data Source	Data is retrieved from the investigative case management system, TECS. Data query results identify the number of criminal arrests, audits, and/or amount of monetary fines levied against companies for a specific time period.
Data Collection Methodology	Under federal law, employers are obligated to ensure their employees are eligible to work in the United States. When immigration-related questions arise regarding the accuracy of I-9 forms or other documentation for employer personnel, an audit may be performed by ICE to investigate possible violations. Arrests and various forms of sanction can occur based upon the outcome of these audits. After an employer has been audited, sanctioned, or arrested, the record is entered into the TECS system. A data request is sent to the HSI Executive Information Unit (EIU) from the Budget Formulation and Strategic Planning Unit. EIU returns an excel spreadsheet with the number of criminal arrests, audits, and/or amount of monetary fines levied against companies for a specific time period.
Reliability Index	Reliable
Explanation of Data Reliability Check	Case information in TECS is verified and audited by the HSI Data Quality Unit on a monthly basis.

Performance Measure	Percent of detention facilities found in compliance with the national detention standards by receiving a final acceptable inspection rating
Program	Enforcement and Removal Operations (ERO)
Description	This measure gauges the percent of detention facilities that have received an overall rating of acceptable or above within the Enforcement and Removal Operations (ERO) National Detention Standards Program as measured against the Performance Based National Detention Standards. Through a robust inspections program, the program ensures facilities utilized to detain aliens in immigration proceedings or awaiting removal to their countries do so in accordance with the Performance Based National Detention Standards.
Scope of Data	All facilities on the authorized facility's list are included in this measure. Authorized facilities include detention centers that have been inspected by ERO/Custody Operations law enforcement personnel, or their Subject Matter Experts (SME), to ensure the facility meets all requirements of the ICE/ERO National Detention Standards provisions.
Data Source	The annual review rating is contained in formal inspection reports provided by the Detention Standards Compliance Unit (DSCU) contractor and is further reviewed by the DSCU. The information from these reports will be compiled to determine the agency-wide percentage of facilities receiving acceptable or above rating.
Data Collection Methodology	Data for this measure is collected by annual inspections, which are then evaluated by ERO inspectors. These inspections review the current National Detention Standards that apply to all facilities, and rate whether the facility is in compliance with each standard. Based on these ratings, the compliance for each facility is calculated. This information is communicated in formal reports to the program and the ERO Inspections and Audit Unit and the Detention Standards Compliance Unit at ERO Headquarters, which oversees and reviews all reports. The program reports semi-annually on agency-wide adherence with the Detention Standards based on calculating the number of facilities receiving an acceptable or better rating, compared to the total number of facilities inspected.
Reliability Index	Reliable
Explanation of Data Reliability Check	The program reviews all reports of detention facilities inspections conducted by the contractor. Inspections that receive a final rating of "Acceptable" or above are reviewed by the Detention Standards Compliance Unit (DSCU) and the Inspections and Audit Unit. Inspections that receive deficient or at-risk rating are reviewed by DSCU SMEs.

Performance Measure	Percent of ICE removals that support current enforcement priorities (Retired Measure)
Program	Enforcement and Removal Operations (ERO)
Description	This measure describes the percentage of aliens removed by ICE Enforcement and Removal Operations (ERO) that, by posing a threat to national security, border security and public safety, represent the Department’s current enforcement priorities.
Scope of Data	Data will be retrieved from the Investigative Case Management system (ICM), to include all validated records of significant transnational worksite investigations. The following shall constitute the Department's civil immigration enforcement priorities: Priority 1 (threats to national security, border security, and public safety), Priority 2 (misdemeanants and new immigration violators), and Priority 3 (other immigration violations, which includes those who have been issued a final order of removal on or after January 1, 2014). This guidance is outlined in DHS Memo Policies for the Apprehension, Detention and Removal of Undocumented Immigrants dated 20 November 2014.
Data Source	Data are stored in the ICE Integrated Decision Support (IIDS) system data warehouse and maintained by ERO’s Statistical Tracking Unit (STU). The IIDS reflects officer-entered data into DHS’s case management system and its tables are refreshed nightly and provide data with a 36-hour delay.

Data Collection Methodology	When an alien is processed, an ERO officer selects which priority category the alien falls under and provides accompanying rationale within DHS' case management system. ICE ERO's Law Enforcement Systems and Analysis group queries the ICE IIDS to determine both the total number of removals, as well as the priority of those removals during the reporting period. IIDS queries cross-check priority selections with additional priority-relevant data about the removal (e.g., date of issuance for a final order of removal) to ensure data reliability. The final calculation is made by dividing the number of top Priority 1 removals by the number of total removals.
Reliability Index	Reliable
Explanation of Data Reliability Check	The IIDS, ERO's main data warehouse, is routinely maintained for accuracy. Law Enforcement Systems and Analysis' STU has internal control measures in place to check data reliability. STU validates queries each week to benchmark against prior weeks' reported figures, which are archived internally. Data abnormalities are examined by the STU analyst to identify any technical issues and adjusted accordingly. The corrected data model is archived and used moving forward. If the data are determined to have potential data quality issues due to Field input, the STU analyst will work in conjunction with the STU officers to perform a case review in addition to a review of the alien's criminal history in the front-end applications. Any major data quality issues and anomalies are shared with the Data Quality and Integrity Unit to potentially facilitate the Field fixing or addressing a larger-scale issue with the front-end applications.

Performance Measure	Percent of removal orders secured by ICE attorneys that support current enforcement priorities (Retired Measure)
Program	Office of Principal Legal Advisor (OPLA)
Description	This measure indicates the percent of total removal orders secured by OPLA attorneys that support the Department's highest enforcement priorities. OPLA attorneys play an integral role in enforcing the nation's immigration laws by litigating cases in immigration court and securing orders of removal against those found to be in the United States illegally.
Scope of Data	The scope of data will consist of removal order cases with an Immigration Judge (IJ) order date occurring during the fiscal year that supports the Department's highest current stated priorities: Priority 1 (threats to national security, border security, and public safety) and Priority 2 (misdemeanants and new immigration violators). This guidance is outlined in DHS Memo Policies for the Apprehension, Detention and Removal of Undocumented Immigrants dated 20 November 2014.
Data Source	The information will be retrieved from the Principal Legal Advisor's Network (PLAnet) and the Enforcement Integrated Database (EID).
Data Collection Methodology	OPLA analysts retrieve Alien File (A-File) information for cases with an IJ order from PLAnet and provide a data file comprised of those A-File numbers to ERO. ERO then matches the relevant civil immigration enforcement priority information to each A-File number and returns the data file to OPLA. OPLA analysts then calculate the percentage of removal orders that are Priority 1 or Priority 2. OPLA then analyzes the data and provides a written explanation of results.
Reliability Index	Reliable
Explanation of Data Reliability Check	OPLA's Knowledge Management Division and Field Legal Operations attorneys review and confirm the accuracy of the data presented.

Performance Measure	Percent of significant Homeland Security Investigation cases that result in a disruption or dismantlement
Program	Homeland Security Investigations (HSI)
Description	This measure reports on the percent of significant transnational criminal investigations that resulted in a disruption or dismantlement. "Disruption" is defined as impeding the normal and effective operation of the targeted organization. "Dismantlement" is defined as destroying the organization's leadership, financial base and network to the degree that the organization is incapable of operating and/or reconstituting itself. ICE investigations cover a broad range of areas, including national security threats, financial and smuggling violations (including illegal arms exports), financial crimes, commercial fraud, human trafficking, narcotics smuggling, child pornography/exploitation and immigration fraud.
Scope of Data	Data will be retrieved from the Investigative Case Management system (ICM), to include all validated records of significant transnational worksite investigations.
Data Source	Specific case information will be entered through the use of the Significant Case Report (SCR) Module in ICM.
Data Collection Methodology	Substantive case information during the investigative process is entered into ICM, eventually reflecting indictment, conviction, and/or case closure. This data is validated for accuracy, prior to any reporting. For this measure, a data request will be sent to the HSI Executive Information Unit (EIU). EIU will return an Excel spreadsheet with approved SCR transnational cases by year. A percentage of approved SCR cases with approved disruptions or dismantlements within a specific time period is then derived at the end of the time period by comparing it to closed SCR cases within the time period and all open SCR cases. All open SCR cases refers to the total number of cases that are open at the beginning of the fiscal year as well as cases that are open throughout the year that is being reported. As cases are closed or dismantled/disrupted, they continue to be included in the denominator for calculation purposes.
Reliability Index	Reliable
Explanation of Data Reliability Check	All significant criminal investigations will be approved by a panel represented by HSI, which includes HSI Operations, HSI International Operations and Intelligence. The panel will validate the information provided and determine which nominated cases indeed meet the criteria of investigations resulting in the disruption or dismantlement of significant transnational investigations.

Performance Measure	Total number of illegal immigrants who were returned or removed from the U.S. (New Measure)
Program	Enforcement and Removal Operations (ERO)
Description	This measure describes the total number of illegal immigrants returned and/or removed from the United States by ICE Enforcement and Removal Operations (ERO). The measure includes both immigrants who have entered the country illegally, but do not already have prior criminal conviction, along with those who have had a prior criminal conviction. This measure provides a complete picture of all the returns and removals accomplished by the program to ensure illegal immigrants do not remain in the United States.
Scope of Data	The measure captures the sum of all illegal immigrants returned and/or removed by ICE ERO. Immigration violators can be classified into two groups: non-criminal and criminal. Non-criminal immigration violators include all those identified as illegally present with no previous criminal convictions. Criminal immigration violators would include all those identified who are illegally present with criminal convictions, such as a misdemeanor or felony.

Data Source	Data is maintained in the Alien Removal Module of the ENFORCE database. This database is maintained at headquarters and the data entry occurs at Enforcement and Removal Operations (ERO) Field Offices throughout the country. Tools in the Integrated Decision Support System (IIDS) are used to query the Alien Removal Module and produce reports to calculate the final results for this measure. The IIDS data warehouse is maintained by ERO's Statistical Tracking Unit (STU).
Data Collection Methodology	Enforcement and Removals Operations field offices are responsible for the entry and maintenance of data regarding the removal and return of illegal immigrants. When an illegal immigrant is removed and/or returned from the United States, case officers in the field will indicate in the database the case disposition and date the removal/return occurred in the database. Officers track the status of administrative processes and/or court cases and indicate when actual removals occur in the Alien Removal Module of the ENFORCE database. Reports generated from the Alien Removal Module using IIDS determine the number of convicted illegal immigrants returned/removed from the country during the specified time.
Reliability Index	Reliable
Explanation of Data Reliability Check	The IIDS, ERO's main data warehouse, is routinely maintained for accuracy. Law Enforcement Systems and Analysis' Statistical Tracking Unit (STU) has internal control measures in place to check data reliability. STU validates queries each week to benchmark against prior weeks' reported figures, which are archived internally. Data abnormalities are examined by the STU analyst to identify any technical issues and adjusted accordingly. The corrected data model is archived and used moving forward. If the data are determined to have potential data quality issues due to Field input, the STU analyst will work in conjunction with the STU officers to perform a case review in addition to a review of the illegal immigrant's criminal history in the front-end applications. Any major data quality issues and anomalies are shared with the Data Quality and Integrity Unit to potentially facilitate the Field fixing or addressing a larger-scale issue with the front-end applications.

National Protection and Programs Directorate

Performance Measure	Percent of annual risk and vulnerability assessments completed for twenty-three cabinet level agencies and one-third of all non-cabinet level agencies
Program	Cybersecurity
Description	This measure assesses how many risk and vulnerability assessments (RVAs) DHS provides each year and compares that result to the total number of targeted federal, civilian Executive Branch agencies for that year. Each year, DHS will target twenty-three cabinet level agencies and one-third of the remaining 102 federal, civilian Executive Branch agencies. Therefore, each of the targeted cabinet level agencies will receive an annual RVA, and the other targeted agencies will receive triennial RVAs. DHS leverages cybersecurity assessment methodologies, commercial best practices and threat intelligence integration to conduct the RVAs that enables cybersecurity stakeholders to better develop decision making and risk management guidance.
Scope of Data	The scope of the data includes all of the assessment findings from the National Cybersecurity Assessment and Technical Services (NCATS) Risk and Vulnerability Assessments (RVAs). The cabinet-level agencies consist of non-defense CFO Act agencies that receive annual assessments and an additional 102 smaller agencies and departments that receive an RVA every three years.

Data Source	Assessment and countermeasure data are collected and stored by the NCATS team using a spreadsheet that tracks RVA engagements. In the future, an NPPD or Office of Cybersecurity and Communications -wide customer relationship management tool will be used. RVAs include external (remote) non-credentialed scanning along with penetration testing. Measurements are tracked and stored on the Cybersecurity Assurance Lab network where the penetration testing and remote scans are conducted.
Data Collection Methodology	A team lead will track the progress of the assessment, which is scoped out with the stakeholder in the pre-assessment walkthrough. The team lead will then walk through the assessment methodology and conduct a series of testing that was identified by the stakeholder. The information derived from the tests will then populate a draft report deliverable. The data used to create the report is maintained in a spreadsheet by the NCATS program. Information on the spreadsheet includes name of finding, service impacted (if any), detailed finding, NIST Control (if any), standard remediation write up, default finding severity.
Reliability Index	Reliable
Explanation of Data Reliability Check	Each assessment concludes with a final report. The metric will be compared to the report.

Performance Measure	Percent of calls made by National Security/Emergency Preparedness users during emergency situations that DHS ensured were connected
Program	Emergency Communications
Description	This measure gauges the Government Emergency Telecommunications Service (GETS) call completion rate. The GETS call completion rate is the percent of calls that a National Security/Emergency Preparedness (NS/EP) user completes via public telephone network, landline, or wireless, to communicate with the intended user/location/system/etc., under all-hazard scenarios. Hazard scenarios include terrorist attacks or natural disasters such as a hurricane or an earthquake.
Scope of Data	The scope of the data is all calls initiated by a national security emergency preparedness user when the Public Switched Network experiences major congestion, typically due to the occurrence of a natural or man-made disaster such as a hurricane, earthquake, or terrorist event.
Data Source	The data sources are reports from the GETS priority communications systems providers integrated by the GETS program management office.
Data Collection Methodology	Data is captured during the reporting period when the public switched network communication experiences major congestion. The information is collected within the priority service communications systems and provided to NS/EP communications government staff and integrated by the GETS program management office. Based on information from these reports, the program calculates call completion rate.
Reliability Index	Reliable
Explanation of Data Reliability Check	Carrier data is recorded, processed, and summarized on a quarterly basis in accordance with criteria established by management. Data collection has been ongoing for GETS since 1994. All data collected is also in accordance with best industry practices and is compared with previous collected data as a validity check.

Performance Measure	Percent of contract security force evaluations conducted at high-risk facilities resulting in no countermeasure-related deficiencies (New Measures)
Program	Federal Protective Service
Description	This performance measure provides the percentage of Facility Security Level IV facilities identified with no countermeasure-related deficiencies during contract security force evaluations conducted during each fiscal year quarter. Countermeasure-related deficiencies are the total of covert security testing (investigative operation used to identify deficiencies in security countermeasures, training, procedures, and technology) deficiencies and countermeasure (access control, alarms, barriers, communications, guard force, screening, and surveillance) deficiencies identified during post inspections. Level IV is defined as high risk based on the Interagency Security Committee Standards as having over 450 federal employees; high volume of public contact; more than 150,000 square feet of space; tenant agencies that may include high-risk law enforcement and intelligence agencies, courts, judicial offices, and highly sensitive government records.
Scope of Data	This performance measure includes deficiencies identified during FPS managed contract security force evaluations (which encompasses covert security testing deficiencies and countermeasure deficiencies identified during post inspections) at Facility Security Level IV facilities. Targets of testing include, but are not limited to, Protective Security Officer's (PSO) training, procedures, attentiveness, and their ability to recognize weapons, explosives, and other prohibited items being introduced into a Federal facility as prescribed by the PSO contracts and Post Orders.
Data Source	Post inspection deficiencies are captured in the Contract Oversight Reporting Tool (CORT). Covert security testing results are captured in the Treasury Enforcement Communication System II (TECS II) and the outputs are reported in FPS Enterprise Information System (EIS).
Data Collection Methodology	This performance measure captures the total contract security force evaluation deficiencies (covert security testing deficiencies and countermeasure deficiencies identified during post inspections) identified during each quarter of a Fiscal Year. Covert security testing is implemented by FPS Special Agents. Covert security testing is conducted using FPS-approved scenarios and various inert components and devices. Two post inspections are conducted at each Level IV facility per week. Each post inspection includes the measurement of countermeasure deficiencies (access control, alarms, barriers, communications, guard force, screening, and surveillance). The data is collected and entered into the systems (CORT, TECH II, and EIS) by the agent who conducts the covert testing. TMD mission support personnel run the reports in EIS and extracts/exports the data to an excel file.
Reliability Index	Reliable
Explanation of Data Reliability Check	Contract security force evaluation results are provided to FPS Policy and Strategic Planning Division for review, quality assurance, and performance measure reporting.

Performance Measure	Percent of customers implementing at least one cybersecurity assessment recommendation to improve critical infrastructure and federal network security
Program	Infrastructure Protection
Description	The DHS National Cyber security and Communications Integration Center (NCCIC) administers cybersecurity vulnerability assessments and provides mitigation recommendations to customers, including federal, critical infrastructure owners and operators, and state, local, tribal, and territorial (SLTT) partners. This measure provides insight into the percentage of customers reporting implementation of one or more improvements based on recommendations following an assessment.

Scope of Data	The scope is the responses to post assessment surveys from the Industrial Control Systems – Computer Emergency Response Team (ICS-CERT), Stakeholder Engagement Critical Infrastructure Resilience (SECIR), and National Cybersecurity Assessment & Technical Services team (NCATS) assessments. Customers are sent a survey after 180 days asking if they implemented any of the recommended actions from the assessment. Survey responses received during the reporting period will be used to calculate the results. The result is the total from the following surveys: ICS-CERT: # reporting one or more improvements based on recommendations; Industrial Control Systems (ICS) - Federal Critical Infrastructure Assessment; ICS - Critical Infrastructure Assessment; SECIR: # reporting their organization has implemented at least one recommended improvement; Cyber Resilience Review: NCATS: # reporting at least one vulnerability as Partially or Fully Mitigated; Risk & Vulnerability Assessment.
Data Source	1. ICS-CERT Program Metrics Workbook 2. CRR Assessment Tracker 3. RVA Status Tracking (NCATS internal tracking spreadsheet)
Data Collection Methodology	A remote data collection method is employed, using Tableau software, to access NCATS and ICS-CERT internal tracking spreadsheets. An automated report is generated on the percentage of ICS-CERT assessment customers, reporting (via survey) an improvement in capabilities. Cyber Resilience Review (CRR) results are reported to the Office of Cyber Security & Communications (CS&C) by Stakeholder Engagement and Critical Infrastructure Resilience (SECIR). The number of positive responses will be divided by the total number of submissions to calculate the percentage.
Reliability Index	Reliable
Explanation of Data Reliability Check	1. NCATS - Data is reviewed by NCATS analysts and NCCIC Leadership before reporting to CS&C 2. SECIR – Data is reviewed by the branch chief before reporting to CS&C 3. ICS-CERT - Survey responses are logged into the ICS-CERT Program Metrics Workbook and data for this measure is pulled directly from this workbook and reviewed by NCCIC Leadership before reporting to CS&C The CS&C front office reviews all results before final reporting to DHS.

Performance Measure	Percent of facilities that are likely to integrate vulnerability assessment or survey information into security and resilience enhancements
Program	Infrastructure Protection
Description	This measure demonstrates the percent of facilities that are likely to enhance their security and resilience by integrating Infrastructure Protection vulnerability assessment or survey information. Providing facilities with vulnerability information allows them to understand and reduce risk of the Nation's critical infrastructure.
Scope of Data	The results are based on all available data collected during the fiscal year through vulnerability assessments. "Security and resilience enhancements" can include changes to physical security, security force, security management, information sharing, protective measures, dependencies, robustness, resourcefulness, recovery, or the implementation of options for consideration.
Data Source	Data from interviews with facilities following vulnerability assessments and surveys are stored in the Infrastructure Survey Tool (IST), which is input into a central Link Encrypted Network System residing on IP Gateway. The Office of Infrastructure Protection owns the final reporting database.

Data Collection Methodology	Infrastructure Protection personnel conduct voluntary vulnerability assessments on critical infrastructure facilities to identify protective measures and security gaps or vulnerabilities. Data are collected using the web-based IST. Following the facility's receipt of the survey or assessment, they are contacted via an in-person or telephone interview. Feedback is quantified using a standard 5-level Likert scale where responses range from "Strongly Disagree" to "Strongly Agree." Personnel at Argonne National Laboratory conduct analysis of the interview to determine the percent of facilities that have responded that they agree or strongly agree with the statement that, "My organization is likely to integrate the information provided by the [vulnerability assessment or survey] into its future security or resilience enhancements." This information is provided to Infrastructure Protection personnel who verify the final measure results before reporting the data.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data collection is completed by trained and knowledgeable individuals familiar with the knowledge, skill, and ability to determine effective protective measures. Additionally, the data go through a three tier quality assurance program that ensures the data collection is in line and coordinated with methodology in place. The quality assurance is conducted by the program and methodology designers providing a high level of confidence that data entered meets the methodology requirements. Any questionable data are returned to the individual that collected the information for clarification and resolution. Updates to the program or changes to questions sets are vetted by the field team members prior to implementation. Training is conducted at least semi-annually either in person or through webinar. Immediate changes or data collection trends are sent in mass to the field so that all get the message simultaneously.

Performance Measure	Percent of Facility Security Committee Chairs (or designated officials) satisfied with the level of security provided at federal facilities
Program	Federal Protective Service
Description	This measure assesses the effectiveness of protection and security services provided by the Federal Protective Service (FPS) to Facility Security Committee (FSC) Chairs, or their designated officials, through surveying their overall customer satisfaction. The FSC Chairperson is the representative of the primary tenant and is the primary customer of FPS Facility Security Assessments and countermeasure consultation. This will enable FPS to make better informed decisions to enhance the services it provides to its tenants.
Scope of Data	The scope of this measure are the FSC Chairs and Designated Officials (DO) who serve as a proxy for all tenants. Each federal facility that FPS services is represented by at least one FSC Chair or DO; some FSC Chairs and DOs represent multiple facilities. If a federal facility is occupied by more than one agency, it is still represented by only one FSC Chair or DO. FSC Chairs and DOs are federal employees of one of the agencies that occupies space in the federal facility. FSC Chairs and DOs receive the FPS Facility Security Assessment (FSA) and are consulted with regarding countermeasures. As the primary customers of FPS, FSC Chairs and DOs have the greatest amount of interaction with FPS personnel and services. In addition, FSC Chairs and DOs understand the security issues at the facilities they represent from the tenant standpoint, so they are qualified to serve as proxies for tenants.

Data Source	Data are captured via a survey FPS administers to FSC Chairs (or designated officials) to assess overall satisfaction with FPS provided services. The survey is made accessible and available to all Facility Security Committee Chairs (or designated officials). Respondents rate their satisfaction using a five-point Likert scale, in which the potential responses range from 1 ("Strongly Disagree") to 5 ("Strongly Agree"). The survey is administered through SurveyMonkey. The final results are exported from SurveyMonkey to an Excel spreadsheet. This spreadsheet is validated and used to conduct results analysis at FPS HQ.
Data Collection Methodology	The survey will be administrated on an annual basis in late Q3 or early Q4. Invitations to take the survey will be sent to FSC Chairs and DOs utilizing SurveyMonkey's email invitation capability. Survey access is tied to a unique link provided in the email message for each user. This survey includes a question targeted at understanding customers' overall satisfaction with FPS services. The question, "Overall, what is your satisfaction level with FPS services?" employs a five-point Likert scale for respondents to rate satisfaction. The percentage of tenants satisfied is derived from the total number of respondents who provide a greater than neutral response divided by the total number of respondents.
Reliability Index	Reliable
Explanation of Data Reliability Check	The complete list of FSC Chairs and DOs, including contact information, is vetted with each of FPS' eleven regions to validate that those individuals are currently serving as FSC Chairs and DOs and that the contact information is up to date. The anonymous survey is sent to each FSC Chair and DO on the validated list through SurveyMonkey's invitation tool. SurveyMonkey's survey functionality ensures data reliability from a collection standpoint because it ensures individuals can only submit responses to the survey once. The survey results undergo multiple rounds of review beginning with the survey administration team and continuing up through the Director of FPS.

Performance Measure	Percent of federal, civilian executive branch personnel for whom EINSTEIN intrusion prevention system coverage has been deployed (Retired Measure)
Program	Cybersecurity
Description	This measure gauges the intrusion prevention coverage provided by EINSTEIN 3 Accelerated (E3A) that is currently operating on civilian executive branch networks. E3A has the capacity to both identify and block known malicious traffic. This performance measure assesses the extent to which DHS has deployed at least one E3A countermeasure to protect federal, civilian executive branch Chief Financial Officer (CFO) Act agencies. This measure calculates the percentage of CFO Act personnel that are protected by at least one E3A countermeasure.
Scope of Data	All federal, civilian executive branch personnel are included in this measure. Data are based on self-reported federal, civilian executive branch CFO Act Department or Agency (D/A) Personal Identity Verification (PIV) counts as required by Homeland Security Presidential Directive-12, the date on which the participating CFO Act D/A successfully completes cutover (signifying deployed protection by E3A), and the service(s) selected by the participating CFO Act D/A. CFO Act D/A PIV counts provide an estimate of the number of personnel (federal and contractor) assigned to that CFO Act D/A. In addition, DHS also uses the estimated number of privileged and unprivileged network accounts (for both federal and contractor) at each D/A through Federal Information Security Management Act (FISMA) reporting. DHS combines the PIV counts (aka "seat count") data gathered through E3A deployment, and the FISMA network account data to create an "integrated seat count".

Data Source	Federal, civilian executive branch CFO Act D/A PIV counts, number of privileged and unprivileged FISMA network accounts, the services selected, and cutover dates are tracked on the LAN-A hosted E3A Executive Reporting Tracker, which is a Microsoft Excel spreadsheet. The Network Security Division (NSD) Mission Engineering & Technology (ME&T) populates the dates when the Departments and Agencies become covered by an E3A service, updates D/A integrated seat counts, and tracks status towards cutover.
Data Collection Methodology	EINSTEIN intrusion prevention system coverage is considered "deployed" when the D/A successfully completes routing its traffic through a Domain Name Service (DNS) server/service and/or Simple Mail Transfer Protocol (SMTP) server/service to be filtered; this is also known as the cutover date. If the D/A opts to use one countermeasure (e.g., DNS before getting SMTP) prior to getting the second, the earlier date is used as the cutover date. When the cutover is completed, all D/A seats are considered protected. When completing the cumulative quarterly percentage, the numerator consists of the sum of the "integrated seat count" of all CFO Act D/A having a cutover date prior to the reporting date and having selected either DNS and/or SMTP; the sum of all known D/A seats forms the denominator. This fraction is multiplied by 100 to obtain the percentage.
Reliability Index	Reliable
Explanation of Data Reliability Check	The Network Security Division team will update the E3A Executive Reporting Tracker with additional D/A PIV count and FISMA network account numbers, D/A cutover dates, and selected E3A services. The Network Security Division will review and validate the data.

Performance Measure	Percent of high-risk facilities that receive a facility security assessment in compliance with the Interagency Security Committee (ISC) schedule
Program	Federal Protective Service
Description	This measure reports the percentage of high risk (Facility Security Level 3, 4 and 5) facilities that receive a facility security assessment (FSA) in compliance with the ISC schedule. An FSA is a standardized comprehensive risk assessment that examines credible threats to federal buildings and the vulnerabilities and consequences associated with those threats. Credible threats include crime activity or potential acts of terrorism. Each facility is assessed against a baseline level of protection and countermeasures are recommended to mitigate the gap identified to the baseline or other credible threats and vulnerabilities unique to a facility. Requirements for the frequency of federal building security assessments are driven by the ISC standards with high risk facility assessments occurring on a three year cycle.
Scope of Data	The scope of this measure includes all high risk facilities with a security level of 3, 4, and 5. An FSA is considered completed when the assessment is presented to the FSC Chairperson or Designated Official and the package is signed in acknowledgement of receipt. This is documented in the FSA Manual, March 2014.
Data Source	Data is collected in the Modified Infrastructure Survey Tool (MIST) and is owned and maintained by the Federal Protective Service's (FPS's) Risk Management Division (RMD).
Data Collection Methodology	Results from each assessment are collected in MIST by inspectors. At the end of each reporting period, the percent of high risk facilities that receive an FSA is divided by the number of scheduled assessments for that period. The performance period for this measure is three years. The denominator for this measure is the total number of FSL 3, 4, and 5 facilities scheduled to be assessed within the three-year cycle. The numerator is the number of FSL 3, 4, and 5 facilities assessed within the three year cycle.
Reliability Index	Reliable

Explanation of Data Reliability Check	FSA results are consolidated and reviewed by FPS's RMD for quality assurance and performance measure reporting.

Performance Measure	Percent of incidents detected by the U.S. Computer Emergency Readiness Team for which targeted agencies are notified within 30 minutes
Program	Cybersecurity
Description	The United States Computer Emergency Readiness Team (US-CERT) detects malicious cyber activity targeting federal agencies. This measure assesses the percent of incidents directed at federal agencies and detected by the US-CERT for which agencies are informed of this malicious activity within 30 minutes. This measure demonstrates US-CERT's ability to share situational awareness of malicious activity with its federal agency stakeholders through the EINSTEIN intrusion detection systems and other tools. The numerator for this measure is the number of notifications within 30 minutes and the denominator is the total of incidents detected.
Scope of Data	The range of data includes all malicious cyber activity detected by Einstein (E2) and the notification time to that affected agency by the US-CERT team. This information is stored in the system of records, Remedy.
Data Source	Tableau, a graphical reporting tool, is used to pull data from Remedy (our official incident repository) using MySQL query which is maintained by the Helpdesk. This measurement will be reported by the Business Transformation Unit to CS&C Enterprise Performance Management Office.
Data Collection Methodology	The NCCIC Business Transformation Unit (BTU) extracts this number on a monthly and quarterly basis from the incident management system, Remedy. An MS-Excel file is created using the Tableau business intelligence tool, from the SQL database in Remedy. The response data is collected in Remedy through an automated e-mail system that is used to send information to a pre-determined point of contact at the affected agency. The date and time of the response is time stamped in the Remedy database when e-mail notification is sent. This information is used to determine which incidents met the 30 minute notification target for this measure. The results are calculated by taking the difference from the Detected Date and the Submitted Date for the respective date range (e.g., Q1 of FY12), which is the notification time. Once all the notifications times have been calculated, the number of incidents resulting in notification within 30 mins is divided by the total number of incidents.
Reliability Index	Reliable
Explanation of Data Reliability Check	The date time stamps stored in the fields Report Date and Submit Date are computer generated. The formula is entered into Excel and checked by US-CERT leadership and performance management personnel to ensure quality.

Performance Measure	Percent of incidents detected or blocked by EINSTEIN intrusion detection and prevention systems that are attributed to Nation State activity (New Measure)
Program	Cybersecurity
Description	This measure demonstrates the EINSTEIN intrusion detection and prevention systems' ability to detect and block the most significant malicious cyber-activity by Nation States on Federal civilian networks. Nation States possess the resources and expertise to not only develop sophisticated cyber-attacks but sustain them over long periods of time. Thus the indicators that EINSTEIN deploys to detect and block malicious cyber-activity should focus on methods and tactics employed by Nation States. The overall percentage of incidents related to Nation State activity is expected to increase through greater information sharing with partners and improved indicator development, which will result in better incident attribution.

Scope of Data	Performance measure data is based on DHS NCCIC ticketing system (BMC Remedy) data. The specific scope of data for this measure is Remedy incident tickets, created as a result of an EINSTEIN alert, with Focused Operations (FO) designation, which is populated by DHS analysts based on information provided by the indicator creator. Specific FO designations are correlated to nation-state activity. Incident tickets generated based on EINSTEIN detections and blocks are identified by filtering on specific fields. Incidents identified as false positives are excluded. Malicious activity data will NOT be related to a specific Focused Operations number or nation-state actor.
Data Source	The data source is the reporting Microsoft Structured Query Language database copied from the NCCIC ticketing system (currently BMC Remedy).
Data Collection Methodology	A remote data collection method is employed using Tableau to access Remedy data and generate an automated report on all tickets created for EINSTEIN detection and blocking, which have a Focused Operations number populated. The calculation is the number of tickets with a Focused Operations number divided by the total number of tickets generated for the reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	Potential issues for data reliability exist due to difficulties with initial attribution to nation-state actors. This function is executed through a documented work instruction that is updated annually, or as required, and quality assurance checks are performed daily by team leads. Many of the indicators used for this measure are received from trusted external partners.

Performance 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
Program	Cybersecurity
Description	This performance measure assesses the extent to which DHS has contractually made available Continuous Diagnostics and Mitigation (CDM) tools to monitor events on their networks to participating federal civilian executive branch agencies. Once DHS has made the tools available through contract award, agencies must still take action to deploy and operate CDM on their networks. By making CDM tools available to agencies, they will be able to more effectively manage coordinated threats to their network.
Scope of Data	The scope of the data includes all available data from the Federal Agencies participating in CDM Phase 3. The parameters used to define the data included in this measure are the number of agencies with signed Memoranda of Agreement (MOA) to participate in CDM and are included in the task order groupings to have CDM Phase 3 tools and services delivered. The scope captures progress in achieving delivery of CDM Phase 3 tools and services to agencies so that they can monitor their networks and better understand what is happening on their network.
Data Source	The Office of Cybersecurity and Communications' CDM Program Office will track CDM Blanket Purchase Agreement Task Orders for Phase 3 progress via contract deliverables and progress reports provided by Continuous Monitoring as a Service (CMaaS) providers to the contracting officer at General Services Administration Federal Systems Integration and Management Center (GSA FEDSIM). Each event is captured directly in contract documentation for each participating agency on a monthly basis. Signed MOAs are documented by the CDM Program Office and updated as changes occur.
Data Collection Methodology	The GSA Federal Systems Integration and Management Center provides monthly reports on Phase 3 contracts. These reports are analyzed by the CDM Program Office and data for this measure are documented. The CDM Program Office measures the number of agencies with signed MOAs that have had CDM Phase 3 tools and services delivered through contract award. The measure is calculated by dividing the total number of agencies with signed MOAs with Phase 3 delivered by the total number of agencies with signed MOAs participating in CDM Phase 3.

Reliability Index	Reliable
Explanation of Data Reliability Check	The CDM Program Office will validate and accept each contract deliverable after a review for completeness and accuracy.

Performance Measure	Percent of performance standards implemented by the highest risk chemical facilities and verified by DHS
Program	Infrastructure Protection
Description	This measure reports the percent of applicable risk based performance standards (RBPS) that are approved and implemented within site security plans (SSPs) or alternative security programs (ASPs) for Tier 1 and Tier 2 facilities that are compliant with the Chemical Facility Anti-terrorism Standards (CFATS) regulation. Following submission of a proposed SSP/ASP by a covered facility, the CFATS regulatory authority will conduct an "authorization inspection" of the covered facility to verify that the SSP/ASP is compliant with the CFATS regulation. For this measure, SSPs/ASPs determined to meet the RBPS requirements with current and planned measures will be approved. Upon approval of its SSP/ASP, the covered facility is required to fully implement the existing measures that are described in the SSP/ASP.
Scope of Data	The scope of this data includes all of the chemical facilities that have been given a risk based classification of Tier 1 or 2. The number of facilities identified as Tier 1 or 2 changes over time.
Data Source	Reported data are the resulting summaries from queries against internal systems and are stored in the Chemical Security Assessment Tools Suite (CSATs). CSATs is used to provide facility identification and registration, to identify facilities that meet the Department's criteria for high risk chemical facilities, and store the methodologies to record and initially evaluate security vulnerability assessments (SVAs) and to create and store respective site security plans (SSPs) and alternate security programs (ASPs). CSATs is a secure web-based system.
Data Collection Methodology	High-risk chemical facilities provide originating source data via the CSATs system. Infrastructure Security Compliance Division (ISCD) HQ staff and inspection cadre posts added information and status to the CSATs system that includes Chemical Security Evaluation and Compliance System (CHEMSEC) applications as a course of normal operations. The success percentage for this measure will be based upon: the number of approved RBPS measures of Tier 1 and Tier 2 regulated facilities that have been implemented (existing and planned with past completion dates). This number does not include those planned RBPS with future completion dates. This number is then divided by the total number of applicable RBPS measures for facilities receiving a final tiering letter (tiers 1-2 inclusive) (TRBPSFTL). Formula: Approved and Implemented RBPS (Tiers 1 and 2) ÷ TRBPSFTL (Tier 1 + Tier 2) = %. Additional details on the calculation methodology are available in ISCD's GPRA Measure Guidance.
Reliability Index	Reliable
Explanation of Data Reliability Check	The accuracy of data captured and reported via the CSATs system is validated during the Systems Engineering Life Cycle (SELC) phases (deployment readiness and testing). Information is reviewed by Infrastructure Security Compliance Division Director/Deputy Director, leadership at the Office of Infrastructure Protection, and NPPD leadership.

Performance Measure	Percent of respondents indicating that operational cybersecurity information products provided by DHS are helpful
Program	Cybersecurity
Description	This measure assesses whether the products that the DHS National Cybersecurity and Communications Integration Center (NCCIC) provides are helpful for its customers. A customer survey will be used to acquire data on how helpful information provided by the NCCIC is for its stakeholders.

Scope of Data	This measure is limited to customer feedback from a survey covering the Office of Cybersecurity and Communications' (CS&C) NCCIC information products.
Data Source	The data source for this performance measure is a customer feedback survey available across the www.us-cert.gov web pages used by the NCCIC and its DHS components. The survey contains the standard Departmental question intended to elicit the degree of customer satisfaction with the helpfulness of the product. The questions asks customers to answer "Was the information helpful?" on a four-point rating scale (yes, somewhat, no, not applicable). A "yes" response will be considered to have met the criteria for "helpful." NPPD will aggregate the results obtained based on the survey metadata, and maintain the results in the NCCIC Business Transformation Unit and the CS&C Enterprise Performance Management Office.
Data Collection Methodology	Each quarter, the NCCIC will disseminate a customer satisfaction survey to the following stakeholder groups: Critical infrastructure owners and operators, Federal agency Security Operations Centers, and State and local Chief Information Security Officers and their staff. The survey sent to these specific stakeholder groups will have a unique identifier attached to the response in order to control for public access to the survey. Only those surveys with the unique stakeholder identifier will be analyzed for this measure. One question is used to collect data for this measure: "Was the information helpful?" In addition to collecting feedback through disseminated surveys, a sample of NCCIC stakeholders will be interviewed each quarter during customer feedback sessions, which will include the use of the survey. The Paperwork Reduction Act number for this survey is 1601-0014.
Reliability Index	Reliable
Explanation of Data Reliability Check	Survey responses will be collected and maintained by NCCIC Business Transformation Unit, US Computer Emergency Response Team Communications, and CS&C Enterprise Performance Management Office (EPMO) and shared with relevant CS&C divisions and programs in the ordinary course of business. Data will be validated by program manager reviews in relevant divisions and programs and by the EPMO Performance Management branch.

Performance Measure	Percent of respondents reporting that DHS critical infrastructure information will inform their decision making on risk mitigation and resilience enhancements
Program	Infrastructure Protection
Description	This measure will report the percent of critical infrastructure partners who participated in education, training, exercise, and information sharing activities developed or coordinated by the Office of Infrastructure Protection and indicated that the information and products received are useful for informing their risk management programs and influencing future decision-making regarding safety and/or security improvements and/or resilience enhancements at their facilities. Active outreach efforts and effective public-private partnerships on critical infrastructure issues help to reduce risk and increase resilience across the country.
Scope of Data	The scope includes quantifiable feedback received from critical infrastructure partners participating in sector-specific and cross-sector education, training, exercise, and information sharing activities conducted or coordinated by the Sector Outreach and Programs Division (SOPD). The activities include, but are not limited to webinars, facilitated workshops, seminars, instructor-led courses, computer-based training, tabletop exercises, and information products such as technical guidelines, handbooks, and recommended practices. This measure includes a range of activities developed and implemented for the six sectors led by the Office of Infrastructure Protection, which include chemical, commercial facilities, critical manufacturing, dams, emergency services, and nuclear sectors, as well as cross-sector engagements with local, state, and regional partners.

Data Source	The data supporting this measure come from feedback from public and private critical infrastructure partners participating in SOPD activities and programs. Activity evaluation forms are systematically collected by individual Sector Specific Agencies (SSA) corresponding to the six sectors led by the Office of Infrastructure Protection as well as personnel involved in cross-sector education, training, exercise, and information sharing activities. The information is reviewed and consolidated by SOPD front office personnel into a standard tracking database developed using Microsoft Excel. The database is owned and maintained by the SOPD Front Office.
Data Collection Methodology	Data collection is conducted through voluntary submissions of standardized evaluation forms that are made available to public and private critical infrastructure partners distributed and collected at the conclusion of education, training, exercise, and information sharing activities. Individual feedback is quantified using a standard 5-level Likert scale, in which the potential responses range from "Strongly Disagree" to "Strongly Agree." The measure is calculated as the number of respondents answering “Agree” or “Strongly Agree” with the statement that, "The information received in the activity or product will effectively inform my decision making regarding safety and security risk mitigation and resilience enhancements” and then divided by the total number of respondents.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data will be collected by SOPD designated personnel in coordination with the IP Strategy and Policy Office (Measurement and Reporting). The corresponding SOPD branch chiefs will be responsible for the validity of the data collected and generated in support of this measure. SOPD Front Office personnel will be responsible for working closely with project and activity leads to develop standard operating procedures for data collection, consolidation, and storage. Periodic quality checks will be conducted to identify anomalies or missing values and ensure data accuracy and reliability.

Performance Measure	Percent of significant (critical and high) vulnerabilities identified by DHS cyber hygiene scanning of federal networks that are mitigated within the designated timeline (New Measure)
Program	Cybersecurity
Description	This measure calculates the percent of significant (critical and high) vulnerabilities identified through 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. DHS provides cyber hygiene scanning to agencies to aid in identifying and prioritizing vulnerabilities based on their severity for agencies to make risk based decisions regarding their network security. Identifying and mitigating the most serious vulnerabilities on a network in a timely manner is a critical component of an effective cybersecurity program.
Scope of Data	The scope of data for this measure is all significant (critical and high) vulnerabilities identified by cyber hygiene scanning on federal networks that were either mitigated during, or were active greater than or equal to the designated timeline for mitigation (15 days for critical; 30 days for high) during the measurement period. The timeline begins when a critical or high vulnerability is first detected on a scan and it ends when the critical or high vulnerability is no longer visible on the scan.
Data Source	The data source is a data storage on a client access license (CAL) that is maintained by the cyber hygiene scanning team.

Data Collection Methodology	An analyst will identify the range of vulnerabilities for the reporting period according to the measure scope. Data analysis software will be used to run a report on the percentage of criticals and highs that were mitigated within the designated timeline. The total number of critical and high vulnerabilities, as well as the number of each mitigated within the designated timeline will be reported each quarter. The cumulative result will be calculated using the following formula: (# of Critical Vulnerabilities mitigated within 15 days) + (# of High Vulnerabilities mitigated within 30 days) divided by (Total # of Critical and High Vulnerabilities).
Reliability Index	Reliable
Explanation of Data Reliability Check	The Cyber Hygiene Scanning team within the National Cybersecurity Assessments and Technical Services (NCATS) division will review the algorithm to query the data and the quarterly result for this measure to ensure correct data collection and calculation procedures were used. NPPD Strategy, Policy, and Plans will also review the quarterly results and accompanying explanations prior to final submittal to DHS.

Performance 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
Program	Emergency Communications
Description	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. The result is calculated by identifying the number of States and Territories scoring a "4" or "5" on a 5-point scale where1 indicates little-to-no capability and 5 indicates that they have all or nearly all of the Operational Communications capabilities required to meet their targets. That number forms the numerator, which is divided by 56 and multiplied by 100 to achieve the percentage.
Scope of Data	Data is from the Threat and Hazards 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. Each of the 56 States and Territories must, as a pre-condition for receiving DHS preparedness grant funds, complete this process.
Data Source	As part of the broader Threat and Hazards Identification and Risk Assessment (THIRA) and State Preparedness Report (SPR) process, through the State Administrative Agency (SAA), each State and Territory works with the jurisdictions within their boundaries to assess their present levels of Operational Communications capabilities relative to the target capabilities set forth in their THIRA. Data is reported to FEMA annually using a standardized format (the THIRA-SPR Unified Reporting Tool). The THIRA is a four step common risk assessment process that maps risks to a defined set of Core Capabilities; one is "Operational Communications."

Data Collection Methodology	Through the THIRA, each State and Territory is required to establish a target capability level which reflects the highest capability level they may need based on their identified threats and hazards. Within the SPR, each State and Territory is required to rate their current capabilities on a scale of 1 (little-to-no capability) to 5 (have all or nearly all of the Operational Communications capabilities required to meet their targets). Annually, each jurisdiction sets a Target score and Capability Assessment score. Participants update target levels of performance specific to their jurisdiction for each of the 31 core capabilities and then assess their ability to meet those unique targets. The percent increase in operational communications capabilities is calculated by taking the total number of States and Territories that have a rating of "4" or "5 " and dividing the total by 56 (the total number of States & Territories) and multiplied by 100 to achieve the percentage.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data is collected by FEMA and shared with OEC who compile the performance results. CS&C Enterprise Performance Management Office receives the performance results on an annual basis and maintains a standard operating procedure to check performance results against underlying data sources.

Performance Measure	Percent of survey respondents that were satisfied or very satisfied with the timeliness and relevance of cyber and infrastructure analysis based products
Program	Integrated Operations
Description	The Office of Cyber and Infrastructure Analysis (OCIA) produces infrastructure analytic products for DHS customers to make meaningful risk investment and resource allocation decisions in both crisis and steady state environments in order to reduce the impacts of infrastructure disruptions. In order for our customers to apply the knowledge gained from our products they must have the right information in a timely manner to inform decisions. Survey respondents comment on their level of satisfaction with both timeliness and relevance (two separate questions) of OCIA's analytic products which, in turn, provides OCIA with feedback that will be used to improve future products. OCIA averages the two responses for one metric. This is relevant to OCIA achieving its mission since the purpose of OCIA's analytic products are to inform decision-makers. Their feedback matters to the core of OCIA's purpose and is important to help OCIA gauge its progress toward accomplishing its mission.
Scope of Data	The data is pulled from feedback surveys that are attached to OCIA products and are voluntarily submitted electronically to OCIA. The number of survey results is limited to 1100 respondents per the OMB (Office of Management and Budget) approval on the Paperwork Reduction Act (PRA) approval form (OMB Control Number 1670-0027). Sampling is not used and the data is compiled and then presented as a cumulative result for the quarter and cumulative result for the fiscal year.
Data Source	Surveys are submitted to a centralized inbox on a voluntary basis from stakeholders that received OCIA products. The inbox is managed by the OCIA Office of Management Operations. These surveys are archived on the DHS Shared Drive folder with restricted access. The Performance Analyst then records survey feedback in an Excel spreadsheet by assigning number values to the quantitative feedback in order to aggregate the responses and run percentages. The analyzed data is then presented in a PowerPoint presentation and stored on the DHS Shared Drive.

Data Collection Methodology	Performance analyst imports the survey responses into Excel and conducts analysis to obtain percentages of respondents satisfied with both timeliness and relevance. The percentage of customers who are satisfied or very satisfied is calculated by summing the number of respondents who were "satisfied" or "very satisfied" with both timeliness and relevance and dividing by the total number of respondents. Surveys with an "N/A" response to either question are discarded. For example, if 1 customer reports "very satisfied" with timeliness but "somewhat dissatisfied" with relevance, 1 customer reports "somewhat satisfied" with timeliness but "N/A" for relevance, and 4 customers report "satisfied" or "very satisfied" with both timeliness and relevance, then 4 out of 5 responses meet the requirement for a result of 80%. Performance Analyst creates metrics report in PowerPoint to present to OCIA leadership on a quarterly basis or as requested by OCIA leadership.
Reliability Index	Reliable
Explanation of Data Reliability Check	Once the SPP analyst records and analyzes the data in Excel, there is a second analyst to cross-check the data entry and analysis and provide a peer review to check for accuracy.

Performance Measure	Percent of traffic monitored for cyber intrusions at civilian Federal Executive Branch agencies (Retired Measure)
Program	Cybersecurity
Description	This measure assesses DHS's scope of coverage for malicious activity across those non-DOD Chief Financial Officers (CFO) Act and Trusted Internet Connection Access Provider (TICAP) Federal Executive Branch civilian agency networks. Federal Executive branch network monitoring uses EINSTEIN 2 intrusion detection system sensors, which are deployed to Trusted Internet Connections locations at agencies or Internet Service Providers. These sensors capture network flow information and provide alerts when signatures, indicative of malicious activity, are triggered by inbound or outbound traffic. The federal government's situational awareness of malicious activity across its systems will increase as more networks are monitored and the methodology will require data normalization to account for the addition of large numbers of networks.
Scope of Data	The measure includes the non-DOD CFO Act agencies and the TICAP Federal Executive Branch civilian agencies. Percentage is determined by compiling and averaging estimates provided by the Departments and Agencies (D/As) of percent of total traffic monitored on their respective networks. The individual percentages are currently reported to OMB.
Data Source	From data reported to NCSD from the agencies.
Data Collection Methodology	For TICAP locations with operational sensors: Once EINSTEIN installations are successfully tested (including a formal Installation Test & Checkout Review) notification is provided to the respective program managers. The number of installations is tracked and published by NCPS program managers. For D/As percentage of traffic monitored (consolidated): Each TICAP Agency currently tracks and reports the estimated percent of traffic consolidated (monitored) to DHS on a yearly basis. DHS also tracks each CFO Act Agency that obtains EINSTEIN 2 coverage through an Internet Service Provider. EINSTEIN is already fully deployed and operational at each Internet Service Provider. Tracking for these agencies is binary--the information provided to DHS indicates either 100% consolidation through the ISP or 0% consolidation. DHS reports TICAP and non-TICAP CFO Act agency information to OMB on an individual D/A basis.
Reliability Index	Reliable
Explanation of Data Reliability Check	The completion of EINSTEIN installations are validated by the respective program managers during the review process. The percentage of traffic consolidated (monitored) is a best-effort estimate provided by the respective D/As to DHS and OMB.

Science and Technology Directorate

Performance Measure	Percent of Apex technologies or knowledge products transitioned to customers for planned improvements in the Homeland Security Enterprise
Program	Research, Development, and Innovation
Description	This measure gauges the transition of high priority, and high value research and development projects known as Apex projects. Apex technologies and knowledge products are quickly delivered to improve homeland security operations. Apex products consist of cross-cutting, multi-disciplinary efforts which employ 3 to 5 year innovation cycles from project inception through operational testing.
Scope of Data	This measure encompasses the Apex technology or knowledge products to be transitioned as determined by the Homeland Security Advanced Research Projects Agency (HSARPA) and Support to the Homeland Security Enterprise and First Responders Group (FRG) leadership prior to the beginning of the fiscal year. A successful transition is considered to be the ownership and/or operation of a technology or knowledge product by a customer within the Homeland Security Enterprise. When applicable, this includes transition outcomes specifically from Apex engines, which provide a centralized pool of solution development resources for Apex projects and the broader S&T organization.
Data Source	The system of record is the quarterly data call spreadsheet submitted by the HSARPA and FRG front offices to the S&T Performance Team through the S&T ExecSec process. This spreadsheet is completed by both HSARPA and FRG, then provided back to the S&T Performance Team for review and management.
Data Collection Methodology	The status of each transition of Apex technology or knowledge product is gathered from the individual divisions within HSARPA and FRG from a variety of sources including final reports, test or pilot results collected during trials, and various reviews (technology reviews and portfolio reviews); HSARPA and FRG senior leadership are briefed on end results, metrics, current status, go/no go decisions, as well as milestone success. For the percent result of this measure, the total number of Apex technologies and/or products transitioned (numerator) is divided by the total number of planned Apex technologies and/or products to be transitioned within the fiscal year (denominator), then multiplied by 100. This information is captured in a quarterly data call spreadsheet submitted by HSARPA and FRG to the S&T Performance Team.
Reliability Index	Reliable
Explanation of Data Reliability Check	Following the collection and analysis of data by program managers and divisions, the Directors of HSARPA and FRG review the data to ensure accuracy and consistency, approve the status, and submit the data to the Science and Technology's Performance Team within the Finance and Budget Division's Budget and Performance Branch. The S&T Performance Team provides a third data reliability review before results are finalized and submitted to DHS.

Performance Measure	Percent of planned cybersecurity products and services transitioned to government, commercial and open sources
Program	Research, Development, and Innovation
Description	This measure reflects the percent of identified and completed planned transitions of cybersecurity products and/or services (e.g. technologies, tools, capabilities, standards, knowledge products) within Science & Technology Directorate's Cyber Security Division projects to government, commercial or open sources. The percent reported is reviewed using the number of planned transition milestones stated in the Cyber Security Division's budget execution plan for the fiscal year, and the explanation that is provided in each quarterly performance data call. The Program identifies, funds, and coordinates cyber security research and development resulting in deployable security solutions. These solutions include user identity and data privacy technologies, end system security, research infrastructure, law enforcement forensic capabilities, secure protocols, software assurance, and cybersecurity education.
Scope of Data	This measure encompasses the transitions of cybersecurity products and/or services expected by the Science & Technology Directorate's Cyber Security Division (CSD) prior to the beginning of the fiscal year. A successful transition is considered to be the ownership and operation of a technology or knowledge product by a customer within the Homeland Security Enterprise. A "transition" may include, but is not limited to completion/delivery of a product, capability or service, release of a knowledge product, publication of standards, demonstration of a capability. During Q4 of each fiscal year, CSD works with the S&T Performance Team to identify expected transitions for the upcoming Fiscal Year. Once defined, that number serves as the baseline denominator for the measure for the given fiscal year.
Data Source	The source of the data is the individual project schedules and planning documents maintained by each Program Manager and their Systems Engineering and Technical Assistance support contractor. The system of record is the quarterly data call spreadsheet completed and submitted by the CSD front office to the S&T Performance Team through the S&T ExecSec process. This spreadsheet is completed by the CSD front office and provided back to the S&T Performance Team for review and management.
Data Collection Methodology	The CSD Front Office requests feedback from the applicable Program Managers during quarterly performance data calls from the S&T Performance Team, and the Program Managers indicate whether the transition has occurred. If on-going and the transition is still likely to occur, Program Managers provide the expected quarter of completion within the subject fiscal year. If a transition will not occur during the given fiscal year, the Program Manager provides details as to why not (e.g., delays due to development or budget). For the percent result of this measure, the total number of CSD products and/or services transitioned (numerator) is divided by the total number of planned CSD products and/or services to be transitioned within the fiscal year (denominator), then multiplied by 100. This information is captured in a quarterly data call spreadsheet submitted by CSD front office to the S&T Performance Team.
Reliability Index	Reliable
Explanation of Data Reliability Check	Following the collection and analysis of data by program managers, the Director of CSD reviews the data to ensure accuracy and consistency, approves the status, and submits the data to the Science and Technology's Performance Team within the Finance and Budget Division's Budget and Performance Branch. The S&T Performance Team provides a third data reliability review before results are finalized and submitted to DHS.

Transportation Security Administration

Performance Measure	Average number of days for DHS Traveler Redress Inquiry Program (TRIP) redress requests to be closed
Program	Aviation Screening Operations
Description	This measure describes the average number of days for the processing of traveler redress requests, excluding the time for the traveler to submit all required documents. DHS TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs or crossing U.S. borders. DHS TRIP is part of an effort by the Departments of State and Homeland Security to welcome legitimate travelers while securing our country from those who want to do us harm. This measure indicates how quickly the program is providing redress to individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs or crossing U.S. borders.
Scope of Data	The scope of this measure is all closed cases for each month from the time DHS TRIP receives a complete redress application—one that includes all required documents to the time DHS TRIP closes that application (i.e., all processing/analysis has been completed and the applicant has been provided a final response letter). The amount of time does not include the time requests are pending while the applicant provides required documents. Sampling is not used in this process; the calculation is based on 100% of the cases that meet the criteria.
Data Source	The source of the data is the Redress Management System (RMS), a database which tracks all redress requests received via the DHS internet portal, e-mail, and by regular mail. Civil Rights and Liberties, Ombudsman, and Traveler Engagement division owns the database.
Data Collection Methodology	Redress program specialists pull data from the Redress Management System using existing reports of closed cases that show the average amount of time it is taking to close a case. The timeliness metric measures time DHS TRIP receives a complete redress application—one that includes all required documents to the time DHS TRIP closes that application (i.e., all processing/analysis has been completed and the applicant has been provided a final response letter). The amount of time does not include the time the applicant takes to provide required documents. The final number represents the average amount of time it takes DHS TRIP to close a case. The number is reported to TSA and DHS senior leadership on a monthly and quarterly basis.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data is auto generated from the Redress Management System and redress program specialists double checks the work to pull the data. The Director and Operations Manager review daily reports to ensure the data is complete and accurate. These reports include the given measure along with other measures/indicators that assist with corroboration.

Performance Measure	Percent of air carriers operating from domestic airports in compliance with leading security indicators
Program	Other Operations and Enforcement
Description	This measure identifies air carrier compliance for U.S. flagged aircraft operating domestically with leading security indicators. These critical indicators are derived from security laws, rules, regulations, and standards. A leading security indicator is a key indicator that may be predictive of the overall security posture of an air carrier. Identifying compliance with the key indicators assesses air carrier's vulnerabilities and is part of an overall risk reduction process. Measuring compliance with standards is a strong indicator of system security.

Scope of Data	The scope of this measure includes all U.S. passenger-only carriers subject to Transportation Security Administration transportation rules and regulations.
Data Source	Air carrier inspection results are maintained in the Performance and Results Analysis System (PARIS), which serves as the official source of data repository for the Office of Compliance's Regulatory activities.
Data Collection Methodology	Compliance Inspections are performed in accordance with an annual work plan. That plan specifies frequencies and targets for inspection based on criteria established by the Office of Compliance. When inspections are completed, the results are entered into the Performance and Results Information System which and are subsequently used to calculate the results for this measure. The result for this measure is reported quarterly and annually and is calculated as the total of "in compliance" inspections divided by the total inspections for the reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data reliability is ensured through a series of actions. There are system record tracking audit trails and spot audit checks, followed by a management review and validation process at the headquarters level.

Performance Measure	Percent of attended interchanges of rail cars containing rail security sensitive materials transiting into or through high-threat urban areas (New Measure)
Program	Other Operations and Enforcement
Description	This measure identifies the level of attended high risk railcars interchanged between freight railroad carriers, freight rail hazardous materials shippers, and freight rail hazardous receivers in highly populated areas. An attended interchange of rail cars is a loading/offloading of hazardous freight between RSSM rail carrier to carrier, RSSM rail carrier to receiver, and RSSM shipper to carrier. TSA personnel regularly witness these exchanges as part of their compliance inspections. The secure transfer of custody of these rail cars strengthens transportation security and potentially impacted populations at these critical points in the freight rail supply chain.
Scope of Data	The scope of this measure includes all RSSM interchanges which are witnessed by TSA Compliance personnel. These interchanges occur between RSSM rail carrier to carrier, RSSM rail carrier to receiver, and RSSM shipper to carrier. TSA Compliance personnel witness interchanges at established (high risk) freight rail interchange points throughout their area of operations based on guidelines and frequencies established at the beginning of each fiscal year.
Data Source	Data for this measure is documented and maintained within the Performance and Results Information System (PARIS).
Data Collection Methodology	All Compliance inspections are entered into the Performance and Results Information System; this data is then used to calculate the results of this performance measure. The result of this measure will be calculated by the percentage of inspected security measures relating to the chain of custody and control requirements that were determined to be “In Compliance” with the Code of Federal Regulations. Out of the total planned operations established at the beginning of each fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data reliability is ensured through a series of actions. The process of entering a record into PARIS requires review and approval by a TSA official who has been delegated that authority, generally a first line supervisor, Assistant Federal Security Director – Inspections, or other individual exercising management authority. These inspections are also randomly reviewed as part of additional quality control measures by Surface Regional Security Inspectors.

Performance Measure	Percent of daily passengers receiving expedited physical screening based on assessed low risk
Program	Aviation Screening Operations
Description	This measure gauges the percent of daily passengers who received expedited physical screening because they meet low risk protocols or have been otherwise assessed at the checkpoint as low-risk. TSA PreCheck incorporates modified screening protocols for eligible participants who have enrolled in the TSA PreCheck program as well as other known populations such as known crew members, active duty service members, members of Congress and other trusted populations. In an effort to strengthen aviation security while enhancing the passenger experience, TSA is focusing on risk-based, intelligence-driven security procedures and enhancing its use of technology in order to focus its resources on the unknown traveler.
Scope of Data	The scope of this measure is the percentage daily of passengers who received expedited screening out of the total nationwide airport throughput based on assessed low risk either through TSA PreCheck, Known crewmember (KCM), Managed Inclusion, or some other form of expedited screening process out of the total number of daily passengers. Known Suspected Terrorists are always ineligible, as well as those listed on the PreCheck Disqualification Protocol.
Data Source	TSA's Performance Management Information System (PMIS) and KCM System.
Data Collection Methodology	Data on individuals who underwent expedited physical screening is collected at each screening lane and entered daily into the PMIS system. Information regarding the number of airline flight and cabin crew personnel is collected automatically within the KCM system and reported by KCM portal location and also entered in PMIS. Daily data runs are completed within the Office of Security Operations and compiled into a daily report. Daily information is also provided for each airport reflecting the number of travelers who received expedited screening based on whether they were designated as lower risk via Secure Flight, or were included via the Managed Inclusion program. Information is generally collected and entered into PMIS for each hour in which the screening lane was in operation, and periodic reports on hourly expedited throughput are generated to gage efficiency of the operation. This information will be is calculated each quarter, with results being reported cumulatively.
Reliability Index	Reliable
Explanation of Data Reliability Check	PMIS data is required to be collected and entered each day for every screening lane in operation. Missing information is immediately flagged for follow-up with the specific airport. Data on individuals eligible for expedited screening from Secure Flight and the number of individuals who actually received expedited screening at the airport allows for daily reliability and accuracy checks. Data anomalies are quickly identified and reported back to the airport for resolution.

Performance Measure	Percent of domestic cargo audits that meet screening standards
Program	Other Operations and Enforcement
Description	This measure gauges the compliance of shippers with cargo screening standards. Enforcing and monitoring cargo screening standards is one of the most direct methods TSA has for overseeing air cargo safety. TSA conducts these audits of shippers based on cargo regulations specified in Title 49 Code of Federal Regulations Part 1540 and these audits include: training, facilities, acceptance of cargo, screening, certifications, identification verification, and procedures. Ensuring successful cargo screening means having a safe, fast flow of air commerce and reduces the risk of criminal and terrorist misuse of the supply chain. The objective is to increase the security posture and compliance rate for each entity conducting domestic cargo screening.
Scope of Data	The scope of this data includes all cargo screening inspections completed by the Transportation Security Inspectors (TSI) at domestic locations.

Data Source	The data to support this measure is contained in the Performance and Results In formation System (PARIS) which serves as the official source of data repository for the Compliance Branch of the Office of Security Operations. Every time an entity is inspected the data is entered into PARIS by the domestic field inspector TSI. All findings are required to be entered into PARIS and tracked.
Data Collection Methodology	TSIs enter the results of every domestic inspection into PARIS. The data for this measure is then calculated based on the reporting form PARIS. The result for this measure is calculated by dividing the total number of successful domestic cargo audits (successful meaning those resulting in no Civil Penalty) divided by the total number of domestic cargo audits.
Reliability Index	Reliable
Explanation of Data Reliability Check	Inspections are completed per the TSI Compliance Work Plan. These inspections are entered into PARIS and are randomly reviewed by the Regional Security Inspectors (RSI) for Cargo for accuracy.

Performance Measure	Percent of foreign airports that serve as last points of departure and air carriers involved in international operations to the United States advised of necessary actions to mitigate identified vulnerabilities in order to ensure compliance with critical security measures (Retired Measure)
Program	Other Operations and Enforcement
Description	This index combines: (1) percent of foreign airports serving as Last Point of Departure (LPD) to the U.S. notified of critical vulnerabilities and accompanying recommendations, and (2) percent of foreign air carriers operating flights from these foreign airports and U.S. air carriers operating from any foreign airport regardless of destination notified of violations of critical regulations and accompanying recommendations/follow-up action. TSA evaluates/documents security at foreign airports with service to U.S., airports from which U.S. air carriers operate, and other sites on a 5-point scale against critical International Civil Aviation Organization (ICAO) aviation and airport security standards. TSA assess compliance with these standards and provides feedback to the host governments for awareness and recommended follow-up action. Identifying and notifying air carriers of non-compliance with critical regulations mitigates air carrier vulnerabilities and reduces risk.
Scope of Data	Airport assessments reflect information collected by Transportation Security Specialists during evaluation of implementation of ICAO aviation security standards at LPD foreign airports with direct service to the U.S. and those airports from which U.S. air carriers operate, regardless of destination. Attention focuses on critical standards across 5 categories: Aircraft & Inflight Security, Passenger & Cabin Bag Screening, Hold Baggage Security, Cargo/Catering Security, and Access Control. Assessment is done using a risk informed approach that includes threat, vulnerability, and consequence ratings: low-risk airports every 3 years; medium-risk airports every 2 years; high-risk airports yearly.
Data Source	The data to support foreign airport assessments is contained in Foreign Airport Assessment Program (FAAP) reports prepared by Transportation Security Specialists (TSSs) following each airport assessment. Completed reports are submitted by the TSSs in Regional Operation Centers (ROCs) to the ROC Managers and stored in a database maintained by the Office of Global Strategies (OGS). Each FAAP report contains data and observations collected during the assessment and highlights any shortfalls in security. Air carrier inspection results are maintained in TSA's Performance and Results Information System (PARIS), which serves as the official data repository for TSA's regulatory activities. The OGS and PARIS databases also store accompanying information indicating that notification of shortfalls was provided to the host government and air carriers following airports assessments and air carrier inspections.

Data Collection Methodology	A standard template is used for collecting/reporting data on airport assessments. Vulnerability ratings are assigned by Global Compliance leadership to ensure consistent application of the ratings from 1 (no shortfalls) through 5 (instances of egregious non-compliance). Results are entered into the OGS database at TSA headquarters. The measure is calculated by OGS headquarters staff who identify airports receiving notification of vulnerability scores of 4 or 5 in any of the critical ICAO standards. Compliance inspections for air carriers are performed according to an annual work plan specifying frequencies/targets for inspection based on criteria established by OGS including risk methodology. Inspection results are entered into PARIS and are used to calculate the data. OGS headquarters staff identify notification/follow-up action with air carriers in question. The index averages the percentage of airports and air carriers notified of non-compliance with leading security indicators.
Reliability Index	Reliable
Explanation of Data Reliability Check	TSSs submit a comprehensive airport assessment report to ROC Managers. Reports are reviewed for quality and consistency and forwarded through senior leadership in Global Compliance to the Assistant Administrator, OGS, for final approval. This process may result in inquiries to a TSA Representative or the TSS for clarifying information. Analysis for strengths and weaknesses, consistency or divergence from other airports, trends, and smart practices also occurs from these reviews. Results are maintained for each assessed airport as well as consolidated into a report of overall security posture of the airports relative to the ICAO standards. Results are also shared with the foreign airport and host government to determine next steps and proposed areas of cooperation and assistance. Data reliability for air carrier assessments is ensured through system record tracking audit trails and spot audit checks followed by a management review and validation process at the headquarters level.

Performance Measure	Percent of foreign last point of departure (LPD) airports that take action to address identified vulnerabilities (New Measure)
Program	Other Operations and Enforcement
Description	This measure gauges the percent of foreign airports that are the last point of departure (LPD) to the United States that implemented corrective or other mitigation strategies to address vulnerabilities identified during security assessments. The Office of Global Strategies (OGS), through coordination and cooperation with international aviation partners, mitigates risk by identifying vulnerabilities at foreign LPD airports, promoting best practices, and developing mitigation strategies to ensure international aviation security. The effectiveness of this program is an acceptable percentage of foreign LPD airports that have taken action to address identified vulnerabilities.
Scope of Data	The scope is all foreign LPD airports visited within the fiscal year that have any identified vulnerabilities. LPD airports that have reported closed identified vulnerabilities or have open vulnerabilities with a corrective action plan or other mitigation strategies within the year are included in the reported data
Data Source	The data source is the Global Risk Analysis and Decision Support (GRADS) Vulnerability Report to determine all open and reported closed vulnerabilities at foreign LPD airports. OGS maintains this database and ensures its accuracy on a constant basis. Furthermore, Global Compliance (GC) and Analysis and Risk Mitigation (ARM) conduct weekly quality control and validation activities to ensure the accuracy of the data entered into the GRADS system.

Data Collection Methodology	As required in the established GRADS Business Rules and the Foreign Airport Assessment Program (FAAP) Standard Operating Procedures (SOP), OGS personnel are required to enter all vulnerabilities identified into the GRADS system for foreign LPD airports. Once a vulnerability has been identified and added into GRADS, status updates include standard updates (regular updates based on continued visits and observations) as well as mitigation updates (corrective action plans or actions taken by host government/aviation partners) are required to track the lifecycle of the vulnerability until resolved. Global Compliance will run a semi-annual report and validate that all identified vulnerabilities, both open and reported closed, have a clear description of the specific vulnerability as well as a defined corrective action plan listed in the status update section, to include any dates observed, expected resolution dates, root cause, and description in the comments section that clearly describes
Reliability Index	Reliable
Explanation of Data Reliability Check	As part of the FAAP process, OGS personnel are required to enter and review every identified vulnerability in the GRADS system. Once the vulnerability has been added into the GRADS system, the Vulnerability Approver in GRADS must approve all vulnerabilities submitted. If the data is incomplete, the Vulnerability Approver must reject the vulnerability and provide comments to justify the rejection in GRADS. In addition, GC Desk Officers and Program Analysts will be responsible to conduct validation reports and quality control reports for OGS senior leadership to track all identified vulnerabilities.

Performance Measure	Percent of international cargo audits that meet screening standards
Program	Other Operations and Enforcement
Description	This measure gauges the compliance of international shippers with cargo screening standards. Enforcing and monitoring cargo screening standards is one of the most direct methods TSA has for overseeing air cargo safety. TSA conducts these audits of shippers based on cargo regulations specified in Title 49 Code of Federal Regulations Part 1540 and these audits include: training, facilities, acceptance of cargo, screening, certifications, identification verification, and procedures. Ensuring successful cargo screening means having a safe, fast flow of air commerce and reduces the risk of criminal and terrorist misuse of the supply chain. The objective is to increase the security posture and compliance rate for each entity conducting domestic cargo screening.
Scope of Data	The scope of this data includes all cargo screening inspections completed by the Transportation Security Inspectors (TSI) at international locations.
Data Source	The data to support this measure is contained in the Performance and Results Analysis System (PARIS) which serves as the official source of data repository for the Compliance Branch of the Office of Global Strategies. Every time an entity is inspected the data is entered into PARIS by the TSI. All findings are required to be entered into PARIS and tracked.
Data Collection Methodology	TSIs enter the results of every domestic inspection into PARIS. The data for this measure is then calculated based on the reporting form PARIS. The result for this measure is calculated by dividing the total number of successful domestic cargo audits (successful meaning those resulting in no Civil Penalty) divided by the total number of domestic cargo audits.
Reliability Index	Reliable
Explanation of Data Reliability Check	Inspections are completed per the Master Work Plan. These inspections are entered into PARIS and are randomly reviewed by the Transportation Security Specialist for Cargo for accuracy.

Performance Measure	Percent of overall compliance of domestic airports with established aviation security indicators
Program	Other Operations and Enforcement
Description	This measure provides the percent of domestic airports assessed that comply with established security standards and practices related to aviation security. Security indicators are key indicators that may be predictive of the overall security posture of an airport. Identifying compliance with the key indicators assesses airport vulnerabilities and is part of an overall risk reduction process. Measuring compliance with standards is a strong indicator of system security.
Scope of Data	The scope of this measure includes all U.S. airports that regularly serve operations of an aircraft operator as described in 49 CFR part 1544 §1544.101(a)(1): "a scheduled passenger or public charter passenger operation with an aircraft having a passenger seating configuration of 61 or more seats".
Data Source	Airport inspection results are maintained in the Performance and Results Information System (PARIS), which serves as the official source of data repository for TSA's Office of Security Operations compliance's Regulatory activities.
Data Collection Methodology	Compliance Inspections are performed in accordance with an annual work plan, which specifies frequencies and targets for inspections based on criteria established by the Office of Security Operations/Compliance. Each inspection is based on a standard set of inspection prompts that are derived from the requirements of 49 CFR 1542. Prompts are the objective means by which TSA assesses the effectiveness of an airport's systems, methods, and procedures designed to thwart attacks against the security of passengers, aircraft, and facilities used in air transportation. Each prompt is phrased in a declarative sentence to provide the Inspector with a Yes/No response. When inspections are completed, the results are entered into PARIS and are used to calculate the results for this measure. The percentage reported represents the total prompts in compliance divided by total inspection prompts, aggregated for all airports subject to the requirement.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data reliability is ensured through a series of actions. The process of entering a record into PARIS requires review and approval by a TSA official who has been delegated that authority, generally a first line supervisor, Assistant Federal Security Director, Manager, team lead, or other individual exercising management authority. Under no circumstances is an inspection, investigation, or incident record be approved by the same individual who created that record. This system of checks and balances provides for improved quality and data integrity.

Performance Measure	Percent of overall level of implementation of industry agreed upon Security and Emergency Management action items by mass transit and passenger rail agencies
Program	Other Operations and Enforcement
Description	This measure provides the rate of implementation by mass transit, light and passenger rail, bus, and other commuter transportation agencies with established security standards and practices related to six critical Security Action Items (SAIs). These six SAIs are key indicators of the overall security posture of a mass transit and passenger rail transportation system. Measuring implementation of these six SAIs assesses transit vulnerabilities and is part of an overall risk reduction process.

Scope of Data	The scope of the data is limited to the largest mass transit and passenger rail systems based on passenger volume (average weekday ridership > 60,000) that have agreed to participate in the Baseline Assessment for Security Enhancement (BASE) program. BASE assessments are completed jointly by a team of Transportation Security Inspectors and participating mass transit and passenger rail systems. The BASE program assesses whether comprehensive Security and Emergency Management Action Items that are critical to an effective security program, including security plans, training, exercises, public awareness, and other security areas, are in place.
Data Source	The source of the data is the assessments completed by a team of Transportation Security Inspectors and transit agencies. Transportation Security Inspectors document assessment results by placing the information in a central database on the TSA computer system, which is analyzed by staff members at Headquarters.
Data Collection Methodology	TSA assesses mass transit and passenger rail modes through the Baseline Assessment for Security Enhancement (BASE) program for 17 Security and Emergency Management Action Items. The 17 Action Items resulted from a coordinated review and update among TSA, Federal Transit Administration, and the Mass Transit Sector Coordinating Council. Action Items cover a range of areas foundational to an effective security program, with emphasis on 6 Security Action Items (SAIs): defined responsibilities for security and emergency management; background investigations of employees and contractors; security training; exercises and drills; using a risk management process to assess and manage threats, vulnerabilities and consequences; and public awareness and preparedness campaigns. Achieving an Effectively Implementing rating requires a score of 70 or higher in each of these six critical SAIs. Periodic review and completion of needed refinements remains a key component of this program.
Reliability Index	Reliable
Explanation of Data Reliability Check	When assessments are completed, findings are entered into a central database and are subsequently used to calculate the results for this measure, which are reviewed and analyzed by staff members at Headquarters to determine trends and weaknesses within the Security and Emergency Management Action Item areas. Quality reviews are performed on assessment data at multiple points in the process. Senior Transportation Security Inspector Program staff and Mass Transit staff perform quality reviews on the BASE assessment reports. These reviews may result in inquiries to clarify information and inconsistencies in evaluation and correct any erroneous data. Findings from these quality reviews are applied to lessons learned and best practices that are incorporated into basic and ongoing training sessions to improve the quality and consistency of the data and data collection process. This system of checks and balances provides for improved quality and data integrity.

Performance Measure	Percent of passenger data submissions that successfully undergo Secure Flight watch list matching
Program	Aviation Screening Operations
Description	This measure will report the percent of qualified message submissions received from the airlines that are successfully matched by the Secure Flight automated vetting system against the existing high risk watch lists. A qualified message submission from the airlines contains passenger data sufficient to allow successful processing in the Secure Flight automated vetting system. Vetting individuals against high risk watch lists strengthens the security of the transportation system.
Scope of Data	This measure relates to all covered flights operated by U.S. aircraft operators that are required to have a full program under 49 CFR 1544.101(a), 4. These aircraft operators generally are the passenger airlines that offer scheduled and public charter flights from commercial airports.
Data Source	The data source is SLA_RAW_DATA table from the SLA database.

Data Collection Methodology	Ad-hoc reports will be created in the Reports Management System to pull both the number of Boarding Pass Printed Results and the number of unique qualified data submissions received from U.S. and foreign aircraft operators out of the Service Level Agreement (SLA) database for a specified date range. These numbers will be compared to ensure 100% of the qualified data submissions are vetted using the Secure Flight automated vetting system.
Reliability Index	Reliable
Explanation of Data Reliability Check	Vetting analysts review a report (produced daily) by the Secure Flight Reports Management System. An analyst then forwards the data to Secure Flight leadership for review. Once reviewed, reports are forwarded to the TSA Office of Intelligence and Analysis management, TSA senior leadership team (SLT), as well as the DHS SLT. It is also distributed to the TSA Office of Security Policy and Industry Engagement, and the TSA Office of Global Strategies.

Performance Measure	Percent of TSA regulated entities inspected per fiscal year by Transportation Security Inspectors
Program	Other Operations and Enforcement
Description	This measure identifies the percent of the regulated entities that have been inspected in a fiscal year. Inspection activity is a key indicator that may be predictive of the overall security posture of an air carrier, indirect air carrier, airports, and certified cargo screening facilities. Identifying compliance with the key indicators assesses an entities vulnerabilities and is part of an overall risk reduction process. Conducting inspections is part of an overall risk reduction process, which leads to a strong indicator of system security.
Scope of Data	The scope of this measure includes all U.S. regulated entities only that are subject to Transportation Security Administration transportation rules and regulations.
Data Source	Regulated entity inspection results are maintained in the Performance and Results Analysis System (PARIS), which serves as the official source of data repository for the Office of Compliance's Regulatory activities. PARIS houses compliance activities completed in accordance with the National Work Plan and accounts for security related activities completed outside of the National Work Plan scope such as incident response and entity outreach.
Data Collection Methodology	Compliance Inspections are performed in accordance with an annual work plan. That plan specifies frequencies and targets for inspections of regulated entities based on criteria established by the Office of Compliance. When inspections are completed, the results are entered into the Performance and Results Information System which and are subsequently used to calculate the results for this measure. The result for this measure is reported annually and is calculated as the total of "inspectable entities" divided by the total number of entities inspected for the reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data reliability is ensured through a series of actions. There are system record tracking audit trails and spot audit checks, followed by a management review and validation process at the headquarters level.

U.S. Citizenship and Immigration Services

Performance Measure	Average of processing cycle time (in months) for adjustment of status to permanent resident applications (I-485)
Program	Immigration Examinations Fee Account
Description	An I-485, Application to Register for Permanent Residence or Adjust Status, is filed by an individual to apply for permanent residence in the United States or to adjust their current status. This measure assesses the program's ability to meet its published processing time goals by reporting on the volume of pending applications and petitions by Center or Field Office.
Scope of Data	This measure is based on the volume in Active Pending status of I-485 applications. Applications are classified in an Active Suspense category if a visa number for an application is not available and the application has been pre-adjudicated or if the case is awaiting additional evidence from the customer. Active Suspense cases are not included in this measure. Active Suspense categories include: Pending Request for Evidence or Intent to Deny/Revoke; Visa Unavailable. Additionally, the measure only includes the aggregate of I-485 Adjustment based on eligibility from Employment, Family, certain Cuban nationals and All Other. It excludes I-485 Adjustment based on Refugee, Asylee or Indochinese Status.
Data Source	Offices self-report data to the USCIS Office of Performance & Quality (OPQ) primarily through the Performance Reporting Tool (PRT). The National Benefits Center (NBC) also sends an import file (text file) to OPQ which contains data on I-485 cases at the NBC. The PRT submissions by the offices, as well as the NBC import file are uploaded into a database.
Data Collection Methodology	On a monthly basis, OPQ collects performance data on I-485 applications received, completed, and pending through PRT and through NBC's import file. The data is then used to calculate the average cycle time, expressed in months relative to the volume of applications/petitions in Active Pending status. The cycle time, reflected in months (e.g. 4.0 months), measures only the pending volume in Active Pending status, deducting from Gross Pending the total volume of cases subject to customer-induced delays and Department of State visa availability, categorized as Active Suspense.
Reliability Index	Reliable
Explanation of Data Reliability Check	OPQ conducts monthly quality control reviews of the data reported to ensure data integrity.

Performance Measure	Average of processing cycle time (in months) for naturalization applications (N-400)
Program	Immigration Examinations Fee Account
Description	An N-400, Application for Naturalization, is filed by an individual applying to become a United States citizen. This measure assesses the program's ability to meet its published processing time goals by reporting on the volume of pending applications by Center or Field Office.
Scope of Data	This measure is based on the volume in Active Pending status of N-400 applications. Applications are classified in an Active Suspense category if the applicant has failed the English/Civics requirement and is waiting the statutory period between testing attempts, if the applicant has requested rescheduling of the required interview, or if the case is awaiting additional evidence from the customer. Active Suspense cases are not included in this measure. Active Suspense categories include: Pending Request for Evidence or Intent to Deny/Revoke and Pending Re-exam as requested by the customer. The measure excludes naturalization applications based on eligibility from service in the Armed Forces of the United States.

Data Source	Offices self-report data to the USCIS Office of Performance & Quality (OPQ) primarily through the Performance Reporting Tool (PRT). The National Benefits Center (NBC) also sends an import file to OPQ which contains data on N-400 non-military cases at the NBC. In addition, the Nebraska Service Center (NSC) submits an Excel report to OPQ for cases associated with spouses of members of the Armed Forces. The PRT submissions by the offices, as well as the NBC import file and the NSC Excel file are uploaded into a database.
Data Collection Methodology	On a monthly basis, OPQ collects performance data on N-400 applications received, completed, and pending through PRT, NBC's import file, and NSC's Excel file. The data is then used to calculate the average cycle time, expressed in months relative to the volume of applications in Active Pending status. The Cycle Time, reflected in months (e.g. 5.0 months), measures only the pending volume in Active Pending status, deducting from Gross Pending the total volume of cases subject to customer-induced delays, categorized as Active Suspense.
Reliability Index	Reliable
Explanation of Data Reliability Check	OPQ conducts monthly quality control reviews of the data reported to ensure data integrity.

Performance Measure	Percent of applications for citizenship and immigration benefits not approved following a potential finding of fraud
Program	Fraud Prevention and Detection Account
Description	This measure reflects the agency's capacity to prevent fraud, abuse, and exploitation of the immigration system, and address systemic vulnerabilities that threaten its integrity. By not approving (denial, abandonment, withdrawal, etc.) benefits to individuals potentially attempting to commit fraud and who were not eligible for a waiver or exemptions, USCIS is actively eliminating vulnerabilities, and identifying ways to continue to deter and prevent fraud in the future. As a result, those instances where benefits are approved should be very low.
Scope of Data	A sample of case management entities that contain Statements of Findings (SOFs) of "Fraud Found" are used for this measure. Sample sizes are taken to achieve or exceed a .05 margin of error. The sample size will be a minimum of 1,000 cases. USCIS limits data to those fraud investigations completed in the previous fiscal year and stored at the National Records Center. The completion of a fraud investigation is followed by additional adjudications processing time and then records transferring time to the National Records Center. Therefore, while many of the fraud investigations may be completed in one fiscal year they may not have final adjudicative decisions made and be permanently stored until the following year.
Data Source	A sample of case management entities will be pulled from the FDNS-Data System (DS) and physical alien files will be reviewed. The results of the review are stored electronically on a SharePoint page and can be produced for review.
Data Collection Methodology	The percentage will be estimated using a sample of cases from the Fraud Detection and National Security Data System (FDNS-DS), which contain Statements of Findings (SOFs) of "Fraud Found". The sample cases will be physically reviewed in order to identify if a benefit was denied. If a benefit was granted after a SOF of "Fraud Found", the reason will be identified. Cases where a legal waiver, statutory exemption, additional information (e.g. Request for Evidence) that overcame the initial finding of fraud, multiple SOFs associated on the same case management entity, or the case was resolved by the courts will be excluded from the final percentage calculation as legitimate exemptions. Pending applications are not included in the calculation.
Reliability Index	Reliable
Explanation of Data Reliability Check	In cases where a benefit was approved after a finding of "Fraud Found", each A-file will be rated by at least two personnel to cross validate the survey results. A third, senior reviewer is available in rare cases where reviewers disagree on the reason for an approved benefit.

Performance Measure	Percent of customers satisfied with the citizenship and immigration-related support received from the National Customer Service Center
Program	Immigration Examinations Fee Account
Description	This measure gauges the overall customer rating of the support received from the National Customer Service Center. This measure is based on the results from the following areas: 1) Accuracy of information; 2) Responsiveness to customer inquiries; 3) Accessibility to information; and 4) Customer satisfaction.
Scope of Data	The National Customer Service Center (NCSC) captures the telephone numbers of incoming calls and the level of service reached by each call. The data is then downloaded into a master file, resulting in a database with approximately 120,000 phone numbers. Duplicate phone numbers and calls with duration of less than one minute are eliminated. The data is then randomized using a query which randomly assigns different values to each record and sorts the records by value. The first 5,000 records are selected. The telephone number data is retrieved for the week preceding the execution of the phone survey so that the target population is contacted for the survey within approximately one week of having called the NCSC 800-Line to capture the customers' most recent experience.
Data Source	Data is captured via phone interview and stored in a Statistical Package for the Social Sciences (SPSS) database.
Data Collection Methodology	On a monthly basis, data is captured from the survey sample. Data is collected using prescribed totals for different categories of callers, and from that month's population a random sample is contacted. The data collection continues until a sufficient number of respondents complete the survey. The survey question that pertains to this measure is "How satisfied were you with your entire experience the last time you called the 800-Line. This includes the recording and any agency representatives." Reports are then generated to calculate the results for this measure.
Reliability Index	Reliable
Explanation of Data Reliability Check	The survey is performed by an independent contractor and the results are reported using standard statistical practices to ensure the appropriate level of confidence.

Performance Measure	Percent of students enrolled in classes under the Citizenship and Integration Grant Program that show educational gains
Program	Immigration Examinations Fee Account
Description	This measure reports on the success of grant recipients to increase knowledge of English necessary for students receiving services under the program to pass the naturalization test. Under the Citizenship and Integration Grant Program, grant recipients are required to use a nationally normed standardized test of English language proficiency for student placement and assessment of progress. This measure evaluates the percentage of students receiving these services who demonstrate an increase in score
Scope of Data	This measure will draw on cumulative English language proficiency test results for Q1-Q3 of the fiscal year; Q4 data is not included due to the lag in the receipt of performance data. The measure will only include results from students who receive services from a grant recipient and were pre- and post-tested.

Data Source	The data source is the Office of Citizenship (OoC) Database Management Tool owned by OoC and is located on the USCIS Enterprise Collaboration Network (ECN). The measure will be tracked using quarterly grant recipient performance reports submitted in MS Excel format. For each permanent resident who receives citizenship instruction and/or naturalization application services under the grant program, each grant recipient must provide information on the services actually provided, including dates of enrollment in citizenship class and pre and post-test scores. These reports are submitted quarterly within 30 days of the conclusion of each quarter. The data contained in each quarterly report is then reviewed, uploaded into the data source, and analyzed by Office of Citizenship program officers.
Data Collection Methodology	Grant recipients complete and submit quarterly reports via email within 30 days of the end of each quarter. The calculation is the total number of students who were pre and post-tested and who scored higher on the post-test divided by the total number of students who were pre and post-tested through Q3.
Reliability Index	Reliable
Explanation of Data Reliability Check	The reliability of this measure will be established through uniform data collection and reporting procedures, ongoing follow-up with grant recipients on information included in the quarterly reports, and through onsite monitoring visits, as necessary. All grant recipients will receive training at the beginning of the performance period on how to complete the quarterly report forms. The Office of Citizenship will provide written feedback on each quarterly report, and will ask grant recipients for clarification if there are questions about information in the reports. The Office of Citizenship will annually conduct onsite monitoring visits to approximately one-third of all new grant recipients. During these visits, program staff members review records (e.g. student intake forms, classroom attendance sheets, student assessment scores, copies of filed Form N-400s, etc.) that were used to compile data for the quarterly reports.

Performance Measure	Percent of workers determined to be "Employment Authorized" after an initial mismatch
Program	Employment Status Verification
Description	This measure assesses the accuracy of the E-verify process by assessing the percent of employment verification requests that are not positively resolved at time of initial review.
Scope of Data	Only E-Verify cases where a Tentative Non-Confirmation (or “initial mismatch”) results in a finding of “Employment Authorized” are within the scope of this measure.
Data Source	Data source for this measure is stored in the Verification Information System (VIS), a USCIS’s centralized composite information system used to verify immigration status from various DHS databases for benefits determination and employment authorization.
Data Collection Methodology	All steps of the E-Verify process are automatically captured in VIS as they occur, and records of each case are made available for reporting purposes. A standardized summary of case outcomes is retrieved quarterly, providing both the numerator and denominator for this measure.
Reliability Index	Reliable
Explanation of Data Reliability Check	E-Verify transaction data are extracted quarterly from the VIS by the contractor that manages VIS. An algorithm is then applied to the data to remove all duplicate and invalid queries. The data are referred to the USCIS Verification Division for review and clearance.

U.S. Coast Guard

Performance Measure	Availability of maritime navigation aids
Program	Operations and Support
Description	This measure indicates the hours that short-range federal Aids to Navigation are available. The aid availability rate is based on an international measurement standard established by the International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) (Recommendation O-130) in December 2004. A short-range Aid to Navigation is counted as not being available from the initial time a discrepancy is reported until the time the discrepancy is corrected.
Scope of Data	The measure is the hours short range Aids to Navigation were available as a percent of total hours they were expected to be available.
Data Source	The Integrated Aids to Navigation Information System (I-ATONIS) is the official system used by the U.S. Coast Guard to store pertinent information relating to short-range aids to navigation.
Data Collection Methodology	Trained personnel in each District input data on aid availability in the Integrated Aids to Navigation Information System (I-ATONIS) system. The total time short-range Aids to Navigation are expected to be available is determined by multiplying the total number of federal aids by the number of days in the reporting period they were deployed, by 24 hours. The result of the aid availability calculation is dependent on the number of federal aids in the system on the day the report is run. The calculation is determined by dividing the time that Aids are available by the time that Aids are targeted to be available.
Reliability Index	Reliable
Explanation of Data Reliability Check	To ensure consistency and integrity, data entry in the I-ATONIS system is limited to specially trained personnel in each District. Quality control and data review is completed through U.S. Coast Guard and National Ocean Service processes of generating local Notices to Mariners, as well as by designated Unit and District personnel. Temporary changes to the short-range Aids to Navigation System are not considered discrepancies due to the number of aids in the system on the day the report is run.

Performance Measure	Fishing regulation compliance rate
Program	Operations and Support
Description	The U.S. Coast Guard uses the percentage of fishing vessels observed at sea complying with domestic regulations as a measure of the Coast Guard's activities and their impact on the health and well-being of U.S. fisheries and marine protected species. This specific measure reflects the percent of boardings at sea by the U.S. Coast Guard during which no significant violations of domestic fisheries regulations are detected.
Scope of Data	This measure addresses compliance in and around domestic fisheries. Most inspections take place on U.S. commercial fishing vessels inside the U.S. Exclusive Economic Zone (EEZ), but the measure also includes inspections of (a) U.S. commercial and recreational fishing vessels outside the U.S. EEZ, (b) foreign fishing vessels permitted inside the U.S. EEZ, (c) recreational fishing vessels in the U.S. EEZ, and (d) U.S. commercial and recreational fishing vessels inside the portion of state waters that extends from three to nine nautical miles seaward of the boundary line.
Data Source	Boardings and violations are documented by U.S. Coast Guard Report of Boarding Forms and entered into the Marine Information for Safety and Law Enforcement (MISLE) database.

Data Collection Methodology	U.S. Coast Guard units enter their enforcement data directly into the MISLE database after completion of fisheries enforcement boardings. Each year a compliance rate is calculated for the data quality. This is determined by dividing the total number of Living Marine Resources boardings without a significant number of violations by the total number of Living Marine Resources boardings
Reliability Index	Reliable
Explanation of Data Reliability Check	The program manager reviews entries into MISLE database monthly and compares to other sources of information (i.e., after-action reports, message traffic, etc.) to assess reliability of the database. District, Area, and Headquarters law enforcement staffs review, validate, and assess the data on a quarterly basis as part of the Law Enforcement Planning and Assessment System.

Performance Measure	Interdiction rate of foreign fishing vessels violating U.S. waters (New Measure)
Program	Operations and Support
Description	This measure reports the percent of detected incursions into the U.S. Exclusive Economic Zone (EEZ) by foreign fishing vessels that are interdicted by the Coast Guard. Preventing illegal foreign fishing vessels from encroaching on the Exclusive Economic Zone (EEZ) is a priority for the Coast Guard. Foreign fishing fleets steal a valuable resource, resulting in a total economic loss to the American public. Protecting the integrity of the nation's maritime borders and ensuring the health of U.S. fisheries is a vital part of the Coast Guard mission.
Scope of Data	The measure includes foreign vessels illegally fishing inside the U.S. Exclusive economic Zone (EEZ) detected by the Coast Guard and incursions by foreign fishing vessels reported by other sources, which reports or intelligence are judged by Coast Guard operational commanders as valid enough to order a response. The Magnuson-Stevens Act, Title 16 of the U.S. Code defines terms necessary for identifying an incursion—such as fishing, fishing vessel, foreign fishing, etc.—and establishes an exemption for recreational fishing.
Data Source	Source data is collected from Living Marine Resource Enforcement Summary Reports and recorded in the Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) system.
Data Collection Methodology	Results for a given year are the number of Coast Guard interdictions of foreign fishing vessels expressed as a percentage of the total number of incursions into the U.S. Exclusive Economic Zone (EEZ) by foreign fishing vessels detected by the Coast Guard, or reported by other sources and judged by operational commanders as valid enough to order a response.
Reliability Index	Reliable
Explanation of Data Reliability Check	To ensure consistency and integrity, MISLE data entry is controlled through program logic and pull-down menus that require key elements, prohibit the inappropriate, and limit choices to pre-determined options. The LMR Enforcement Summary Report purpose, format and submission requirements, and guidance on the use of MISLE, are provided in the Maritime Law Enforcement Manual. Comprehensive training and these user guides help ensure reliability, and the application itself contains embedded Help screens. Additionally, District summaries of EEZ cases are reviewed monthly by Areas and submitted to the Coast Guard Office of Maritime Law Enforcement (CG-MLE), and these and other sources of information are used to assess the reliability of the MISLE database.

Performance Measure	Migrant interdiction effectiveness in the maritime environment
Program	Operations and Support
Description	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.

Scope of Data	This measure tracks interdiction of migrants from all nationalities attempting direct entry by maritime means into the United States, its possessions, or territories.
Data Source	Interdiction information is obtained through the U.S. Coast Guard Marine Information for Safety and Law Enforcement (MISLE) database, and Customs and Border Protection records.
Data Collection Methodology	The interdiction rate compares the number of migrants interdicted at sea by U.S. Coast Guard, other law enforcement agencies, or foreign navies, and deceased migrants recovered from smuggling events, to the total number of migrants interdicted at sea plus the migrants that landed in the US, its territories, or possessions. Migrant landing information is obtained through the analysis of abandoned vessels, other evidence of migrant activity that indicate the number of migrants evading law enforcement, successfully landing in the U.S., migrants captured by law enforcement entities in the U.S., and self-reporting by migrants (Cuban migrants are allowed to stay once arriving in the U.S. and typically report their arrival). The U.S. Coast Guard Intelligence Coordination Center compiles and analyzes landing information. Data collection is managed by the Migrant Interdiction Program Manager.
Reliability Index	Reliable
Explanation of Data Reliability Check	The numbers of illegal migrants entering the U.S. by maritime means, particularly non-Cubans, is subject to estimating error due to migrant efforts to avoid law enforcement. Arrival numbers for Cubans tend to be more reliable than other nationalities as immigration law allows Cubans to stay in the US once reaching shore, which encourages self-reporting of arrival. Over the last 5 years, Cubans have constituted approximately one quarter to one half of all maritime migrant interdictions. Migrant landing information is validated across multiple sources using established intelligence rules that favor conservative estimates.

Performance Measure	Number of breaches at high risk maritime facilities (New)
Program	Operations and Support
Description	This measure reports the number of breaches of security incidents at facilities subject to the Maritime Transportation Security Act (MTSA) where no Transportation Security Incident has occurred, but established security measures have been circumvented, eluded or violated. MTSA facilities are a high risk subset of the national waterfront facility population given the nature of their activities and/or the products they handle; which pose a greater risk for significant loss of life, environmental damage, or economic disruption if attacked. MTSA regulated facilities constitute a more than 3400 high-risk subset of all waterfront facilities. They are facilities that handle certain dangerous cargoes, liquid natural gas or transfer oil or hazardous materials in bulk; or receive foreign cargo vessels greater than 100 gross tons, U.S. cargo vessels greater than 100 gross tons carrying certain dangerous cargoes, or vessels carrying more than 150 passengers.
Scope of Data	The scope of this measure includes incidents that occur at any of the more than 3,400 maritime facilities subject to Maritime Transportation Security Act regulation, which are investigated and confirmed incidents where no Transportation Security Incident has occurred, but established security measures have been circumvented, eluded or violated.
Data Source	The data source for this measure is the Coast Guard Marine Information for Safety and Law Enforcement (MISLE) database as a Breach of Security Investigation.
Data Collection Methodology	Qualified Coast Guard Inspectors investigate incidents reported to the National Response Center by MTSA regulated facilities where security measures have been circumvented, eluded or violated. Verified incidents are documented in the Coast Guard Marine Information for Safety and Law Enforcement (MISLE) database as a Breach of Security Investigation. Results for a given year are the total number of confirmed breaches of security that occurred over the past 12-months at any of the more than 3,400 MTSA regulated facilities.

Reliability Index	Reliable
Explanation of Data Reliability Check	To ensure consistency and integrity, MISLE data entry is controlled through program logic and pull-down menus that require key elements, prohibit the inappropriate, and limit choices to pre-determined options. Comprehensive training and user guides help ensure reliability and the MISLE application itself contains embedded Help screens. Data verification and validation is also affected through regular records review by the Office of Investigations and Casualty Analysis (CG-INV) and Coast Guard Program managers.

Performance Measure	Number of detected incursions of foreign fishing vessels violating U.S. waters (Retired Measure)
Program	Operations and Support
Description	This measure is the number of detected illegal fishing incursions into the U.S. Exclusive Economic Zone (EEZ). Incursions detected by both the U.S. Coast Guard and other sources are included when the reports are judged by operational commanders as being of sufficient validity to order resources to respond.
Scope of Data	This measure includes incursions of foreign fishing vessels detected by the U.S. Coast Guard or other sources that results in either: 1) significant damage or impact to U.S. fish stocks (based on volume extracted or status of stock targeted); 2) significant financial impact due to volume and value of target fish stocks; 3) significant sovereignty concerns due to uncertainty or disagreement with foreign neighbors over the U.S. EEZ border. Standard rules of evidence (i.e. positioning accuracy) do not apply in determining detections; if a detection is reasonably believed to have occurred, it is counted. Reports of foreign fishing vessels illegally fishing inside the U.S. EEZ are counted as detections when these reports are judged by operational commanders as being of sufficient validity to order available resources to respond.
Data Source	Data for the measure are collected through the Marine Information for Safety and Law Enforcement (MISLE) system and from U.S. Coast Guard units patrolling the Exclusive Economic Zone. The information is consolidated at U.S. Coast Guard HQ through monthly messages from the Area Commanders.
Data Collection Methodology	Data for the measure are collected through the MISLE system and from U.S. Coast Guard units patrolling the Exclusive Economic Zone. The information is consolidated at U.S. Coast Guard HQ through monthly messages from the Area Commanders. The number of incursions is calculated by including incursions of foreign fishing vessels detected by the U.S. Coast Guard or other sources that results in: significant damage or impact to U.S. fish stocks (based on volume extracted or status of stock targeted); significant financial impact due to volume and value of target fish stocks; significant sovereignty concerns due to uncertainty or disagreement with foreign neighbors over the U.S. EEZ border.
Reliability Index	Reliable
Explanation of Data Reliability Check	The program manager (CG-3RPL) reviews entries into MISLE database monthly and compares to other sources of information (i.e., after action reports, message traffic, etc.) to assess reliability of the database.

Performance Measure	Percent of people in imminent danger saved in the maritime environment
Program	Operations and Support
Description	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. The number of lives lost before and after the U.S Coast Guard is notified and the number of persons missing at the end of search operations are factored into this percentage. Several factors hinder successful response including untimely distress notification to the U.S Coast Guard, incorrect distress site location reporting, severe weather conditions at the distress site, and distance to the scene.

Scope of Data	One hundred percent of the maritime distress incidents reported to the U.S. Coast Guard are collected in the Marine Information for Safety and Law Enforcement (MISLE) database. The scope is narrowed to include only cases where there was a positive data element in the field lives saved, lives lost before notification, lives lost after notification, or lives unaccounted for. The scope of this data is further narrowed by excluding any case reports with eleven or more lives saved and/or lost in a single incident. Data accuracy is limited by two the rescuer's subjective interpretation of the policy criteria for the data point lives saved (for instance, was the life saved or simply assisted).
Data Source	The data source is the U.S. Coast Guard's MISLE database.
Data Collection Methodology	Operational units input Search and Rescue data directly into the MISLE database. Program review and analysis occurs at the Districts, Area, and Headquarters levels. First, one hundred percent of the maritime distress incidents reported to the U.S. Coast Guard are collected in the MISLE database. Then, these reports are narrowed to include only cases where there was a positive data element in the fields lives saved, lives lost before notification, lives lost after notification, or lives unaccounted for. The scope of this data is further narrowed by excluding any case reports with eleven or more lives saved and/or lost in a single incident, which would overweight and mask other trends. After the data is properly scoped, the percentage of people in imminent danger saved in the maritime environment is calculated by dividing the number of people saved by the total number of people in imminent danger.
Reliability Index	Reliable
Explanation of Data Reliability Check	Checks on data input are made by individual case owners during the case documentation processes. Data is reviewed by the SAR Mission Coordinator either at the District or Sector level. This review occurs when cases are validated during a Search and Rescue case and after a case is concluded when the case is reviewed by individuals formally charged with that review. Data is also verified quarterly by the Headquarters program manager via data extraction and checks for anomalies within the data. The database includes built-in prompts to check questionable data.

Performance Measure	Security compliance rate for high risk maritime facilities (Retired Measure)
Program	Operations and Support
Description	This measure is a leading indicator of maritime facility security and resiliency in our nation’s ports. Compliance of high risk (Maritime Transportation Security Act (MTSA)) facilities is determined based upon finding a major problem during an inspection, requiring a notice of violation or civil penalty. MTSA facilities are a high risk subset of the national waterfront facility population given the nature of their activities and/or the products they handle; which pose a greater risk for significant loss of life, environmental damage, or economic disruption if attacked. This subset is approximately 3,100 facilities. The Coast Guard completes one scheduled and one unscheduled inspection on each facility annually. This measure provides insight into resiliency by verifying MTSA facilities maintain proper access safeguards and exercise approved plans/procedures to prevent and react to security emergencies; making them better suited to resist, adapt, and recover to adversity or disruption.

Scope of Data	MTSA facilities are a high risk subset of the entire national waterfront facility population given the nature of their activities and/or the products they handle; which pose a greater risk for significant loss of life, environmental damage, or economic disruption if attacked. MTSA regulation applies to facilities that: handle dangerous cargoes, liquid natural gas, or transfer oil or hazardous materials in bulk; or receive vessels that: carry more than 150 passengers, are foreign cargo vessels greater than 100 gross tons, or are U.S. cargo vessels greater than 100 gross tons carrying dangerous cargoes as prescribed by Federal Regulations. This does not apply to facilities that have a waiver or exemption including facilities that: are U.S. military, do not store minimum established amounts of dangerous cargoes, are shipyards, or are deemed public access facilities. This measure includes the results from annual Coast Guard security inspections conducted on all MTSA-regulated facilities
Data Source	The data source is Marine Information for Safety and Law Enforcement database (MISLE).
Data Collection Methodology	Results of MTSA compliance examinations and security spot checks are entered into the Marine Information for Safety and Law Enforcement database. Data is collected centrally by a HQ-level office responsible for compliance. The percent is calculated by dividing the number of MTSA facilities who did not receive a notice of violation and/or civil penalty by the total number of MTSA facilities inspected.
Reliability Index	Reliable
Explanation of Data Reliability Check	There is no material inadequacy in the data, i.e., those that significantly impede the use of program performance data by agency managers and government decision makers.

Performance Measure	Three-year average number of serious marine incidents
Program	Operations and Support
Description	This measure reports the three-year average number of Serious Marine Incidents as defined by 46 CFR 4.03-2, which include: death or injury requiring professional treatment beyond first aid, reportable property damage greater than $100,000, actual or constructive loss of certain vessels, discharge of oil of 10,000 gallons or more; or a discharge of a reportable quantity of a hazardous substance.
Scope of Data	This measure reports the three-year average number of serious marine incidents as defined in 46 CFR 4.03-2. Serious Marine Incidents include any marine casualty or accident defined by 46 CFR 4.03-1 which meets defined thresholds. These 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.
Data Source	Serious Marine Incidents are recorded in the Marine Information for Safety and Law Enforcement (MISLE) database
Data Collection Methodology	To obtain serious marine incidents, investigations recorded in the MISLE database are counted. Commercial mariner deaths and injuries include casualties of crewmembers or employees aboard U.S. commercial vessels in U.S. waters. Passenger deaths and injuries include casualties from passenger vessels operating in U.S. waters (disappearances or injuries associated with diving activities are excluded). Oil discharges of 10,000 gallons or more into navigable waterways of the U.S. and reportable quantities of hazardous substances, whether or not resulting from a marine casualty, are included. The three-year average for a given year is calculated by taking the average of the number of serious marine incidents for the most recent three years. Due to delayed receipt of some reports, published data is subject to revision with the greatest impact on recent quarters.
Reliability Index	Reliable

Explanation of Data Reliability Check	To ensure consistency and integrity, MISLE data entry is controlled through program logic and pull-down menus that require key elements, prohibit the inappropriate, and limit choices to pre-determined options. Comprehensive training and user guides help ensure reliability and the application itself contains embedded Help screens. MISLE system quality control, and data verification and validation, is affected through regular review of records by the U.S. Coast Guard Office of Investigations and Analysis. MISLE system quality control, and data verification and validation, is affected through regular review of records by the Coast Guard Office of Investigations and Casualty Analysis.

U.S. Secret Service

Performance Measure	Amount of dollar loss prevented by Secret Service cyber investigations (in millions)
Program	Field Operations
Description	This measure is an estimate of the direct dollar loss to the public prevented due to cyber investigations by Secret Service. The dollar loss prevented is based on the estimated amount of cyber losses that would have occurred had the offender not been identified nor the criminal enterprise interrupted. The measure reflects the Secret Service's efforts to reduce cyber related financial losses to the public.
Scope of Data	This measure is an estimate of the direct dollar loss to the public prevented due to cyber crime investigations by the Secret Service. Error is due to lag time in data entry or corrections to historical data.
Data Source	The Cyber Crimes Loss Prevented measure is collected from the Field Investigative Reporting System (FIRS). This system is used by all Secret Service investigative field offices, and provides a means of record keeping for all case and subject information.
Data Collection Methodology	The Secret Service collects data on its cyber investigations through its case management system known as the Field Investigative Reporting System (FIRS). Data is input to FIRS via Secret Service personnel located in field offices throughout the United States and overseas. Data pertaining to this particular measure (loss prevented) are extracted from FIRS by designated cyber crime case violation codes and the dates these cases were closed. The data is then aggregated up to the highest levels by month, year, office, and Service-wide. This information is then reported through various management and statistical reports to Secret Service headquarters program managers, field offices, and the Department of Homeland Security.
Reliability Index	Reliable
Explanation of Data Reliability Check	FIRS has many features built into it in order to provide the most accurate data possible. Along with the mainframe security features, there are many edit checks built into the applications to ensure the accuracy and validity of the data. Only authorized headquarters and field personnel have access to the applications, and they are governed by specific procedures to input case and arrest data. An annual audit is conducted and recurring verification reports are generated and reviewed to reduce errors and ensure data accuracy.

Performance Measure	Financial crimes loss prevented through a criminal investigation (in billions)
Program	Field Operations
Description	An estimate of the direct dollar loss to the public that was prevented due to Secret Service intervention or interruption of a criminal venture through a criminal investigation. This estimate is based on the likely amount of financial crime that would have occurred had the offender not been identified nor the criminal enterprise disrupted, and reflects the Secret Service's efforts to reduce financial losses to the public attributable to financial crimes.
Scope of Data	This measure reports an estimate of the direct dollar loss prevented due to Secret Service intervention/interruption of a criminal venture through a criminal investigation. Error is due to lag time in data entry or corrections to historical data.
Data Source	The Financial Crimes Loss Prevented measure is collected from the Field Investigative Reporting System (FIRS). This system is used by all Secret Service investigative field offices, and provides a means of record keeping for all case and subject information.
Data Collection Methodology	The Secret Service collects data on its multitude of criminal investigations through its case management system known as the Field Investigative Reporting System (FIRS). Data is input to FIRS via Secret Service personnel located in field offices throughout the United States and overseas. Data pertaining to this particular measure (loss prevented) are extracted FIRS by designated financial crime case violation codes and the dates these cases were closed. The data is then aggregated up to the highest levels by month, year, office, and Service-wide. This information is then reported through various management and statistical reports to Secret Service headquarters program managers, field offices, and the Department of Homeland Security.
Reliability Index	Reliable
Explanation of Data Reliability Check	FIRS has many features built into it in order to provide the most accurate data possible. Along with the mainframe security features, there are many edit checks built into the applications to ensure the accuracy and validity of the data. Only authorized headquarters and field personnel have access to the applications, and they are governed by specific procedures to input case and arrest data. An annual audit is conducted and recurring verification reports are generated and reviewed to reduce errors and ensure data accuracy.

Performance Measure	Number of cyber mitigation responses
Program	Field Operations
Description	This measure represents the number of cyber mitigation responses provided by the U.S. Secret Service (USSS). The USSS responds to organizations that suspect a malicious network intrusion has occurred and implements mitigation responses to secure the network(s). Each cyber mitigation response involves one or more of the following activities related to a particular network intrusion: identifying potential victims/subjects, notifying victims/subjects, interviewing victims/subjects, confirming network intrusion, supporting mitigation of breach activity, and retrieving and analyzing forensic evidence. State or federal arrests resulting from and/or related to these intrusions are measured separately.
Scope of Data	Performance data is based on the number of cyber mitigation responses conducted by the USSS within the given reporting period.
Data Source	The scope of this measure includes all cyber mitigation response data is collected from an application in the Field Investigative Reporting System (FIRS) called the Network Intrusion Action Center (NIAC). This system is used by all USSS investigative field offices and provides actionable intelligence for network defense.

Data Collection Methodology	Data pertaining to this measure is extracted from the NIAC system on a quarterly basis and aggregated by the quarter and fiscal year entered. This information is then reported through various management and statistical reports to USSS headquarters program managers, field offices, and the Department of Homeland Security.
Reliability Index	Reliable
Explanation of Data Reliability Check	Only authorized USSS personnel have access to the applications. Once the data has been aggregated, it is double checked for verification and to ensure data accuracy.

Performance Measure	Number of financial accounts recovered (in millions)
Program	Field Operations
Description	This measure represents the number of financial accounts recovered during cyber investigations. Financial accounts include bank accounts, credit card accounts, PayPal and other online money transfer accounts.
Scope of Data	This measure represents the number of financial accounts recovered during cyber investigations.
Data Source	The Financial Accounts measure is collected from the Field Investigative Reporting System (FIRS). This system is used by all Secret Service investigative field offices, and provides a means of record keeping for all case and subject information.
Data Collection Methodology	The Secret Service collects data on its cyber investigations through its case management system, Field Investigative Reporting System (FIRS). Data is input FIRS via Secret Service personnel located in field offices throughout the United States and overseas. Data pertaining to this particular measure (financial accounts recovered) are extracted from FIRS by designated cyber crime case violation codes and the dates these cases were closed. The data is then aggregated up to the highest levels by month, year, office, and Service-wide. This information is then reported through various management and statistical reports to Secret Service headquarters program managers, field offices, and the Department of Homeland Security.
Reliability Index	Reliable
Explanation of Data Reliability Check	FIRS has many features built into it in order to provide the most accurate data possible. Along with the mainframe security features, there are many edit checks built into the applications to ensure the accuracy and validity of the data. Only authorized headquarters and field personnel have access to the applications, and they are governed by specific procedures to input case and arrest data. An annual audit is conducted and recurring verification reports are generated and reviewed to reduce errors and ensure data accuracy.

Performance Measure	Number of law enforcement individuals trained in cybercrime and cyber forensics both domestically and overseas
Program	Field Operations
Description	This measure represents the number of individuals trained in cybercrime and cyber forensics by the Secret Service. This specialized technical training occurs both domestically and overseas in an effort to strengthen our ability to fight cyber crime.
Scope of Data	This measure captures the total number of individuals trained by the Secret Service in cybercrime and cyber forensics.
Data Source	Data on individuals trained by the USSS is currently collected through internal tracking devices. We are attempting to move towards an enterprise solution to allow for easier dataset extraction and analysis.

Data Collection Methodology	Data is entered through internal tracking devices by authorized Secret Service personnel. Quarterly data is then extracted from the database and aggregated up to the highest levels by month and year. Training data is collected and aggregated by the number of individuals who attend each training class. Because of this, the potential exists for counting unique individuals multiple times if they attend more than one training per fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	Only authorized Secret Service personnel have access to the applications. Once the data has been aggregated, it is double checked for verification and to ensure data accuracy.

Performance Measure	Percent of currency identified as counterfeit
Program	Field Operations
Description	The dollar value of counterfeit notes passed on the public reported as a percent of dollars of genuine currency. This measure is calculated by dividing the dollar value of counterfeit notes passed by the dollar value of genuine currency in circulation. This measure is an indicator of the proportion of counterfeit currency relative to the amount of genuine U.S. Currency in circulation, and reflects our efforts to reduce financial losses to the public attributable to counterfeit currency.
Scope of Data	This measure is an indicator of the proportion of counterfeit currency relative to the amount of genuine U.S. currency in circulation. The measure reports the dollar value of counterfeit notes passed on the public as a percent of dollars of genuine currency. Past audits indicate that overall error rates are less than one percent. Error is due to lag time in data entry or corrections to historical data.
Data Source	All Counterfeit program measures are collected from the Counterfeit/Contraband System. This system is used by all Secret Service investigative field offices, and provides a means of record keeping for all case and subject information.
Data Collection Methodology	The Secret Service collects data on global counterfeit activity through the Counterfeit Tracking Application database. Data is input to the Counterfeit Tracking Application via Secret Service personnel located in field offices throughout the United States and overseas. Data pertaining to this particular measure are extracted from the Counterfeit Tracking Application by designated counterfeit note classifications, their dollar value, and the dates the counterfeit data was recorded in the system. The counterfeit data (dollar value of notes passed on the public) is then aggregated up to the highest levels by month, year, office, and Service-wide and then compared to the amount of US dollars in circulation (reported from the US Department of the Treasury). This information is then calculated as a percent and reported through various management and statistical reports to Secret Service headquarters program managers, field offices, and the Department of Homeland Security.
Reliability Index	Reliable
Explanation of Data Reliability Check	The Counterfeit Tracking Application database has many features built into it in order to provide the most accurate data possible. Along with the mainframe security features, there are many edit checks built into the applications to ensure the accuracy and validity of the data. Only authorized headquarters and field personnel have access to the applications, and they are governed by specific procedures to input case and arrest data. Recurring verification reports are generated and reviewed to ensure data accuracy.

Performance Measure	Percent of National Center for Missing and Exploited Children (NCMEC) examinations requested that are conducted
Program	Field Operations
Description	This measure represents the percentage of Secret Service computer and polygraph forensic exams conducted in support of any investigation involving missing or exploited children in relation to the number of computer and polygraph forensic exams requested.

Scope of Data	The scope of this measure is the total number of requested examinations requested to support other law enforcement investigations with missing and/or exploited children cases. Exams are completed at Secret Service field offices and headquarter offices.
Data Source	Number of computer and forensic exams conducted is collected from the Electronic Crimes Special Agent Program (ECSAP), used by the Electronic Crimes Special Agent Program personnel to report forensic examination findings.
Data Collection Methodology	The Secret Service collects computer and polygraph forensic exam data that relate to missing or exploited children investigations through an application in its Field Investigative Reporting System. Data is input to Field Investigative Reporting System via Secret Service personnel located in field offices. Data pertaining to this particular measure are extracted from Field Investigative Reporting System by designated missing or exploited children violation codes and the dates these exams were completed. The data is then aggregated up to the highest levels by month, year, office, and Service-wide and then compared to the number of computer and polygraph forensic exams requested by the National Center for Missing and Exploited Children. This information is then reported as a percent through various management and statistical reports to Secret Service headquarters program managers.
Reliability Index	Reliable
Explanation of Data Reliability Check	Only authorized headquarters and field personnel have access to the applications, and they are governed by specific procedures to input case data. Recurring verification reports are generated and reviewed to ensure data accuracy.

Performance Measure	Percent of National Special Security Events that were successfully completed
Program	Protective Operations
Description	This measure is a percentage of the total number of National Special Security Events (NSSEs) completed in a Fiscal Year that were successful. A successfully completed NSSE is one where once the event has commenced, a security incident(s) inside the Secret Service - protected venue did not preclude the event's agenda from proceeding to its scheduled conclusion.
Scope of Data	The security of protectees is the ultimate priority of the Secret Service. The Secret Service conducts after action reviews to gauge performance of specific protective operations. These reviews are used to measure how successfully the Secret Service performed its mission and what can be done to increase efficiency without compromising a protectee or event. There is no error rate for this measure.
Data Source	This program measure originates from the protective event or visit.
Data Collection Methodology	The Secret Service completes an After-Action Report following every National Special Security Event. This comprehensive report depicts all aspects of the event to include any and all incidents that occurred during the event. Subsequently, the After-Action reports are reviewed to determine the number of National Special Security Events that were successfully completed. This information is then calculated as a percentage and reported through various management and statistical reports to Secret Service headquarters program managers.
Reliability Index	Reliable
Explanation of Data Reliability Check	Any breach of Protective Operations would be immediately known and subject to a thorough investigation.

Performance Measure	Percent of protectees that arrive and depart safely
Program	Protective Operations
Description	This measure gauges the percent of travel stops where Secret Service protectees arrive and depart safely. The performance target is always 100%.

Scope of Data	This measure is an indicator of the percentage of travel stops where protectees arrive and depart safely. The number of protective stops protectees arrive and depart safely divided by the total number of protective stops protectees arrive and depart.
Data Source	Protective stops information is collected from the Agent Management & Protection Support System. This system is used by Secret Service protective divisions, and provides a means of record keeping for all protective stops information.
Data Collection Methodology	Results from Protective Operations, as well as any incident that may occur, are immediately reported by detail leaders to the Special Agent in Charge, who submits an After Action Report to Protective Operations program managers, and are disseminated within the organization for further analysis. Analysts collect protective travel stops for domestic protectees, foreign dignitaries, and campaign protectees and aggregate the totals into one measure. The number of incident-free protection stops is divided by the total number of protection stops to achieve a percent outcome.
Reliability Index	Reliable
Explanation of Data Reliability Check	Program managers and Operations Research Analysts continually monitor and review performance, including all instances of arrival and departure. Any breach of Protective Operations would be immediately known and subject to a thorough investigation.

Performance Measure	Percent of total protection activities that are incident-free at the White House Complex, Vice President's Residence, and other protected facilities
Program	Protective Operations
Description	This measure gauges the percent of instances where the Secret Service provides incident free protection to the White House Complex, Vice President's Residence, and other protected facilities. An incident is defined as someone who is assaulted or receives an injury from an attack while inside the White House Complex, Vice President's Residence, or other protected facility.
Scope of Data	Performance data is based on the percentage of days where incident-free protection is provided to persons (protectees, staff/employees, guests, and the public) inside the White House Complex, the Vice President's Residence, and other protected facilities.
Data Source	The Secret Service conducts after action reviews to gauge performance of specific protective operations. These reviews are used to measure how successfully the Secret Service performed its mission and what can be done to increase efficiency without compromising a protectee or event.
Data Collection Methodology	Results from Protective Operations, as well as any incident that may occur, are immediately reported by detail leaders to the Special Agent in Charge, who submits an After Action Report to Protective Operations program managers, and are disseminated within the organization for further analysis. Analysts aggregate this information and report it by the number of days incident free protection was provided at facilities during the fiscal year divided by the number of days in the fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	Program managers and Operations Research Analysts continually monitor and review performance. Any breach of Protective Operations would be immediately known and subject to a thorough investigation.

Performance Measure	Terabytes of data forensically analyzed for criminal investigations
Program	Field Operations
Description	This measure represents the amount of data, in terabytes, seized and forensically analyzed through Secret Service investigations and those conducted by partners trained at the National Computer Forensic Institute (NCFI). The training of these law enforcement partners substantially enhances law enforcement efforts to suppress the continually evolving and increasing number of cyber and electronic crime cases affecting communities nationwide.
Scope of Data	This measure captures the amount of data seized and forensically analyzed through Secret Service cyber investigations and investigations conducted by partners trained at the National Computer Forensic Institute (NCFI).
Data Source	Both Secret Service and partner forensic data is collected from an application in the Field Investigative Reporting System (FIRS). FIRS is used by the Electronic Crimes Special Agent Program personnel to report forensic examination findings. USSS partners do not have access to FIRS. Partners submit their terabytes seized information through a standardized form to their USSS contact. The USSS contact then enters this information directly into a partners data collection table in FIRS.
Data Collection Methodology	The Secret Service collects computer and polygraph forensic exam data through an application in its Field Investigative Reporting System (FIRS). Both USSS and partner data is input to FIRS via Secret Service personnel located in field offices. Data pertaining to this particular measure are extracted from FIRS, including the number of terabytes examined, dates these forensic exams were completed, and who completed each exam. The data is then aggregated up to the highest levels by month, year, and office.
Reliability Index	Reliable
Explanation of Data Reliability Check	Only authorized Secret Service personnel have access to the applications, which are governed by specific procedures to input case data. Recurring verification reports are generated and reviewed to ensure data accuracy.

FY 2016-2017 Agency Priority Goal (APG) Measures

APG: Enhance Federal Network Security

Performance Measure	Percent of annual assessments completed for the twenty-three cabinet level agencies and one-third of all non-cabinet level agencies
Program	Infrastructure Analysis
Description	This measure assesses how many risk and vulnerability assessments (RVAs) DHS completes each year and compares that result to the total number of targeted Federal, civilian Executive Branch agencies for that year. Each year, DHS will target 23 cabinet level agencies and one-third of the remaining 102 Federal, civilian Executive Branch agencies. Therefore, each of the targeted cabinet level agencies will receive an annual RVA, and each other targeted agency will receive triennial RVAs. DHS leverages cybersecurity assessment methodologies, commercial best practices and threat intelligence integration that enables cybersecurity stakeholders to better develop decision making and risk management guidance. The RVA team consists of subject matter experts in penetration testing methodology and tactical delivery, which includes focusing on web applications, networks, databases, wireless, mobile computing, cloud security, social engineering, social media, and intelligence gathering.
Scope of Data	The scope of the data includes all of the assessment findings from the National Cybersecurity Assessment and Technical Services (NCATS) Risk and RVAs. This includes the 23 cabinet-level agencies and one-third of the remaining 102 Federal, civilian Executive Branch agencies.
Data Source	Assessment and countermeasure data are collected and stored by the NCATS team using a spreadsheet that tracks RVA engagements. In the future, an NPPD or Cybersecurity & Communications-wide customer relationship management tool will be used. RVAs include external (remote) non-credentialed scanning along with penetration testing. Measurements are tracked and stored on the Cybersecurity Assurance Lab network where the penetration testing and remote scans are conducted.
Data Collection Methodology	A team lead will track the progress of the assessment, which is scoped out with the stakeholder in the pre-assessment walkthrough. The team lead will then walk through the assessment methodology and conduct a series of testing that was identified by the stakeholder. The information derived from the tests will then populate a draft report deliverable. The data used to create the report is maintained in a spreadsheet by the NCATS program. Information on the spreadsheet includes name of finding, service impacted (if any), detailed finding, NIST Control (if any), standard remediation write up, default finding severity. The calculation is derived by dividing the number of completed assessments by the total number required for the fiscal year, which would be 57 (23 cabinet-level agencies + 1/3 of 102 remaining agencies).
Reliability Index	Reliable
Explanation of Data Reliability Check	Each assessment concludes with a final report. The metric will be compared to the report by the NCCIC Business Transformation Unit.

Performance Measure	Percent of DHS cybersecurity and cyber law enforcement components participating in automated indicator sharing
Program	Infrastructure Analysis

Description	The Federal government can better protect itself through increased information sharing. Specifically, automation will increase the speed and volume of threat indicators that can be shared within government, within the private sector, and between government and the private sector. DHS, which operates EINSTEIN intrusion detection and prevention capabilities, and individual federal, civilian Executive Branch agencies, can expedite their threat detection and blocking through the automated receipt of threat indicators. In addition to establishing an automated environment for machine-speed sharing across the Federal Government, subject to appropriate privacy safeguards, various DHS components can receive and contribute threat indicators to this environment. This measure assesses the extent to which individual DHS components are participating in this automated indicator sharing environment.
Scope of Data	DHS cybersecurity components are those DHS components with security operation centers (SOCs). This measure includes: DHS Office of Chief Information Officer (OCIO), National Protection and Programs Directorate (NPPD), United States Secret Service (USSS), Immigration Customs Enforcement (ICE), United States Coast Guard (USCG), Customs Border Protection (CBP), Transportation Security Administration (TSA), Federal Law Enforcement Training Center (FLETC), Federal Emergency Management Agency (FEMA), U.S. Citizenship and Immigration Services (USCIS).
Data Source	An Excel file maintained by DHS National Cybersecurity & Communications Integration Center (NCCIC) Technology Support Services (TSS) calculates, per month, how many are participating in AIS. Participation in AIS can be with the private sector, federal, state, local, tribal, territorial, and DHS Components; however, the data for this measure is only specific to DHS Components. The file is available on TSS SharePoint site for approved users.
Data Collection Methodology	Participation in AIS is determined through the implementation and testing process, which is tracked by a spreadsheet maintained by DHS NCCIC. To be classified as participating, the component Security Operations Center (SOC) must successfully complete operational testing of one or more type of information flow through the Trusted Automated Exchange of Indicator Information (TAXII) server. Results will be tracked through monthly reviews and reported to DHS on a quarterly basis. The denominator for this measure consists of the total number of cybersecurity and cyber law enforcement components within DHS. The numerator is the number of DHS components participating in automated information sharing.
Reliability Index	Reliable
Explanation of Data Reliability Check	The AIS program will make available the data files of the TAXII server. NPPD/Cyber Security & Communications (CS&C) Enterprise Performance Management Office (EPMO) will validate the data by quarterly reviewing the logs of the TAXII server to verify that components that are reported to be sharing data via AIS are doing so.

Performance Measure	Percent of federal, civilian executive branch personnel for whom EINSTEIN intrusion prevention system coverage has been deployed
Program	Protect Infrastructure
Description	This measure gauges the intrusion prevention coverage provided by EINSTEIN 3 (E^3A) Accelerated that is currently operating on civilian executive branch networks. E^3A has the capacity to both identify and block known malicious traffic. This performance measure assesses the extent to which DHS has deployed at least one E^3A countermeasure to protect federal, civilian executive branch Chief Financial Officer (CFO) Act agencies. This measure calculates the percentage of CFO Act personnel that are protected by at least one E3A countermeasure.
Scope of Data	Data are based on all self-reported federal, civilian executive branch CFO Act Department or Agency (D/A) Personal Identity Verification (PIV) counts as required by Homeland Security Presidential Directive-12, the date on which the participating CFO Act D/A successfully completes cutover (signifying deployed

	protection by E3A), and the service(s) selected by the participating CFO Act D/A. CFO Act D/A PIV counts provide an estimate of the number of personnel (federal and contractor) assigned to that CFO Act D/A; subsequently it provides an approximation of size with respect to the .gov population.
Data Source	Federal, civilian executive branch CFO Act D/A PIV counts, the services selected, and cutover dates are tracked on the LAN-A hosted E3A Executive Reporting Tracker, which is a Microsoft Excel spreadsheet. The Network Security Division (NSD) Mission Engineering & Technology (ME&T) populates the dates when the Departments and Agencies become covered by an E3A service, updates D/A PIV counts, and tracks status towards cutover.
Data Collection Methodology	EINSTEIN intrusion prevention system coverage is considered "deployed" when the D/A successfully completes routing its traffic through a Domain Name Service (DNS) server/service and/or Simple Mail Transfer Protocol (SMTP) server/service to be filtered; this is also known as the cutover date. If the D/A opts to use one countermeasure (e.g., DNS before getting SMTP) prior to getting the second, the earlier date is used as the cutover date. When the cutover is completed, all D/A seats are considered protected. When completing the cumulative quarterly percentage, the numerator consists of the sum of all CFO Act D/A PIV counts (aka "seat" in the reporting tracker) having a cutover date prior to the reporting date and having selected either DNS and/or SMTP; the sum of all known D/A seats forms the denominator. This fraction is multiplied by 100 to obtain the percentage.
Reliability Index	Reliable
Explanation of Data Reliability Check	The NSD ME&T team will update the E^3A Executive Reporting Tracker with additional D/A PIV counts, D/A cutover dates, and selected E3A services.

Performance Measure	Percent of participating federal, civilian executive branch agencies for which Phase 1 and 2 continuous diagnostics and mitigation tools have been delivered to monitor their networks
Program	Protect Infrastructure
Description	This performance measure assesses the extent to which DHS has contractually delivered Continuous Diagnostics and Mitigation (CDM) Phase 1 (asset management) and Phase 2 (user management) services and tools to participating Federal civilian executive branch agencies. Once DHS has delivered the tools through contract award, agencies must still take action to deploy and operate CDM on their networks. By making asset and user management tools available, agencies can begin to actively manage the risk on their networks.
Scope of Data	The scope of the data includes all available data from the Federal Agencies participating in CDM Phase 1 and Phase 2. The parameters used to define the data included in this measure are the number of agencies with signed Memorandums of Agreement (MOA) to participate in CDM and are included in the task order groupings to have CDM Phase 1 and Phase 2 tools and services delivered to them. The scope captures progress in awarding the contract to deliver CDM Phase 1 and Phase 2 tools and services to agencies so that they can monitor their networks for what is on their network (Phase 1) and who is on their network (Phase 2).
Data Source	The Office of Cybersecurity and Communications' CDM Program Office will track CDM Blanket Purchase Agreement Task Order 2 (Phase 1), Task Order PRIV [Privileges] (Phase 2), and Task Order CRED [Credentials and Authentication Management] (Phase 2), progress via Contract deliverables and progress reports provided by Continuous Monitoring as a Service (CMaaS) providers to the contracting officer at General Services Administration Federal Systems Integration and Management Center (GSA FEDSIM). Each event is captured directly in contract documentation for each participating agency on a monthly basis. Signed MOAs are documented by the CDM Program Office and updated as changes occur.

Data Collection Methodology	GSA FEDSIM provides monthly reports on Phase 1 and Phase 2 contracts. These reports are analyzed by the CDM Program Office and data for this measure are documented. The CDM Program Office measures the number of agencies with signed MOAs that have had CDM Phase 1 and Phase 2 Tools and Services delivered. The measure is calculated by dividing the total number of agencies with signed MOAs with Phase 1 and Phase 2 delivered through contract award, by the total number of agencies with signed MOAs participating in CDM Phase 1 and Phase 2.
Reliability Index	Reliable
Explanation of Data Reliability Check	The CDM Program Office will validate and accept each contract deliverable after a review for completeness and accuracy.

Performance Measure	Percent of participating federal, civilian executive branch agencies for which Phase 3 continuous diagnostics and mitigation tools have been delivered to monitor their networks
Program	Protect Infrastructure
Description	This performance measure assesses the extent to which DHS has contractually delivered Continuous Diagnostics and Mitigation (CDM) Phase 3 (event management) services and tools to participating federal civilian executive branch agencies. Once DHS has delivered the tools through contract award, agencies must still take action to deploy and operate CDM on their networks. By making event management available to agencies, they will now be able to more effectively manage coordinated threats to their network.
Scope of Data	The scope of the data includes all available data from the Federal Agencies participating in CDM Phase 3. The parameters used to define the data included in this measure are the number of agencies with signed Memoranda of Agreement (MOA) to participate in CDM and are included in the task order groupings to have CDM Phase 3 tools and services delivered. The scope captures progress in achieving delivery of CDM Phase 3 tools and services to agencies so that they can monitor their networks and better understand what is happening on their network.
Data Source	The Office of Cybersecurity and Communications' CDM Program Office will track CDM Blanket Purchase Agreement Task Orders for Phase 3 progress via contract deliverables and progress reports provided by Continuous Monitoring as a Service (CMaaS) providers to the contracting officer at General Services Administration Federal Systems Integration and Management Center (GSA FEDSIM). Each event is captured directly in contract documentation for each participating agency on a monthly basis. Signed MOAs are documented by the CDM Program Office and updated as changes occur.
Data Collection Methodology	GSA FEDSIM provides monthly reports on Phase 3 contracts. These reports are analyzed by the CDM Program Office and data for this measure are documented. The CDM Program Office measures the number of agencies with signed MOAs that have had CDM Phase 3 tools and services delivered through contract award. The measure is calculated by dividing the total number of agencies with signed MOAs with Phase 3 delivered by the total number of agencies with signed MOAs participating in CDM Phase 3.
Reliability Index	Reliable
Explanation of Data Reliability Check	The CDM Program Office will validate and accept each contract deliverable after a review for completeness and accuracy.

APG: Enhance Disaster Preparedness and Response

Performance Measure	Average annual percentage of administrative costs for field operations, as compared to total program costs
Program	Management and Administration
Description	These measures allows FEMA to understand what share of its disaster expenditures are administrative costs compared to the share that FEMA grants to survivors as assistance. It helps FEMA know if the agency is being efficient in the way it provides disaster assistance. This particular measure is for FEMA's most common disasters – less than $50M.
Scope of Data	The results are based on all available data and not a sample of data for Major Disasters under $50M. The measure only applies to Major Disasters (DRs). It does not apply to Emergency Declarations (EMs), Fire Management Assistance Grants (FMAGs) or any other administrative costs in the disaster relief fund. Administrative Costs are those costs which are classified in IFMIS (Integrated Financial Management Information System) as "Administrative" in FEMA's system of record, Enterprise Data Warehouse (EDW) reports and Financial Information Tool (FIT) reports. Examples include but are not limited to salaries and benefits, travel, facilities.
Data Source	The data is collected and stored in IFMIS. It is reported via FIT reports and in the Automated COP, both of which also pull data directly from IFMIS. OCFO owns IFMIS and the FIT reports. ORR owns the Automated COP.
Data Collection Methodology	The data is collected via IFMIS and reported in FIT reports. The remaining steps can be conducted by an analyst using data from a FIT report, but have been automated in the Automated COP. The data is organized so that disasters are first separated by their size which is determined by the total actual federal dollars obligated. Small disasters have total actual federal obligations less than $50M. An administrative cost percentage is calculated for each disaster and is the (Total Administrative Costs for that disaster)/ (Total Obligations for that disaster). To create the score for each year, the analyst groups all disasters declared in that year of the same size and calculates the average administrative cost percentage across all those disasters (Sum of Admin Cost Percentages of Each Disaster)/Total Number of Disasters). This results in three scores per year, one each for small, medium, and large disasters. Since the data is organized by the fiscal year of the declaration, but transactions are likely to occur on disasters in years after the declaration fiscal year. The score for each year will be captured and reported on September 30, one full fiscal year after the declaration fiscal year. So, the score for FY15, will be available on September 30, 2016.
Reliability Index	Reliable
Explanation of Data Reliability Check	For this particular measure, the results are drawn from a Financial System that undergoes a rigorous financial management process that includes internal controls and audit controls.

Performance Measure	Operational readiness rating of FEMA's specialized incident workforce cadres
Program	Response and Recovery
Description	This measure gauges the overall readiness of 23 cadres in the Incident Management Workforce (IMW) by examining staffing, training, and equipping variables of qualified personnel. The IMW are the primary first responders that provide services to disaster survivors immediately after an event and support Response and Recovery operations. The ability to gauge readiness provides key information for ensuring that qualified and equipped personnel are available to respond to a disaster examining the below variables: 1. Staffing Category Variable: % of Force Structure currently on board; % of force strength available; % of force strength deployed

	2. Training Category Variable: % of force strength qualified; % of qualified personnel currently available; % of all trainees who have completed their qualification sheets but still need to demonstrate performance. 3. 3. Equipping Category Variable: Percent of Reservists 1-1-1* ready * The Reservist has a laptop, RSA token, and a phone
Scope of Data	The results are based on all available data and not a sample of data. The data included in this performance measure are an aggregate of measures of staffing, training, and equipping readiness categories.
Data Source	The data source is the Cadre Operational Readiness and Deployability Status (CORDS) Report that measures the overall readiness of the incident management workforce for all 23 cadres. The Response Directorate's Incident Management Workforce Division (IWMD) pulls this data bi-weekly from the Deployment Tracking System.
Data Collection Methodology	IWMD pulls data from the Deployment Tracking System. The CORDS report algorithm measures 3 readiness categories and assigns an overall Cadre Readiness metric called its Deployability Rating (D-Rating of 1-5) to each cadre and the organization as a whole. The D-Rating applies a weight to each individual factor used to determine the final score: 50% Staffing, 35% Training, 15% Equipping. This weighting recognizes staffing as the critical element of an expeditionary workforce. Training and Equipping are instrumental to success and efficiency, but in an emergency, having people on-hand and available is most important. The formula for measuring the D-Rating is: [(Force Strength * .5) + (Availability of Force Strength * .15) + (Inverse of Deployed * .35)] *.5 = Staffing [(Qualified &Available * .35) + (Trainees with Academics Complete * .15) + (Qualified Force Strength * .5)] * .35 = Training (Equipment Ready * .15) = Equipping Staffing + Training + Equipping = Weighted Average
Reliability Index	Reliable
Explanation of Data Reliability Check	Cadres conduct quality assurance/quality management reviews of Deployment Tracking System (DTS) data to ensure the system accurately reflects the individuals within their cadre and individuals within the cadres are carrying accurate FEMA Qualification System (FQS) titles. If the cadre data is incorrect, the Cadre will work with IWMD to correct the data based upon internal data management processes. Once verified, reliable data will be made in the system immediately. IWMD conducts quality assurance/quality management reviews of DTS data to ensure the system accurately reflects deployment and qualifications related data reflected in the system is accurate. If deployment or qualifications data is incorrect, IWMD works with the Cadre or Program Office to change the data based upon internal data management processes. Once verified, reliable data will be made in the system immediately.

Performance Measure	Percent of FEMA Individual Assistance services that are delivered in a timely, effective and efficient manner
Program	Response and Recovery
Description	This is a weighted percent that reflects FEMA's role in delivering quality services to disaster survivors. This measure is based upon three categories: program services, supporting infrastructure, and customer satisfaction. Sub-elements within these three categories include providing temporary housing assistance and case management; having available grant management and internet and telephone registration systems; ensuring call centers respond quickly and business staff are in place; and, delivering these services to enhance customer satisfaction of those receiving individual assistance from FEMA following a disaster. Recovery assistance helps individuals affected by disasters and emergencies return to normal quickly and efficiently.

Scope of Data	The scope of this measure is for all federal disaster assistance activity within the reporting year. Data collected as part of the customer satisfaction sub-element uses a random sample of applicants who registered with FEMA and received assistance within the previous fiscal quarter. Customer Satisfaction results in Q1 of each fiscal year reflect the sentiment of applicants from disasters declared in the Q4 of the previous year.
Data Source	Several FEMA-owned data systems and sources are used to provide data for this measure. Data on the eligible applicants provided temporary housing assistance within 60 day of a disaster and the State grant award of Disaster Case Management come from the Individual Assistance (IA) Grants Management System. The availability of the IA Grants Management System and Internet and Telephone Registration System availability comes from the Office of the Chief Information Officer Daily Operational Report. Call Center Average Answer Time comes from the Call Center Database. The Recovery Human Capital Report provides data on IA, National Processing Service Center, and the Business Management Division Organizational Fill. Data on the IA Customer Service Satisfaction Survey comes from the Customer Satisfaction Assessment Team report.
Data Collection Methodology	The Strategic Analysis and Reporting section collects, conducts a peer review and analyzes all data. Once validated, data are grouped into three categories and weighted for the composite score. Weighting is as follows: program services are 40 percent, supporting infrastructure 35 percent and customer satisfaction 25 percent. Program services are the percent of eligible applicants provided temporary housing assistance within 60 days of a disaster and the awarding of a Disaster Case Management State Grant Award within 120 days of the Governor's request. Supporting infrastructure is the percent of time the Individual Assistance (IA) grants management system is available, the percent of time the internet system is available, the percent of calls answered within two minutes for the Call Center, and IA's organizational fill. Customer satisfaction is the percent of people who express satisfaction after receiving an IA grant in the previous quarter.
Reliability Index	Reliable
Explanation of Data Reliability Check	Recovery Reporting and Analysis Division manually checks the completeness and validity for Output factor data against status reports from the Chief Human Capital, Chief Financial, and Chief Procurement Officers. HQ Recovery Individual Assistance Division checks Preparedness, Awareness, Access, and Action factor data using its IT systems and associated reporting tools, and its Executive Communications Unit (ECU).

Performance Measure	Percent of National Exercise Program (NEP) exercises demonstrating substantive whole community partnership and participation
Program	Preparedness and Protection
Description	This measure tracks the percent of National Exercise Program (NEP) exercises with partners from the private and non-profit sectors, including nongovernmental organizations, that sponsor an exercise or is a major participant. The intent of the measure is to increase the percentage of private-sector entities conducting exercises by soliciting their participation in the NEP. Their participation as an exercise sponsor or major participant is key to FEMA's ability to promote the whole community approach to validating the capabilities needed to achieve the goal of more secure and resilient nation.
Scope of Data	All of the exercises identified in the NEP Cycle Calendar of Events are included in the scope of data for this performance measure. The NEP Cycle Calendar of Events is continuously updated throughout the two-year NEP cycle. Over the two-year period, National Exercise Division (NED) solicits private sector, faith based, and nongovernmental participants by working through FEMA regions to identify exercise opportunities for private sector participation or sponsorship. NED also works through intra- and inter-agency private sector liaisons to provide outreach on the NEP to promote the benefits of exercises, identify exercise

	opportunities, and potential exercise sponsors. Only those NEP exercises with a private and nonprofit sector exercise sponsor or major participant are included in the calculation of the performance measure.
Data Source	Information about the private and non-profit organizations that participate as an exercise sponsors or major participants can be found in NEP nomination forms; exercise objectives for individual exercises are identified in Situation Manuals and After Action Reports. Along with the number of exercises, exercise type, date, and location, the NED maintains the name of the exercise, name of the exercise sponsor, and exercise objectives contributed by major participants in an Excel spreadsheet. NED owns the final reporting database.
Data Collection Methodology	Staff from NED compiles the information from NEP nomination forms, Situation Manuals, and After Action Reports. The numerator for this measure will be determined by counting the number of exercises on the NEP Cycle Calendar of Events where the nomination form or After Action Report identifies a nongovernmental partner as a sponsor or where an individual Situation Manual or After Action Report identifies an exercise objective as having been contributed by a private nonprofit sector partner. The denominator for this measure will be the number of exercises on the NEP Calendar of Events.
Reliability Index	Reliable
Explanation of Data Reliability Check	There is no material inadequacy in the data to significantly impede the use of program performance data.

Performance Measure	Percent of states and territories that have achieved an intermediate or above proficiency to address their targets established through their THIRA
Program	Preparedness and Protection
Description	This measure assesses the percentage of state and territorial State Preparedness Report (SPR) ratings at or above the 3.0 threshold when averaging across the planning, organization, equipment, training, and exercise (POETE) elements rated by grantees for each core capability. The measure is calculated by averaging SPR POETE ratings for each core capability that a state or territory has identified as high-priority. If a state's or territory's average SPR rating for its high-priority core capability POETE elements is 3.0 or higher, it is counted toward the measure. To increase the rating for one POETE element of a core capability by one point, a state/territory would have to increase capability by as much as 20 percent.
Scope of Data	The scope of this measure includes all 50 states and six territories.
Data Source	States and territories assess their current core capability levels relative to their own capability targets annually through the State Preparedness Report (SPR). This annual self-assessment provides detailed data on the number of states and territories whose capability levels increase or decrease each year. SPR data used in this measure are a self-assessed rating for each POETE solution area and a priority (high, medium, or low) for each core capability. The data are collected using Microsoft Excel from the official states' and territories' responses to the annual SPR capability assessment that is submitted to the National Preparedness Assessment Division (FEMA\NPD\NPAD). The analysis is done using Excel.
Data Collection Methodology	For each core capability, states and territories assess their preparedness levels in each of the five solution areas—planning, organization, equipment, training, and exercises (POETE). They use a five-point scale for each assessment, where level one indicates little-to-no capability, and level five indicates that they have all or nearly all of the capability required to meet their target. The data are obtained from state and territory SPRs submitted to FEMA each year. The Excel based data analysis tool will extract SPR data into a raw data worksheet. NPAD will calculate the measure from the raw data.
Reliability Index	Reliable
Explanation of Data Reliability Check	States and territories receive substantial technical assistance (TA) on conducting the THIRA and submitting their capability levels estimates through the SPR. TA takes the form of published guidance (Comprehensive Preparedness Guide (CPG)

	201: THIRA Guide, Second Edition), workshop sessions in the FEMA Regions, and just-in-time instruction during the assessment period. SPR submissions are routed through the Homeland Security Grant Program State Administrative Agency to ensure it represents all preparedness stakeholders in the jurisdiction. The Regional Federal Preparedness Coordinator and/or his or her staff review all state, territorial, and other eligible grantee THIRA submissions in their area of responsibility. The review ensures that the submitted THIRAs are developed in alignment with CPG 201.

APG: Combatting Transnational Criminal Organizations

Performance Measure	Number of criminal arrests linked to transnational criminal organizations targeted by the Joint Task Forces
Program	Cross cutting initiative that involves the DHS Joint Task Forces and multiple Component programs.
Description	This measure indicates the number of criminal arrests of associated persons of Transnational Criminal Organizations (TCOs) targeted by the Joint Task Forces. Arrest of persons identified as having connections to the most dangerous and damaging criminal and smuggling operations is a necessary step toward the disrupting and dismantling of these organizations. By removing key operatives in a TCO network, we are working to impact the ability of the TCO to continue operations as usual. A criminal arrest could potentially rise to the level of disrupting a TCO if it leads to changes in the organizational leadership and/or changes in methods of the operation.
Scope of Data	This measure includes all arrests of individuals by ICE and CBP that are linked to organizations who have been targeted by the JTFs Each JTF will use a list of prioritized targets that will be measured against.
Data Source	JTF- I will enter all criminal arrest information into the TECS system. Criminal arrest information from CBP will be stored in the JTF-W measure tracking tool which will be maintained in the Homeland Security Information Network (HSIN).
Data Collection Methodology	Once a criminal is arrested by either CBP or ICE the case information will be entered into the Components respective databases. On a quarterly basis, JTF-I will send out the TCO measure data collection tool to JTF-W. Next, JTF-W will pull the appropriate data from the JTW-W Measure tracking tool and send the data to JTF-I. JTF-I will take the data received JTF-W and consolidate it, along with their own input.
Reliability Index	Reliable
Explanation of Data Reliability Check	The results for this measure are assessed quarterly and undergo review by DHS components/JTFs. For JTF-I; once an agent enters criminal arrest information into TECS it will undergo a review from the agent's group supervisor. The record will also be reviewed at the ICE/HSI headquarters level. For JTF-W once the data for the measure has been entered into the JTF-W metrics measure tracking tool, it's reviewed for accuracy by the officer/agents commander, and then reviewed by the director.

Performance Measure	Number of JTF operations executed against transnational criminal organizations targeted by the Joint Task Forces
Program	Cross cutting initiative that involves the DHS Joint Task Forces and multiple Component programs.
Description	This measure reports the number of operations that have been planned by the JTFs that were actually executed via integrated component operations. The JTFs provide a deliberate joint operational approach to achieve unity of effort and greater levels of security in their areas of responsibility. The JTFs lead and coordinate threat-based, targeted, integrated operations. This measure

	communicates the execution of these written JTF plans intended to best utilize available resources to counter Transnational Criminal Organizations (TCOs).
Scope of Data	This measure includes all formalized JTF-E and JTF-W written operation plans against prioritized TCO targets. The scope of operations may include but are not limited to: deliberately planned or surge operations, such as targeted enforcement operations, existing routine operations, newly developed operations, and consolidated joint operations. The span of any of the aforementioned may range from a matter of days to years as required.
Data Source	Results for this measure will be tracked in the JTF-W Operations Tracking Tool (JTF-W OTT) which stores all of the targets information as well as the results (consequence applied) of targeted enforcement action against each target (individual linked/associated to the priority organizations). JTF-E data for this measure will be stored in and extracted from various approved component databases and information sharing systems. JTF-E will maintain a list of prioritized, active, and planned operations as part of its annual deliberate planning process. Results will be maintained and reported by Intelligence and Operations staff.
Data Collection Methodology	The JTFs will construct integrated operational plans to disrupt and degrade the TCO activities. JTF-E and JTF-W will maintain a list of these planned operations. As planned operations are executed, each JTF will examine expected outcomes/outputs and assess if operations have accomplished the desired objectives. Those that meet desired objectives will be considered executed plans and recorded in their respective databases. On a quarterly basis, JTF-I will send out the TCO measure data collection excel spreadsheet to JTF-E and JTF-W, and they will pull the appropriate data from their respective systems of record and send it to JTF-I. JTF-I will take the data received from JTF-E and JTF-W and add together the number of operations executed.
Reliability Index	Reliable
Explanation of Data Reliability Check	JTF-W and JTF-E will maintain and distribute the formal list of approved operational plans. Having a written approved plan provides the reliability check for those operations included in this measure. The number of executed operational plans will be reviewed by area commanders/supervisors to ensure that determinations that written plans have been executed are accurate.

Performance Measure	Percent of transnational criminal organizations targeted by the Joint Task Forces that are disrupted or dismantled
Program	Cross cutting initiative that involves the DHS Joint Task Forces and multiple Component programs.
Description	This measure represents the number of disruptions and dismantlements compared to the total number of Transnational Criminal Organizations (TCOs) that have been identified as a priority target by the Joint Task Forces (JTFs). Through targeting based on intelligence, risk, and threat the JTFs assist in helping the Department best utilize its resources in order to have the largest impact on disrupting and dismantling the TCOs that pose the biggest threat impacting our Nation's southern border and approaches regions. Daily actions are taken to counter and degrade these threats, but true disruptions and dismantlements of TCOs are hard won battles. This measure communicates our greatest and most enduring successes against these criminal organizations, to remove these threats and demonstrate the gains to border security made possible through coordinated law enforcement campaigns.
Scope of Data	JTF-W and JTF-I will have a pre-identified list of targeted TCOs which will serve as the denominator for this measure. The numerator includes the operations and significant investigations that had an approved disruption or dismantlement of the targeted TCOs. A disruption occurs when efforts have successfully impeded the normal and effective operation of the target organization or targeted criminal

	activity as they occur, as indicated by changes in the organizational leadership and/or changes in methods of the operation of the target organization or targeted criminal activity. A dismantlement is when the cumulative impact of disruption efforts destroy the targeted organization's leadership and network to the point that the organization is incapable of reconstituting itself.
Data Source	For JTF-I, data is entered in the Significant Case Report (SCR) Module in TECS. Data inputs from JTF-W will be stored in the JTF-W measure tracking tool.
Data Collection Methodology	Each JTF has a process to document significant cases that are to be nominated for a disruption/dismantlement. These nominated operations/investigations are then reviewed to confirm they meet the definitions. For JTF-I, these nominations are reviewed by the Significant Case Review (SCR) process in HSI. For JTF-W the nominations are evaluated by a review panel made up of representatives from JTF-W Headquarters Operations and Intelligence Sections, JTF-W Corridor Commanders or their representatives, and representatives from JTF-I and JTF-E. The JTF-E nomination process includes coordinating nominations with component investigation and intelligence entities which are then reviewed, prioritized, and approved by JTF-E prior to submission to JTF-I for consideration. On a quarterly basis, JTF-I will send out the TCO measure data collection excel spreadsheet and JTF-W will pull the appropriate data from their tracking tool and send it to JTF-I. JTF-I will consolidate the data with their own inputs. The number of reported disruptions and dismantlements will be divided by the number of identified targeted TCOs to calculate the percent.
Reliability Index	Reliable
Explanation of Data Reliability Check	Both JTF-I and JTF-W have multi-level reviews of the results for validation prior to consolidation and external reporting. Once an agent or officer enters significant investigation or operational information into their appropriate system of records, it is then reviewed by the next level in their chain of command, either the agent's group supervisor or the Commander. Internal reviews of the data occur prior to the review panel evaluation by JTF-W, or the peer and Significant Case Review process for JTF-I. These panels serve as an additional reliability check on whether the operations/cases are truly a disruption or dismantlement.

Performance Measure	Pounds of drugs seized linked to transnational criminal organizations targeted by the Joint Task Forces
Program	Cross cutting initiative that involves the DHS Joint Task Forces and multiple Component programs.
Description	This measure represents the number of pounds seized for any illicit drugs as a result of interdiction actions against Transnational Criminal Organizations (TCOs) targeted by the Joint Task Forces. Disrupting the flow of illegal drugs is critical for drugs provide a major revenue stream for TCO operations. This measure reflects drugs that are both physically seized and also those that are jettisoned over the side of a boat. A drug seizure could potentially rise to the level of disrupting a TCO if it leads to changes in the organizational leadership and/or changes in methods of the operation.
Scope of Data	This measure includes all drugs seized by CBP, USCG and ICE, from significant investigations that have been targeted by JTF-E, JTF-W, and JTF-I. In the case of JTF-E and USCG, drugs jettisoned over the side of a boat (otherwise deemed irretrievable) are included in the measure. Each JTF will identify a list of targets that will be measured against.
Data Source	Each JTF will utilize their respective systems of record for tracking drug seizures, such as TECS and the Consolidated Counter Drug Database.
Data Collection Methodology	Each JTF/Component will regularly enter their respective drug seizure information into their unique databases. Case numbers in TECS Drug seizures from the JTF-E that are entered into TECS will be linked to JTF-I significant investigations. On a quarterly basis, JTF-I will send out the TCO measure data collection excel spreadsheet to JTF-E and JTF-W. JTF-E and JTF-W will pull the appropriate data from their respective systems of record and send it to JTF-I. JTF-

	I will take the data received from JTF-E and JTF-W and consolidate it along with their own inputs.
Reliability Index	Reliable
Explanation of Data Reliability Check	The results for this measure are assessed quarterly and undergo review by DHS components/JTFs. For JTF-I once an agent enters criminal arrest information into TECS it will undergo a review from the agent's group supervisor. The record will also be reviewed at the ICE/HSI headquarters level. For JTF-W once the data for the measure has been entered into the JTF-W metrics measure tracking tool, it's reviewed for accuracy by the officer/agents commander, and then reviewed by the director. For JTF-E/USCG the CCDB is the authoritative source for drug seizures. The CCDB is an interagency-vetted database that is reviewed quarterly.

Performance Measure	Total amount of currency and/or monetary instruments seized of transnational criminal organizations targeted by the Joint Task Forces
Program	Cross cutting initiative that involves the DHS Joint Task Forces and multiple Component programs.
Description	This measure represents the total dollars seized for any currency or monetary instrument against any Transnational Criminal Organizations (TCOs) targeted by the Joint Task Forces. Monetary instruments are defined in 31 USC § 5312 (3) and includes items such as bank accounts, checks, savings bonds, virtual currency, and stocks. Seizing currency and monetary instruments could potentially rise to the level of disrupting a TCO if it leads to changes in the organizational leadership and/or changes in methods of the operation.
Scope of Data	This measure includes all currency and monetary items seized by CBP, USCG, and ICE from significant investigations targeting TCOs who have been targeted by JTF-E, JTF-W, and JTF-I. Each JTF will identify a list of targets that will be measured against.
Data Source	The JTFs will utilize a combination of component approved databases to capture and extract data, such as TECS, the Marine Information for Safety and Law Enforcement (MISLE), and the JTF-W measure tracking tool which will be maintained in the Homeland Security Information Network (HSIN).
Data Collection Methodology	Upon seizing currency through operations, each JTF/Component will enter their respective currency seizure case information into their unique databases. On a quarterly basis, JTF-I will send out the TCO measure data collection tool JTF-E and JTF-W. JTF-E and JTF-W will pull the appropriate data from their respective systems of record and send the data to JTF-I. JTF-I will take the data received from JTF-E and JTF-W and consolidate it, along with their own inputs.
Reliability Index	Reliable
Explanation of Data Reliability Check	The results for this measure are assessed quarterly and undergo review by DHS components/JTFs. For JTF-I once an agent enters currency seizure information into TECS it will undergo a review from the agent's group supervisor. The record will also be reviewed at the ICE/HSI headquarters level. For JTF-W once the data for the measure has been entered into the JTF-W metrics measure tracking tool, it's reviewed for accuracy by the officer/agents commander, and then reviewed by the director. Within the JTF-E, the program manager reviews entries into MISLE database monthly and compares to other sources of information to assess reliability of the database. District, Area, and Headquarters law enforcement staffs review, validate, and assess the data on a quarterly basis as part of the Law Enforcement Planning and Assessment System.

FY 2018-2019 Agency Priority Goal (APG) Measures

APG: Enhance Southern Border Security

Performance Measure	Miles of Southern Border with additional pedestrian wall
Program	Border Security Operations
Description	This measure reflects the total number of additional miles of primary pedestrian wall along the Southern Border with Mexico in places where no pedestrian wall existed previously. The number of miles are determined by prioritization of impedance and denial requirements according to unique needs and conditions along the border. Pedestrian wall barriers along the highest risk areas of the Southern Border will improve impedance and denial capabilities, a key part of the Operational Control (OPCON) framework.
Scope of Data	This measure represents the number of additional miles of primary pedestrian wall built along the Southern Border, adding new miles to the quantity of such wall that is already in place. Primary pedestrian wall is a contiguous, physical wall or other similar secure, contiguous, and impassable physical barrier directly on or very near the international border. Not included in the scope of this measure are other types of wall that exist on the Southern Border include vehicle barriers, and secondary/enforcement zone wall that runs parallel to primary impedance-and-denial infrastructure, adding an additional layer of protection and providing advantage for law enforcement agents. Physical barriers constructed along Northern and Coastal Border sectors are not included in this measure.
Data Source	Information on all infrastructure, to include wall infrastructure, is collected via geospatial data consolidated in the Geographical Information System (GIS) held both in the Facilities Management and Engineering Organization (OFAM) Border Patrol and Air and Marine Program Management Office (BPAM PMO), and at U.S. Border Patrol Headquarters. Official reporting on all infrastructure, including wall, is directly from the GIS to ensure consistency and the ability to track to the specific location of each asset. All of the GIS information is available and linked to the project database in the Facilities and Infrastructure Tracking Tool (FITT). Additionally, once constructed all wall is available in the CBP Enterprise Geospatial Information Services (eGIS) system.
Data Collection Methodology	The type and location of wall chosen for construction is determined by identifying needs based on terrain characteristics; levels of activity; sophistication of threat; mobility; and entrenchment of the threat to achieve strategic objectives. The BPAM PMO Program Manager is responsible for managing the data associated with this measure, ensuring all project information including GIS data is captured in the correct system of record. The GIS Specialist and Project Analyst supporting the BPAM PMO ensure accurate information is tracked and coordinated with the project team(s). The live GIS and FITT data are able to be updated daily; however, there are specific timelines associated with data pulls and reporting. FITT schedule imports are completed the first Friday of each month. All other data is updated weekly. Data is extracted to report the miles of Southern Border with additional pedestrian wall.
Reliability Index	Reliable

Explanation of Data Reliability Check	The quality-control process includes analysis conducted within the project team in coordination with the U.S. Border Patrol. Every week during construction, the GIS data is exported and analyzed by the BPAM PMO staff to ensure any changes and updates are tracked. Additionally, the historic process for a large-scale fence/wall program has included the contractor building the fence to collect the mileage daily to cross compare and validation of completion. GIS data includes a monthly share between U.S. Border Patrol Headquarters and the BPAM GIS team to cross-compare data, conduct quality control, and ensure all assets are captured accurately.

Performance Measure	Percent of Southern Border sectors that have implemented the Operational Control framework
Program	Border Security Operations
Description	This measure represents the percent of the nine U.S. border patrol sectors that have implemented the Operational Control (OPCON) framework as a means to increase border security. These operational plans describe specific efforts designed to improve results in the three elements of the OPCON framework: impedance and denial; situational awareness; and applying a law enforcement resolution. By implementing these plans, progress will be made in meeting the overarching goal of border security.
Scope of Data	The scope of this measure includes all nine U.S. Border Patrol sectors along the Southern Border that have written operational plans that will contribute to the implementation of the OPCON framework. The operational plans will include initiatives, objectives, and narratives describing specific efforts to improve results in each of the three elements of the OPCON framework: impedance and denial; situational awareness; and applying a law enforcement resolution. The Northern and Coastal Border sectors are not included in this measure.
Data Source	The U.S. Border Patrol Headquarters Planning Division will use Excel spreadsheets to track the status of all submitted operational plans. The tracking spreadsheet will be maintained and stored at U.S. Border Patrol Headquarters' Planning Division. All nine sector operational plans will be stored at U.S. Border Patrol Headquarters and at the respective sector headquarters.
Data Collection Methodology	U.S. Border Patrol Headquarters will provide the operational plan template and work with each of the nine U.S. Border Patrol sectors to establish their operational plans. Each of the nine U.S. Border Patrol sectors will electronically submit their operational plans to Headquarters. The U.S. Border Patrol Headquarters Planning Division will track each sector's submission at the end of each quarter and report the measure results based on the results of each sector's operational plan received.
Reliability Index	Reliable
Explanation of Data Reliability Check	Each sector will be electronically submitting their operational plans for OPCON and the U.S. Border Patrol leadership review and approval.

Performance Measure	Percent of Southern Border sectors with which the U.S. Border Patrol has coordinated to determine how Operational Control (OPCON) standards apply to the sectors' areas of responsibility
Program	Border Security Operations
Description	This measure calculates the percent of the nine U.S. Border Patrol's Southern Border sectors that have, first, received the briefing on the new Operational Control (OPCON) strategy; and, second, have had discussions with U.S. Border Patrol Headquarters regarding how the OPCON measures framework can apply to their area of responsibility. This effort will inform the baseline from which the OPCON measures are developed for each of the sectors by aligning existing measures related to the Southern Border to the three elements of the OPCON framework: impedance and denial; situational awareness; and applying a law enforcement resolution.

Scope of Data	The results are based on the number of facilitated briefings delivered on the new OPCON strategy to all the nine U.S. Border Patrol sectors along the Southern Border. The scope of the measure also includes the coordination efforts to address how the OPCON measures framework can apply to all nine sectors' areas of responsibility. The Northern and Coastal Border sectors are not included in this measure.
Data Source	The U.S. Border Patrol Headquarters Planning Division will collect, report, and store the data on a Word document and various Excel spreadsheets.
Data Collection Methodology	The U.S. Border Patrol Headquarters Planning Division will be keeping track of those sectors that have been briefed using an Excel spreadsheet. U.S. Border Patrol Planning Division will also keep track of the sectors that have coordinated how their existing measures align to the OPCON framework on an Excel spreadsheet. Sector offices will report on those measures through established databases and U.S. Border Patrol will report on how many sectors have established a framework at the end of each quarter. A sector is counted as applying OPCON when they are able to report on their OPCON measures can be rolled up to determine their OPCON score.
Reliability Index	Reliable
Explanation of Data Reliability Check	U.S. Border Patrol Planning Division will validate all data using available administrative information. U.S. Border Patrol Headquarters' Planning Division will report to leadership regarding the progress of briefing the new OPCON strategy to the nine Southern Border sectors and establishing the measures framework with existing measures to assess OPCON.

Performance Measure	Percent 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
Program	Border Security Operations
Description	In order to gain situational awareness of potential illicit activity in remote, low-risk areas of the southern border, the U.S. Border Patrol aims to reach detection sites of activity in remote low-risk areas within 24 hours. This measure gauges U.S. Border Patrol's ability to meet that goal to ensure that determinations of the nature of detected activity are properly assessed and addressed.
Scope of Data	This measure encompasses all geospatial intelligence-informed reports of potential illicit activity in remote low risk areas on the Southern Border. This measure includes all miles of the southern land border that have been determined by each southwest U.S. Border Patrol sector to be low flow and low risk areas. This measure does not include the northern border or maritime domain. A response is defined as when a U.S. Border Patrol sector receives an e-mail notification from an analyst and deploys U.S. Border Patrol Agents to investigate the detected activity.
Data Source	The data source is initiated from e-mail notifications and individual Field Information Reports (FIR) which are stored in CBP Intelligence Reporting System – Next Generation (IRS-NG) and maintained by CBP Office of Information Technology.
Data Collection Methodology	When the collection platform detects potential illicit activity the Office of Intelligence sends an e-mail notification to the appropriate U.S. Border Patrol sector. The Sector then deploys Border Patrol Agents to respond. The clock officially starts on the response when the e-mail notification is sent and is recorded by the responding sector. The arrival time of the Agents at the coordinates provided in the notification is recorded as the response time in the FIRSs. The measure will be reported quarterly by the U.S. Border Patrol southern land border sectors to U.S. Border Patrol Headquarters.
Reliability Index	Reliable

Explanation of Data Reliability Check	The responding Agent drafts the FIRs, which is then reviewed by a supervisor. Data is compared to source documents to validate data. The Patrol Agent In Charge must review and give final approval on all FIRs submitted. All FIRs must be created and approved within 72 hours of notification.

Performance Measure	Percent of U.S. Border Patrol agents who are trained and certified to perform enforcement actions
Program	Border Security Operations
Description	The measure assesses training readiness of U.S. Border Patrol agents. Increasing agents' levels of basic and advanced training enhances U.S. Border Patrol's capability to perform mission-essential tasks. Border Patrol agents are the only CBP resources capable of many essential law enforcement functions on the U.S. border. As agent numbers fluctuate, fully trained, deployable agents can mitigate agent-hiring shortfalls. Agents complete extensive Academy Basic Training and are required throughout their career to maintain certification in areas such as Quarterly Firearms Proficiency and Use of Force Policy. In addition, because each sector has unique climate, terrain, and operational environment, each USBP sector has different region-specific training requirements. These specialties include handling canines, counter-tunnel operations, horse patrol, All-Terrain-Vehicle (ATV), radiation detection, and snowmobile training.
Scope of Data	This measure encompasses every person categorized as a Border Patrol agent (GS-1896 classification) in the U.S. Border Patrol. U.S. Border Patrol agents carry that classification from the moment they enter duty. To be considered fully trained, U.S. Border Patrol agents must meet minimum requirements, including the successful completion of the U.S. Border Patrol Academy Basic Training and post-Academy Field Training Unit instruction and testing, as well as maintaining certifications in Quarterly Firearms Proficiency, Use of Force Policy Training, and Intermediate Use of Force. In addition, each sector determines required region-specific training based on operating environment and threat. Each sector's Chief Patrol Agent determines region-specific, specialty training requirements based on mission requirements and capability assessments related to the local operating environment and terrain.
Data Source	The data source will be the quarterly U.S. Border Patrol Resource Readiness report, which gets its data from U.S. Border Patrol's training-record databases (the Performance and Learning Management System (PALMS) system and Training, Records, and Enrollment Network (TRAEN) system); the Firearms, Armor and Credentials Tracking System (FACTS), and individual sector training-personnel analysis. As training courses and certifications are completed, supervisory personnel ensure documentation of those accomplishments in systems that include PALMS, TRAEN, FACTS, and the Border Patrol Enforcement Tracking System (BPETS).
Data Collection Methodology	As agents complete training courses training personnel enter their progress into one of the data sources listed in the Data Source section. The Chief Patrol Agent's (CPA) designee collects data from the systems of record to populate the sector's quarterly Resource Readiness Report (RRR), an Excel spreadsheet that list the required training based on the sector's Table of Organization (TO) and the CPA's mission-needs determination. Agents occupy a position on a sector's TO from the moment they enter on duty, making it possible for a sector to have untrained agents on it's TO. The CPA's designee compiles the data into the RRR and reports it to USBP Headquarters, where the overall percentage is computed by dividing the number of agents who have completed the required training by the total number of assigned agents; or in the region-specific-training categories, by dividing the number of agents trained in a specialty by the number required by the CPA.
Reliability Index	Reliable

Explanation of Data Reliability Check	The data being reported will be sourced by U.S. Border Patrol sector and station leadership directly from the systems of record (i.e., PALMS, TRAEN, FACTS, BPETS), as well as official sector-specific mechanisms. For audit purposes when needed, the data in the Resource Readiness Report can be traced directly back to those systems of record.

Performance Measure	Rate of interdiction effectiveness along the Southwest Border between ports of entry
Program	Border Security Operations
Description	This measure reports the percent of detected illegal entrants who were apprehended or turned back after illegally entering the United States between the ports of entry on the Southwest border. The U.S. Border Patrol achieves this desired strategic outcome by maximizing the apprehension of detected illegal entrants or, confirming that illegal entrants return to the country from which they entered; and by minimizing the number of persons who evade apprehension and can no longer be pursued.
Scope of Data	The scope includes all areas of the Southwest border that are generally at or below the northern most checkpoint within a given area of responsibility, and applies the following data filters: In Border Zones: Includes all Apprehensions, Got Aways (GA), and Turn Backs (TB). In Non-Border Zones: Includes apprehended subjects who have been identified as being in the U.S. illegally for 30 days or less, does not include GA and TB. Definitions: Apprehension: A deportable subject who, after making an illegal entry, is taken into custody and receives a consequence. Gotaway: A subject who, after making an illegal entry, is not turned back or apprehended and is no longer being actively pursued by Border Patrol agents. Turn Back: A subject who, after making an illegal entry into the US, returns to the country from which he/she entered, not resulting in an apprehension or GA.
Data Source	Apprehension, gotaway, and turnback data is captured by U.S. Border Patrol agents at the station level. Apprehensions are entered into the e3 Processing (e3) system, and all data entered via e3 resides in the Enforcement Integrated Database (EID), the official system of record for this data, which is under the purview of the U.S. Border Patrol Headquarters Statistics and Data Integrity (SDI) Unit. The physical database is owned and maintained by Immigrations and Customs Enforcement (ICE). Gotaways and Turnbacks are entered into the CBP Enforcement Tracking System 1 (BPETS1), which resides with Office of Border Patrol. BPETS1 is under the purview of and is owned by the Enforcement Systems Unit.
Data Collection Methodology	Apprehension data is entered into e3 by Border Patrol Agents (BPAs) at the station level as part of the standardized processing procedure. BPAs use standard definitions for determining when to report a subject as a GA or TB. Some subjects can be observed directly as evading apprehension or turning back; others are acknowledged as GAs or TBs after BPAs follow evidence that indicate entries have occurred, such as foot sign, sensor activations, interviews with apprehended subjects, camera views, communication between and among stations and sectors, and other information. Data input into the BPETS1 system occurs at the station level. The e3 Processing application and BPETS1 are used continuously to document apprehension, GA, and TB data. Calculation of the measure is done by the Headquarters SDI Unit and is: (Apprehensions + TB)/Total Entries. Total entries is the sum of Apprehensions, TBs, and GAs.
Reliability Index	Reliable

Explanation of Data Reliability Check	Border Patrol Agents in Charge ensure all agents are aware of and utilize proper definitions for apprehensions, GAs and TBs at their respective stations. They also ensure the necessary communication takes place between and among sectors and stations to ensure accurate documentation of subjects who may have crossed more than one station's area of responsibility. In addition to station level safeguards, the Headquarters Statistics and Data Integrity (SDI) Unit validates data integrity by utilizing various data quality reports. Data issues are corrected at the headquarters level, or forwarded to the original inputting station for correction. All statistical information requested from within DHS, U.S. Border Patrol, or external sources are routed through the centralized Headquarters office within U.S. Border Patrol. The SDI Unit coordinates with these entities to ensure accurate data analysis and output.

APG: Strengthen Federal Cybersecurity

Performance Measure	Percent of significant (critical and high) vulnerabilities identified by DHS cyber hygiene scanning of federal networks that are mitigated within the designated timeline
Program	Cybersecurity
Description	This measure calculates the percent of significant (critical and high) vulnerabilities identified through 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. DHS provides cyber hygiene scanning to agencies to aid in identifying and prioritizing vulnerabilities based on their severity for agencies to make risk based decisions regarding their network security. Identifying and mitigating the most serious vulnerabilities on a network in a timely manner is a critical component of an effective cybersecurity program.
Scope of Data	The scope of data for this measure is all significant (critical and high) vulnerabilities identified by cyber hygiene scanning on federal networks that were either mitigated during, or were active greater than or equal to the designated timeline for mitigation (15 days for critical; 30 days for high) during the measurement period. The timeline begins when a critical or high vulnerability is first detected on a scan and it ends when the critical or high vulnerability is no longer visible on the scan.
Data Source	The data source is a data storage on a client access license (CAL) that is maintained by the cyber hygiene scanning team.
Data Collection Methodology	An analyst will identify the range of vulnerabilities for the reporting period according to the measure scope. Data analysis software will be used to run a report on the percentage of criticals and highs that were mitigated within the designated timeline. The total number of critical and high vulnerabilities, as well as the number of each mitigated within the designated timeline will be reported each quarter. The cumulative result will be calculated using the following formula: (# of Critical Vulnerabilities mitigated within 15 days) + (# of High Vulnerabilities mitigated within 30 days) divided by (Total # of Critical and High Vulnerabilities).
Reliability Index	Reliable
Explanation of Data Reliability Check	The Cyber Hygiene Scanning team within the National Cybersecurity Assessments and Technical Services (NCATS) division will review the algorithm to query the data and the quarterly result for this measure to ensure correct data collection and calculation procedures were used. NPPD Strategy, Policy, and Plans will also review the quarterly results and accompanying explanations prior to final submittal to DHS.

Performance Measure	Percent of DHS endpoints identified with high and critical vulnerabilities relating to hardware and software that are patched within 30 days
Program	
Description	This measure assesses how effectively the Information Technology (IT) operations teams within DHS are able to remediate high and critical risk vulnerabilities identified through the Continuous Diagnostics and Mitigation (CDM) program on the DHS network. The vulnerabilities identified in this measure relate to "What is on the network" in terms of hardware and software. The CDM tool set provides near real time Security IT vulnerability details to DHS officials. By quickly addressing these vulnerabilities, DHS will close security gaps to provide greater protection of its critical IT infrastructure. DHS was the first agency to receive CDM and it is anticipated that the initial tools to monitor endpoints on the DHS network will be fully implemented across the Department by October 2018. The implementation of these tools will enable DHS to measure the speed in which critical and high vulnerabilities are mitigated.
Scope of Data	The scope for this measure will be all Information Technology computer endpoints (to include workstations, servers, printers, routers, switches) that will be scanned by the Continuous Diagnostics and Mitigation (CDM) automated tools set every 72 hours. The CDM automated tool will categorize each identified vulnerability based on its severity. Only those vulnerabilities categorized as high or critical will be included. The time to patch will start for each vulnerability once it is identified in the Information Security Vulnerability Management (ISVM) alert. The time will stop once the vulnerability is no longer identified in CDM tool scans.
Data Source	The program office will use the scan data from the Continuous Diagnostics and Mitigation (CDM) automated tools set which is stored in the DHS HQ CDM Component Management Enclave (CME) Splunk tool. The Splunk tool is used to gather, correlate, and provide a dashboard of vulnerabilities for the operations team to address. The Splunk tool also collects ISVM information from vendor websites and internal data bases. The final reporting for these data sources will be done by the DHS Chief Information Security Office.
Data Collection Methodology	Every 72 hours the automated tool will scan all computer assets. Every 24 hours the Splunk tool will pull ISVM from vendor websites and internal data bases. These data sets are then used to provide a dashboard of the current vulnerability status as well as quarterly trending. The numerator for this measure is the number of high and critical vulnerabilities that were patched within 30 days of the current quarter, vulnerabilities that were identified inside of 30 days of the end of the previous quarter but were patched within the 30 day timeframe during the current quarter. The denominator will be the total number of high and critical vulnerabilities that were identified during the reporting period. This number will include those vulnerabilities that were identified, and not patched, during the last 30 days of the previous quarter, and those vulnerabilities that were identified, and patched, during the last 30 days of the current reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	All vulnerability data will be verified by the Federal Information Security Management Act system Information System Security Officer (ISSO) and Information System Security Manager (ISSM). Once verified by the ISSO/ISSM the component Chief Information System Officer (CISO) will submit the information to the Office of the Chief Information Security Office for final approval.

Performance Measure	Percent of participating federal, civilian executive branch agencies with an active Continuous Diagnostics and Mitigation (CDM) data feed into the DHS managed Federal Dashboard
Program	Cybersecurity
Description	This measure calculates the percent of participating federal, civilian executive branch agencies with an active Continuous Diagnostics and Mitigation (CDM) data exchange with the DHS managed CDM Federal Dashboard. These exchanges demonstrate the successful deployment, integration, display, and exchange of data pertaining to CDM for agencies on Agency Dashboards and summary information at the Federal Dashboard. For a data feed to be established to successfully share information, the infrastructure to do so must first be in place between the agency and DHS. Deploying CDM and establishing data feeds between DHS and Federal agencies will enable greater visibility and management of the vulnerability and security status of Federal IT networks.
Scope of Data	The scope of this measure are the 23 federal civilian CFO act agencies, and the remaining mid to small sized agencies that receive CDM shared services, that have established an active CDM Phase 1 data connection with the Federal Dashboard. The mid to small sized agencies receiving the shared service will be counted as one additional agency once shared service connectivity has been established with the Federal Dashboard. Agencies receiving the shared service option will be counted individually and only once all participating agencies achieve connectivity to the Federal Dashboard will the shared service additional agency be counted as one. An agency will be counted as having an active data exchange with the Federal Dashboard once data from the agency is visible on the Federal Dashboard.
Data Source	The source of the information for this measure is received from the CDM Federal Dashboard
Data Collection Methodology	The CDM Program Management Office will track the connections of agencies to the Federal Dashboard at the end of each reporting period and will report the measure results based on the following formula: (# of civilian CFO Act agencies (23) with an active connection + # of Shared Service agencies with active connections / 40) / (23 civilian CFO Act agencies (23) + 1 Shared Service agency).
Reliability Index	Reliable
Explanation of Data Reliability Check	Upon collection of the quarterly data, the Test Manager, Federal Dashboard Program Manager, the System Engineer, and the CDM Program Manager will review the data to verify agency connections and ensure its accuracy. NPPD Strategy, Policy, and Plans will also review the quarterly results and accompanying explanations prior to submittal to DHS.

Performance Measure	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
Program	Cybersecurity
Description	This measure calculates the percent of participating federal, civilian executive branch agencies in the Continuous Diagnostics and Mitigation (CDM) program whose data relating to user activities on their network is visible on the DHS managed Federal Dashboard. The data pertaining to "Who is on the Network" demonstrates the successful deployment, integration, display and exchange of data pertaining to this particular CDM capability that focuses on restricting network privileges and access to only those individuals who need it to perform their duties. The data that is visible to the agencies is at the individual/object level while the Federal Dashboard will provide DHS with summary level vulnerability and security information. Deploying CDM and sharing information with Federal agencies will enable greater DHS visibility and management of the security of Federal IT networks.

Scope of Data	The scope of this measure are the 23 federal civilian CFO act agencies, and the remaining mid to small sized agencies that receive CDM shared services, that have established an active CDM connection with visible Phase 2 data on the Federal Dashboard. The mid to small sized agencies receiving the shared service will be counted as one additional agency once shared service connectivity has been established with the Federal Dashboard. Agencies receiving the shared service option will be counted individually and only once all participating agencies' data is visible to the Federal Dashboard will the shared service additional agency be counted as one. An agency will be counted in the numerator once their data pertaining to CDM Phase 2 is visible on the Federal Dashboard.
Data Source	The source of the information for this measure is received from the CDM Federal Dashboard
Data Collection Methodology	The CDM Program Management Office will track agency data on the Federal Dashboard at the end of each reporting period and will report the measure results based on the following formula: (# of civilian CFO Act agencies (23) with visible CDM Phase 2 data + (# of Shared Service agencies with visible CDM Phase 2 (data)) / 40) / (23 civilian CFO Act agencies (23) + 1 Shared Service agency).
Reliability Index	Reliable
Explanation of Data Reliability Check	Upon collection and calculation of the quarterly data, the Test Manager, Federal Dashboard Program Manager, the System Engineer, and the CDM Program Manager will review the data to verify its accuracy. NPPD Strategy, Policy, and Plans will also review the quarterly results and accompanying explanations prior to final submittal to DHS.

Performance 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
Program	Cybersecurity
Description	This performance measure assesses the extent to which DHS has contractually made available Continuous Diagnostics and Mitigation (CDM) tools to monitor events on their networks to participating federal civilian executive branch agencies. Once DHS has made the tools available through contract award, agencies must still take action to deploy and operate CDM on their networks. By making CDM tools available to agencies, they will be able to more effectively manage coordinated threats to their network.
Scope of Data	The scope of the data includes all available data from the Federal Agencies participating in CDM Phase 3. The parameters used to define the data included in this measure are the number of agencies with signed Memoranda of Agreement (MOA) to participate in CDM and are included in the task order groupings to have CDM Phase 3 tools and services delivered. The scope captures progress in achieving delivery of CDM Phase 3 tools and services to agencies so that they can monitor their networks and better understand what is happening on their network.
Data Source	The Office of Cybersecurity and Communications' CDM Program Office will track CDM Blanket Purchase Agreement Task Orders for Phase 3 progress via contract deliverables and progress reports provided by Continuous Monitoring as a Service (CMaaS) providers to the contracting officer at General Services Administration Federal Systems Integration and Management Center (GSA FEDSIM). Each event is captured directly in contract documentation for each participating agency on a monthly basis. Signed MOAs are documented by the CDM Program Office and updated as changes occur.

Data Collection Methodology	The GSA Federal Systems Integration and Management Center provides monthly reports on Phase 3 contracts. These reports are analyzed by the CDM Program Office and data for this measure are documented. The CDM Program Office measures the number of agencies with signed MOAs that have had CDM Phase 3 tools and services delivered through contract award. The measure is calculated by dividing the total number of agencies with signed MOAs with Phase 3 delivered by the total number of agencies with signed MOAs participating in CDM Phase 3.
Reliability Index	Reliable
Explanation of Data Reliability Check	The CDM Program Office will validate and accept each contract deliverable after a review for completeness and accuracy.

Performance Measure	Percent of incidents detected or blocked by EINSTEIN intrusion detection and prevention systems that are attributed to Nation State activity
Program	Cybersecurity
Description	This measure demonstrates the EINSTEIN intrusion detection and prevention systems' ability to detect and block the most significant malicious cyber activity by Nation States on Federal civilian networks. Nation States possess the resources and expertise to not only develop sophisticated cyber-attacks but sustain them over long periods of time. Thus the indicators that EINSTEIN deploys to detect and block malicious cyber activity should focus on methods and tactics employed by Nation States. The overall percentage of incidents related to Nation State activity is expected to increase through greater information sharing with partners and improved indicator development, which will result in better incident attribution.
Scope of Data	Performance measure data is based on DHS NCCIC ticketing system (BMC Remedy) data. The specific scope of data for this measure is Remedy incident tickets, created as a result of an EINSTEIN alert, with Focused Operations (FO) designation, which is populated by DHS analysts based on information provided by the indicator creator. Specific FO designations are correlated to nation-state activity. Incident tickets generated based on EINSTEIN detections and blocks are identified by filtering on specific fields. Incidents identified as false positives are excluded.
Data Source	The data source is the reporting Microsoft Structured Query Language database copied from the NCCIC ticketing system (currently BMC Remedy).
Data Collection Methodology	A remote data collection method is employed using Tableau to access Remedy data and generate an automated report on all tickets created for EINSTEIN detection and blocking, which have a Focused Operations number populated. The calculation is the number of tickets with a Focused Operations number divided by the total number of tickets generated for the reporting period. The result of that calculation is then multiplied by 100 to receive the percentage.
Reliability Index	Reliable
Explanation of Data Reliability Check	Potential issues for data reliability exist due to difficulties with initial attribution to nation-state actors. This function is executed through a documented work instruction that is updated annually, or as required, and quality assurance checks are performed daily by team leads. Many of the indicators used for this measure are received from trusted external partners.

Performance Measure	Percent of significant vulnerabilities (critical and high) mitigated within 6 months following a DHS assessment of a Federal Agency high-value asset
Program	Cybersecurity
Description	This measure calculates the percentage of significant vulnerabilities (critical and high) identified during a Risk and Vulnerability Assessment (RVA) of a High Value Asset (HVA) that the receiving agency has mitigated within six months of the final report being submitted to the agency to conclude the assessment. RVAs are performed on identified HVAs across the federal government to identify vulnerabilities associated with the Federal Government's most sensitive IT systems and data. As part of the assessment, the HVA owner agency receives a list of critical and high vulnerabilities to remediate and agencies provide monthly updates on progress. As agency vulnerability mitigation processes improve, more vulnerabilities should be mitigated in shorter time. Mitigating significant vulnerabilities relating to the Federal Government's most sensitive data and systems is critical to preventing potential cyber incidents.
Scope of Data	The scope of data for this measure is all critical and high vulnerabilities identified during a RVA assessment of a HVA for which the sixth month from the RVA Final Report submission falls within the measurement period. To be counted as mitigated, the agency must confirm that the vulnerability has been mitigated in its final report to DHS six months after the conclusion of the RVA.
Data Source	The source of the data for this measure are the agency RVA Final Reports.
Data Collection Methodology	Upon completion of the RVA assessment of the HVA, agencies have a six month period before they must submit a RVA Final Report on progress towards mitigating vulnerabilities discovered during the assessment. Upon receipt of the final report an analyst will review the report and will determine the total numbers of critical and high vulnerabilities from those assessments, as well as the number resolved. The cumulative result will be calculated using the following formula: (# of Critical and High vulnerabilities resolved within 6 months) / (Total # of Critical and High vulnerabilities identified for which the 6th month of the final report submission falls within the measurement period).
Reliability Index	Reliable
Explanation of Data Reliability Check	The quarterly data will be reviewed for accuracy by the Federal Network Resilience Program Office. The Enterprise Performance Management Office (EPMO) within the Cybersecurity & Communications division will also review the data for anomalies and correct calculation prior to final review by NPPD Strategy, Policy, and Plans before final submittal to DHS.

Homeland
Security

Homeland
Security