Homeland Security

FY 2021-2023

Annual Performance Report

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.

About this Report

The U.S. Department of Homeland Security Annual Performance Report (APR) for Fiscal Years (FY) 2021-2023 presents the Department's mission programs, progress summaries, performance measure results and FY 2022 and FY 2023 targets. It also summarizes information on other key initiatives in the DHS Performance Management Framework related to the Strategic Review and our Agency Priority Goals (APG). Also included are other key management initiatives, and a summary of our performance challenges and high-risk areas identified by the DHS Office of the Inspector General (OIG) and the Government Accountability Office (GAO). The report is consolidated to incorporate our annual performance plan and annual performance report.

For FY 2020, the Department's Performance and Accountability Reports consist of the following three reports:

- DHS Agency Financial Report | Publication date: November 12, 2021
- DHS Annual Performance Report | Publication date: April 19, 2022
- DHS Report to our Citizens (Summary of Performance and Financial Information) | Publication date: April 22, 2022

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

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 that is shared with leadership and external stakeholders. 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, *Preparation, Submission, and Execution of the Budget*, and the *Reports Consolidation Act of 2000* (P.L. No. 106-531) further delineate this responsibility by requiring agencies to ensure completeness and reliability of the performance data they report by putting management assurance procedures in place[1].

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

[1] *Note: Circular A-11, PART 6, THE FEDERAL PERFORMANCE FRAMEWORK FOR IMPROVING PROGRAM AND SERVICE DELIVERY, Section 240.26 Definitions.* Data limitations. In order to assess the progress towards achievement of performance goals, the performance data must be appropriately valid and reliable for intended use. Significant or known data limitations should be identified to include a description of the limitations, the impact they have on goal achievement, and the actions that will be taken to correct the limitations. Performance data need not be perfect to be valid and reliable to inform management decision-making. Agencies can calibrate the accuracy of the data to the intended use of the data and the cost of improving data quality. At the same time, significant data limitations can lead to bad decisions resulting in lower performance or inaccurate performance assessments. Examples of data limitations include imprecise measurement and recordings, incomplete data, inconsistencies in data collection procedures and data that are too old and/or too infrequently collected to allow quick adjustments of agency action in a timely and cost-effective way.

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 publicly reported set of measures. This process employs a tool known as the PMDF that provides a structured format to operationally describe every measure we publicly report in our performance deliverables. The PMDF provides instructions on completing all data fields and includes elements such as the measure name, description, scope of data included and excluded, where the data is collected and stored, a summary of the data collection and computation process, and what processes exist to double-check the accuracy of the data to ensure reliability. These data fields on the form reflect GAO's recommended elements regarding data quality.[2] The PMDF is used as a change management tool to propose and review new measures, make changes to existing measures, and to retire measures we want to remove from our strategic and management measure sets. This information is maintained in a Department central data repository, discussed next, and is published annually as Appendix A to our Annual Performance Report.

Central Information Technology Repository for Performance Measure Information

All of DHS's approved measures are maintained in the OneNumber tool, Performance Management (PM) System, which is a unique cube in the architecture of the OneNumber tool that also contains outyear planning and budget information. The PM System is a web-based IT system accessible to all relevant parties in DHS and was just deployed Department-wide in July of 2020. The system has specific access controls which allows for the management of the Department's performance plan and the capturing of performance results by designated system users. The PM System stores all historical information about each measure including specific details regarding: description; scope; data source; data collection methodology; and explanation of data reliability check. The data in the system are then used as the source for quarterly and annual Performance and Accountability reporting. Finally, the performance data in the PM System are used to populate the Department's business intelligence tools to provide real-time information to interested parties.

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 strategic measure planning and reporting actions at the end of each fiscal year. Components describe their

[2] 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.

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.

Independent Assessment of the Completeness and Reliability of Performance Measure Data

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

Management Assurance Process for GPRAMA Performance Measure Information

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

The DHS Office of Risk Management and Assurance, within the Office of the CFO, oversees the management of internal controls and the compilation of many sources of information to consolidate into the Component Head and the Agency Assurance Statements. The Agency Financial Report contains statements 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 APR.

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

Countering Weapons of Mass Destruction Office

Performance Measure	Percent of Acquisition programs to counter Chemical, Biological, Radiological, and Nuclear threats that meet all Key Performance Parameter requirements (New Measure)
Program	Capability and Operational Support
Description	This measure gauges progress in the delivering of an acquisition program's Key Performance Parameters (KPP). KPPs are key system capabilities that must be met for a system to meet its operational goals. The government will not accept new acquisitions if KPPs are not met. KPPs have both a threshold and an objective and to be accepted by the government, the prototype must perform between these two values.
Scope of Data	The population includes programs beginning at Acquisition Decision Event (ADE)-2C or ADE-3, whichever occurs first.
Data Source	The KPP requirements for each acquisition are captured from Acquisition Program Baselines (APBs) and Operational Requirements Documents (ORDs). Each acquisition's KPP performance data is captured from Test and Evaluation reports, Technical Review Board (TRB) reports, and signed FOC Achievement Memoranda. Performance against the KPPs reported during the Component Acquisition Executive (CAE) semi-annual review.
Data Collection Methodology	Each program establishes a Requirements Verification Traceability Matrix (RVTM) that documents each KPP, threshold requirement, objective requirement, and method of validation. Each KPP is evaluated through one or more of the following mechanisms: Test, Analysis, Demonstration, or Inspection (TADI). The results of the TADI are included in the RVTM.
Reliability Index	Reliable
Explanation of Data Reliability Check	APB and ORDs are formal documents with clearly specified KPPs. Test and Evaluation and TRB reports reflect a thorough, independent look at system performance and its ability to meet KPPs. These data sources can be objectively compared to determine if KPP requirements are being met.

Performance Measure	Percent of Acquisition programs to counter Chemical, Biological, Radiological, and Nuclear threats that meet their Acquisition Program Baseline schedule and cost thresholds (New Measure)
Program	Capability and Operational Support
Description	This measure gauges Chemical, Biological, Radiological, and Nuclear (CBRN) acquisitions meeting their cost and schedule plans. If cost or schedule exceeds each Acquisition's Program Baseline (APB) by more than ten percent, then the acquisition is considered to be in breach. If a program is in breach, there are a series of activities the program needs to complete to rectify and receive authority to proceed. This measure is a key indicator of the effectiveness of program management efforts for each acquisition.
Scope of Data	The population includes acquisition programs that have not yet reached Full Operational Capability (FOC) and those that have reached FOC during the current annual evaluation period. Only acquisitions that are on the DHS Major

	Acquisition Oversight List (MAOL) are included in this measure. FOC is achieved only when both CWMD designates an acquisition program in FOC and all supported Component(s) have signed an FOC Achievement Memorandum.
Data Source	Each acquisition program has its own tool to track cost and schedule against the APB plan. Acquisition programs enter cost and schedule data into DHS INVEST on a monthly basis.
Data Collection Methodology	Acquisition program managers are regularly updating and managing cost and schedule data. Annually, acquisition program managers are required to provide written evidence of cost and schedule performance against the APB. Analysts combine the results in a summary Excel spreadsheet and calculate first whether each acquisition is within its cost and schedule, and then the percent of all acquisitions that are within their APBs. The denominator is all planned cost and schedule parameters and the numerator is those that have been achieved consistent with the APB plan.
Reliability Index	Reliable
Explanation of Data Reliability Check	APBs are formal documents that typically include quantitative schedule baselines. Whether and when a key event has occurred can usually be determined by reviewing written documentation. ADM, CARB, TRB, and similar reports receive high-level management attention to ensure accuracy. These data sources can be objectively compared to APB thresholds to determine if schedule requirements are being met. Additionally, ongoing data calls and reporting requirements (e.g., monthly Acquisition Division Issue papers, Quarterly Performance Reviews, status of funds, and spend plan) provide regular oversight of data reliability. Acquisition programs are also reviewed at semi-annual Component Acquisition Executive (CAE) Program Reviews, in which the PM presents a comprehensive brief of progress towards meeting the stated requirements. CAE provides annual certification to PARM.

Performance Measure	Percent of BioWatch laboratories meeting expectation for scored proficiency tests to ensure they can identify known microorganisms of interest
Program	Capability and Operational Support
Description	This measure gauges whether BioWatch laboratories evaluating environmental samples for biological agents meet program quality assurance expectations to ensure they can identify known microorganisms of interest. These BioWatch laboratories are a network of public health laboratories. Periodic proficiency tests are performed at these laboratories to gauge proficiency on sample processing, analysis, and results reporting procedures, and these laboratories must meet expectations for operational preparedness. The BioWatch Program provides early warning of a bioterrorist attack in more than 30 major metropolitan areas across the country to help plan an effective, coordinated, and rapid response.
Scope of Data	The population being measured is the percent of the BioWatch laboratories that meet expectations from proficiency testing during a year. Up to three tests are conducted per year per laboratory. Proficiency tests will be given to all 30 BioWatch laboratory teams, that is 30 laboratory teams across 29 sites (one lab tests twice per day and has two separate teams which are tested separately). The denominator is the total number of annual proficiency tests, which may vary annually by laboratory. Laboratories may be excluded from the proficiency tests when the Director of Quality Assurance or Director of Laboratory Operations determine the proficiency testing is going to impact the biodetection mission. Examples may include staff shortage, facility impacts, or continuity of operations activation.

Data Source	Annual assessments and proficiency test reports of affiliated BioWatch laboratories. The individual laboratory reports are stored in individual laboratory files on the Homeland Security Information Network (HSIN). The laboratory results are provided in a table in the report. A report consolidating all laboratory results is provided to DHS CWMD.
Data Collection Methodology	The BioWatch program compiles the data from a report provided by the Quality Assurance (QA) contractor who develops the proficiency test. The proficiency test is developed in accordance with guidelines in the international standard ISO 17043:2010 Conformity assessment. Data is submitted to the QA contractor who compiles, assesses and verifies the integrity of the data. The report is reviewed by the BioWatch Director for Quality assurance and the Director for Laboratory Operations. Results of the tests for the year are then combined to calculate the final annual proficiency score. This will be accomplished by the sum of the number of laboratories meeting expectation across all tests (numerator) and dividing that by the sum of the number of laboratories participating in each proficiency test (denominator). For example, if all 30 lab teams participate in three proficiency tests in a year (denominator), and all meet expectation (numerator), the percent would be calculated by 90/90 X 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	The BioWatch program uses proficiency tests of affiliated laboratories in order to assess their functional capability to analyze and report on biological events and pathogens. Data reliability is assessed by the Quality Assurance Contractor in accordance with the international standard ISO 17043:2010 Conformity assessment — General requirements for proficiency tests. The QA contractor is required to be accredited to this international standard as an element of their contract. Measures are implemented to prevent labs from comparing results during the test.

Performance Measure	Percent of identified federal, state, local, tribal, and territorial stakeholders receiving the National Biosurveillance Integration Center reports (New Measure)
Program	Capability and Operational Support
Description	This measure assesses percent of identified FSLTT stakeholders receiving the NBIC reports. Identified stakeholders includes new individuals or groups receiving NBIC reports as well as removal of any recipients electing not to receive future reports or for which the email address is no longer valid. Only active stakeholder accounts are measured as the total recipient population. This measure only covers direct email recipients. The measure does not account for recipients among the several interagency portals, including HSIN, that receive a direct feed of NBIC reports. This measure also does not cover re-distribution of emailed reports by known recipients to other members of their organization or community of interest who are unknown to NBIC and which is a frequent practice of some NBIC recipients.
Scope of Data	The scope of this measure includes all active FSLTT stakeholder accounts receiving NBIC reports. The measure will analyze the percent of identified active FSLTT stakeholder accounts receiving NBIC products at the end of the quarter versus the beginning the quarter. Stakeholder accounts include both an individual FSLTT or an FSLTT group (such as a distribution list). This measure only covers direct email recipients.
Data Source	National Biosurveillance Integration Center (NBIC) People Database. NBIC Stakeholder Tracking. NBIC federal personnel manage the data source and reports findings.
Data Collection Methodology	To begin tracking, the NBIC Strategy and Outreach Section queries the NBIC People Database for the total FSLTT stakeholder population. This information is

	added to the "NBIC Stakeholder Tracking" Excel file to maintain a record of the stakeholder number at quarterly intervals. Any recipients electing not to receive reports are removed from the database, and inactive accounts are removed from the database on a weekly basis. On the first business day of each month, the NBIC Strategy and Outreach Section queries the NBIC People Database for the total active FSLTT stakeholder accounts. This information is then exported into an NBIC Stakeholder Tracking Excel file. On a quarterly basis, the annual target is determined. To guard against calculation errors, the quarterly results are reviewed by the NBIC Strategy and Outreach Section Lead who double checks the inputs and makes program adjustments as required.
Reliability Index	Reliable
Explanation of Data Reliability Check	To ensure data reliability, monthly and quarterly data inputs are reviewed by the NBIC Strategy and Outreach Section Lead to identify potential anomalies, errors, or gaps in data collection, analysis, and reporting. The number of identified FSLTT stakeholders receiving NBIC products is reviewed with NBIC's Director or Deputy Director quarterly. Also, the compact and repair function on the database is run at least monthly, and database is manually scrubbed to ensure data accuracy and consistency twice annually.

Performance Measure	Percent of annual Research and Development program and project milestones successfully achieved
Program	Research and Development
Description	This measure will gauge how well Research and Development program and project activities and their progress milestones are executed by DNDO's Transformational and Applied Research Directorate against numerous types of projects that are planned for and budgeted each year. A steady or slightly increasing number of milestones met is an indicator of effective program management.
Scope of Data	CWMD's Transformational and Applied Research Directorate Research and Development program and project milestone completions will be measured.
Data Source	Data are recorded by CWMD's Transformational and Applied Research Directorate for numerous types of projects that are planned for and budgeted each year. Program Managers compile and track data information in the project databases.
Data Collection Methodology	R&D program and project activities - and their progress milestones - are executed by DNDO's Transformational and Applied Research Directorate. Data are recorded by CWMD's Transformational and Applied Research Directorate for numerous types of projects that are planned for and budgeted each year. Program Managers compile and track data information in the project databases.Program managers will be responsible for reporting to the owner of a TAR database for this measure, and on a quarterly basis the GPRA point of contact will be required to report the number of milestones met to the component GPRA point of contact.
Reliability Index	Reliable
Explanation of Data Reliability Check	CWMD leadership supervising program/project managers review the data submitted by program/project managers to ensure accuracy and consistency, approves the status and explanation of milestones, and submits the data to the CWMD Performance Team. The CWMD Performance Team provides a third data reliability review before results are finalized and submitted to the CWMD GPRA representative.

Customs and Border Protection

Performance Measure	Average number of repeat apprehensions or encounters for persons along the Southwest Border between ports of entry
Program	Border Security Operations
Description	This measure reports the average number of apprehensions under Title 8 and encounters under Title 42 for deportable individuals who have been apprehended multiple times by the U.S. Border Patrol over a twelve-month rolling period. This average provides an indicator of whether factors such as the consequence delivery system are driving down the number of attempts of those to illegally cross into the U.S. within the nine sectors of the Southwest Border. Effective and efficient application of consequences for illegal border crossers should, over time, reduce the average number of apprehensions and encounters and reduce overall recidivism.
Scope of Data	Deportable illegal entrants that have or receive a Fingerprint Identification Number (FIN), who are apprehended under Title 8 or encountered under Title 42 multiple times within a twelve-month rolling period, are included in calculating this measure. The scope includes only those apprehensions or encounters that 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, and thus are not included in calculating the data for this measure.
Data Source	Apprehension and encounter data are captured by Border Patrol Agents at the station level and 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 U.S. Immigrations and Customs Enforcement (ICE).
Data Collection Methodology	Data relating to apprehensions and encounters are entered into e3 by Border Patrol Agents at the station level as part of the standardized processing procedure. Data input can be made by any agent who knows the details of the apprehension or encounter. This data is typically reviewed regularly at the station, sector or Headquarters level observing trends to provide feedback to the field on operational activity. Calculation of this measure completed by the SDI Unit at Border Patrol Headquarters and is the average number of time individuals have been apprehended or encountered during the 12-month rolling period.
Reliability Index	Reliable
Explanation of Data Reliability Check	All apprehension and encounter 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 and encounter 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 SDI 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	Number of joint operations conducted along the Northern Border by Border Patrol Agents and Canadian law enforcement partners
Program	Border Security Operations

Description	This measure tracks the number of initiated joint operations formalized in Operations Orders, which define levels of participation and dedication of resources for U.S. and Canadian partners. All Category 1, 2, or 3 operations, initiated with Canadian law enforcement agencies as partners, involving any one of the program's eight Northern Border sectors--Blaine, Spokane, Havre, Grand Forks, Detroit, Buffalo, Swanton, and Houlton are included. These bilateral law enforcement efforts between Customs and Border Protection and Canadian law enforcement partners at federal, provincial, territorial, and municipal (local) levels enhance both countries' ability to ensure legal trade and travel, while mitigating border security threats, including illicit activity by criminal organizations and other bad actors.
Scope of Data	Each of the joint operations included in the scope of this measure trace from a specific Operations Order recorded in the Border Patrol Enforcement Tracking System (BPETS) during a particular reporting period. Operations Orders fall into one of three approval categories: A Category 1 plan must receive approval from a Sector Chief Patrol Agent; a Category 2 plan requires approval from a Sector Chief Patrol Agent, a legal review, and authorization from the program's Deputy Chief; and a Category 3 plan requires approval from Sector Chief Patrol Agent, a legal review, and approval by the program's Chief. Starting with all Operations Orders in BPETS, this measure counts all Category 1, 2, or 3 operations, initiated with Canadian law enforcement agencies as partners, involving any one of the program's eight Northern Border sectors--Blaine, Spokane, Havre, Grand Forks, Detroit, Buffalo, Swanton, and Houlton.
Data Source	The Operations Order module of the Border Patrol Enforcement Tracking System (BPETS), maintained at the program's Headquarters, provides data used for this performance measure.
Data Collection Methodology	The program does not classify an operation as initiated until an Order covering that operation has completed review and approval at the appropriate level of authority. Program staff then record approved Operations Orders in BPETS, maintained at the program's headquarters. Analysts calculate this measure by summing the number of approved Category 1, 2, or 3 initiated or closed Northern border orders during the appropriate timeframe.
Reliability Index	Reliable
Explanation of Data Reliability Check	Program staff record approved Operations Orders in BPETS. The approving official first reviews the operations order, then manually activates the plan in BPETS. The operations plan then becomes active and ready for execution. If changes to the plan occur, the approval process begins again. Program guidelines require after-action reports (AARs), which staff must record in BPETS upon completion of all operations stored in this system. For any operation active for more than three days, program staff must file an AAR at least once every 90 days to document the ongoing operation's status. On a monthly basis, Component headquarters staff verify the status of joint operations by reviewing Operations Orders and comparing these against scheduled dates and AARs. Component headquarters staff produce quarterly data integrity reports on the BPETS joint operations, allowing the identification and correction of errors and/or omissions.

Performance Measure	Number of joint operations conducted along the Southwest Border by Border Patrol Agents and Mexican law enforcement partners
Program	Border Security Operations
Description	This measure tracks the number of initiated joint operations formalized in Operations Orders, which define levels of participation and dedication of resources for U.S. and Mexican partners. All Category 1, 2, or 3 operations, initiated with Mexican law enforcement agencies as partners, involving any one

	of the program’s nine Southwest Border sectors--San Diego, El Centro, Yuma, Tucson, El Paso, Marfa, Del Rio, Laredo, and Rio Grande Valley are included. These bilateral law enforcement efforts between Customs and Border Protection and Mexican law enforcement partners at federal, state, and municipal (local) levels enhance both countries’ ability to ensure legal trade and travel, while mitigating border security threats, including illicit activity by criminal organizations and other bad actors.
Scope of Data	Each of the joint operations included in the scope of this measure trace from a specific Operations Order recorded in the Border Patrol Enforcement Tracking System (BPETS) during a particular reporting period. Operations Orders fall into one of three approval categories: A Category 1 plan must receive approval from a Sector Chief Patrol Agent; a Category 2 plan requires approval from a Sector Chief Patrol Agent, a legal review, and authorization from the program’s Deputy Chief; and a Category 3 plan requires approval from Sector Chief Patrol Agent, a legal review, and approval by the program’s Chief. Starting with all Operations Orders in BPETS, this measure counts all Category 1, 2, or 3 operations, initiated with Mexican law enforcement agencies as partners, involving any one of the program’s nine Southwest Border sectors--San Diego, El Centro, Yuma, Tucson, El Paso, Marfa, Del Rio, Laredo, and Rio Grande Valley.
Data Source	The Operations Order module of the Border Patrol Enforcement Tracking System (BPETS), maintained at the program’s Headquarters, provides data used for this performance measure.
Data Collection Methodology	The program does not classify an operation as initiated until an Order covering that operation has completed review and approval at the appropriate level of authority. Program staff then record approved Operations Orders in BPETS, maintained at the program’s headquarters. Analysts calculate this measure by summing the number of approved Category 1, 2, or 3 initiated or closed Northern border orders during the appropriate timeframe.
Reliability Index	Reliable
Explanation of Data Reliability Check	Program staff record approved Operations Orders in BPETS. The approving official first reviews the operations order, then manually activates the plan in BPETS. The operations plan then becomes active and ready for execution. If changes to the plan occur, the approval process begins again. Program guidelines require after-action reports (AARs), which staff must record in BPETS upon completion of all operations stored in this system. For any operation active for more than three days, program staff must file an AAR at least once every 90 days to document the ongoing operation’s status. On a monthly basis, Component headquarters staff verify the status of joint operations by reviewing Operations Orders and comparing these against scheduled dates and AARs. Component headquarters staff produce quarterly data integrity reports on the BPETS joint operations, allowing the identification and correction of errors and/or omissions.

Performance Measure	Percent of apprehensions at Border Patrol checkpoints
Program	Border Security Operations
Description	Checkpoints are facilities used by the Border Patrol to monitor traffic on routes of egress from areas on the Southwest and Northern borders. Checkpoints are an integral part of the Border Patrol's defense-in-depth, layered strategy. As such, measurements of activities occurring at checkpoints serve not only to gauge checkpoint operational effectiveness, but also serve as barometers of the effectiveness of the Border Patrol's overall national border enforcement strategy to deny illegal entries into the United States. This measure examines one component of checkpoint activity, the number of persons apprehended by

	Border Patrol agents at checkpoints, divided by all Border Patrol apprehensions made nationwide.
Scope of Data	The scope of this measure includes apprehensions from all permanent and tactical checkpoints, as a percent of all apprehensions by the Border Patrol nationwide during the fiscal year.
Data Source	Summary records from the Checkpoint Activity Report, a web-based application, reside in the Border Patrol Enforcement Tracking System (BPETS). All Border Patrol apprehensions nationwide are recorded in the Enforcement Integrated Database (EID). Apprehension data is entered into the e3 Processing system by Border Patrol Agents at the Station level. The e3 system continuously updates the 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 Office of Chief Information Officer.
Data Collection Methodology	Daily records of apprehensions at each checkpoint (permanent and tactical) are entered by personnel at each checkpoint into the Checkpoint Activity Report, which is contained within BPETS. All Border Patrol apprehensions nationwide are also entered into the e3 system. Information from these systems is extracted quarterly to calculate the numerator, the number of apprehensions at checkpoints, and the denominator, the total number of apprehensions nationwide.
Reliability Index	Reliable
Explanation of Data Reliability Check	Multi-level reviews are conducted to ensure the reliability of the checkpoint apprehension rate. The Checkpoint Activity Report is reviewed by the Supervisory Border Patrol Agents at the station level; by second level Supervisory Border Patrol Agents at the sectors; and by the Border Patrol Headquarters program manager, who conducts a final review reliability check. The Checkpoint Activity Report database is designed with built-in validation to identify errors in data entry. Data are analyzed for compliance of established data protocols and accuracy.

Performance Measure	Percent of people apprehended or encountered multiple times along the Southwest Border between ports of entry
Program	Border Security Operations
Description	This measure examines the percent of deportable individuals who have entered the U.S. illegally and been apprehended or encountered multiple times by the Border Patrol along the Southwest Border. It serves as an indicator of the potential impact of the Border Patrol's consequence delivery system to deter future illegal crossing activity into the U.S. The consequence delivery system divides border crossers into categories, ranging from first-time offenders to people with criminal records, and delivers a consequence for illegal crossing based on this information. Effective and efficient application of consequences for illegal border crossers should, over time, reduce overall recidivism. The measure factors in border crossing activity just within a twelve-month rolling period.
Scope of Data	Deportable illegal entrants that have or receive a Fingerprint Identification Number (FIN), who are apprehended under Title 8 or encountered under Title 42 multiple times within a twelve-month rolling period, are included in calculating this measure. The scope includes only those apprehensions or encounters that 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, and thus are not included in calculating the data for this measure.
Data Source	Apprehension and encounter data are captured by Border Patrol Agents at the station level and 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 U.S. Immigrations and Customs Enforcement (ICE).
Data Collection Methodology	Data relating to apprehensions and encounters are entered into e3 by Border Patrol Agents at the station level as part of the standardized processing procedure. Data input can be made by any agent who knows the details of the apprehension or encounter. This data is typically reviewed regularly at the station, sector or Headquarters level observing trends to provide feedback to the field on operational activity. Calculation of this measure completed by the SDI Unit at Border Patrol Headquarters and is the number of individuals that have been apprehended multiple times during the 12-month rolling period, divided by the total number of individuals apprehended or encountered during the same time period.
Reliability Index	Reliable
Explanation of Data Reliability Check	All apprehension and encounter 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 and encounter 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 SDI 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 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 Southwest and Northern Borders
Program	Border Security Operations
Description	This measure gauges the percent of time agents reach remote low-risk areas to assess notifications of potential illegal activity and make a determination of the nature of this activity. The goal is for Border Patrol Agents to respond to these notifications in remote low risk areas within 24 hours. If not accomplished in a timely fashion, the evidence degrades and determinations cannot be made regarding the nature of the potentially illicit activity. Responding to notifications of activity provides valuable information in terms of both the nature of the detected activity, as well as with confirming whether or not the area continues to be low risk. This measure contributes to our situational awareness and ability to secure the border.
Scope of Data	This population for this measure encompasses all geospatial intelligence-informed reports of potential illicit activity in remote areas along the Southern and Northern land border (excluding Alaska) that Border Patrol sectors have determined to be low flow and low risk. This measure does not include the maritime domain. A response is defined as the time when a Border Patrol Agent arrives at the coordinates for the detection site that was communicated by the Office of Intelligence (OI).
Data Source	The data source is mined from e-mail notifications and individual Field Information Reports (FIR), which are stored in CBP's Intelligence Reporting

	System – Next Generation (IRS-NG) and maintained by CBP's Office of Information Technology.
Data Collection Methodology	When unmanned aircraft systems or other U.S. Government collection platforms detect potential illicit activity, OI sends an e-mail notification to the appropriate Border Patrol Sector. The Sector then deploys Border Patrol Agents to respond to the potential illicit activity. The clock officially starts when the e-mail notification is sent by the OI. The arrival time of Agents at the coordinates provided by the OI is recorded as the response time. Agent response time entries are reviewed by the Patrol Agent In Charge of the Sector Intelligence Unit (SIU) before formally transmitted to OI. A Border Patrol Assistant Chief in OI extracts the FIRs data into an excel spreadsheet, calculates the response times, and then determines what percent of all notifications did agents reach the designated coordinates within 24 hours. The results are then provided to analysts in the Planning Division, who report the results to Border Patrol leadership and to other relevant parties.
Reliability Index	Reliable
Explanation of Data Reliability Check	In the field, the SIU Patrol Agent In Charge reviews and gives approval on all FIR reports prior to their being submitted to OI. After the result is calculated, it is then transmitted to the Planning Division with Sector specific information, including number of notifications and the percent of responses within 24 hours. Analysts review the trend data over quarters to identify anomalies. These are then shared with the Border Patrol Chief and the Chief of the Law Enforcement Operations Directorate to confirm the data and determine how the Sector plans to address any shortfalls.

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. Agents complete extensive Academy Basic Training and are required throughout their career to maintain time-limited certifications in areas such as Firearms Proficiency, Intermediate Use of Force, and Use of Force Policy. In addition, because each sector has a unique climate, terrain, and operational environment, each sector has differing region-specific training requirements. These specialties include handling canines, counter-tunnel operations, horse patrol, All-Terrain-Vehicle (ATV), radiation detection, and snowmobile training. As agent numbers fluctuate, fully trained, deployable agents can mitigate agent-hiring shortfalls. Increasing agents' levels of basic and advanced training enhances the capability to perform mission-essential, law enforcement tasks.
Scope of Data	This measure encompasses every person categorized and assigned as a Border Patrol agent (GS-1896 classification). To be considered fully trained, Border Patrol agents must meet minimum requirements, including the successful completion of Academy Basic Training and post-Academy Field Training Unit instruction and testing, as well as maintaining time-limited certifications in Firearms Proficiency, and a sequence of trainings in Use of Force Policy and techniques for 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	Multiple systems provide the data for this measure, including: a quarterly Resource Readiness Report, fed data from program training-record databases—the Performance and Learning Management System (PALMS); Training, Records,

	and Enrollment Network (TRAEN) system; the Firearms, Armor and Credentials Tracking System (FACTS); and individual sector training-personnel analysis. As agents complete training courses and certifications, 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 each agent's progress into one of the above-listed data sources. 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 listing 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 its TO. The CPA's designee compiles the data into the RRR and submits data to 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. The data is aggregated by the Logistics Division in the Mission Readiness Operations Directorate at U.S. Border Patrol Headquarters. For audit purposes when needed, the data in the Resource Readiness Report can be traced directly back to those systems of record.

Performance Measure	Percent of U.S. Border Patrol equipment assessed as mission ready to support law enforcement operations
Program	Border Security Operations
Description	The measure assesses readiness of equipment used daily in law-enforcement operations between ports of entry for three categories of equipment--Agent Support, Vehicles/Mobility, and Surveillance. Agent supports include hand-held radios, pistols, personal radiation-detection devices, and canines. Vehicles and mobility supports include off-road patrol vehicles, road patrol vehicles, all-terrain vehicles, and snowmobiles. Surveillance resources include integrated fixed towers, mobile video-surveillance systems, remote video-surveillance systems, and low-light visual gear. Information about the availability of required equipment in useful condition enhances the program's ability to perform law enforcement tasks.
Scope of Data	The scope of this measure includes all of the records concerning the serviceability of equipment used in direct support of law enforcement operations across program sectors. Using an evaluation of the operating environment, terrain, and range of threats in a particular program sector, each sector's Chief Patrol Agent (CPA) determines sector-specific equipment requirements based on mission needs in that sector. Each program sector regularly accounts for and records the type, number, and serviceability of all equipment required to support law enforcement using information technology systems operated and maintained by the program.
Data Source	Data for this performance measure come from Resource Readiness Reports (RRRs), Excel spreadsheets prepared in each sector on a quarterly basis. The RRRs draw data from several systems of record, including the Vehicle Management Information System (VMIS); the Canine Tracking System (K9TS); the Firearms, Armor and Credentials Tracking System (FACTS), and the Personal Property

	Module in the Systems Application Process (SAP) tool. Equipment from sectors also provides a source of total inventory of equipment items and their operational status. Sector equipment records will vary by type based on geographic and climate conditions. Sector personnel record the status and serviceability of equipment at regular intervals, and supervisory personnel verify that information for accuracy.
Data Collection Methodology	Program staff in each sector track physical inventory and status of equipment in one of the above-listed data sources. In each sector, staff designated by the CPA collect data from program systems of record to populate that sector's quarterly RRR. Sectors provide the RRR to program Headquarters analysts. Program HQ staff then calculate overall equipment readiness by dividing the total number of mission-capable pieces of equipment by the total number of pieces of equipment in inventory across all program sectors, multiplied by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	Whenever necessary for audit purposes, Headquarters and/or sector staff can trace data in RRRs directly back to the program's 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 under Title 8, encountered under Title 42, and those who were turned back after illegally entering the United States between ports of entry along the Southwest Border. The rate includes apprehensions, encounters, and turn backs to the total estimate of illegal entrants that includes these three groups and also those who got away without being apprehended. Border Patrol achieves desired results by maximizing the apprehension of detected illegal entrants, 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 (a Got-Away in border zones or a No Arrest in non-border zones). This measure is a key indicator of the Border Patrol's law enforcement and resolution impact, a key component of the Operational Control framework.
Scope of Data	The scope includes all Southwest Border areas that are south of the northernmost checkpoint within a given area of responsibility. In Border Zones, it includes all apprehensions, encounters, Turn-Backs (TB), and Got-Aways (GA). In non-Border Zones, it includes all apprehensions, encounters, and No Arrests (NA). An apprehension is a deportable illegal entrant who is taken into custody and receives a consequence. An encounter is an illegal entrant subject to 85 Fed Reg 17060. A GA is an illegal entrant who is not turned back, apprehended, or encountered and is no longer being actively pursued in a border zone. A NA is a subject identified as a result of a non-border-zone tracking action that does not result in an apprehension or encounter but is determined by agents to involve illicit cross-border activity. A TB is a subject who, after making an illegal entry into the United States, returns to the country from which he/she entered, not resulting in an apprehension, encounter, or GA.
Data Source	Apprehension, encounter, GA, NA, and TB data is captured by Border Patrol Agents at the station level into several systems. Apprehensions and encounters 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 U.S. Immigrations and Customs Enforcement (ICE). GA's, TB's, and NA's are recorded

	in the Intelligent Computer Assisted Detection (ICAD) Tracking Sign-cutting and Modeling (TSM) application, which resides with the U.S. Border Patrol. TSM is under the purview of and is owned by the U.S. Border Patrol's Enforcement Systems Unit.
Data Collection Methodology	Data relating to apprehensions and encounters are 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, NA, or TB in the TSM system. Some subjects can be observed directly as evading apprehension/encounter or turning back; others are acknowledged as GA's, NA's, or TB's after BPAs follow evidence that indicate entries have occurred, such as foot sign, sensor activations, interviews with subjects in custody, camera views, communication between and among stations and sectors, and other information. Calculation of the measure is done by the U.S. Border Patrol Headquarters Statistics and Data Integrity (SDI) Unit; the numerator is the sum of apprehensions and encounters and TBs, divided by the total entries, which is the sum of apprehensions, encounters, TBs, GAs, and NAs.
Reliability Index	Reliable
Explanation of Data Reliability Check	Patrol Agents in Charge ensure all agents at their respective stations are aware of and use proper definitions for apprehensions, encounters, GA's, NA's, and TB's. 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, SDI validates data integrity by using various data quality reports. The integrity of Turn-Back, Got-Away, and No Arrest data is monitored at the station and sector levels. Data issues are corrected at the headquarters level, or forwarded to the original inputting station for correction. All statistical information requests are routed through the centralized headquarters office within Border Patrol and SDI coordinates with these entities to ensure accurate data analysis and output is provided.

Performance Measure	Air mission launch rate
Program	Integrated Operations
Description	This measure captures the percent of all requests made for aircraft to which the program could respond, absent gaps in available assets and crew. Capacity to launch aircraft when stakeholders request an aerial response is a core program capability. Requests for aerial response received by an AMO operational location for either planned or unplanned missions is entered into a database, followed by the result of the request. If the mission is flown, it is counted as a launch, and if the mission is not fulfilled, it is counted as a no launch. No launches may be impacted by asset maintenance, capability, other higher priority missions, or unavailable crew. This measure provides a readiness indicator and helps to identify potential problems requiring correction.
Scope of Data	The scope of this measure includes all requests received for the program's aircraft to launch for either planned or unplanned missions. Requests received by aircraft already airborne lie outside of the scope of this measure. If the program cannot provide an aircraft in response to a request, AMO enters one of the following two 'no-launch' explanations within AMO control: 1) asset unavailable (maintenance, capability, other higher priority), or 2) crew unavailable.
Data Source	The Tasking Operations Management Information System (TOMIS), owned by the program and maintained by the Component Office of Information and Technology, provides the data used to calculate this performance measure.
Data Collection Methodology	When an operational facility receives a request for aerial response, staff enter the request and record the result of the request into TOMIS. If the program

	fulfills a request for aerial support, the fulfilled request counts as a 'launch' for purposes of this measure. If the program cannot fulfill a request, the unfulfilled request counts as a 'no launch' for purposes of this measure. Unit- and branch-level supervisors in the program verify and approve TOMIS records in accordance with established policy. Extracting data from TOMIS, Headquarters personnel in the Operations Data division divide total no launches within AMO control (numerator) by the number of launches plus the total no launches within AMO control (denominator), multiplied by 100 to calculate the mission launch rate.
Reliability Index	Reliable
Explanation of Data Reliability Check	Unit- and branch-level supervisors verify and approve TOMIS records in accordance with the established program policy. Contractor and Government staff at program Headquarters separately reconcile this data on a monthly basis.

Performance Measure	Percent of detected conventional aircraft incursions resolved along all borders of the United States
Program	Integrated 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 is 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	Compliance rate for Customs-Trade Partnership Against Terrorism (CTPAT) members with the established CTPAT security guidelines
Program	Trade Operations
Description	This measure reports the overall compliance rate with established minimum security criteria during initial and periodic validations of Customs Trade Partnership against Terrorism (CTPAT) members' supply chain security procedures. CTPAT Supply Chain Security Specialists and the CTPAT participant jointly conduct a validation visit assessing the participant's import supply chain

	security procedures to determine if procedures in place meet current guidelines or criteria, make recommendations, and recognize best practices. Validations may be initiated based on: security related anomalies, strategic threat posed by geographic regions, other risk related information, or strategic import volume. Companies assessed as compliant meet minimum criteria for continued participation in CTPAT. Failure to meet specified criteria results in companies' suspension or removal from CTPAT. Compliance by the trade community with security guidelines enhances the security of cargo shipped to the U.S.
Scope of Data	This measure's population includes the results of all initial or periodic validations (Certified, Validated, Suspended, or Removed) based on the validation results uploaded to the CTPAT Portal during a reporting period. Under the Security and Accountability for Every Port (SAFE Port) Act of 2006, companies in their first year of CTPAT participation must successfully complete a validation by a CTPAT Supply Chain Security Specialist, and all validated members must successfully complete a re-validation within three years of their initial validation. Members' CTPAT status listed as Certified or Validated after a validation visit are included in the reported results. Members listed as a Suspended or Removed after a validation are excluded from the results.
Data Source	The program maintains an internal database, known as the CTPAT Portal database, accessed through the CTPAT Portal, which contains a variety of data pertaining to the CTPAT community. The CTPAT Portal's capabilities include automatic uploading of reports from completed validations and updating each member company's CTPAT status (Certified, Validated, Suspended, or Removed) based on the validation results.
Data Collection Methodology	CTPAT members initially upload their self-reported Company Supply Chain Security Profile to the CTPAT Portal. CBP CTPAT Supply Chain Security Specialists conduct onsite reviews of the profile procedures and document the results of validations through Validation Reports uploaded to the CTPAT Portal database. For a given reporting period, program analysts query the CTPAT Portal database to obtain the number of companies with a status of Certified or Validated following a validation and the total number of validations performed. The total of Certified and Validated members is divided by the total number of validations to get the results for this measure.
Reliability Index	Reliable
Explanation of Data Reliability Check	Supply Chain Security Specialists collect validation results and associated documentation. Each Supply Chain Security Specialist's supervisor reviews these results and documentation. The reviewing supervisor often receives assistance from another supervisor tasked with oversight for that validation. HQ-level program managers complete an additional review of Validation Reports, analyzing and addressing anomalies identified from summary data.

Performance Measure	Cost savings benefit for Customs-Trade Partnership Against Terrorism members (in millions)
Program	Trade Operations
Description	This measure reports estimated cost savings across the air, rail, land, and sea modes attributable to waived cargo examinations achieved during a given reporting period by companies participating in the Customs Trade Partnership Against Terrorism (CTPAT). CTPAT provides a suite of capabilities to facilitate compliance with laws and rules including the Automated Targeting System, which reviews bill and entry data pertaining to cargo destined for a U.S port of entry to assess the security risk associated with each shipment. Compliance with CTPAT's minimum criteria for supply-chain security allows Partners access to

	streamlined business processes and reduced inspection-related delays, which reduce operating costs and enhances the security of cargo shipped to the U.S.
Scope of Data	This measure's scope includes all of the data on original customs and trade transactions during a particular reporting period recorded in information technology systems including the Automated Commercial Environment's Tracer capability, Automated Targeting System's Cargo Enforcement Reporting and Tracking System, and the Customs Trade Partnership Against Terrorism Portal database. In addition, this measure uses data from a 2010 University of Virginia study of multi-modal transportation costs, which estimates average costs attributable to delays for CBP processing in air, rail, sea, and land modes. This study included a survey asking transporters if they could assess costs attributable to CBP delays, and if so, how much these delays cost them. This survey included responses from 1,756 transporters and estimated average costs of delay by mode with a ±2.0 percent margin of error.
Data Source	Program-owned information systems containing data underlying this measure include the Automated Commercial Environment, which provides trade community members a suite of capabilities to facilitate compliance with laws and rules; the Automated Targeting System, which reviews bill and entry data pertaining to all land, sea, or air cargo destined for a U.S port of entry to assess the security risk associated with each shipment; and the Customs Trade Partnership Against Terrorism (CTPAT) Portal database, used to collect, record, and assess information provided to the program by Partner companies. In addition, this measure uses data from a 2010 University of Virginia study of multi-modal transportation costs, which estimates total cost savings attributable to waived examinations for the vessel, air, and truck modes.
Data Collection Methodology	To construct the result for a particular reporting period, HQ staff extract data from ACE and ATS. For each mode of transportation (air, rail, sea, land), program staff query systems for 1) the rate at which CBP examines shipments made by companies not participating in CTPAT and 2) the number of shipments made by companies participating in CTPAT, i.e. those not subject to the relevant CBP examination. The product of these two numbers estimates the number of examinations avoided by participation in CTPAT for each transport mode. Analysts then multiply this number by the estimated average cost of CBP-attributable delays for that mode, adjusted for inflation—this quantity estimates the cost avoided by CTPAT participants for each mode in a given reporting period. Summing each of these avoided-cost estimates across the air, rail, land, and sea modes produces the result for the period.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data used to calculate this performance measure principally comes from the Automated Commercial Environment and the Automated Targeting System (ATS), both program-owned systems of record employing highly automated data-transfer and processing capabilities. The program's Customs Trade Partnership Against Terrorism relies upon the data-cross-checking functions available in ATS to ensure data accuracy. HQ staff investigates anomalies in quarterly results, tracing them back to field activities if necessary for clarification, explanation, and correction.

Performance Measure	Monetary savings realized by the trade community from implementation of new capability in the Automated Commercial Environment Information Technology System (in millions)
Program	Trade Operations
Description	This measure estimates monetary savings to the trade community from using capabilities in the program's Automated Commercial Environment (ACE) system.

	The program surveys trade stakeholders to estimate cost savings per transaction for each transaction type, distinguished by use of ACE capabilities including 1) Periodic Monthly Statement Processing, 2) Periodic Monthly Statement Interest, 3) Truck Primary Processing Time, 4) Post Summary Correction, 5) Export Licenses, 6) eBonds, 7) Census Warning Override, 8) Protests, 9) Quota, 10) Export Data Submission, 11) Eliminate Paper 7501 and 12) Entry Type 86. Savings from each capability equals the product of per-transaction savings estimated for each capability and the number of transactions recorded in ACE for each capability. The measure result equals the sum of the estimated savings for all capabilities. Tracking savings from automation of trade processes gauges how the program balances support for trade growth with enforcing U.S. rules.
Scope of Data	The unit of analysis for this measure is the estimated monetary savings realized by trade stakeholders from using one of the above-listed ACE capabilities to process a transaction during a given reporting period. The sum of estimated savings from the use of each ACE capability produces the result for that period. An ACE capability ordinarily consists of automated processes including the submission of data by stakeholders which may trigger responses by the program. The population of this measure includes all data from transactions processed by the program using the above-listed capabilities deployed in the ACE system.
Data Source	Through a contractor, the program administers the ACE system and maintains the data contained in the system relating to all transactions conducted. Around the tenth day of each month, program staff in the program’s Accountability and Evaluation (A&E) Branch create and save ad hoc queries using ACE’s Business Objects reporting tool. These queries extract transaction-level data in volume for each of the system’s capabilities.
Data Collection Methodology	Program staff administer surveys to the trade community to develop estimates of cost savings per transaction for each transaction type, i.e., each of the Automated Commercial Environment’s in-scope capabilities. Analysts in the program’s Accountability and Evaluation (A&E) Branch estimate total savings from each ACE capability in a given reporting period by multiplying the per-transaction estimate for each capability by the number of transactions for each ACE capability during that period. Analysts produce the results by summing the estimated savings across all in-scope capabilities for the reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	The program ensures data reliability using the ACE system’s built-in validation process as the system of record for each capability, which checks that the measure calculated in each reporting period reflects the total number of records extracted. In addition, the program verifies reliability through a process to review the quality of the contractor’s deliverables in advance of acceptance by the program’s Accountability and Evaluation Branch (A&E). As the process owner, A&E takes responsibility for detection of anomalies and associated corrective actions.

Performance Measure	Number of shipments seized as a result of intellectual property rights violations
Program	Trade Operations
Description	This trade measure counts the number of seizures made by CBP and U.S. Immigration and Customs Enforcement (ICE) for Intellectual Property Rights (IPR) violations. The term 'shipment' includes a wide range of cases, from an individual traveler in possession of one item, to international mail, and palletized commercial shipments of large quantities of items violating IPR. CBP seizures generally occur at or near a port of entry, while ICE seizures generally result from domestic and international customs-enforcement activities by Homeland Security Investigations. IPR infringement undermines the economic vitality of the

	United States by reducing the competitiveness of U.S. industry, threatens national security due to infiltration of counterfeit parts in the supply chain for defense systems and other critical infrastructure, and poses risks to the health and safety of consumers. CBP and ICE contribute to U.S. national and economic security by seizing these countified goods.
Scope of Data	This measure's scope includes all shipments seized by CBP and ICE for Intellectual Property Rights (IPR) violations during a particular reporting period. The term 'shipment' includes a wide range of cases, from an individual traveler in possession of one item that violates IPR, to international mail, to a palletized commercial shipment of a very large number of items violating IPR. CBP seizures generally involve the Office of Field Operations at or near a port of entry, while ICE seizures generally result from domestic and international customs-enforcement activities by Homeland Security Investigations.
Data Source	Data for this measure come from the Seized Assets and Case Tracking System (SEACATS), owned by CBP and operated by the Office of Field Operations. SEACATS contains data from all IPR-related seizures by CBP and ICE, updated in near-real time.
Data Collection Methodology	Immediately following the end of the quarter, program staff extract data for the previous quarter's seizures from SEACATS. Staff then compile this information, grouping seized products into categories to highlight current areas of enforcement focus. Program staff count each shipment only once, even if that shipment includes multiple lines or multiple counterfeit product types. Summing these counts across all product types produces the performance measure for a particular reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	Analysts maintain quality control with an automated process based on updated business rules to ensure that the final measure reflects the total number of cases extracted, and a manual review of selected cases to ensure correct categorization. The validation process covers both CBP and ICE seizures since both agencies use SEACATS as their system of record for IPR seizures, and components resolve any discrepancies through CBP's Intellectual Property Rights Center of Excellence.

Performance Measure	Percent of cargo by value imported to the United States by participants in CBP trade partnership programs
Program	Trade Operations
Description	This measure reports all cargo imported to the United States through CBP trade partnership programs as a share of the total value of all cargo imported. Partnership programs include both the Customs Trade Partnership against Terrorism (CTPAT) and the Importer Self-Assessment (ISA) program. CBP works with the trade community through these voluntary public-private partnership programs to adopt tighter security measures throughout their international supply chain in exchange for benefits, such as a reduced number of inspections, shorter wait times at the border, and/or assignment of a Supply Chain Security Specialist to a partner firm. Trade partnership programs enhance the security of the supply chain by intercepting potential threats before the border while expediting legal trade.
Scope of Data	The population of this measure includes all cargo imported to the United States. Cargo imported through CTPAT and ISA CBP trade partnership programs is reported in the results. A variety of trade actors participate in these programs, such as importers, carriers, brokers, consolidators/third-party logistics providers, marine port-authority and terminal operators, and foreign manufacturers. Each

	CTPAT and ISA member is assigned a unique identification number that is entered in ATS and ACE with each unique import-entry shipment.
Data Source	CBP stores relevant data on cargo imports in two CBP information technology systems, the Automated Targeting System (ATS) and the Automated Commercial Environment (ACE). Reports for this measure are extracted from the ACE Reports module and the ATS Analytical Selectivity Program.
Data Collection Methodology	For each shipment of cargo imported to the United States, the broker responsible for the shipment transmits information electronically to ATS and ACE under a unique import-entry number, including individual lines with a Harmonized Tariff Schedule of U.S. numbers and monetary line values. CBP's Office of International Trade extracts data on all shipments from ATS and ACE on a quarterly basis. Import-entries completed by trade partnership members are filtered by their CTPAT or ISA shipper number. After extraction of the imports' monetary line values, (OT) analysts calculate the measure for a particular reporting period by dividing the sum of import values associated with ISA or CTPAT importers by the total value of all imports.
Reliability Index	Reliable
Explanation of Data Reliability Check	Both field-level and HQ-level analysts complete monthly internal monitoring of this measure's processes and data quality. As part of compiling and reporting results for this measure, CBP also compares source data for the measure in ATS and ACE to separate data sets and measures in ACE Reports and the Analytical Selectivity Program.

Performance Measure	Percent of import revenue successfully collected
Program	Trade Operations
Description	This measure assesses the effectiveness of ensuring that the importers pay the proper amount of taxes and duties owed on imports. Importers must deposit the revenue owed, which they estimate based on type of import, declared value, country of origin, and quantity being imported. CBP impacts the results by implementing enforcement actions and providing guidance and estimation tools that serve to reduce importer fraud, negligence, and misunderstanding in estimating revenue owed. Results are used to determine the need for additional or changed policies, enforcement actions, and guidance. This measure aligns to the goal of protecting national economic security, facilitating fair trade, supporting the health and safety of the American people, and ensuring a level playing field for U.S. industry. External factors such as foreign governments that support importer noncompliance and unforeseen changes in policy and trades laws may result in underpayment of import revenue.
Scope of Data	The unit of analysis is an import (i.e., a commodity or set of merchandise being imported) as defined by an entry line on the CBP Entry Summary Form 7501 that describes the import (e.g., type, value, origin, etc.). The attribute is the net of importers' over- and underpayments of duties and taxes owed on the import. The population includes all of the imports for a given time period, excluding non-electronic informal entries. Each year, the Trade Compliance Measurement (TCM) program creates a stratified sample based on sampling rules (aka user defined rules) that account for changes in the import population and risk factors. A post-entry review of the selected sample is used to identify the amount of over-/underpayment for each import (entry line) in the sample. The net total under-/overpayment across imports is known as the revenue gap. The revenue gap for the sample is used to estimate the revenue for the population with a 95 percent confidence level.
Data Source	Data resides in CBP's Automated Targeting System (ATS) with User Defined Rules (UDR) that help identify the sample. Program staff record findings from the Trade

	Compliance Measurement (TCM) review in CBP's Automated Commercial Environment (ACE) information technology system, using ACE's Validation Activity (VA) function. On a monthly basis, a TCM analyst download the data from ATS into a local MS Access datafile for analysis. The CBP Performance Management and Analysis Division (PMAD) within the Office of Accountability is responsible for preparing a report of the measure results, provided by TCM, to CBP leadership and reporting them to PA&E. Since the post-entry reviews of the samples are not completed until January 31 of the following fiscal year, the annual result reported at the end of the current fiscal year is an estimate. The estimate is updated in the one-number system once the final result is available.
Data Collection Methodology	The determination of the under-/overpayment of revenues owed on the import in the sample is carried out by teams of import entry specialists located in the CBP field offices. Each office is responsible to review entry lines for imports under their jurisdiction. After receiving a sample of entry lines via ACE VA, each review team checks the importer's estimate of validate the duties, taxes, and fees owed for each import and records the amount of under-overpayment with a Validation Activity Determination (VAD) stored in ACE. A TCM statistician retrieves the VAD data in ACE using SQUEL, transfers it to an MS Access datafile, uses standardized Statistical Analysis System (SAS) commands to calculate the measure result for a given period. The statistician sends the measure results for a given period to PMAD. The calculation is [1-(Estimated Revenue Gap/Total Collectable Revenue)] x100.
Reliability Index	Reliable
Explanation of Data Reliability Check	HQ staff host quarterly conference calls with field locations for open discussion of any issues and provides reports to field locations in the event requiring remediation. Analysts document this oversight, sharing this documentation annually with outside auditors as evidence of program control.

Performance Measure	Percent of imports compliant with U.S. trade laws
Program	Trade Operations
Description	This measure gauges the results of an annual CBP review of imports into the U.S., which assesses imports' compliance with U.S. trade laws, including laws related to customs revenue. CBP's Trade Compliance Measurement (TCM) program covers a population of all consumption and anti-dumping/countervailing duty (AD/CVD) transaction types, reporting the share of all transactions free from major discrepancies, excluding informal entries, excluding non-electronic informal entries comprising about 15 percent of entries. Reviewing transactions to ensure that imports remain legally compliant and free of major discrepancies facilitates lawful trade flows.
Scope of Data	This measure's scope includes data on all import transaction types involving antidumping- or countervailing-duty (AD/CVD) payments, maintained in CBP's Automated Targeting System (ATS). Each year, CBP's Trade Compliance Measurement (TCM) program creates a statistical sample of AD/CVD import-entry lines from a population of such imports. Program staff stratify the sample lines by importers' assignment to one of CBP's operational Centers of Excellence and Expertise and the Importer Self-Assessment (ISA) program.
Data Source	Data resides in CBP's Automated Targeting System (ATS) with User Defined Rules (UDR) for processing. Program staff record findings from the Trade Compliance Measurement (TCM) review in CBP's Automated Commercial Environment (ACE) information technology system, using ACE's Validation Activity (VA) function.
Data Collection Methodology	At the start of each fiscal year, program staff define rules in ATS to construct a stratified random sample of import-entry lines from the previous year's data on imports, risk, volume, value, and compliance history. Data processing identifies

	import-entry records containing a major discrepancy, defined by specified criteria reaching a specific threshold. Examples include a discrepancy in value or a clerical error producing a revenue loss exceeding $1,000.00; an intellectual property rights violation; or a country of origin discrepancy placing it in the top third of revenue losses or resulting in a revenue loss exceeding $1,000.00. Analysts determine the share of the sample which includes a major discrepancy under the criteria specified: This Major Transactional Discrepancy rate is subtracted from 1 and multiplied by 100 to determine the percent in compliance.
Reliability Index	Reliable
Explanation of Data Reliability Check	ATS identifies user-defined summary lines of entry transactions, which opens a Validation Activity in ACE. Each CBP field office reviews the identified summary line transaction for compliance, and records findings with a Validation Activity Determination stored in ACE. CBP HQ analysts extract VAD data from ACE monthly, and a statistician resident in CBP's Trade Analysis and Measures Division compiles and reviews statistics monthly and at year-end.

Performance Measure	Percent of inbound cargo identified as potentially high-risk that is assessed or scanned prior to departure or at arrival at a U.S. port of entry
Program	Trade Operations
Description	This measure reports the percent of international cargo coming to the U.S. via air, land, and sea, which CBP identified as potentially high-risk and then assessed or scanned prior to departure from a foreign port of origin or upon arrival at a U.S. port of entry to address security concerns. CBP assesses risk associated with a particular cargo shipment using information technology (IT) systems. Shipments include a wide range of cargo, from international mail to a palletized commercial shipment of packaged items. An automated system check flags a shipment as potentially high-risk when information meets specified criteria, which triggers actions in the field such as assessing or scanning of potentially high-risk shipments. Assessing, resolving, and scanning potentially high-risk cargo prior to departure from ports of origin or upon arrival at ports of entry ensures public safety and minimizes impacts on trade through effective use of risk-focused targeting.
Scope of Data	This measure's scope includes bill and entry data pertaining to all cargo from international mail to a palletized commercial shipment of packaged items in the land, sea, or air environments destined for a U.S. port of entry. The scope of reported results includes all shipments with final disposition status of assessed or scanned prior to departure.
Data Source	CBP collects and maintains this information on systems of record owned by CBP, including the Automated Commercial System (ACS), the Automated Export System (AES), the Automated Commercial Environment (ACE), TECS, and systems owned by partner governments and the private sector. All of these systems feed data in real time to the CBP's Automated Targeting System (ATS), which assesses the security risk associated with each shipment. ATS reviews bill and entry data pertaining to all destined for a U.S port of entry, identifying shipments as potentially high-risk using scenario-based modelling and algorithms. The ATS Exam Findings Module (EFM) contains the data used by the program to determine the disposition of cargo flagged as potentially high-risk.
Data Collection Methodology	Shippers and brokers provide manifest data for cargo through several systems feeding into ATS, which compiles the set of shipments scored as high-risk. CBP officers review information in ATS on high-risk shipments; resolve or mitigate security concerns; determine cases requiring more examination; and record findings from this review in ATS EFM. Program officers enter findings in the ACE for land shipments, a mandatory requirement for release of trucks and cargo at

	land ports of entry. Using data compiled in the ATS Exam Findings Module during a reporting period, program analysts calculate the results by counting all shipments scored as potentially high-risk and counting the subset of potentially high-risk shipments with final disposition status effectively determined. The number of status-determined potentially high-risk shipments is divided by the total number of potentially high-risk shipments, and multiplied by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	Supervisors periodically extract data on findings from examinations of potentially high-risk shipments from the Automated Targeting System's Exam Findings Module for review and validation of data entered by CBP officers in the field. Supervisors identify anomalies in findings data and ensure immediate corrective action(s) to ensure data integrity. Program HQ staff compiles this measure quarterly, provides it to program leadership and DHS. HQ staff investigates anomalies in quarterly results, tracing them back to field activities if necessary for clarification, explanation, and correction.

Performance Measure	Total value of Intellectual Property Rights seizures (in billions)
Program	Trade Operations
Description	This measure reports the percent of international cargo coming to the U.S. via air, land, and sea, which CBP identified as potentially high-risk and then assessed or scanned prior to departure from a foreign port of origin or upon arrival at a U.S. port of entry to address security concerns. CBP assesses risk associated with a particular cargo shipment using information technology (IT) systems. Shipments include a wide range of cargo, from international mail to a palletized commercial shipment of packaged items. An automated system check flags a shipment as potentially high-risk when information meets specified criteria, which triggers actions in the field such as assessing or scanning of potentially high-risk shipments. Assessing, resolving, and scanning potentially high-risk cargo prior to departure from ports of origin or upon arrival at ports of entry ensures public safety and minimizes impacts on trade through effective use of risk-focused targeting.
Scope of Data	This measure's scope includes all shipments seized by CBP and ICE for Intellectual Property Rights (IPR) violations during a particular reporting period. The term "shipment" includes a wide range of cases, from a single item that violates IPR, to international mail, to a palletized commercial shipment of a very large number of items violating IPR. CBP seizures generally involve the Office of Field Operations at or near a port of entry, while ICE seizures generally result from domestic and international customs-enforcement activities by Homeland Security Investigations.
Data Source	Data for this measure come from the Seized Assets and Case Tracking System (SEACATS), owned by CBP and operated by the component's Office of Field Operations. SEACATS contains data from all IPR-related seizures by CBP and ICE, updated in near-real time. SEACATS also contains MSRPs entered as an official record of the mission program, following market research by import specialists and approval by supervisory industry experts. Sources for MSRPs include the Commerce Department's Bureau of Economic Analysis and industry retailers' indexes.
Data Collection Methodology	Immediately following the end of the quarter, program staff extract data for the previous quarter's seizures from SEACATS. Staff then compile this information, grouping seized products into categories to highlight current areas of enforcement focus. Program staff count each shipment only once, even if that shipment includes multiple lines or multiple counterfeit product types. Staff first calculate the total value for each product type seized during the reporting

	period, multiplying the number of products of each type by the MSRP for each product type. Summing these values across all product types produces the performance measure for a particular reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	Analysts maintain quality control with an automated process based on updated business rules to ensure that the final measure reflects the total number of cases extracted, and a manual review of selected cases to ensure correct categorization. The validation process covers both CBP and ICE seizures since both agencies use SEACATS as their system of record for IPR seizures, and components resolve any discrepancies through CBP's Intellectual Property Rights Center of Excellence.

Performance Measure	Amount of smuggled outbound currency seized at the ports of entry (in millions)
Program	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. Data are extracted quarterly and tabulated for reporting requirements.
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	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 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. Data are extracted quarterly and tabulated for reporting requirements.
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 Global Entry members with no security-related violations
Program	Travel Operations
Description	This measure calculates the percent of Global Entry (GE) members who are found to have no violations that would provide a legitimate reason to suspend or revoke a person’s GE membership during the course of the fiscal year. CBP checks all GE members against major law enforcement databases every 24 hours. The measure demonstrates the effectiveness of the GE trusted traveler program at correctly identifying low-risk travelers and quickly incorporating any changes in traveler risk-status that result in suspension or removal to ensure that all active GE members meet required security protocols at all times.
Scope of Data	The measure covers all individuals who are current enrollees of the CBP GE trusted traveler program during the course of the Fiscal Year.
Data Source	All data is pulled from the Trusted Traveler Program membership database, which is an automated system maintained by CBP, that records individual security-related information for all GE enrollees.
Data Collection Methodology	The CBP National Targeting Center checks all current GE members against major law enforcement databases every 24 hours to identify any GE members who have a law enforcement violation, derogatory information related to terrorism, membership expiration, or any other legitimate reason to warrant suspending or revoking trusted status and conducting a regular primary inspection. Reports are generated from the Trusted Traveler Program database to calculate the results for this measure on a quarterly basis.
Reliability Index	Reliable
Explanation of Data Reliability Check	CBP conducts frequent queries against the law enforcement databases used by the National Targeting Center (NTC) throughout the various enrollment steps, including at initial GE application, during the in-person interview, and throughout GE program membership on a 24-hour basis. The system allows CBP to perform vetting and re-vetting in real time. The derogatory information is captured and taken under consideration immediately upon being recorded in the law enforcement databases. This update of the initial vetting and the recurrent 24-hour re-vetting quickly assesses violations and criminal information that could render a member ineligible to participate in the program. In addition, CBP conducts system checks, random examinations, and document screening to verify data and program reliability.

Performance Measure	Percent reduction of processing and wait times for members of Global Entry and other Trusted Traveler programs compared to non-members
Program	Travel Operations

Description	This measure highlights the benefit of membership in Global Entry and other Trusted Traveler programs by demonstrating the reduction in delays (processing and wait times) experienced by Global Entry and other trusted program members when entering the U.S. in comparison to regular travelers.
Scope of Data	Successful Global Entry/Trusted Traveler kiosk crossings are recorded in TECS for confirmed passengers, with specific start and completion time data that enables CBP to calculate accurate individual processing times for all crossings. The Global Enrollment System (GES) contains Trusted Traveler program member data for all Trusted Traveler programs. Using the recorded data, the average delay time for travelers enrolled in Global Entry can be calculated and compared with the average wait time for regular travelers who are not members to determine the time savings experienced as a benefit of Global Entry/Trusted Traveler membership.
Data Source	OIT maintains a database of successful Trusted Traveler kiosk crossings, which are recorded in TECS. The regular traveler data is obtained from the Airport Wait Times Console, which contains an extract of individual traveler data from TECS. TECS is the system of record for CBP law enforcement transaction data.
Data Collection Methodology	Data collection is highly automated. The OIT database contains information gathered electronically from kiosk crossings of enrollees in one of the CBP Trusted Traveler Programs, which include Global Entry, FAST, NEXUS, and SENTRI. This information is extracted from the database and merged with GES data before successful kiosk crossings are recorded in TECS for confirmed passengers. This information is then extracted to compile enrollment statistics broken out by Trusted Traveler program.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data is tested and verified every day for the previous day's kiosk entries and every flight and passenger is reviewed for data anomalies and corrected as necessary.

Cybersecurity and Infrastructure Security Agency

Performance Measure	Number of new hires made under the Cyber Talent Management System (Retired Measure)
Program	Cybersecurity
Description	This measure demonstrates progress towards an initial hiring target for the newly created Cyber Talent Management System (CTMS). The CTMS is an exempted personnel hiring system that is tailored to the unique education, certifications, approaches, and processes for the cybersecurity workforce. The CTMS system includes a focus on the capability of people, not the duties of the position; a focus on continuous development and refreshment of cybersecurity capabilities; and recognizes that mission needs and talent shifts occur across the Department, resulting in the ability to move individuals around the Department seamlessly. Hiring cyber professionals under this new system is critical to aligning prospective cybersecurity talent to the most pressing cybersecurity needs and will allow these technical professionals to accelerate their careers as rapidly as their aptitudes allow.
Scope of Data	The scope for this measure are all hires that are made under the CTMS authority for the reporting period out of the total population of cyber hires. Not all cyber hires will initially be made under this hiring authority. This measure only includes those CISA hires made under the new CTMS authority.

Data Source	The data source for this metric will be the CISA Pipeline which is the system of record that Human Capital specialists use to manage and track recruitments. CISA will extract data from the CTMS system that will be maintained by DHS CHCO, to ensure that only CISA hires are counted towards this measure.
Data Collection Methodology	As data from CTMS becomes available, OCHCO analysts will extract data and upload updates to the CISA Pipeline. Personnel identified as hired under the CTMS authority in Pipeline during the reporting period are the numerator for this measure, divided by the total cyber hires using all hiring authority, and multiplied by 100 to get the result.
Reliability Index	Reliable
Explanation of Data Reliability Check	Every quarter the Human Capital Service Team within CHCO reviews and verifies the data to ensure that the data was properly extracted from CTMS and that the number of new hires is correct. Results for this measure will be reported on a template provided by the Performance Management Branch (PMB) within the Office of Strategy, Policy, and Plans. Analysts within PMB will review quarterly results for consistency and adherence to the measure's defined scope and calculation.

Performance Measure	Percent of critical and high configuration-based vulnerabilities identified through high value asset assessments mitigated within 30 days (Retired Measure)
Program	Cybersecurity
Description	This measure reports the percent of critical and high configuration-based vulnerabilities identified in High Value Assets (HVA) assessments that have been mitigated within 30 days. HVA assessments are performed across the Federal Government to identify vulnerabilities associated with the most sensitive IT systems and data. Configuration-based vulnerabilities are those that can be more quickly be mitigated by agencies through such actions as changing security settings, software or configuration changes, patching software vulnerabilities, and adjusting user account privileges. Agencies report monthly to the program on the status of mitigating these configuration-based vulnerabilities. The results indicate if agencies are resolving less complex HVA vulnerabilities within the government-wide goal of 30 days.
Scope of Data	The population for this measure is all critical and high configuration-based vulnerabilities that are mitigated during the fiscal year. HVA vulnerabilities include both those identified in Risk and Vulnerability Assessments and Security Architecture Reviews. HVAs are those assets within federal agencies and departments they self-nominate as high value and do not include Department of Defense or the Intelligence Community assets. The value being assessed are those vulnerabilities mitigated within 30 days. The data included in this measure is based on Agency reports delivered to the program between September of the previous fiscal year to August of the current fiscal year.
Data Source	Each HVA vulnerability has a mitigation plan that the responsible agency serves as the data source for vulnerability status. These plans serve as the data source for determining configuration based vulnerabilities mitigation status. These plans are emailed to CISA by the agency and saved on the Homeland Security Information Network (HSIN). The program analysts record results of configuration-based vulnerability resolution in a spreadsheet that is stored HSIN. The CISA HVA program is responsible for oversight of these data sources.
Data Collection Methodology	After receiving a final HVA assessment report, agencies develop initial mitigation plans within 30 days and then report monthly on the status of mitigating their configuration based vulnerabilities. The submitted plan is reviewed by an analyst to determine if the milestones and objectives of the plan meet the objectives identified from the remediation recommendation of the assessment. Once the

	final plan has been submitted, an analyst will review the remiedation steps to verify that they meet the original plan objectives. These results are then recorded by the analyst on the tracking spreadsheet. The result is calculated by dividing the number of configuration-based vulnerabilities mitigated within 30 days of initial identification by all vulnerabilities mitigated during a fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	The results will be reviewed for accuracy by the Cybersecurity Division Capacity Building Office by comparing the master spreadsheet data with the individual agency submissions. The CISA Office of Strategy, Policy, and Plans will consolidate findings and transmit to DHS.

Performance Measure	Percent of critical and high vulnerabilities identified through cyber hygiene scanning mitigated within the designated timeframe (Retired Measure)
Program	Cybersecurity
Description	This measure calculates the percent of significant (critical and high) vulnerabilities, identified through cyber hygiene scanning, that have been mitigated within the specified timeline. For critical vulnerabilities, mitigation is required within 15 days from point of initial detection, and for high vulnerabilities mitigation is required within 30 days. Cyber hygiene scanning prioritizes vulnerabilities based on their severity as a means for agencies to make risk-based decisions regarding their network security. Identifying and mitigating vulnerabilities on a network in a timely manner is a critical component of an effective cybersecurity program, as it is critical to maintaining operational availability and integrity of IT systems.
Scope of Data	The scope of data for this measure is: 1) all significant (critical and high) vulnerabilities identified by cyber hygiene vulnerability scanning on internet-accessible devices; 2) all critical and high vulnerabilities detected in previous scanning that were mitigated during the measurement period; and 3) all critical and high vulnerabilities that 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 for mitigation 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 detected. When a vulnerability finding is 'closed' due to it being marked as a false positive (i.e. a reported finding that incorrectly indicates a specific vulnerability or setting is present on a stakeholder’s internet-accessible devices), it is not included in the calculation for this measure.
Data Source	Cyber hygiene scans utilize two tools: Nmap for host discovery, and Nessus for scanning identified hosts for known vulnerabilities. Results from these scans are collected with a Client Access License (CAL) and stored on an internal DHS network that is operated and maintained by the Cyber Hygiene Scanning Team.
Data Collection Methodology	This measure gauges the total number of critical and high vulnerabilities compared to those mitigated within the designated timeframes. A vulnerability’s age is calculated from when it is first detected on a scan to when it is no longer visible on the scan. Subsequent scanning tracks a vulnerability for 90 days after it appears closed to ensure the vulnerability isn’t simply unresponsive to a scan. If a vulnerability is re-detected within 90 days, it is re-opened using the original date of detection, and included in subsequent cumulative calculations. Data analysis software will be used to run a report on the percent of criticals and highs that were mitigated within the designated timeframe. The result is calculated by adding the number of critical vulnerabilities mitigated within 15 days plus the number of high vulnerabilities mitigated within 30 days divided by total number of both open and closed critical and high vulnerabilities.
Reliability Index	Reliable

Explanation of Data Reliability Check	The Cyber Hygiene Scanning team within the CISA Cyber Assessments Team will coordinate with the CISA Insights Branch to review the algorithm to query the data and the quarterly result for this measure to ensure correct data collection and calculation procedures were used. CISA Program Analysis & Evaluation will also review the quarterly results and accompanying explanations prior to final submittal to DHS.

Performance Measure	Percent of potential malicious cyber activity notifications where impacted agencies were alerted within the specified timeframe (Retired Measure)
Program	Cybersecurity
Description	The measure tracks the percent of potential malicious cyber activity notifications identified as credible where the affected agency is alerted within the specified timeframe. Potential malicious cyber activity on federal networks is detected by automated tools through the National Cyber Protection System (NCPS) alert-based detection function. The system sends automated notifications to analysts within NCPS, who then manually review the notification(s), confirm if a potential credible threat exists, and if so, the affected agency is sent an email for their further exploration. The specified timeframe to notify affected agencies of potential malicious cyber activity is 18 hours for FY20 and 12 hours for FY21.
Scope of Data	The population of data includes cases of potential malicious cyber activity entered into the Remedy system. Notifcation times associated with these credible potential malicious cyber activity cases form the basis for this measure. The specified timeframe to notify affected agencies of potential malicious cyber activity is 18 hours for FY20 and 12 hours for FY21.
Data Source	NCPS sends alerts of potential malicious activity to program analysts. Computer Network Defense (CND) analysts create a case in the Remedy system if there appears to be credible malicious activity. Tableau, a graphical reporting tool, pulls data from Remedy to calculate this measure, Remedy tickets are maintained by the Integrated Operations Division (IOD) Helpdesk. Cybersecurity Division (CSD) manages both the NCPS and Remedy systems.
Data Collection Methodology	When the NCPS detects potential malicious cyber activity, it sends a notification to analysts, who review the notifications, and if credible, creates a case in the Remedy system which includes the initial NCPS alert time and an email is sent to the affected agency. The initial detection time is recorded in the NCPS system when it notifies the analyst team of the potential threat (the first notification time is used if multiple notifications occur for the same threat). The agency notification time is the date time stamp recorded when the email is sent from the Remedy system to the agency. The time to notify for each case is calculated by subtracting the initial detection time from the agency notification time. The Process, Metric and Reporting Analysts extract information from Remedy to Tableau to calculate the time to notify, and what percent of cases fall within the specified window.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data collection, review and vetting will be conducted by CSD Strategy and Resources Office (S&R) Process, Metrics and Reporting Analysts monthly and at each quarter in collaborations with CSD Branch Chiefs to assess validity, consistency and identify potential issues early on during the APG/GPRA reporting period.

Performance Measure	Percent of all state and territory emergency communications interoperability components operating at the highest levels
Program	Emergency Communications

Description	The measure identifies the current level of emergency communications interoperability maturity across 56 states and territories as defined by the National Council of Statewide Interoperability Coordinators (NCSWIC) Interoperability Markers. The 24 markers cover a range of interoperability factors including governance, standard operating procedures, technology, training and exercises, usage, and others, allowing states and territories to benchmark their progress and enhance their capabilities for interoperable communications. Each state and territory self-evaluate their interoperability maturity annually against all 24 interoperability components. Markers operating as “defined” or “optimized” based on best practices are considered the highest levels. Interoperable emergency communications capabilities enable first responders and government officials to continue to communicate during response to incidents or disasters.
Scope of Data	The measure covers the current status of the NCSWIC Interoperability Markers for all 56 states and territories, evaluating their interoperability capability along one of three maturity ratings: initial, defined, or optimized for each of the 24 markers. The 24 standardized markers cover a range of interoperability factors including governance, standard operating procedures, technology, training and exercises, usage, and others, allowing states and territories to benchmark their progress and enhance their capabilities for interoperable communications. “Initial” indicates little to no maturity reached on a particular marker, “defined” means a moderate level of maturity, and “optimized” means the highest level of maturity based on best practices.
Data Source	ECD staff coordinates with the Statewide Interoperability Coordinator (SWIC) for each state or territory to review each marker and the maturity levels to most accurately capture their current state. The data is initially entered by Emergency Communications (ECD) staff on an Excel spreadsheet on SharePoint and migrated to a Tableau-based analytics tool. The maturity level data (initial, defined and optimized) for each of the 24 markers is consistently identified in a drop-down list in excel.
Data Collection Methodology	NCSWIC Interoperability Markers data are collected and analyzed to determine the current state and trends of interoperability progress across the nation. ECD staff support SWICs with a self-evaluation of their capabilities along the 24 Interoperability Markers, indicating whether the state’s level of maturity is “initial,” “defined,” or “optimized”. The data is initially located on an Excel spreadsheet on SharePoint and migrated to a data analytics tool. Data is extracted from Tableau using a manual query that filters “defined” and “optimized” ratings. The numerator is the number of total markers reported by states/territories that are either “defined” + “optimized divided by 1344 [24 markers x 56 states and territories]. The result is multiplied by 100 to determine the percentage.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data is collected from SWICs with assistance and guidance from ECD coordinators to ensure consistency. ECD staff review and validate information with the SWIC on a regular basis to ensure the most current information is captured, measure progress, and inform ECD service delivery. This information will be reviewed by the ECD Performance Management Manager.

Performance Measure	Percent of emergency communication grant recipients compliant with SAFECOM guidance requirements (Retired Measure)
Program	Emergency Communications
Description	This measure gauges the percent of grant recipients in compliance with requirements in the SAFECOM Guidance on Emergency Communications Grants.

	SAFECOM began as part of the Presidential E-Government Initiative to improve public safety interoperability, allowing emergency responders to communicate effectively before, during, and after emergencies and disasters. Department of Homeland Security (DHS) grant recipients investing in emergency communications are required to comply with SAFECOM Guidance. The guidance promotes the use of established best practices to ensure investments in emergency communications are interoperable. This measure tracks the improvement in grant recipients meeting SAFECOM requirements to ensure emergency communications investments are interoperable.
Scope of Data	The scope includes all active DHS grants that are required to follow the SAFECOM Guidance. The results are based on a checklist developed from Appendix D of the SAFECOM Guidance - Compliance Requirement for DHS Grants. Due to awards being made at the end of the FY, reporting is delayed by one cycle. For example, information pertaining to the FY19 awards will be collected and reported on in FY20.
Data Source	Data for this measure is gathered through the Grants Reporting Tool's Biannual Strategy Implementation Report (BSIR) submission which is managed by Federal Emergency Management Agency (FEMA). Only the BSIR report for the close of the fiscal year is used for this measure. The SAFECOM checklist developed to indicate compliance with SAFECOM Appendix D requirements for each grant is saved in the Emergency Communications Division (ECD) internal SharePoint site. Consultations and decisions regarding if grantees are reporting sufficient data to demonstrate compliance are saved in the SAFECOM Grant Guidance Compliance spreadsheet.
Data Collection Methodology	On an annual basis, grant recipients self-report via their BSIR submissions data related to compliance with SAFECOM Guidance. These submissions are verified by federal staff through the annual monitoring process, and compliance based on the requirements listed in Appendix D of the SAFECOM Guidance are recorded in a checklist for each grant recipient. Then program experts consult with FEMA analysts to determine, based on the checklist, whether the grantee is reporting sufficient data to demonstrate compliance. The calculation for this measure is the number of grantees compliant with SAFECOM guidance divided by the total number of grantees.
Reliability Index	Reliable
Explanation of Data Reliability Check	BSIR submissions by grant recipients are validated through the annual monitoring process. ECD National Planning and Policy Sub-Division reviews the checklist collaboratively with the FEMA Grant Programs Director's Office (GPD) program analysts and make judgments regarding grantee compliance with the requirements.

Performance Measure	Percent of landline priority calls successfully connected using the Government Emergency Telecommunications Service Landline Network
Program	Emergency Communications
Description	This measure gauges the reliability and effectiveness of the Government Emergency Telecommunications Service (GETS) by assessing the completion rate of calls made through the service. The GETS call completion rate is the percent of calls that a National Security/Emergency Preparedness (NS/EP) user completes via public telephone network to communicate with the intended user/location/system/etc. GETS is accessible by authorized users at any time, most commonly to ensure call completion during times of network congestion caused by all-hazard scenarios, including terrorist attacks or natural disasters (e.g., hurricane or earthquake).

Scope of Data	The measure covers total GETS usage so the scope of the data is all calls initiated by NS/EP users on the Public Switched Network, including test calls and GETS usage during exercises, such as National Level Exercises (NLEs).
Data Source	Data is obtained through Monthly Performance Reports (MPRs) from the carriers: AT&T, Sprint, and Verizon. The reports contain information on daily GETS call attempts to include date of call attempt, time of call attempt, call duration, originating digit string and location, terminating digit string and location, and disposition of the call attempt [answered, busy, ring no answer, invalid PIN (GETS Personal Identification Number)], and network announcement.
Data Collection Methodology	Each quarter, ECD analyzes all MPRs, and EPRs if applicable, from that time period to calculate the overall and event-specific call completion rates.
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 GETS program management. All data collected is also in accordance with best industry practices and is compared with previous collected data as a validity check by ECD analysts. The results are reviewed for clarity and consistency before final submission.

Performance Measure	Percent of wireless priority calls successfully connected using the Wireless Priority Service
Program	Emergency Communications
Description	This measure gauges the reliability and effectiveness of the Wireless Priority Service (WPS) by assessing the completion rate of calls made through the service. The WPS call completion rate is the percentage of wireless priority calls that a National Security and Emergency Preparedness (NS/EP) user completes via public cellular network to communicate with the intended user, location, system, etc. WPS is accessible by authorized users at any time, most commonly to ensure call completion during times of network congestion caused by all-hazard scenarios, including terrorist attacks or natural disasters. (e.g., hurricane or earthquake).
Scope of Data	The measure covers total WPS usage. The scope of the data is all wireless calls initiated by NS/EP users on the Public Switched Network, including test calls and WPS usage during exercises, such as National Level Exercises (NLEs).
Data Source	Data is obtained through Monthly Performance Reports (MPRs) from the carriers: AT&T, Sprint, and Verizon. The reports contain information on daily WPS call attempts to include date, time, duration, originating digit string and location, terminating digit string and location, and disposition of the call attempt. [There are the inherent limitations of wireless networks (e.g., mobility, radio channel capacity and design constraints)].
Data Collection Methodology	Each quarter, ECD analyzes all MPRs, and EPRs if applicable, from that time period to calculate the overall and event-specific call completion rates. Based on information from these reports, the program calculates call completion rate: defined as a percentage (%) = (Successful Valid Call Attempts) / (Blocked Valid Call Attempts + Successful Valid Call Attempts), where a “Valid Call Attempt” is a WPS attempt with a *272 valid prefix by an authorized user. A valid call attempt is considered “blocked” if it is unable to gain access to the random-access network or if unable to reach the intended endpoint due to network congestion. If one or more “Code Red” events have been initiated during a quarter that would produce EPRs, or if there are any national-level events causing network congestion, then event-specific call completion rates will also be reported in the supporting narrative submitted along with the overall result.
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 WPS program management. All data

	collected is also in accordance with best industry practices and is compared with previous collected data as a validity check by ECD analysts. The results are reviewed for clarity and consistency before final submission.

Performance Measure	Number of Continuing Education Units issued through bombing prevention training
Program	Infrastructure Security
Description	This measure captures the number of International Association for Continuing Education and Training (IACET) Continuing Education Units (CEU) issued to stakeholders by the Office for Bombing Prevention (OBP). It provides an indication of the value of OBP accredited training to federal, state, local, territorial, tribal, and private sector partners continuing education needs. As an IACET accredited provider, OBP has multiple courses that award CEUs to the participant upon successful course completion. The IACET accreditation and CEUs issued validate that the training meets American National Standards Institute (ANSI) criteria for continuing education requirements and meets stakeholder needs for awarding and maintaining professional certifications, licenses, or memberships to perform their respective role(s) in preventing, protecting against, responding to, and/or mitigating bombing incidents.
Scope of Data	The data underlying the measure is bounded by the number of course participants who successfully complete OBP Counter-IED Risk Mitigation training. Participants must pass a learning assessment in the form of a written test and/or practical evaluation by OBP instructors at the conclusion of each training event before CEUs can be awarded. This will not be a sampling but will be results based on all available data. Courses are thematic in nature and focus on bombing prevention awareness, performance and management.
Data Source	The results of learning assessments are entered into the Center for Domestic Preparedness Training Administration Suite and are then consolidated by personnel within the OBP Counter-IED Training and Awareness Section (CTAS) into a Microsoft Excel spreadsheet (CTAS Operations Workbook) located on DHS CISA SharePoint for analysis and compiled into a quarterly product for review by OBP leadership. OBP owns the final reporting database.
Data Collection Methodology	The measure is calculated by multiplying the total number of participants successfully completing the assessment by the number of CEUs awarded per individual course. Each individual course awards different amounts of CEUs, therefore this action is repeated for every course that is accredited to award CEUs. The results are then added together to compile the total number of CEUs issued.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data will be collected by OBP designated personnel. The corresponding OBP Unit Chief is responsible for the validity of the data collected and generated in support of this measure. OBP Leadership is 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. The data and result for this measure will be submitted to analysts at the CISA HQ level for their review and concurrence. This provides a final check for any potential errors in data collection, calculation, or scoping.

Performance Measure	Percent of applicable Executive Branch Departments and Agencies that have reported compliance with Interagency Security Committee policies and standards
Program	Infrastructure Security

Description	This measure communicates the percentage of applicable Executive Branch Departments and Agencies that reported compliance data into the Interagency Security Committee (ISC) Compliance System (ISC-CS). Executive Branch Departments and Agencies complete a 20-question organizational benchmark questionnaire that evaluates their compliance with ISC policies and standards. Monitoring Executive Branch Department and Agency compliance with ISC Policies and Standards is a requirement in Executive Order 12977. Compliance with ISC policies and standards enhances security and resilience and reduces risk to the Nation's critical infrastructure.
Scope of Data	The scope is the number of applicable Executive Branch Departments and Agencies that submitted answers to all 20 organizational benchmark questions in the benchmark questionnaire to the ISC-CS out of the population of the 74 Executive Branch Departments and Agencies listed in the 2018 publication of the US government Manual.
Data Source	The ISC-CS serves as the primary data source and has the capability to create reports for Departments and Agencies who have submitted compliance data. The data is sourced from ISC-CS Program Scorecard Report, which is operated by the ISC program office.
Data Collection Methodology	The compliance benchmark data is submitted to the ISC-CS. Analysts within the program generate the Program Scoreboard Report from the system. The Program Scoreboard Report is a pre-formatted report that the ISC-CS can generate upon analyst request. The report provides a summary of each Executive Branch Department or Agency's submission, thereby indicating that a successful submission has been completed. The measure is calculated as the number of applicable Executive Branch Departments and Agencies that submitted data divided by the 74 required Departments and Agencies, multiplied by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	The ISC creates the Program Scorecard Report and spot checks the results with the data located in the ISC-CS to ensure that there are no anomalies or inconsistencies. The ISC keeps a record of all Agencies providing compliance data, ensuring that all Departments and Agencies are accounted for and properly identified. The data and result for this measure will be submitted to analysts at the CISA HQ level for their review and concurrence. This provides a final check for any potential errors in data collection, calculation or scoping.

Performance Measure	Percent of Chemical Facility Anti-Terrorism Standards high-risk facilities inspected per fiscal year by Chemical Security Inspectors
Program	Infrastructure Security
Description	This measure identifies the percentage of Chemical Facility Anti-Terrorism Standards (CFATS) high-risk chemical facilities that received an authorization or compliance inspection during a fiscal year. Authorization inspections are conducted to ensure Site Security Plans (SSPs) adhere to risk based performance standards that leads to the Department's approval of the SSP. Follow-on compliance inspections ensure adherence to the approved SSP. Inspections are a key indicator used to predict the overall security posture of a CFATS high-risk chemical facility and identify compliance with the risk-based performance standards. Assessing a CFATS high-risk chemical facility's vulnerabilities and compliance is part of an overall risk reduction process to enhance security.
Scope of Data	The scope of this measure includes all authorization and compliance inspections completed at high-risk chemical facilities that are regulated under the CFATS regulation out of the total population of CFATS high-risk chemical facilities included on the annual work plan.

Data Source	CFATS high-risk chemical facilities inspection results are maintained in the Infrastructure Security Compliance Division (ISCD) Portal, which serves as the official source of data repository for ISCD. The ISCD portal houses inspection activities completed in accordance with the CFATS regulation.
Data Collection Methodology	Inspections are performed in accordance with an annual work plan which specifies frequencies and targets for inspections of CFATS high-risk chemical facilities based on criteria established by Infrastructure Security Compliance Division. When inspections are completed, the results are entered into the ISCD Portal which are subsequently used to calculate the results for this measure. The result for this measure is reported quarterly to show progress and is calculated by dividing the total number of CFATS high-risk chemical facilities inspected by the total number of CFATS high-risk chemical facilities at the end of the reporting period, multiplied by 100.
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 facilities that are likely to integrate vulnerability assessment or survey information into security and resilience enhancements
Program	Infrastructure Security
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. 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.
Scope of Data	The scope of this measure includes all critical infrastructure facilities that received a vulnerability assessment during the fiscal year.
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 respondents reporting that the counter improvised explosive device information provided by DHS is a valuable resource to support their responsibilities (Retired Measure)
Program	Infrastructure Security
Description	This measure provides an indication of the value of information sharing via the Technical Resource for Incident Prevention (TRIPwire) to a diverse array of homeland security stakeholders (federal, state, local, territorial, tribal, and private sector partners) related to improvised explosive device (IED) threats and corresponding preparedness measures. TRIPwire users complete voluntary questionnaires on a quarterly basis rating their satisfaction with the utility of the information provided by TRIPwire. This ensures that TRIPwire's information sharing capabilities are keeping pace with what users seek and need to support their responsibilities.
Scope of Data	The data underlying the measure is bounded by the number of registered TRIPwire users who respond to the voluntary questionnaire. Occupations of users vary (e.g., federal, state, or local law enforcement, emergency manager, federal or state counter-terrorism, homeland security or intelligence unit); therefore, the applicability and use of the information provided in each user respondent's responsibilities will vary.
Data Source	The responses to the questionnaire are consolidated by personnel within the TRIPwire unit into a Microsoft Excel spreadsheet for analysis and compiled into the TRIPwire Quarterly Questionnaire product for review by Office for Bombing Prevention (OBP) leadership. OBP owns the final reporting database.
Data Collection Methodology	TRIPwire registered users have the opportunity to complete a quarterly voluntary questionnaire providing feedback on their satisfaction with TRIPwire as a resource. 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 with the numerator being the number of respondents answering 'Agree' or 'Strongly Agree' with the statement that, 'TRIPwire is a valuable resource to support my responsibilities,' and then divided by the denominator of the total number of respondents to the question; the result is then multiplied by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data will be collected by OBP designated personnel. The corresponding OBP Unit Chief will be responsible for the validity of the data collected and generated in support of this measure. OBP Leadership 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 respondents reporting that the counter-improvised explosive device training provided by DHS enhances their preparedness to perform their jobs
Program	Infrastructure Security
Description	This measure provides an indication of whether CISA's counter-improvised explosive device (IED) training enhances the preparedness of a diverse array of homeland security stakeholders (federal, state, local, and private sector partners) to perform their respective role(s) in preventing, protecting against, responding to, and/or mitigating bombing incidents. Training participants complete a voluntary questionnaire at the completion of every training iteration rating the degree to which the training increased their preparedness. This measure calculates the percentage of participants reporting that the training will increase their preparedness, response to and mitigation of bombing incidents. This measure provides important feedback to CISA regarding how C-IED information is received by homeland security stakeholders, and demonstrates CISA's contribution to enhancing national capabilities to prevent, protect against, respond to, and mitigate bombing incidents.
Scope of Data	The data underlying the measure is bounded by the number of course participants who respond to the voluntary questionnaire and subsequently provide a response to the specific correlating question. The population for this survey includes individuals participating in the suite of counter-IED trainings provided by OBP. Courses are thematic in nature and focus on awareness, performance and management.
Data Source	Training participants are encouraged at the conclusion of training to complete a voluntary questionnaire providing feedback on the degree to which their preparedness was enhanced as a result of the training. Specifically, participants are asked, 'As a result of the counter-IED training provided by OBP, I am better prepared to execute my role in preventing, protecting against, responding to, and/or mitigating bombing incidents.' The responses to this one question are consolidated by personnel within the Office for Bombing Prevention (OBP) Counter-IED Training and Awareness Section (CTAS) into a Microsoft Excel spreadsheet for analysis and compiled into a quarterly questionnaire product for review by Office for Bombing Prevention (OBP) leadership. OBP owns the final reporting database.
Data Collection Methodology	Quarterly results are calculated with the numerator being the number of respondents answering 'Agree' or 'Strongly Agree' with the statement that, 'As a result of the counter-IED training provided by OBP, I am better prepared to execute my role in preventing, protecting against, responding to, and/or mitigating bombing incidents,' and then dividied by the denominator of the total number of respondents to the question. The result is then multiplied by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data will be collected by OBP designated personnel. The corresponding OBP Unit Chief will be responsible for the validity of the data collected and generated in support of this measure. OBP Leadership 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 state and local jurisdiction election security information products and services delivered within 30 days of request (Retired Measure)
Program	Infrastructure Security
Description	This measure reports the delivery of election security information products/services requested by state and local jurisdictions within 30 days of

	receiving all information necessary to create the final version of the product, within 15 days of receiving final approval of the product from the requestor, or by the desired delivery date specified by the requestor, whichever is latest. These information products/services: (1) improve state and local officials' understanding of and ability to communicate election security risks, vulnerabilities, and priorities both widespread and unique to their respective jurisdictions and election infrastructure and (2) increase awareness among state and local jurisdictions of other CISA election security resources and services. Election security information helps state and local jurisdictions protect against cyberthreats to the electoral process and results.
Scope of Data	The population of the data encompasses all requests for any of the following election security products: State and County Snapshot Posters, Emergency Response Guide Posters, Election Security Field Guide and Emergency Contact Cards. The scope of the results are the requests that are delivered within 30 days, (approved within 15 days, or delivered by the desired delivery date specified by the requestor), whichever is latest. Requests for additional products from states who have already received products will be excluded.
Data Source	The information products/services requested and completed are stored in the ESI Information Products database. The CISA/NRMC election security team will maintain state and local jurisdictions election security information products/services requests/completions database. The database contains the list of state and local jurisdictions election security information product/ services requests, the initial date of request to CISA/NRMC, date information was last requested from the state or locality, date the state or locality last provided requested information, and date the request was completed.
Data Collection Methodology	The CISA/NRMC performance analyst conducts a quarterly data call of every product/service requested and delivered to a local or state jurisdiction. The performance analyst will calculate the percentage using the total number of state and local jurisdictions election security information product/services requests completed within 30 days divided by the total number of state and local jurisdictions election security information product/services requests that were met within the 30 day target and requests with initial request dates older than 30 days and that were not completed during prior reporting periods.
Reliability Index	Reliable
Explanation of Data Reliability Check	Once the performance analyst records and analyzes the data, there is a second analyst to cross-check the data entry and analysis and provide a peer review to check for accuracy. The data and result for this measure will be submitted to analysts at the CISA HQ level for their review and concurrence. This provides a final check for any potential errors in data collection, calculation or scoping.

Federal Emergency Management Agency

Performance Measure	Number of community and faith-based organizations that receive continuity and preparedness training
Program	Education, Training, and Exercises
Description	This measure reports the number of unique organizations whose representatives attend a FEMA-led training related to continuity and preparedness in a given fiscal year.
Scope of Data	The scope of this measure includes all organizations engaged in activities related to community preparedness and continuity, based on the program's analysis of independently-collected data.

Data Source	The program defines 'community-based organizations' as those focused on providing direct service to individuals locally. While most organizations counted by this measure classify themselves as non-profit groups for tax purposes, whether faith- or community based, this measure also counts for-profit entities. Using data from the Internal Revenue Service, the National Center for Charitable Statistics <http://nccs.urban.org> regularly compiles a profile of the U.S. non-profit sector, categorized by different areas of focus: Using data from 'The Nonprofit Sector in Brief,' FEMA counted more than 225,000 organizations with program emphases of Public Safety, Disaster Preparation and Relief; Housing and Shelter; Healthcare; and Community Improvement. NCCS classifies some groups profiled as focused on more than one of these four areas. Despite the possibility of some 'double-counting,' analysts selected 22,500--roughly ten percent of the estimated population--as this measure's target.
Data Collection Methodology	The program encourages organizations interested in participating in a FEMA-led training to submit a registration form in advance of attending the training. Staff save information from submitted registration forms to a SharePoint sire operated by the Individual and Community Preparedness Division (ICPD). At training events, program staff collect information from participating organizations, confirming the attendance of pre-registered organizations, and adding information about non-pre-registered organizations to the ICPD database. At the end of each reporting period, the number of organizations with data collected when attending program-relevant events provides the performance result for that period.
Reliability Index	Reliable
Explanation of Data Reliability Check	ICPD staff use the aforementioned SharePoint database as a repository to store data from program-relevant trainings and presentations. Program analysts can sort and query records in the SharePoint database to ensure that no organization appears in the count more than once per training or presentation.

Performance Measure	Percent of supervisors of students trained who believe their staff are better prepared as a result of National Fire Academy training
Program	Education, Training, and Exercises
Description	The measure assesses the increase in the level of students trained as reported by individual first-line supervisors. These supervisors observe and report through an on-line survey how training skills are being used on-the-job and whether or not their subordinate is better prepared to respond to disasters and emergencies as a result of the National Fire Academy training they received.
Scope of Data	Approximately 8,000 individuals attend National Fire Academy resident training courses each year. Participants include fire and emergency response personnel and allied professionals. Using an online web-based format, the target population of the data collection includes all supervisors of students trained who have completed an NFA-sponsored on-campus training course. As of this time, the return rate is still being evaluated.
Data Source	Data are obtained from Level 3 training evaluation questionnaires sent to the emergency responder's respective supervisor 4 - 6 months after the training course has ended.
Data Collection Methodology	The NFA uses an online, web-based format. Supervisors of students trained who have completed NFA training are sent a link which enables them to complete the questionnaires online. The data is captured and processed through an Oracle database system.
Reliability Index	Reliable
Explanation of Data Reliability Check	Typically, 60% of the Level 3 evaluation questionnaires are completed and returned. The data is reliable because it is collected directly from the first-line

	supervisor of the student trained. All data is collected and reviewed by the Academy's Training Evaluation Center for completeness prior to report compilation and production. Through the use of descriptive statistics (e.g., respondent demographics and training applications and effectiveness), the homogeneity of the target population and interest in the subject ensure satisfactory levels of validity and reliability based on respondents' ability to provide useful and consistent information.

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 engaged 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 Hazard Mitigation Assistance 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 Benefit to cost ratio 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. These are proven methodologies and have been in use for the past 10 years. To determine the cost effectiveness of a Hazard Mitigation Assistance (HMA) project, FEMA utilizes a benefit-cost ratio, 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 EDW. FEMA HMA staff download relevant data from the EDW, and after making the calculations for an aggregate Benefit to cost ratio 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	Percent of capability building Homeland Security Grant Program projects that align to closing State, Territory, and Urban Area identified capability gaps
Program	Grants
Description	This measure gauges the percent of Homeland Security Grant Program (HSGP) projects that align to capability gaps identified by States, territories, and urban areas in their annual Stakeholder Preparedness Review (SPR) submissions. The capability gaps cover all five mission areas (Prevention, Protection, Mitigation, Response, and Recovery) which support national preparedness. This measure will

	gauge direction of HSGP funds towards projects designed to close capability gaps tied to threats and hazards. The percent value represents how many of the total capability building HSGP projects align to current capability gaps. Capability building projects are those where new capabilities exist that were not operational during the prior year. The results of this measure will support DHS's goal to enhance national preparedness and build core capabilities across the Nation and help narrow capability gaps by driving grantee alignment between their investment and national priorities.
Scope of Data	The scope of this measure reflects grant projects for the Homeland Security Grant Program that were identified as capability building projects. It includes data from the State Homeland Security Program and Urban Areas Security Initiative. FEMA's Comprehensive Preparedness Guide (CPG) 201 3rd Edition defines 'capability built' projects as that will to deliver new capabilities. A project is considered to align to the SPR when it funds a Planning, Organizing, Equipping, Training, and Exercising (POETE) area in a core capability and the state, territory, or urban area indicated having a gap in that POETE area. The measure does not include sustainment projects or management and administration projects as defined in the HSGP Notice of Funding Opportunity. Operation Stonegarden projects are not included in this measure. The data used for this measure are all projects in a fiscal year and focus on projects, not jurisdictions.
Data Source	This measure gathers data from two sources: the Biannual Strategy Implementation Report (BSIR) and Stakeholder Preparedness Review (SPR). The BSIR is a report from grant recipients that collects project level data for HSGP, per reporting requirements listed in the HSGP Notice of Funding Opportunity. It is submitted twice a year [a summer BSIR [(typically in June) and a winter BSIR (typically in December)] and maintained within the Grants Reporting Tool (GRT) by the FEMA Grant Programs Directorate (GPD). The SPR is an annual capability assessment that helps jurisdictions identify their current capabilities relative to the targets outlined in their Threat and Hazard Identification and Risk Assessment (THIRA). For the SPR, communities submit their data by completing the online FEMA Preparedness Toolkit (PrepToolkit) December 31 each year. The data is then cleaned, analyzed, and stored in an Excel database managed and maintained by the FEMA National Preparedness Assessment Division (NPAD).
Data Collection Methodology	NPAD requests BSIR data from GPD and combines it with SPR data from the PrepToolkit into a separate Excel spreadsheet. Using Excel formulas, BSIR grant project data that fall within the subset of projects that build capability are compared to SPR core capability gaps, and indication of alignment is recorded on the excel spreadsheet. Program analysts in NPAD then manually review unaligned projects to ensure accuracy. For projects that do not align, an official Memorandum is sent to the States, territories, and urban areas inquiring on why the projects were not aligned to capability gap; clarifying information may then be provided and information updated. The measure result calculated is number of HSPG build projects aligned to capability gaps divided by the total number of build projects.
Reliability Index	Reliable
Explanation of Data Reliability Check	All data sets used to compute this measure represent NPAD's primary repositories of grant, recipient, and performance data. All systems and spreadsheets are regularly updated by NPAD staff and monitored for quality by experienced analysts. Data acquired from GPD are subject to equivalent examination to guarantee accuracy and reliability. After the measure results are calculated, a second analyst independently replicates the analysis to ensure accuracy of the results. After this check, senior managers in NPAD review the findings and cases where State, territory, or urban area projects and gaps do not

	align. If confirmed, a Memorandum is issued to the relevant State or territory regarding the discrepancy of the alignment information. Through these communications States, territories, and urban areas may offer clarifying information that offers a second reliability check on the accuracy of the project alignment information to capability gaps.

Performance Measure	Percent of prime grant awards closed within 365 calendar days from the end date of the Period of Performance
Program	Grants
Description	This measure gauges FEMA's ability to close expired grant awards in a timely manner defined as 365 calendar days from the period of performance (POP) end date. 'Expired grant awards' refers to any open grant or federal assistance provided from FEMA to a direct recipient that is beyond the established POP end date. This does not include grants that have been issued by the direct recipient to a sub-recipient. 2CFR 200.343 allows the recipient up to 90 days after the POP end date to submit all final reports, then allows the federal awarding agency one year after the receipt and acceptance of all required final reports to complete all closeout actions. Timely closeout of expired grant awards is an indication of effective grant management and minimizes the amount of invalid obligated funds in our financial records for expired grants.
Scope of Data	The scope of the reported data includes expired prime grant awards for Non-Disaster and Disaster programs that are not more than 365 days beyond POP end date at the beginning of the assessed fiscal year, as well as closed awards from the assessed fiscal year. The population includes all Non-Disaster and Disaster programs more than 365 days beyond the POP at the beginning of the assessed fiscal year, as well as closed awards from the assessed fiscal year. POP end dates are fixed but may be extended with approval. The Grants Program Directorate uses the latest POP end date available for every award when calculating and reporting data. Expired grants older than the previous fiscal year are not counted and will be tracked separately for an internal measure looking at decreasing the grant backlog. Grants issued by the direct recipient to a sub-recipient are excluded.
Data Source	The Master Repository is the tracking tool used to record, track, and document open and closed grant awards within FEMA. The Master Repository is managed and housed by the Grants Program Directorate (GPD), who will be responsible for utilizing monthly data pulls from our financial system combined with regular validations from Regional and headquarters (HQ) offices, to update and maintain an accurate and complete Master Repository. GPD is responsible for calculating and submitting the results which includes validating with the HQ and Regional grant offices.
Data Collection Methodology	GPD conducts monthly data pulls from the financial system. The numerator is the number of awards closed in the assessed fiscal year that meet the goal of closure within 365 days from the POP end date. For example, if the POP end date is July 1, 2019 and the award is closed by September 1, 2019 this award is counted in the numerator. The denominator comprises two categories: The first is the total number of awards with a POP end date within the fiscal year prior to the assessed fiscal year that are currently open (e.g. fiscal year 2019 includes all awards with a POP end date in fiscal year 2018 that are still open). The second category is total number of awards closed in the assessed fiscal year, excluding awards that were more than 365 days beyond POP end date at the beginning of the assessed fiscal year. Awards closed that were closed within 365 days from the POP end date are divided by the total awards from the previous and current fiscal year with open POPs.

Reliability Index	Reliable
Explanation of Data Reliability Check	GPD conducts multiple validations internally, with the Regions and with the Office of the Chief Financial Officer (OCFO), of the data to ensure accuracy and completeness. Monthly, each Regional and HQ grant office validates newly opened and closed awards; quarterly, each Regional and HQ grant office validates the completeness of the grants listed in the Master Repository. Annually, GPD coordinates with OCFO for a full baseline assessment of all awards in the repository to ensure completeness and accuracy of the grant award data. Lastly, on a monthly basis, GPD reconciles the Master Repository against data pulls from our grant system and financial system to ensure that period of performance, and open and closed status are correct for every award.

Performance Measure	Percent of communities in high earthquake, flood, and wind-prone areas adopting disaster-resistant building codes
Program	Mitigation
Description	This measure reports the percentage of high-risk communities in 50 states, the District of Columbia, and 5 territories (USVI, PR, Guam, American Samoa, CNMI) adopting building codes containing provisions that adequately address earthquake, flood, and wind hazards. FEMA tracks the number of high-risk communities that have adopted disaster resistant building codes by working with the Insurance Services Office (ISO) Building Code Effectiveness Grading Schedule (BCEGS). ISO collects data from the BCEGS survey daily and evaluates and assigns a grade of 1 (exemplary commitment to building code enforcement) to 10 to gauge adoption of building codes. Adopting disaster-resistant building codes helps strengthen mitigation nationwide to reduce the Nation’s vulnerability to disasters.
Scope of Data	The population of this measure includes communities in 50 states, the District of Columbia, and 5 territories (USVI, PR, Guam, American Samoa, CNMI) in high earthquake, flood, and wind-prone areas as determined by the Insurance Services Office, Inc. (ISO) through their Building Code Effectiveness Grading Schedule (BCEGS) database and research. The two most recent building code editions, covering a time frame of six years of code development, are used to determine if a community has adopted disaster-resistant codes.
Data Source	The source of data for this measure is ISO's BCEGS database which tracks data on building codes adopted by participating jurisdictions from the BCEGS questionnaire. The BCEGS survey data is completed by communities electronically in the BCEGS database. BCEGS database is updated daily to include the latest surveys taken.
Data Collection Methodology	ISO collects data from the BCEGS survey daily and tracks building code adoption. ISO populates the BCEGS database with the survey results. The Mitigation program receives raw data from ISO through their BCEGS database.
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 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.

Performance Measure	Total national investment in mitigation (in billions)
Program	Mitigation
Description	The Federal Insurance and Mitigation Administration (FIMA)—an element of FEMA—defines 'mitigation investment' as an expenditure of resources intended to avoid property damage, reduce the loss of life, or transfer natural-hazard risks in advance of a disaster. This measure refers to such expenditures as 'investments in mitigation.' FY19 results for this measure will focus on expenditures for ten FEMA mitigation programs. Over time, FEMA will determine how to incorporate mitigation investments by other federal agencies and investments by non-federal entities. In both of these instances, FEMA will determine how to value time or other non-monetary investments in mitigation. Such non-federal entities include private-sector firms, non-governmental organizations, non-profit organizations, as well as state, local, tribal, and territorial governments.
Scope of Data	This measure includes data from FEMA as well as data provided by non-FEMA entities that invest in mitigation. Such investments encompass risk-management actions including prevention, property protection, public education/awareness, natural-resource protection, and structural projects. This measure includes the

	direct Grant amounts provided by the Federal Government and the accumulation of labor and other non-monetary investment not funded by grants and its equivalent monetary value. FEMA expects to incorporate data on private-sector investments between FYs 2022 and 2023, explaining the expected year-on-year target increase of 65 percent.
Data Source	Data for this measure will come from MitInvest, an online database within SharePoint which serves as the sole method for FEMA Headquarters and Regional Offices to record information on the status of FEMA's external engagements, partnerships, and investment data related to investments in mitigation.
Data Collection Methodology	For each mitigation investment, FEMA staff complete an internal data-collection instrument (DCI), which provides staff with instructions for documenting how the investment in question supports the recommendations of FEMA's National Mitigation Investment Strategy; the budget obligation of each fiscal year's mitigation investments; and details about how the investment mitigates risk/harm. FEMA transfers this data from DCIs to the MitInvest database. Staff at FEMA headquarters will confirm the investment with submitting Regional or HQ staff, and with any non-FEMA entity involved to validate a connection between the investment and the National Mitigation Investment Strategy. Upon confirmation, staff will add the investment in question to the total monetary amount included in this measure. FIMA will report annually on the status of mitigation investments nation-wide.
Reliability Index	Reliable
Explanation of Data Reliability Check	The MitInvest database is a SharePoint document repository, available via controlled access exclusively through FEMA's intranet. MitInvest staff use documents separate from DCIs submitted to cross-check information about non-FEMA entities and investments. Information saved to MitInvest will inform management decisions, which will motivate effort to ensure the reliability of MitInvest data in addition to requirements to validate this measure's reliability.

Performance Measure	Number of properties covered with flood insurance (in millions)
Program	National Flood Insurance Fund
Description	This measure reports the number of flood insurance contracts in force for properties in the United States, using systems that capture information about policies issued by private insurance carriers who participate in the 'Write Your Own' segment of FEMA's National Flood Insurance Program (NFIP). Insured survivors recover faster and more fully from a flood than uninsured survivors. With this in mind, NFIP has committed resources to increase public understanding of flood risks, while proactively encouraging insurance purchases to reduce losses from all hazards. FEMA will use results from this measure to assess the agency's effectiveness in these regards.
Scope of Data	The scope of this measure includes the total number of flood-insurance contracts in force, starting with those issued by private insurance carriers and insurance partners who participate in NFIP's 'Write Your Own' (WYO) segment. Since 1983, WYO has allowed FEMA and participating property- and casualty-insurance companies to write and service FEMA's Standard Flood Insurance Policy in the companies' own names. The companies receive an expense allowance for policies written and claims processed while the federal government retains responsibility for underwriting losses. The WYO Program operates as part of the NFIP, subject to the Program's rules and regulations.
Data Source	Analysts produce this measure from data available from the Transaction Record Reporting and Processing (TRRP) system operated by NFIP for 'Write Your Own' policies and participants.

Data Collection Methodology	To produce results for this measure, analysts will count the number of flood-insurance contracts in force, as reported by the TRRP or Pivot systems, which store and report contract data from private insurance carriers participating in WYO. Approximately ten days after the end of each month, FEMA checks data in the TRRP system for data anomalies, to ensure accuracy of reporting.
Reliability Index	Reliable
Explanation of Data Reliability Check	WYO's Financial Control Plan Requirements and Procedures provides data concerning reconciliation of policy and claim data submitted to TRRP with monthly financial reports and instructions for editing data. Because of the need for timely financial reconciliation, TRRP only rejects transactions with unreadable money fields or in case of any lack of clarity about how the system can process a transaction. Otherwise, information posts to the database, with potential errors flagged for correction at a later date. NAIS assures the reliability of data stored and reported through the Pivot system.

Performance Measure	Percent of total floodplain mileage mapped with improved engineering standards
Program	National Flood Insurance Fund
Description	This measure reports on the percentage of the total mileage charted in Flood Risk Insurance Maps produced by the program, for which the program has completed a technical review required every five years by statute; see 42 U.S.C. Subchapter III, §4101(e).
Scope of Data	Risk MAP captures deployment data on a quarterly basis, the ten FEMA Regions report quarterly purchases to reflect: 1) The watersheds where they have obligated new funds to conduct discovery and initiate regulatory and/or non-regulatory mapping products and datasets; and 2) approved change requests that change project geography or add discovery activities or regulatory or non-regulatory mapping products and datasets to existing projects.
Data Source	Regions use the Purchase Tracker is used to record, report, and store Risk MAP projects and data for this measure. On a quarterly basis, data are rolled-up and validated on a regional and national scope. The results are reported to the ten FEMA Regions and Headquarters.
Data Collection Methodology	Output from the previous quarterly update cycle is used as a baseline for providing updates on any change requests, new purchases, or study status updates. Within 7 business days following submission from all 10 Regions, a contractor rolls-up the data and performs any geospatial analysis necessary to determine unique project populations that will be counted towards the deployment baseline. On the 7th Business day, an updated National Risk MAP Purchase Tracking sheet will be produced including Regional summaries of deployment and NVUE Initiated. This draft is then posted to the SharePoint site. For quality assurance, Regions review the draft and provide feedback within 2 business days. The contractor will incorporate any comments and produce the final National Risk MAP Purchases / Deployment Baseline for the reporting quarter on the 15th business day following data submission by the Regions.
Reliability Index	Reliable
Explanation of Data Reliability Check	On a quarterly basis, data are rolled-up and validated at the regional and national level by the contractor, which are checked by Federal Insurance and Mitigation Administration staff.

Performance Measure	Deaths per million of the U.S. population due to fire in the U.S.
Program	Preparedness and Protection
Description	This measure reports civilian fire deaths occurring within the U.S. during a calendar year per 1 million people in the U.S. population, estimated for the same year.

Scope of Data	The annual civilian fire death rate is based upon the total number of civilian fire deaths that occur within the U.S. during the calendar year, and U.S. Census Bureau population estimates for that year. Civilian fire death rates are measured in deaths per million population. A death is defined as a civilian fatality as reported to the National Fire Protection Association's (NFPA) National Fire Experience Survey (NFPA Survey) for a given calendar year. Estimates from the NFPA Survey are generally available in Sept. for the preceding year (e.g., fatality estimates for Calendar Year 2006 were available in Sept 2007).
Data Source	The data sources used in calculating this performance measure are fire department responses to the NFPA Fire Experience Survey, and U.S. Census Bureau population estimates. The NFPA survey is a probability sample survey conducted annually, and provides data to derive unbiased national estimates of U.S. civilian fire fatalities. Census Bureau population estimates are generated annually, estimating total U.S. population on July 1 of the relevant year.
Data Collection Methodology	NFPA Survey data are analyzed to produce estimates of fire related civilian fatalities which are used for numerator data; Census Bureau population estimates are used for denominator data.
Reliability Index	Reliable
Explanation of Data Reliability Check	Loss of life data from the National Fire Incident Report System (NFIRS) are also compiled and reviewed by the National Fire Data Center. Statistical weighting and comparison of these data as well as with National Centers for Health Statistics (NCHS) mortality data are done to check for accuracy. A comparison of these data sets to the NFPA fatality data is conducted for consistency and relative veracity.

Performance Measure	Percent of adults that have set aside money for emergencies
Program	Preparedness and Protection
Description	This measure reports the share of all respondents to FEMA's annual National Household Survey who answered affirmatively to questions assessing whether they have set aside money for use in case of emergencies. FEMA has noted that access to financial resources has proven a strong predictor of how well someone can cope in the aftermath of a disaster.
Scope of Data	Annually, FEMA conducts a National Household Survey to understand and assess Americans' attitudes and behaviors regarding emergency preparedness. The scope of this measure includes all responses to questions in the survey which ask whether or not the respondent has set aside money for use in case of emergencies. Through a contractor, FEMA conducts the National Household Survey through telephone interviews.
Data Source	Interviewers capture responses and enter them into a Computer Assisted Telephone Interviewing (CATI) system, owned by the contractor and maintained at the contractor's facilities. The contractor conducting the survey establishes appropriate quality-control measures to ensure that data collection adheres to the outlined standards of the contract.
Data Collection Methodology	FEMA's survey contractor collects data using the CATI system, and completes analysis of responses using two statistical software packages: 1) the Statistical Package for the Social Sciences, and 2) the Statistical Analysis System. When processing the data from the surveys, analysts correct for respondents' unequal probabilities of selection. Analysts also post-stratify sample data according to respondents' geography, age, gender, and race, to account for potential biases such as over- and under-representation of certain population segments to match the distribution derived from the latest-available Current Population Survey estimates. To produce this measure, analysts divide the count of affirmative

	responses to the questions asking whether or not the respondent has set aside money for use in case of emergencies into the total number of responses.
Reliability Index	Reliable
Explanation of Data Reliability Check	The survey contractor certifies that each programmed survey instrument goes through a rigorous quality control process. Rigorous quality assurance extends from the design phase through data collection in the field. 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. FEMA relies on the contractor's processes to ensure data reliability.

Performance Measure	Percent of adults that took multiple preparedness actions at their workplace, school, home, or other community location in the past year
Program	Preparedness and Protection
Description	This measure reports the share of all respondents to FEMA's annual National Household Survey who answered affirmatively to questions assessing whether they had taken more than one preparedness action in the past year, whether taking these actions at their workplace, school, home, or other community location. FEMA has noted that many Americans will experience a disaster or emergency at some point. FEMA emphasizes the importance of a national approach to preparedness, and will use results from this measure to assess the agency's effectiveness in this regard.
Scope of Data	Annually, FEMA conducts a National Household Survey to understand and assess Americans' attitudes and behaviors regarding emergency preparedness. The scope of this measure includes all responses to the questions on the survey which ask whether over the past year the respondent took multiple preparedness actions at their workplace, school, home, or other community location in the past year. Through a contractor, FEMA conducts the National Household Survey through telephone interviews.
Data Source	Interviewers capture responses and enter them into a Computer Assisted Telephone Interviewing (CATI) system, owned by the contractor and maintained at the contractor's facilities. The contractor conducting the survey establishes appropriate quality-control measures to ensure that data collection adheres to the outlined standards of the contract.
Data Collection Methodology	FEMA's survey contractor collects data using the CATI system, and completes analysis of responses using two statistical software packages: 1) the Statistical Package for the Social Sciences, and 2) the Statistical Analysis System. When processing the data from the surveys, analysts correct for respondents' unequal probabilities of selection. Analysts also post-stratify sample data according to respondents' geography, age, gender, and race, to account for potential biases such as over- and under-representation of certain population segments to match the distribution derived from the latest-available Current Population Survey estimates. To produce this measure, analysts divide the count of affirmative responses to the questions asking whether or not the respondent took multiple preparedness actions at their workplace, school, home, or other community location in the past year into the total number of responses.
Reliability Index	Reliable
Explanation of Data Reliability Check	The survey contractor certifies that each programmed survey instrument goes through a rigorous quality control process. Rigorous quality assurance extends from the design phase through data collection in the field. 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. FEMA relies on the contractor's processes to ensure data reliability.

Performance Measure	Percent of time the Integrated Public Alert and Warning System 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 Integrated Public Alert and Warning System (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	Data sources include: US Census bureau data for population; 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.

Performance Measure	Percent of U.S. population covered by FEMA-connected radio stations with electromagnetic-pulse resilience
Program	Preparedness and Protection
Description	This measure reports on the share of U.S. population within range of signals from FEMA-connected radio stations using transmitters hardened against an

	electromagnetic-pulse (EMP) event. FEMA-connected, private-sector radio stations comprise the National Public Warning System (NPWS), one element of FEMA's Integrated Public Alert and Warning System (IPAWS). In voluntary partnership with private stations' owners, FEMA maintains supplementary equipment at these stations to ensure that the President and state- and local-level authorities maintain a resilient capability to communicate with the public in all hazard conditions. FEMA will use results from this measure to assess the agency's effectiveness in this regard.
Scope of Data	FEMA builds, sustains, and operates the National Public Warning System (NPWS) under relevant provisions of the Stafford Act, as well as other Federal statutes and regulations, ensuring direct, real-time knowledge of the number of U.S. radio stations with electromagnetic-pulse (EMP)-resilient equipment. The scope for this measure includes FEMA-connected U.S. radio stations with EMP resilient equipment; the audience reach for each of these stations; and the U.S. population.
Data Source	To determine the audience reach of radio stations with EMP-resilient equipment, analysts use: 1) commercially-available data from Nielsen Audio—formerly Arbitron; 2) data on radio stations' location and transmissions available from the Federal Communications Commission (FCC); and 3) radio-frequency wave-propagation and coverage tools available from the U.S. Geological Survey (USGS). Analysts use data on U.S. population from the 2010 Census, conducted by the Commerce Department's Census Bureau.
Data Collection Methodology	Analysts develop an accounting of the U.S. population capable of tuning-into a FEMA-connected radio station with EMP-resilient equipment as follows. Analysts begin by calculating each radio station's transmission area or service contour using standard FCC methodology, employing data on station power and antenna specifications from an online FCC resource. Based on an expected AM signal level of 0.5 mV/m, an expected FM signal level of 50 dBu, M3 ground-connectivity data from FCC, and three-second terrain data from USGS, analysts calculate the area over which a given station can broadcast. Analysts then compare U.S. Census data for one-kilometer geographic tiles to the radio stations' transmission areas, aggregating population inside these broadcast areas and deducting population from overlapping station-coverage areas. Dividing the aggregated population within broadcast areas of stations with EMP-resilient equipment into the total U.S. population yields the performance measure.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data received by FEMA under commercial contract with Arbitron implies a warranty of accuracy. The completeness and accuracy of physical data and population data employed to develop this measure lie within the responsibility of FCC, USGS, and the Census Bureau, respectively.

Performance Measure	Percent of U.S. population that is covered by a local-level authority authorized and registered to send alerts and warnings to the public using the Integrated Public Alert and Warning System
Program	Preparedness and Protection
Description	This measure tracks the share of U.S. population under the jurisdiction of local authorities to which state governments have granted authorized access to the Integrated Public Alert & Warning System (IPAWS), to allow these local authorities to send alerts and warnings to the public.
Scope of Data	The scope of this measure includes the U.S. population from each county authorized by state governments to send alerts and warnings to the public using the Integrated Public Alert & Warning System (IPAWS). For each county, the program uses current Census data on the U.S. population and counts of sub-

	populations by local jurisdiction. In addition, the program uses its own data on local counties authorized by state governments to send alerts and warnings to the public using IPAWS.
Data Source	For population data, the program uses data on total U.S. population and U.S. population by county provided by the Commerce Department's Census Bureau. For data on counties registered to use IPAWS, the National Continuity Programs directorate maintains a list of jurisdictions registered to use IPAWS, updated and validated quarterly.
Data Collection Methodology	For each period of performance, the program will have 1) a list of agencies registered to use IPAWS, last updated no earlier than the preceding fiscal quarter; 2) data on total U.S. population, decomposed by county. The program uses an electronic spreadsheet application to divide the sum of the populations of U.S. counties with at least one public agency authorized to use IPAWS by the total U.S. population.
Reliability Index	Reliable
Explanation of Data Reliability Check	For population data, the program uses Census Bureau data, which the Bureau verifies and validates: See the Census Bureau's data verification and validation process at https://www.census.gov/programs-surveys/popest/technical-documentation/methodology.html. The program itself maintains a list of non-federal public authorities registered to use the Integrated Public Alert & Warning System (IPAWS), updated quarterly. As the sole grantor of IPAWS access to public authorities, National Continuity Programs can validate data for this measure as NCP extends or rescinds IPAWS access to public authorities.

Performance Measure	Average annual percentage of administrative costs for major disaster field operations, as compared to total program costs
Program	Regional Operations
Description	This measure gauges FEMA's efficiency in providing disaster assistance by indicating what share of its disaster expenditures are administrative costs compared to the share disseminated as grants to survivors as assistance. It helps FEMA know if the agency is being efficient in the way it provides disaster assistance. This measure is for FEMA's most common disasters of less than $50M (Level III).
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, in addition, the disaster administrative cost percentage for specific disasters is reported on in the Automated COP, which also pulls data 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 are conducted by an analyst using data from a FIT report.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. Note: Because the data is organized by declaration year, all of the previously reported numbers will need to be updated
Reliability Index	Reliable
Explanation of Data Reliability Check	The data is collected via IFMIS and reported in FIT reports. The remaining steps are conducted by an analyst using data from a FIT report. The data is organized so that disasters are first separated by their size which is determined by the total actual federal dollars obligated. 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.

Performance Measure	Average number of the incident staff to support small federally-declared disasters
Program	Response and Recovery
Description	This measure reports a five-year average number of incident staff deployed to support small federally-declared disasters. For this measure, the program uses internal data provided by information systems used to manage financial and human resources deployed in declared disasters.
Scope of Data	This measure's scope includes the average number of federal workers supporting small disasters over a five-year period. For each fiscal year, the program maintains records of funds obligated to respond to each federally-declared disaster. The program has developed scale criteria for disasters; those with obligations of $41 million or less qualify as small disasters. The program also maintains records on personnel deployed to disasters and their employment statuses. The program has developed a criterion for 'federal incident workforce' deployed to disasters. For the current year and four preceding years, analysts will count both the workforce deployed to each small disaster, and the number of small disasters declared to calculate a five-year running average.
Data Source	The agency's Field Operations Division operates and maintains a Deployment Tracking System, with records including disaster reference numbers; event start dates; deployed federal personnel; and cumulative federal-workforce days onsite. The agency's Office of the Chief Financial Officer operates and maintains an Integrated Financial Management System, with records including disaster reference numbers and total disaster obligations. Staff in these offices can use these systems to produce reports containing data required to construct this performance measure.
Data Collection Methodology	At the end of each fiscal year, OCFO analysts will use the Integrated Financial Management System to produce a report counting all of the federally disasters declared in that year which satisfy the small-disaster criterion of $41 million or less in total disaster obligations. Field-operations analysts will use the Deployment Tracking System to produce a report counting the number of personnel deployed to each federally declared disaster of $41 million or less in total disaster obligations. For the current year and four preceding years, dividing the total workforce number into the total number of small federally declared disasters over the timeframe yields the performance measure.
Reliability Index	Reliable

Explanation of Data Reliability Check	The Deployment Tracking System contains multiple quality-control checks with regard to deployment data. Plans for the measure specify that both the Office of Response and Recovery and the Office of the Chief Financial Officer will review the final report to ensure data reliability.

Performance Measure	Average timeliness of the individual assistance awards of the Individuals and Households Program (in days)
Program	Response and Recovery
Description	This measure assesses how quickly the program provides disaster relief to qualified individuals and households. Specifically, for individuals or households receiving assistance from the Individuals and Households Program (IHP), this measure reports the average number of days between the submission of an application and the first receipt of an award. By evaluating how quickly disaster survivors receive financial assistance, the program can assess the effectiveness of a critical, customer-facing element of the agency's mission.
Scope of Data	The scope of this measure includes the complete population of all IHP applicants from all active disasters who received their first financial assistance within the reporting period. The measure will include all types of first IHP awards, with the exception of Critical Needs Assistance (CNA). Since this measure refers to applicants' first IHP award, the measure includes data from any given applicant no more than once. CNA involves the award of $500 to individual(s) who are or remain displaced for at least seven days, and require financial assistance to help with critical needs. The program makes CNA awards before completing the proper IHP review, and any CNA funds provided are applied against the first IHP award. In addition to laxer standards of review for CNA, including CNA awards in this measure would double count them, and misrepresent program timeliness.
Data Source	The Individual Assistance Division operates the National Emergency Management Information System (NEMIS) as a system of record for IHP. NEMIS contains all program-pertinent information for registered individuals and households, their current and damaged dwelling locations, inspection results, correspondence and eligibility award decisions, and amounts of IHP assistance. Primary sources of the data include applicants, caseworkers, and inspectors engaged in the registration, casework, and inspection processes. FEMA's Recovery Directorate Operational Data Storage (ODS) database backs-up NEMIS data every 15 minutes, allowing users to extract NEMIS data separately from the live NEMIS production server. Employing this best practice ensures that data extraction does not impact the production server. The Recovery Directorate owns both ODS and NEMIS.
Data Collection Methodology	The Recovery Reporting and Analytics Division (RRAD) extracts data from ODS using queries coded in SQL, a standard language for storing, manipulating and retrieving data in databases. These queries of ODS produce reports in Microsoft Excel format. For each relevant IHP award, reports will include disaster number, identification number for individual/household registration, date of application date, and date of award. Analysts will then import the data into Excel's PowerPivot function, configured to include the following formula for the calculation: Average Days = (Sum of all days between date of application and date of first award) / (number of registration IDs).
Reliability Index	Reliable
Explanation of Data Reliability Check	RRAD will extract and analyze each NEMIS and ODS report after every performance period. The RRAD Analysis Branch, RRAD Reporting Branch, and RRAD Director will share initial findings internally to double-check counts and analysis results. In addition, RRAD will share findings with the Individual Assistance Director and their subject-matter experts for verification and review,

	before sending results for review by senior agency leadership. These reviews will identify and resolve any questions or discrepancies that emerge.

Performance Measure	Composite logistics readiness rate for moving, staging, and delivering commodities and equipment for catastrophic disasters
Program	Response and Recovery
Description	This measure captures the readiness for moving, staging, and delivering commodities and equipment for catastrophic disasters. Four critical factors of logistics readiness are included, each weighted equally at 25% each: Commodities; contracts; human capital; and operating capabilities. Each critical factor is a summation of weighted subcategories based upon life-saving, life-sustaining requirements, along with urgency of need. These planning factors have been identified based upon analyses from previous disasters and disaster scenarios such as the California Cascadia Subduction Zone Earthquake and Tsunami Response Plan. The ability to move and deliver commodities and equipment in a timely manner enables a swift and appropriate response to disasters.
Scope of Data	The scope of the result includes data from four critical factors of logistics readiness, each weighted based on need and availability: Contracts; Commodities; Human Capital; and Operating Capabilities. All four factors and their sub-elements are included in the population including: Commodities: Meals, Water, Generators, Tarps, Housing (TTHUs, tents), Sheeting, Infant Toddler Kits, Cots; Contracts: Inventory, Housing, IT Systems, Equipment Maintenance, Transportation, SCAN LCSC, Dunn Bradstreet Human Capital: Staging Teams, Business Industry & Infrastructure Integration, HQ and Regional Staffing, Transportation Management, Logistics Systems, CADRE, Distribution Centers, Housing, Supply Chain Integration, Property Managers Operating Capabilities: Facilities, Equipment, Property Accountability, Devolution Personnel, State, local, tribal, territorial Distribution Management Plans, Data and Analytics, NBEOC Engagement, ESF-14.
Data Source	There are multiple data sources that are determined by: 1) Comparing equipment authorization tables maintained by Logistics Operations and Distribution Management Divisions to the results of quarterly equipment readiness (operable) status; 2) Pulling on-hand data from the Logistics Supply Chain Management System (LCSMS) and amounts available from active contracts and agreements for Initial Response Resources (IRR); 3) Comparing on-hand personnel as validated by FEMA Human Resources system (FHR) with authorized PINS for PFT, Core and IM Core personnel; and 4) Collecting data on critical contracts and operating capabilities from the respective divisions in LMD. Reporting Program offices include: Supply Chain, Transportation, Business Infrastructure, Logistics Operations, Fleet Management, Logistics Systems, Property Management, CADRE Management and Distribution Management. Within each of these programs areas there are primary and backup SMEs reporting POCs.
Data Collection Methodology	This measure assesses four components of logistics readiness, each weighted equally (25% each) —Commodities; Contracts; Human Capital; and Operating Capabilities. Each of the measure’s four components result from several elements, each of which have a planning factor or target. These planning factors have been identified based upon analyses from previous disasters and disaster scenarios such as the California Cascadia Subduction Zone Earthquake and Tsunami Response Plan. These planning factors document the logistics requirements for each of the elements that make up the four components. To calculate this measure, first each component is individually calculated by dividing

	the total planning factors by the actual counts of each element, and then multiplying the result by the component weight. The four weighted results are then added together to produce the measure's result.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data used to compile this measure resides on information systems subject to control and maintenance by the programs' subject-matter experts, who use this same data to inform and manage program operations. This measure will be tracked by the Distribution Management Division and Logistics Operations Division for the equipment and Initial Response Resources using the Logistics Supply Chain Management System, the official record for property resources. Staffing accountability will be managed by the Incident Workforce Management division of the Logistics Management Directorate. Data are checked for accuracy and completeness by the Logistics Management Center within the Logistics Operations Division to ensure that all standard operating procedures for documenting procurement of items are followed.

Performance Measure	Percent achieved of Incident Management Workforce readiness targets
Program	Response and Recovery
Description	This measure captures FEMA's Incident Management (IM) workforce readiness toward established workforce planning factors required to manage the expected disaster activity across the nation. These models were developed by historical data and subject matter expert inputs. The agency established a planning factor for the number of IM staff in each position and level of qualification necessary to sufficiently manage expected disaster workloads. The workforce planning factors of staffing and qualification, if achieved, will allow FEMA to cover 89% of the nation's typical routine disaster risk workload requirements. The IM workforce is critical in providing direct survivor assistance.
Scope of Data	The scope of the data includes statistics of all incident management employees during the year of reporting. The performance measure is a composite measure made up of two components: force strength and force qualification. The scope of data for force strength is the number of IM workforce on board, or hired, at FEMA. The scope of data for force qualification is based on statistics collected for each member of the IM workforce. These statistics include the associated percentages of required trainings and tasks completed by position.
Data Source	The foundational inputs for the measure are recorded, reported, and stored in FEMA's Deployment Tracking System (DTS). DTS is an SQL database which is accessed and managed by FEMA's Field Operations Directorate (FOD) staff. Planning factors are informed by the Cumulative Distribution Function (CDF) outputs of Event Staffing Models, which relate workloads from expected disaster scenarios to the number of personnel required to manage the workload.
Data Collection Methodology	Data computed for force qualification level begins with taking an individual's overall qualification level based on training and completion percentage. Task completion weighs 75% while training completion weighs 25%. To determine the qualification level of the entire IM workforce, sum all qualification values together then divide the total staff qualification level by the qualification planning factor of 13,605. To calculate force strength, take the total number of IM workforce and divide by the force strength planning factor of 17,670. Lastly, to obtain the composite number, multiple both force strength and qualification results by 0.5 and sum the numbers together.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data used to compile this measure resides on information systems subject to control and maintenance by the programs' subject-matter experts, who use this same data to inform and manage program operations. The measure will be

	tracked and checked for accuracy by analysts and mangers within the FOD. If deployment or qualifications data is incorrect, FOD will work with the Cadre or Program Office to change the data based upon internal data management processes. Once verified, reliable data will be updated in the system immediately.

Performance Measure	Percent of applicants satisfied with simplicity of the Individuals and Households Program
Program	Response and Recovery
Description	This measure provides program managers with disaster survivors' impressions about the simplicity of the procedures required to receive disaster relief from the Individuals and Households Program (IHP). The program collects survivors' impressions of their interactions with IHP using standard surveys, administered by telephone, at three touchpoints of their experience with FEMA. The program sets a threshold for survivors' responses to survey questions to qualify for an overall rating of 'satisfied,' and the measure indicates the share of all questions answered and scored in the reporting period that meet the threshold, i.e. scores of four or five points on the five-point Likert-type scale. Managers will use insights derived from survey results to help drive improvements to IHP. Feedback from disaster survivors will ensure that the program provides clear information and high-quality service in critical, public-facing agency activities.
Scope of Data	This measure's scope includes valid responses to telephone surveys of disaster survivors in jurisdictions qualifying for the Individuals and Households Program (IHP). The Customer Survey and Analysis Section in the Recovery Reporting and Analytics Division conducts three surveys. The Office of Management and Budget (OMB) approved all of the surveys for dissemination. The surveys include a significant share of the registration population, enhancing results' validity. Analysts produce results using five (5) Likert-type-scale questions, each with a five (5)-point scale. Sampling includes all eligible applicants who contacted FEMA. The Initial survey begins about two weeks after registration, with a goal of 1,200 survivors per quarter. The Contact survey begins two weeks after a survivor's call or Internet contact, with a goal of 1,800 survivors per quarter. The Assessment survey begins 30 days after an IHP decision, with a goal of 400 survivors for each disaster declaration.
Data Source	The Customer Survey and Analysis Section (CSAS) in the Recovery Reporting and Analytics Division (RRAD) stores all survey responses in WinCATI (a Computer Assisted Telephone Interviewing system) for easy retrieval, statistical analyses, and reporting. CSAS staff export data from the survey system into a Microsoft Access database, where all survey data resides. RRAD operates and maintains systems used to store customer-survey data.
Data Collection Methodology	Using data stored in Microsoft Access, CSAS staff generate quarterly reports to the RRAD Performance Measurement and Analysis Team (PMAT) to calculate each question's comprehensive result. PMAT loads the results into PowerPivot for automatic calculation. For all surveys completed, PMAT analysts review respondents' answers to each of the five questions. RRAD has determined that answers to any question of 4 or 5 points on the five-point Likert-type scale satisfy the threshold for 'satisfaction with the simplicity of IHP.' Analysts then calculate the share of threshold-clearing answers for each question, and then calculate the average share of threshold-clearing responses across all five questions in the surveys submitted during a given reporting period, which yields the results for the performance measure.
Reliability Index	Reliable

Explanation of Data Reliability Check	A quality-control section monitors CSAS surveyors to ensure correct recording of data provided by applicants. The program engages in training, updating scripts, and coaching to mitigate reliability issues when recording applicant answers. CSAS program analysts and statisticians also review data after completion of surveys to ensure that recorded data accurately reflect what the surveys captured. After these accuracy checks, staff provide analysts with data in Excel format for performance measurement calculations. RRAD compares the raw data to the CSAS results summary. A peer review follows, followed by a supervisory review of the calculations. These multiple steps reinforce program confidence in the data's completeness, accuracy, and validity.

Performance Measure	Percent of applicants satisfied with simplicity of the Public Assistance process
Program	Response and Recovery
Description	This measure gauges the percent of applicants for Public Assistance (PA) grant programs that are satisfied with the simplicity of the process throughout the recovery lifecycle. Simplicity is measured through an initial customer survey and later assessment on the dimensions of Public Assistance (PA) Staff Interactions, Satisfaction with PA Program, Simplicity of the PA process; Simplicity of the PA System, and Simplicity of PA policy. Customer satisfaction data is collected from phone interviews as well as electronic submission of responses through the WinCATI survey system. Satisfied customers represent scores of three or greater on all dimensions of the 23 composite survey questions. Customer experience information is collected to better identify root causes for low satisfaction (primarily in simplicity) to guide future process changes and guidance to provide a more client-focused and user-friendly experience.
Scope of Data	The Customer Survey and Analysis Section (CSAS) within the Recovery Reporting and Analytics Division (RRAD) conducts two telephonic surveys for Public Assistance -- Initial and Assessment. The scope of the results includes all initial and assessment surveys that have an overall score of 3 or greater on a 5-point scale on all 23 questions that comprise the 5 assessed areas. The population includes all initial and assessment surveys conducted during the reporting period.
Data Source	The FEMA Recovery Reporting and Analytics Division's (RRAD) Customer Survey and Analysis Section (CSAS) conducts the surveys to collect the data for the measure. Collection techniques include phone interviews as well as electronic submission of responses through the WinCATI survey system. CSAS has a team of interviewers trained to conduct phone surveys of PA participants. All survey responses are stored in the WinCATI system for easy retrieval, statistical analyses, and reporting. Data are exported from the survey system into Access where all historical data are stored. CSAS generates quarterly reports to the RRAD Performance Measurement and Analysis Team (PMAT) to calculate metric results. PMAT loads the results into PowerPivot for automatic calculation. The Recovery Reporting and Analysis Division is the owner of the customer survey data.
Data Collection Methodology	All eligible applicants who had contact with FEMA (e.g. meetings, e-mails, or phone calls) are surveyed. The Initial survey is done around 60 days after the disaster/emergency declaration for two weeks with up to six contact attempts. The PA Assessment survey is conducted roughly 210 days after initial disaster declaration for two weeks with up to six contact attempts. CSAS generates reports and raw data and sends to RRAD PMAT for calculation. Each category's composite score includes the average scores of individual questions which are equally weighted within the category. Composite scores calculated as: PA Staff interactions has 6 survey questions weighed at 16.666667%; Satisfaction with the PA program has 5 questions at 20%; Simplicity of the PA process has 5 questions

	at 20%; Simplicity of PA System has 3 questions at 33.33%; Simplicity of policy has 4 questions at 25%. PMAT averages the score of all respondents for each of the 23 questions and converts the score into a percent.
Reliability Index	Reliable
Explanation of Data Reliability Check	CSAS surveyors are monitored by a quality control section to ensure data provided by applicants are recorded correctly. Training, updating scripts, and coaching take place to mitigate reliability issues when recording applicant answers. Data are also reviewed by CSAS program analysts and statisticians after the surveys are complete to ensure data accurately reflect what the surveys captured. Once accuracy is insured, data are provided in an Excel format for performance measurement. RRAD compares the raw data to the CSAS results summary. These results are then peer reviewed and followed up by a supervisory review of the calculations. Through these various steps we are confident that the data are complete, accurate, and thoroughly reviewed.

Performance Measure	Percent of critical federal response teams supported by voice, video, and data connectivity using a fully-capable mobile emergency office vehicle
Program	Response and Recovery
Description	The program has identified on-scene availability of a mobile platform for voice, video, and data connectivity as a critical capability for Federal teams managing response and recovery operations. The program has procured Mobile Emergency Office Vehicles (MEOVs) to provide these capabilities for these teams. Using data from systems employed to track and manage the agency’s physical assets, this measure indicates the share of all teams managing response and recovery operations with access to an MEOV during a given fiscal year.
Scope of Data	This measure’s scope includes the share of all recovery teams with immediate access to one of the agency’s MEOVs. Over the course of a given fiscal year, the program procures MEOVs, which provide response and recovery teams with on-scene availability of a mobile platform for voice, video, and data connectivity as a critical capability. MEOVs support relevant response activities conducted by Incident Management Assistance Teams, Incident Support Bases, Urban Search and Rescue Incident Support Teams, and National Disaster Medical System Incident Response Coordination Teams. To track and manage the program’s inventory of MEOVs, program staff use an agency-wide property-management database. The agency’s Office of Response and Recovery maintains a tally of the types and numbers of Federal teams that have validated requirements for support by the program’s Mobile Emergency Response Support Detachments, which include MEOVs.
Data Source	The agency’s Mission Support Bureau maintains and operates the Sunflower Asset Management System (SAMS), an online database which serves as the agency’s official property-management system. The Disaster Emergency Communications Division serves as the program of record for MEOV data stored in SAMS.
Data Collection Methodology	SAMS produces reports detailing the agency-wide inventory of MEOVs. The agency’s Office of Response and Recovery maintains a tally of the types and numbers of Federal teams which have validated requirements for support by the program’s Mobile Emergency Response Support Detachments, which include MEOVs. For any given fiscal year, dividing the total size of the MEOV inventory into the total number of federal response teams yields this performance measure.
Reliability Index	Reliable
Explanation of Data Reliability Check	Both the logistics section of the Disaster Emergency Communications Division and the agency’s fleet-management staff in the agency’s Office of the Chief

	Administrative Officer review reports of MEOV inventory produced by SAMS. These reviews ensure accurate counts of MEOV inventory. The agency's Office of Response and Recovery has responsibility for the types and numbers of Federal response teams which have validated requirements for support by the program's Mobile Emergency Response Support Detachments, which include MEOVs.

Performance Measure	Percent of in-person federal inspections for those that applied for assistance under the Individuals and Households Program
Program	Response and Recovery
Description	When disaster survivors apply for assistance under the Individuals and Households Program (IHP), staff have traditionally conducted in-person inspections to confirm applicants' eligibility. This measure reports the percent of these and other federal inspections completed in-person, versus those leveraging technologies including satellite imagery or digital photos from applicants. Currently, survivors access disaster assistance through a range of programs administered by government and non-government entities, each requiring in-person damage assessment inspections from several different entities for housing assistance. In addition to IHP, the measure also includes inspections by the Small Business Administration (SBA); Substantial Damage Estimates (SDE); the National Flood Insurance Program (NFIP); and Sheltering & Temporary Essential Power (STEP). Managers will see whether the measure declines over time, indicating progress in a critical, public-facing agency activity.
Scope of Data	The scope of this measure includes all inspections completed during each reporting period to determine applicant eligibility for federal housing assistance. Inspections fall into one of two categories: 1) in-person inspections; and 2) inspections completed by leveraging technology, such as satellite imagery or digital photos from applicants. Program staff have access to data on both categories of inspections for each of the following agencies or programs: IHP; Small Business Administration; Substantial Damage Estimates; National Flood Insurance Program; and Sheltering & Temporary Essential Power. The measure counts in-person inspections as a share of the total. The program has begun to promote alternatives to in-person inspections, to expedite processing applications without sacrificing reliability of inspections. Over time, managers expect that in-person inspections' share of total inspections will decline, better serving survivors by enhancing recovery efforts' responsiveness.
Data Source	The Individual Assistance Division maintains and operates the National Emergency Management Information System (NEMIS) as IHP's system of record. NEMIS contains all program-pertinent information for registered individuals and households; their current and damaged dwelling; inspection results; SBA activity; correspondence; and decisions and amounts with regard to eligibility for IHP assistance. Agency and program staff add data to NEMIS through registration, casework, and inspection processes. In addition, the agency maintains an Operational Data Store (ODS), which stores records from NEMIS and other agency systems in a format which facilitates data extraction and analysis. Finally, program staff regularly collect data from SBA on inspections by that agency, provided in an Excel format to facilitate analysis.
Data Collection Methodology	The Recovery Reporting and Analytics Division (RRAD) will collect data from Joint Field Offices and the Federal Insurance & Mitigation Administration for STEP, NFIP and SDE. RRAD will perform data matching and import data into the ODS. RRAD will extract data from ODS for IHP, STEP, NFIP and SDE using SQL, a standard language for storing, manipulating and retrieving data in databases. Final format results will appear in Microsoft Excel. RAD will collect data from SBA in an Excel format. Data will contain disaster number, FEMA registration number,

	source of inspection (IHP, SBA, STEP, NFIP, and SDE), inspection type (in-person, eliminated, or desktop). These data will yield 1) the total number of inspections completed during a reporting period to support applications for housing assistance, and 2) the subset of in-person inspections completed during the same period. Dividing the number of in-person inspections into the total number of inspections produces the performance measure.
Reliability Index	Reliable
Explanation of Data Reliability Check	For each performance period, as a step in reporting this measure, the Recovery Reporting and Analytics Division (RRAD) will extract and analyze an ODS report. RRAD will share initial findings among the Analysis Branch, the Reporting Branch, and the Director to double-check counts and analyses. RRAD will share final numbers with partners in the agency's Individual Assistance Division, SBA, and the agency's Mitigation Directorate for review and verification before submission to senior leadership. Analysts address any questions and review any discrepancies, if necessary.

Performance Measure	Percent of Public Assistance project obligations completed within targeted timeframes
Program	Response and Recovery
Description	This measure evaluates the percent of the Public Assistance (PA) initial grant awards made to state and local government applicants following a Presidential disaster declaration within 189 days. The Timeliness to Initial Award is the time from the county designation date to initial obligation date at the project level (i.e. the time from when an Applicant is eligible for assistance until FEMA makes the Applicant's first funds available to the Recipient for disbursement to the Applicant). Issuing timely public assistance grants reflects the priority of enabling the recovery process and providing assistance in a more efficient and timely manner.
Scope of Data	The population of the metric includes all State-led Public Assistance disaster grants and pilot program projects obligated within the reporting period. The scope of the results are the number of projects that completed their initial obligation of funds within 189 days. Erroneous numbers where the timeliness is negative or there are no obligation dates are removed from the list.
Data Source	The data for the Timeliness to Initial Award component of this metric resides in the Emergency Management Mission Integrated Environment (EMMIE) Enterprise Data Warehouse (EDW). EMMIE is the current official system of record for Public Assistance financial obligations. EDW is an Oracle database, and its data is refreshed nightly between 12:30 AM and 3:30 AM. Data is then imported from the EMMIE EDW into the Public Assistance Grants Manager and is accessible through a Portal Microsoft SQL Server database and is accessible through a SQL Server replicated database connection (FACTRAX-prod). The Recovery Reporting and Analytics Division (RRAD) created a Microsoft SQL Server query to extract the data. PA data is pulled from this database on a quarterly basis per fiscal year (FY). The Public Assistance Division is the owner of the data for all components of this metric. All data is managed and collected by the Recovery Reporting and Analytics Division (RRAD).
Data Collection Methodology	The Timeliness to Initial Award data is generated by EMMIE as the program delivery elements are completed by Public Assistance program staff. RRAD extracts the data from the Grants Manager/Portal SQL Server database at a Project level. The data is then calculated in Microsoft Power BI to determine the percentage of projects meeting or exceeding the target number of days. The calculation is the following for projects obligated in the reporting period: (Number of projects initially obligated within 189 days) / (Total projects

	obligated). Erroneous numbers where the timeliness is negative or there are no obligation dates are removed from the list.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data for this measure is extracted from Enterprise Data Warehouse using an SAP Business Objects queries. The Timeliness to Award query has been worked on and modified by multiple members of the RRAD reports staff, providing multiple levels of peer review. Prior to reporting of the data, it is then reviewed and summarized by the RRAD Performance Measurement and Analysis Team, shared with Subject Matter Experts (SMEs), supervisors, and the PA division for review and validation. During this time, any inconsistencies identified in the data analysis will be corrected.

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 to calculate 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 is 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.

Federal Law Enforcement Training Centers

Performance Measure	Percent of Partner Organizations satisfied with Federal Law Enforcement Training Centers' training
Program	Law Enforcement Training
Description	This measure reflects the effectiveness of Federal Law Enforcement Training Centers' (FLETC's) training based on survey results documenting Partner Organizations' (PO's) satisfaction with the quality of instructional staff, whether FLETC's basic and advanced training addresses the right skills needed for officers and agents to perform their law enforcement duties, whether basic and advanced training prepare officers and agents to perform specific job-related tasks safely and effectively, and overall satisfaction with the training. Responses of "Strongly Agree" and "Agree" are considered satisfied. FLETC provides training to more than 100 POs, 12 of which are within the Department of Homeland Security. The results provide on-going opportunities for improvements incorporated into FLETC training curricula, processes and procedures.
Scope of Data	This measure includes the results from all POs that respond to the PO Satisfaction Survey statements about satisfaction with the quality of instructional staff, whether FLETC's basic and advanced training addresses the right skills needed for officers and agents to perform their law enforcement duties, whether basic and advanced training prepare officers and agents to perform specific job-related tasks safely and effectively, and overall satisfaction with the training. Responses of "Strongly Agree" and "Agree" are considered satisfied. Responses of "Not Applicable" are excluded from the calculations.
Data Source	The source of the data is the FLETC PO Satisfaction Survey administered via a web-based survey program (Verint), which tabulates and calculates the survey results. The PO representative from each PO provides responses to the survey through Verint 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 annually from July to August. The survey uses a six-point Likert scale. Program personnel import the survey data as saved by survey respondents from Verint into Microsoft 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 about satisfaction with the quality of instructional staff, whether FLETC's basic and advanced training addresses the right skills needed for officers and agents to perform their law enforcement duties, whether basic and advanced training prepare officers and agents to perform specific job-related tasks safely and effectively, and overall satisfaction with the training divided by the number of POs that responded to each of the respective statements. Responses of "Not Applicable" are 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 PO key representatives to confirm and discuss their responses.

	Throughout the year other formal and informal inputs are solicited from the PO representatives by FLETC staff and used to validate the survey results. No known data reliability problems exist.

Performance Measure	Percent of Partner Organizations satisfied with the overall Federal Law Enforcement Training Centers' experience
Program	Law Enforcement Training
Description	This measure reflects the satisfaction of Partner Organizations (POs) with the overall Federal Law Enforcement Training Centers (FLETC) experience. The experience is defined as law enforcement training facilities, equipment, and support services (e.g., housing, dining, logistics, recreation, etc.) provided to PO students and training staff. POs that respond to the survey questions as "Strongly Agree" or "Agree" are considered satisfied with the experience. FLETC training programs prepare PO officers/agents to perform their law enforcement duties such as terrorism and other criminal activity against the U.S. and our citizens.
Scope of Data	This measure includes the results from all POs that respond to PO Satisfaction Survey statements about satisfaction with the training facilities, equipment, and support services that FLETC provides. POs that responded, "Strongly Agree" or "Agree" are included in the scope of the results. Responses of Not Applicable are excluded from the calculations.
Data Source	The source of the data is the FLETC PO Satisfaction Survey administered via a web-based survey program (Verint), which tabulates and calculates the survey results. The PO representative from each PO provides responses to the survey through Verint 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 July to August. The survey uses a six-point Likert scale. Program personnel import the survey data as saved by survey respondents from Verint into Microsoft 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" divided by the number of POs that responded to each of the respective statements. Responses of Not Applicable are 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 PO key representatives to confirm and discuss their responses. Throughout the year other formal and informal inputs are solicited from the PO representatives by FLETC staff and used to validate the survey results. No known data reliability problems exist.

Performance Measure	Percent of Partner Organizations that agree the Federal Law Enforcement Training Centers' counterdrug-related training is effective
Program	Law Enforcement Training
Description	This measure reflects the satisfaction of Partner Organizations (POs) with counterdrug-related training provided by the Federal Law Enforcement Training Centers (FLETC) covered in Basic and Center Integrated Basic training programs. The FLETC collaborates with more than 100 POs, both internal and external to the Department of Homeland Security and provides counterdrug courses on Controlled Substance Identification, Drug Recognition, Recognition of Clandestine Labs, Marijuana Cultivation Investigations, Sequential Testing, and Drugs of Abuse. Participants are surveyed to determine whether the course was effective.

Scope of Data	This measure includes the results from all POs that respond to the PO Satisfaction Survey Statement, "FLETC's counterdrug-related basic skills training (i.e. courses titled Controlled Substance Identification, Drug Recognition, Recognition of Clandestine Labs, Marijuana Cultivation Investigations, Sequential Testing, and Drugs of Abuse (covered in FLETC's Center Basic and Center Integrated Basic training programs) is effective." The scope of the results includes the POs that responded, "Strongly Agree" or "Agree." POs that respond "Not Applicable" to the above statement are excluded from the calculations of this measure.
Data Source	The source of the data is the FLETC PO Satisfaction Survey administered via a web-based survey program (Verint), which tabulates and calculates the survey results. The PO representative from each PO provides responses to the survey through Verint and saves the responses online when the survey is completed.
Data Collection Methodology	Data are collected annually from July to August via a PO Satisfaction Survey. The measure is based on responses to Survey Statement, "FLETC's counterdrug-related basic skills training (i.e. courses titled Controlled Substance Identification, Drug Recognition, Recognition of Clandestine Labs, Marijuana Cultivation Investigations, Sequential Testing, and Drugs of Abuse which are covered in FLETC's Center Basic and Center Integrated training programs) is effective." The survey uses a six-point Likert rating scale. Program personnel import the survey data as saved by survey respondents from Verint into Microsoft Excel to generate data charts and tables. The percent is calculated as the total number of POs that responded, "Strongly Agree" or "Agree" to the above statement divided by the number of POs that responded to the above statement.
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 PO key representatives to confirm and discuss their responses. Throughout the year other formal and informal inputs are solicited from the PO representatives by FLETC staff and used to validate the survey results. No known data reliability problems exist.

Immigration and Customs Enforcement

Performance Measure	Average daily population of noncitizens maintained in detention facilities
Program	Enforcement and Removal Operations
Description	This measure reports the average daily count of noncitizens held in detention facilities. The measure reflects the total detention population for a given time period, divided by the total number of days during that time period.
Scope of Data	Actual daily population is a summary of what the Statistical Tracking Unit reported on those corresponding dates for the past week on the Daily Population Report. ICE Detention data exclude Mexican Interior Repatriation Program (MIRP) facilities and Office of Refugee Resettlement (ORR) transfers/facilities, as well as U.S. Marshals Service Prisoners.
Data Source	Data is maintained in the Removal Module of the Enforcement Case Tracking System (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 Removal Module and produce reports to calculate the final results for this measure.

Data Collection Methodology	ERO Field Offices are responsible for the entry and maintenance of data regarding the daily population of noncitizens. The Average Daily Population (ADP) is based on MANDAY Count. A MANDAY is based on whether an individual is in an ERO detention facility for the midnight count. A midnight count represents a detainee in a detention facility at midnight on the given date. For every individual in a facility for the midnight count equates to one MANDAY. The ADP is the number of MANDAYs for a given time period, divided by the number of days in that time period.
Reliability Index	Reliable
Explanation of Data Reliability Check	Headquarters staff validates the completeness and accuracy of the data entered by field offices into the Removal Module through trend analysis to look for 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.

Performance Measure	Average length of stay in detention of all convicted criminal noncitizens prior to removal from the United States (in days)
Program	Enforcement and Removal Operations
Description	This measure provides an indicator of efficiencies achieved in driving down the Average Length of Stay (ALOS) for convicted criminals in ICE detention facilities. Decreases in the ALOS can significantly reduce the overall costs associated with detention prior to removal.
Scope of Data	The scope of this measure includes all criminal noncitizens 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. Noncitizens 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.
Data Source	Data is maintained in the Removal Module of the ENFORCE database. This database is maintained at ICE 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 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 noncitizens in ICE Custody. The length of stay for a noncitizens’s detention stay is calculated by counting the number of days between the noncitizen’s initial book-in date into ICE Custody and their final book-out date. If a noncitizen is booked in and out of ICE custody on the same day, the noncitizen’s length of stay is 0 days. 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.
Reliability Index	Reliable
Explanation of Data Reliability Check	Headquarters staff validate the completeness and accuracy of the data entered by field offices into the 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	Estimated average direct adult bed cost per day for detention
Program	Enforcement and Removal Operations
Description	The measure reports all costs associated with directly supporting the detainment of one individual for one day in an Immigration and Customs Enforcement (ICE) managed immigration detention facility. These cost include bed and detention guard contracts; contracts for detainee provisions, healthcare, building maintenance, in addition to costs such as telecom, utilities, operation and maintenance of facilities; supplies; equipment; postage, and facility compliance/inspection contracts billed to individual facilities.
Scope of Data	The scope of the measure includes all direct costs associated with directly supporting the detainment of one individual adult for one day in an ICE detention facility at the point in time the facility population is counted (ICE refers to this as midnight man day count). A midnight man day represents a detainee in a detention facility at midnight on the given date. Financial data include all obligations and expenditures for the current fiscal year from all active appropriations. These direct cost include bed and detention guard contracts; contracts for detainee provisions, healthcare, building maintenance, and also includes specific costs such as telecom and utilities billed directly to individual facilities and facility compliance/inspection contracts. All indirect cost are excluded, such as headquarters support and liability insurance.
Data Source	Data are derived from two sources: 1) Federal Financial Management System (FFMS) provides financial information on the obligations and expenditures of funds on detention beds. This accounting system is owned by the DHS Office of Financial Management. The second source is Integrated Decision Support (IIDS) (ICE Integrated Decision Support) which provides information on the utilization of beds by ICE detainees. IIDS data is reported by ERO through standardized excel reports. ICE Chief Financial Officer (CFO) owns the reporting of and process to calculate the average daily bed cost, but ERO owns the bed utilization data.
Data Collection Methodology	To derive the estimated adult bed costs, ICE uses the financial data from FFMS and operational data from ICE IIDS. The program measures midnight man days representing the number of people present in a given facility during a count at midnight. Field Offices report this information daily in the IIDS system which includes midnight man days for the current year. IIDS data are entered into ENFORCE by agents in the field. The data is then aggregated from ENFROCE by IIDS and reported by ERO to ICE CFO in an excel spreadsheet. Financial data are collected in FFMS using a combination of funding program and sub-object class code to determine whether the cost was bed related. Obligations and expenditures which are deemed unrelated to direct bed cost are excluded. ICE CFO integrates the ENFORCE data with the financial data using Excel. The average adult bed cost per day is calculated by dividing all the Obligations and Expenditures by the total number of man days in a given reporting period.
Reliability Index	Reliable

Explanation of Data Reliability Check	The Office of Budget and Program Performance conducts periodic manual checks of the FFMS data and IIDS to ensure data quality. In addition, ICE is part of DHS financial audit conducted by external auditor. Any data found to be incorrect is reviewed and updated in the system.

Performance Measure	Number of convicted criminal noncitizens who were returned or were removed from the United States
Program	Enforcement and Removal Operations
Description	This measure includes both the return and removal of noncitizens who have a prior criminal conviction from the United States by ICE Enforcement and Removal Operations (ERO). This measure reflects the program's efforts to ensure convicted criminal noncitizens do not remain in the United States.
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 Removal Module of the ENFORCE database. This database is maintained at ICE 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 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 noncitizens. When a noncitizen 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 Removal Module of the ENFORCE database. Reports generated from the Removal Module using IIDS determine the number of convicted illegal noncitizens 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 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 noncitizens meeting Civil Immigration Enforcement Priorities returned or removed from the U.S. (New Measure)
Program	Enforcement and Removal Operations
Description	This measure gauges the number of noncitizens returned or removed from the U.S. that fall within the three interim priorities, National Security, Border Security, Public Safety, or meet another agency priority determined by a senior

	field manager. Noncitizens are presumed to be a national security priority if they engaged or are suspected of engaging in terrorism related activities, espionage-related activities, or if their apprehension, arrest, or custody is necessary to protect the national security. Noncitizens are presumed to be a border security priority if they were apprehended at the border or port of entry while attempting to enter unlawfully or were not physically present in the United States before November 1, 2020. Noncitizens are presumed to be a public safety priority if they pose a threat to public safety and convicted of an aggravated felony, or qualifying members of criminal gangs and transnational criminal organizations.
Scope of Data	The population includes all returns and removals made during the fiscal year. The unit of analysis is a single return or removal. The attribute that determines whether a return of removal is counted in the results is whether it is associated with one of the three Civil Immigration Enforcement Priorities (CIEP), national security, border, security, public safety, or another priority identified by a senior manager.
Data Source	Enforcement Integrated Database (EID) is the system of record for immigration enforcement actions, including returns and removals. It captures case and subject data related to National Security, Border Security, and Public Safety. Additionally, the Arrest Authorization Request Tool (AART) tracks requests and approvals for priority enforcement actions. Arrests prior to February 22, 2021 will not have AART requests but data was mitigated through October 1, 2021. Law Enforcement and Systems Analysis (LESA) Statistical Tracking Unit (STU) is the office that gathers, analyzes, and submits this data.
Data Collection Methodology	Case ID is entered at the time an AART request is being submitted. In exigent circumstances, AART requests can be entered 24hrs after an arrest is made. STU will identify all returns and removals that fall under the three CIEPs (National Security, Border Security, Public Safety) from data in EID that was recorded through ENFORCE Alien Removal Module (EARM) from case and subject data collected by the AART tool. The total is calculated from the beginning of the fiscal year until the end of the current reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	EID data is run through an automated ETL process to validate and prepare for reporting. Additionally, this data goes through manual data quality checks before results are released for analysis and reporting.

Performance Measure	Percent of all Alternative to Detention participants who demonstrate compliance (New Measure)
Program	Enforcement and Removal Operations
Description	This measure gauges the compliance of participants enrolled in the Alternative to Detention (ATD) process. Participants are noncitizens who, upon release from custody, require supplemental case management support and technology assignment to be successful with release conditions, court hearing attendance, and compliance with final orders of removal while allowing them to remain in their communities. ATD uses contractors for effective case management to assist the participant in ensuring they understand their immigration obligations, can meet basic needs, and are provided continued support while they remain in their communities. Participants who were de-escalated and/or positively terminated after recurring case reviews are considered in compliance. ATD ensures compliance as immigrants move through their immigration court proceedings without detaining them inside detention centers.
Scope of Data	The population includes all case compliance decisions to identify how many times the participant services were de-escalated and/or terminated for positive reasons. The unit of analysis is a single case compliance review. Participants

	have recurring case reviews to determine if they are compliant with their release conditions and there are two possible outcomes: 1, participant is non-compliant and the services are increased or maintained; or 2, participant is compliant, and services are reduced or no longer required to participate (termination). The attribute that includes a case review in the result is whether the participant is compliant and services were reduced or they are terminated.
Data Source	Data will be taken from the ATD – ISAP contractor database: TotalAccess. TotalAccess is proprietary system owned and maintained by the contractor, BI. All information related to ATD – ISAP participants, required case management services, supervision levels, case notes, and technology assignments as maintained here. The information will be requested from BI and will be evaluated by the HQ – ATD Capgemini team.
Data Collection Methodology	Case specialists (contractors who work for BI) and Enforcement and Removal Operations officers are responsible for updating TotalAccess. When a case review is completed, the appropriate personnel go into TotalAccess and provide comments on outcomes and update requirements accordingly whether to de-escalate, terminate, or maintain status quo. Reports are pulled from TotalAccess depending on the information required and the raw data is analyzed. The percent is determined by taking the total number of participants with terminations or reduced services from case reviews and dividing by the total number of all case compliance decisions.
Reliability Index	Reliable
Explanation of Data Reliability Check	TotalAccess is routinely maintained for accuracy and BI has its own quality assurance team that conducts routine audits to ensure accuracy. ERO has officers assigned in the field that also conduct monthly, recurring reviews of the information collected within TotalAccess to determine accuracy while comparing it against the Enforce Alien Removal Module (EARM). HQ – ATD has a quality assurance section and HQ – ATD personnel that also conduct reviews independently of ERO officers and BI staff. These different groups communicate regularly to ensure that data is accurate and reliable.

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
Description	This measure gauges the percent of detention facilities, with an Average Daily Population (ADP) greater than 10, 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 noncitizens in immigration proceedings or awaiting removal to their countries do so in accordance with the Performance Based National Detention Standards.
Scope of Data	The scope of this measure includes all adult facilities on the Authorized Facility's List authorized to house ICE detainees through ERO Detention Management Control Program (DMCP). Per the DMCP, facilities that are used regularly by ICE (i.e., an APD greater than 10) to house adult detainees must be inspected. Once a facility has been inspected by ICE and determined to be appropriate to house adult detainees, the facility is scheduled for routine follow-up inspections and tracked on the Authorized Facility List. 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. Family

	residential centers, or ERO juvenile facilities, staging facilities, or holding rooms that may temporarily hold ICE detainees are not included.
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. 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 Interim Civil Immigration Enforcement Priority Arrests (New Measure)
Program	Enforcement and Removal Operations
Description	This measure gauges the percent of total arrests that fall within the three interim priorities, National Security, Border Security, Public Safety, or who meet another agency priority determined by a senior field manager. Noncitizens are presumed to be a national security priority if they have engaged or are suspected of engaging in terrorism related activities, espionage-related activities, or if their apprehension, arrest, or custody is necessary to protect the national security. Noncitizens are presumed to be a border security priority if they were apprehended at the border or port of entry while attempting to enter unlawfully or were not physically present in the United States before November 1, 2020. Noncitizens are presumed to be a public safety priority if they pose a threat to public safety and were convicted of an aggravated felony, or qualifying members of criminal gangs and transnational criminal organizations.
Scope of Data	The unit of analysis is a single non-citizen arrest. The population includes all non-citizen arrests made within the fiscal year. The attribute whether the arrest is reported in the results is whether the arrest of a non-citizen was related to a Civil Immigration Enforcement Priorities (CIEP) (National Security, Border Security, Public Safety, or who meet another agency priority determined by a senior field manager, such as foreign fugitive referrals, human rights violators, etc.).
Data Source	The Arrest Authorization Request Tool (AART) tracks requests and approvals for priority enforcement actions and Enforcement Integrated Database (EID) tracks all arrests. Law Enforcement and Systems Analysis (LESA) Statistical Tracking Unit (STU) is the office that gathers, analyzes, and submits this data.
Data Collection Methodology	STU will gather all arrest data. The records will be linked by Subject ID to AART records, and arrests with one or more approved AART requests will be included in the final percentage. AART requests are typically entered prior to making an arrest. In exigent circumstances AART requests can be entered 24hrs after an arrest is made. In the event that an arrest is not matched with its AART request, this can be mitigated through October 1, 2021. Arrests prior to that date will not

	have AART requests. The AART Dashboard is an interactive tool for viewing and reporting on AART data, which is supporting using data from the beginning of the fiscal year to the end of the reporting cycle using Subject IDs with national security, border security, public safety, and other related codes. The calculation is the total number of AART priority arrests for national security, border security, public safety, and meeting any other priority areas divided by the total number of arrests.
Reliability Index	Reliable
Explanation of Data Reliability Check	EID data is run through an automated ETL process to validate and prepare for reporting. Additionally, this data goes through manual data quality checks before results are released for analysis and reporting. ERO Case ID is entered at the time an AART request is being submitted. In exigent circumstances AART requests can be entered 24hrs after an arrest is made. In the event that an arrest is not matched with its AART request, this can be mitigated through October 1, 2021. The AART tool was announced to ERO officers on February 22, 2021. Arrests prior to that date will not have AART requests.

Performance Measure	Total number of noncitizens who were returned or removed from the United States (Retired Measure)
Program	Enforcement and Removal Operations
Description	This measure describes the total number of noncitizens returned and/or removed from the United States by ICE Enforcement and Removal Operations (ERO). The measure includes both noncitizens 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.
Scope of Data	The measure captures the sum of all noncitizens 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 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 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 noncitizens. When a noncitizen 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 Removal Module of the ENFORCE database. Reports generated from the Removal Module using IIDS determine the number of convicted noncitizens 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 noncitizen'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	Number of enforcement-related actions against employers that violate immigration-related employment laws (Retired Measure)
Program	Homeland Security Investigations
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	Number of human trafficking and child exploitation victims rescued or assisted (New Measure)
Program	Homeland Security Investigations
Description	This measure reports the number of adult or minor victims rescued or assisted as a result of human trafficking and child exploitation investigations. Human trafficking includes sex trafficking and forced labor trafficking. A child exploitation victim is considered rescued once the victim has been identified, located, and physically removed by agents or a partner agency or provided information (i.e., other types of assistance) that extricates them from the exploitative situation or further abuse. A human trafficking victim is considered assisted and entered into the VAD when a Victim Assistance Specialist makes

	contact and provides information or resources to the victim. Many victims receive additional services such as crisis management and supportive services throughout the investigation.
Scope of Data	The population includes all victims identified by HSI related to human trafficking and child exploitation. The unit of analysis is dependent on victim type. Victims of child exploitation are identified in Type 7 Reports of Investigation (ROI) with the designation of Type 01-Child Exploitation. Victims of human trafficking who receive assistance as described in the Measure Description are recorded in the Victim Assistance Database. The determining attribute for inclusion in this measure is if they were rescued (child exploitation victims) or assisted (human trafficking victims).
Data Source	Child exploitation victim data are stored in the Investigative Case Management (ICM) systems. The data are recorded as a Type 7 ROI, with the attribute (an additional victim type code) of Type 01- Child Exploitation. ICM is maintained by HSI Cyber and Operational Technology. The HSI VAP maintains the VAD to capture victims assisted by Victim Assistance Specialists (VASes) and Victim Assistance Coordinators in the field. Victims are identified in the VAD by investigative category, to include human trafficking victims.
Data Collection Methodology	A special agent identifies a child exploitation victim through investigative activities and submits a Type 7 ROI in ICM with the attribute Type 01 – Child Exploitation. The record is reviewed by the special agent's group supervisor and Special Agent in Charge (SAC). Once approved, the victim is formally identified and is given a victim designation in the investigative case and in ICM. Analysts at Headquarters extract and aggregate the data from ICM by counting the number of victims identified in Type 7 ROIs using Victim Type 01-Child Exploitation. VASes identify human trafficking victims from investigations or from non-governmental organizations and partner law enforcement agencies. The VAS enters the victim data into the VAD when the VAS makes contact and provides information or resources to the victim. When entered into the VAD, the VAS identifies victim type, e.g., human trafficking. Data is extracted from ICM and VAP and summed to get the total number of victims.
Reliability Index	Reliable
Explanation of Data Reliability Check	For victims of child exploitation, the review by the Special Agent's Group Supervisor and SAC provides the initial data reliability check for this data. A second reliability check is conducted when the results produced by analysts are reviewed by leadership in HSI. Budget Formulation and Reporting Unit analysts also conduct quality control verification on all data received through ICM to ensure performance data are accurate, complete, and unbiased. VASes receive training on the proper entry of assisted victims into the VAD. VAP Program Managers have administrative rights to the VAD and regularly review VAS data for completeness.

Performance Measure	Number of significant drug-related illicit trade, travel, and finance investigations that resulted in a disruption or dismantlement
Program	Homeland Security Investigations
Description	This measure reports on the total cumulative number of significant transnational drug investigations that resulted in a disruption or dismantlement. To be considered significant, the high-threat transnational drug-trafficking organizations/individuals must qualify as or have links to a Consolidated Priority Organizational Target (CPOT) or Regional Priority Organizational Target (RPOT) as designated by the Department of Justice, or must earn, launder or move more than $10 million a year in drug proceeds. "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.
Scope of Data	The scope of this measure includes cases that were determined by the Significant Case Review (SCR) process to be a disruption or a dismantlement of high-threat transnational criminal organizations engaged in criminal activity. This criminal activity relates to drug-related cases resulting in a disruption or a dismantlement of high-threat transnational drug-trafficking organizations/individuals linked or with links to a CPOT or RPOT or earn, launder, or move more than $10 million a year in drug proceeds.
Data Source	Data is entered in the SCR module located in the Investigative Case Management (ICM) system. ICM serves as Homeland Security Investigations' (HSI) core law enforcement case-management tool. ICM enables program personnel to create an electronic case file that organizes and links all records and documents associated with an investigation, and to record investigative hours. ICM is the official system of record used to initiate cases, identify case categories, and record and report substantive case information during the investigative process, capturing arrest, indictment, conviction, and case closure. Management of the SCR program resides with the Domestic Operations Division within HSI.
Data Collection Methodology	A Special Agent identifies an investigation as meeting the criteria as an initial significant investigation and completes and submits the Domestic Operations SCR worksheet through his/her chain of command based on predetermined criteria. The SCR is reviewed by the Special Agent's Group Supervisor and the Special Agent in Charge (SAC). Once the SAC has approved the submission, the case is accepted into the SCR process and the Special Agent enters it into the ICM. Cases are then confirmed as significant by a Headquarters Program Manager. An independent team at Headquarters and an SCR panel review the cases and determine whether a disruption or dismantlement occurred and this is recorded in the ICM. HSI analysts at Headquarters extract and aggregate data from ICM. Analysts count the number of disruptions and dismantlements of high-threat transnational drug-trafficking organizations and individuals approved through SCR and add this number to the cumulative total for the fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	The review by the by the Special Agent's Group Supervisor and the SAC provide the initial data reliability check for this data. Confirmation by Headquarters that the case is a significant case is another reliability check. A third reliability check is conducted when the results produced by analysts are reviewed by leadership in HSI. Budget Formulation and Reporting Unit analysts also conduct quality control verification on all data received through ICM to ensure performance data are accurate, complete, and unbiased. The last reliability check is conducted by the Office of the Chief Financial Officer, Performance Analysis and Evaluation Branch, reviewing the information based on historical trends.

Performance Measure	Number of significant Homeland Security Investigation cases that resulted in a disruption or dismantlement
Program	Homeland Security Investigations
Description	This measure reports on the total cumulative number of significant transnational criminal investigations that resulted in a disruption or dismantlement. To be considered significant, the investigation must involve a high-threat transnational criminal organization engaged in criminal activity related to illicit trade, travel, or finance (both drug-related or non-drug-related); counter-terrorism; national security; worksite enforcement; gangs; or child exploitation. "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.
Scope of Data	The population includes validated records from all significant transnational criminal investigations involving a high-threat transnational criminal organization engaged in criminal activity related to illicit trade, travel, or finance (both drug-related or non-drug-related); counter-terrorism; national security; worksite enforcement; gangs; or child exploitation entered in the Investigative Case Management IT system, and accepted into the Significant Case Review (SCR) process based on predetermined criteria. SCRs consist of three types of submissions: an initial significant investigation, a disruption, and a dismantlement. The scope of results includes cases that resulted in a disruption or a dismantlement of high-threat transnational criminal organizations engaged in criminal activity related to illicit trade, travel, or finance (drug or non-drug-related); counter-terrorism; national security; worksite enforcement; gangs; or child exploitation.
Data Source	Data is entered in the SCR module located in the Investigative Case Management (ICM) system. ICM serves as HSI’s core law enforcement case-management tool. ICM enables program personnel to create an electronic case file that organizes and links all records and documents associated with an investigation, and to record investigative hours. ICM is the official system of record used to initiate cases, identify case categories, and record and report substantive case information during the investigative process, capturing arrest, indictment, conviction, and case closure. Management of the SCR program resides with the Domestic Operations Division located at ICE/HSI Headquarters (HQ).
Data Collection Methodology	A Special Agent (SA) identifies an investigation meeting the criteria as an initial significant investigation and completes and submits the Domestic Operations SCR worksheet through his/her chain of command. Once approved by a Domestic Operations Program Manager, the SA enters the SCR in ICM. Cases are confirmed as significant by an HQ Program Manager, the field-based Group Supervisor, and the Special Agent in Charge. An independent team at HQ and an SCR panel review the cases and verify they meet criteria for a significant, disruption, or dismantlement designation which is recorded in ICM. HSI analysts at HQ extract and aggregate data from ICM. Analysts count the total number of disruptions and dismantlements of high-threat transnational criminal organizations engaged in criminal activity approved through SCR during the reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	The SCR is reviewed by the SA’s Group Supervisor and the Special Agent in Charge (SAC). Once the SAC has approved the submission, an HQ panel meets monthly and reviews the SCR. The HQ panel makes a recommendation to the Assistant Director (AD) for Domestic Operations. The final decision on approval lies with the AD. The same data reliability check is used for disruptions and dismantlements, as HSI SAs submit enforcement actions meet the criteria for either a disruption or dismantlement. ICE also conducts quality control verification on all data received through ICM to ensure performance data are accurate, complete, and unbiased.

ICE

Performance Measure	Number of significant national-security and counter-proliferation investigations that resulted in a disruption or dismantlement
Program	Homeland Security Investigations

Description	This measure reports on the cumulative number of significant national security and counter proliferation investigations resulting in a disruption or dismantlement. These include investigations of designees in the Terrorist Identities Datamart Environment; individual watch-listed subjects in the Terrorist Screening Database; investigations related to the proliferation of weapons of mass destruction and other threats to the national security, foreign policy or economy. It also includes investigations of Level One Human Rights Violators, subjects violating the Immigration and Nationality Act, and/or malicious actors engaged in the unlawful procurement of weapons and/or controlled technologies. 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.
Scope of Data	The scope of this measure includes cases that were determined by the Significant Case Review (SCR) process to be a disruption or a dismantlement of high-threat transnational criminal organizations engaged in criminal activity. This criminal activity relates to national security and counter proliferation investigations.
Data Source	Data sources include the: Terrorist Identities Datamart Environment (TIDE) managed by the National Counterterrorism Center; Federal Bureau of Investigation’s Terrorist Screening Database (TSDB); the US government’s Watchlist database containing sensitive national security and law enforcement information; Human rights violators and war criminals tracked by the Human Rights Violators and War Crimes Unit who support investigating HSI offices; Treasury’s Office of Foreign Assets Control (OFAC) list on economic and trade sanctions. Investigation data is entered in the SCR module located in ICE’s Investigative Case Management (ICM) system. ICM is the official system of record and is used to initiate cases, identify case categories, and record and report substantive case information during the investigative process, ultimately capturing arrest, indictment, conviction, and case closure. Management of the SCR program resides with the Domestic Operations Division located at HSI Headquarters.
Data Collection Methodology	A Special Agent identifies an investigation as meeting the criteria as an initial significant investigation and completes and submits the Domestic Operations SCR worksheet through his/her chain of command based on predetermined criteria. The SCR is reviewed by the Special Agent’s Group Supervisor and the Special Agent in Charge (SAC). Once the SAC has approved the submission, the case is accepted into the SCR process and the Special Agent enters it into the ICM. Cases are then confirmed as significant by a Headquarters Program Manager. An independent team at Headquarters and an SCR panel review the cases and determine whether a disruption or dismantlement occurred and this is recorded in the ICM. HSI analysts at Headquarters extract and aggregate data from ICM. Analysts count the number of disruptions and dismantlements from national security and counter-proliferation investigations approved through SCR and add this number to the cumulative total for the fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	The review by the by the Special Agent’s Group Supervisor and the SAC provide the initial data reliability check for this data. Confirmation by Headquarters that the case is a significant case is another reliability check. A third reliability check is conducted when the results produced by analysts are reviewed by leadership in HSI. Budget Formulation and Reporting Unit analysts also conduct quality control verification on all data received through ICM to ensure performance data are accurate, complete, and unbiased. The last reliability check is conducted by the

	Office of the Chief Financial Officer, Performance Analysis and Evaluation Branch, reviewing the information based on historical trends.

Performance Measure	Number of significant non-drug-related illicit trade, travel, and finance investigations that resulted in a disruption or dismantlement
Program	Homeland Security Investigations
Description	This measure reports the total number of significant non-drug-related illicit trade, travel, and finance investigations that resulted in a disruption or dismantlement. Qualifying cases must comprise one of the following: High-threat non-drug-related investigations with repeated exploitation or evasion of global, regional, and national-level movement systems; investigations of Top International Criminal Organization Targets, Extraterritorial Criminal Travel Force cases combatting transnational noncitizen smuggling organizations; cases of human smuggling, human trafficking, counterfeit and dangerous goods, the illicit export of weapons, foreign or domestic public corruption, or benefit/document fraud. "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.
Scope of Data	The scope of this measure includes cases that were determined by the Significant Case Review (SCR) process to be a disruption or a dismantlement of high-threat transnational criminal organizations engaged in criminal activity. This criminal activity relates to non-drug-related illicit trade, travel, or finance.
Data Source	Data is entered in the SCR module located in the Investigative Case Management (ICM) system. ICM serves as Homeland Security Investigations' (HSI) core law enforcement case-management tool. ICM enables program personnel to create an electronic case file that organizes and links all records and documents associated with an investigation, and to record investigative hours. ICM is the official system of record used to initiate cases, identify case categories, and record and report substantive case information during the investigative process, capturing arrest, indictment, conviction, and case closure. Management of the SCR program resides with the Domestic Operations Division within HSI.
Data Collection Methodology	A Special Agent identifies an investigation as meeting the criteria as an initial significant investigation and completes and submits the Domestic Operations SCR worksheet through his/her chain of command based on predetermined criteria. The SCR is reviewed by the Special Agent's Group Supervisor and the Special Agent in Charge (SAC). Once the SAC has approved the submission, the case is accepted into the SCR process and the Special Agent enters it into the ICM. Cases are then confirmed as significant by a Headquarters Program Manager. An independent team at Headquarters and an SCR panel review the cases and determine whether a disruption or dismantlement occurred and this is recorded in the ICM. HSI analysts at Headquarters extract and aggregate data from ICM. Analysts count the number of disruptions and dismantlements from non-drug-related illicit trade, travel, and finance investigations approved through SCR and add this number to the cumulative total for the fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	The review by the by the Special Agent's Group Supervisor and the SAC provide the initial data reliability check for this data. Confirmation by Headquarters that the case is a significant case is another reliability check. A third reliability check is conducted when the results produced by analysts are reviewed by leadership in HSI. Budget Formulation and Reporting Unit analysts also conduct quality control verification on all data received through ICM to ensure performance data are accurate, complete, and unbiased. The last reliability check is conducted by the

	Office of the Chief Financial Officer, Performance Analysis and Evaluation Branch, reviewing the information based on historical trends.

Performance Measure	Number of significant transnational gang investigations that resulted in a disruption or dismantlement
Program	Homeland Security Investigations
Description	This measure reports on the number of significant transnational gang investigations resulting in the disruption or dismantlement of high-threat transnational criminal gangs. These investigations include gang activity as defined by the Racketeering Influenced Corrupt Organization (RICO) and/or the Violent Crime in Aid of Racketeering (VICAR) or similar statutes. "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.
Scope of Data	The scope of this measure includes cases that were determined by the Significant Case Review (SCR) process to be a disruption or a dismantlement of high-threat transnational criminal organizations engaged in criminal activity. This criminal activity relates to high-threat transnational criminal gang activity as defined by the Racketeering Influenced Corrupt Organization (RICO) and/or the Violent Crime in Aid of Racketeering (VICAR) or similar statutes.
Data Source	Data is entered in the SCR module located in the Investigative Case Management (ICM) system. ICM serves as Homeland Security Investigations' (HSI) core law enforcement case-management tool. ICM enables program personnel to create an electronic case file that organizes and links all records and documents associated with an investigation, and to record investigative hours. ICM is the official system of record used to initiate cases, identify case categories, and record and report substantive case information during the investigative process, capturing arrest, indictment, conviction, and case closure. Management of the SCR program resides with the Domestic Operations Division within HSI.
Data Collection Methodology	A Special Agent identifies an investigation as meeting the criteria as an initial significant investigation and completes and submits the Domestic Operations SCR worksheet through his/her chain of command based on predetermined criteria. The SCR is reviewed by the Special Agent's Group Supervisor and the Special Agent in Charge (SAC). Once the SAC has approved the submission, the case is accepted into the SCR process and the Special Agent enters it into the ICM. Cases are then confirmed as significant by a Headquarters Program Manager. An independent team at Headquarters and an SCR panel review the cases and determine whether a disruption or dismantlement occurred and this is recorded in the ICM. HSI analysts at Headquarters extract and aggregate data from ICM. Analysts count the number of disruptions and dismantlements from high-threat transnational criminal gang investigations approved through SCR and add this number to the cumulative total for the fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	The review by the by the Special Agent's Group Supervisor and the SAC provide the initial data reliability check for this data. Confirmation by Headquarters that the case is a significant case is another reliability check. A third reliability check is conducted when the results produced by analysts are reviewed by leadership in HSI. Budget Formulation and Reporting Unit analysts also conduct quality control verification on all data received through ICM to ensure performance data are accurate, complete, and unbiased. The last reliability check is conducted by the Office of the Chief Financial Officer, Performance Analysis and Evaluation Branch, reviewing the information based on historical trends.

Performance Measure	Percent of employee or contractor non-criminal misconduct cases closed within 120 business days (New Measure)
Program	Office of Professional Responsibility
Description	This measure gauges the ability to fully investigate and complete a non-criminal misconduct investigation on an employee or contractor within 120 days of assignment to the Office of Professional Responsibility (OPR). Allegations are initially assessed to determine whether they are retained by OPR to be investigated as serious employee or contractor misconduct, or transferred to an ICE program office for investigation. Non-criminal investigations retained by OPR will be completed within 120 days from the date the case is assigned to OPR.
Scope of Data	The population includes all allegations made against ICE employees and contractors as either: 1) retained by DHS OIG for investigation; 2) retained by OPR as a criminal investigation (no timeline for criminal investigations); 3) retained by OPR to be investigated as administrative misconduct (with a 120-day deadline); 4) referred to the program office as a Management Inquiry for allegations involving less serious misconduct; or 4) referred to the ICE component to review/address, as deemed appropriate. The unit of analysis for this measure are cases retained by OPR (#3). The attribute that makes the case counted in the result is whether the case was closed within 120 days. If the subject retires or is removed from service, the case will be closed and excluded from the numerator.
Data Source	Data is derived from the OPR Joint Integrity Case Management System (JICMS), a case management system utilized by ICE and U.S. Customs and Border Protection (CBP) to capture allegations of criminal and administrative misconduct. ICE uses JICMS to document reports of investigation, arrests, convictions, investigative steps, investigative hours, and disciplinary findings associated with an investigation. The INV PRD displays the total number of administrative completed cases and whether or not they exceed the 120-day standard by referencing the JICMS data column titled “Days (ACD to Close).”
Data Collection Methodology	Allegations are entered into JICMS based on reports received telephonically or written (email, fax, etc.) via the Joint Intake Center (JIC) or OPR field offices. DHS OIG retains a first right of refusal on allegations involving an ICE employee or contractor. If DHS OIG declines to investigate an allegation, the case is routed to the appropriate Special Agent in Charge office for review/assessment. Based on the review/assessment, the case is either assigned to the OPR field office for investigation or transferred to the ICE program office for investigation. The result is calculated by total number of administrative cases retained by OPR that are completed within 120 days (specified in the “Administrative Timeliness” column) divided by the total number of administrative completed cases. Data is cumulative from the start of the fiscal year to the end of the reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data pulled monthly for this measure is quality controlled through a review by leadership within OPR’s Investigative Division.

Performance Measure	Percent of personnel security cases completed within 10 days (New Measure)
Program	Office of Professional Responsibility
Description	This measure gauges the ability to review and assess employment suitability/fitness criteria and make preliminary risk-based determinations that allow applicants to enter on duty prior to the completion of their full background investigation. The 10-day determination window begins once the applicant completes all required security forms (e.g., completed SF-86, fingerprint cards, releases, etc.) and ends when an Entry on Duty risk-based decision is made by a

	personnel security adjudicator. If derogatory information is discovered during preliminary checks, those cases are excluded from the data set because applicants will be given ample time to respond to interrogatories.
Scope of Data	The population consists of new employees and contractors that were selected for positions with ICE. The unit of analysis is a single Entry on Duty risk-based decision made by a personnel security adjudicator on an applicant. The attribute that makes the data eligible to be included in the results is whether the determination was made within the 10-day window. If derogatory information is discovered during preliminary checks, those cases are excluded from the data set because applicants will be given ample time to respond to interrogatories.
Data Source	Data Source is the DHS Integrated Security Management System (ISMS) database. The database houses all personnel security files and has the applicable fields necessary to measure the requirement. Data is uploaded to the share drive via the PSU Weekly Snapshot and pulled directly into Tableau, where it is visualized on the Performance Metrics tab of the OPR PSU Performance Reporting Dashboard (PRD).
Data Collection Methodology	The start date of the 10-day window begins when Personnel Security Assistant (PSA) receives all required security documents from an applicant (i.e., completed SF-86, fingerprint cards, releases, etc.). The PSA enters the date in the "Final Paperwork Received" field of ISMS. The case is then assigned to a Personnel Security Specialist (PSS) and if no derogatory information is found from the security documents and internal computerized checks, the PSS completes a favorable entry on duty (EOD) determination, which allows applicants to start work while the background investigation gets completed. When the case is completed, the completion date is automatically generated. PSU is then able to run reports to determine the percentage of applicants, who have no actionable issues, that were competed within the 10-day timeframe out of the total applicants that submitted security documents.
Reliability Index	Reliable
Explanation of Data Reliability Check	All security documents are received electronically and therefore have dates when the documents arrived. When the last document is received, that date is inputted as "Final Paperwork Received." This is a mandatory field within ISMS and the case cannot be closed without having this date. When the case is completed, the date is automatically generated and posted to the completed date field. Reports are then generated, which can exclude those cases with identified derogatory issues, leaving only those that are the measurable data.

Performance Measure	Percent of semi-annual detention inspections completed (New Measure)
Program	Office of Professional Responsibility
Description	This measure quantifies the legal statute to fully inspect each ICE Detention facility semiannually. Detention facilities (State and Local, Contracted, Federal) that house undocumented detainees for periods in excess of 72 hours and that have an average daily population (ADP) of 10 or more detainees must be inspected twice each year. These inspections performed by the Office of Detention Oversight assess compliance with the ICE National Detention Standards 2000 or 2019, the Performance-Based National Detention Standards 2008 or 2011, or the Family Residential Standards 2020.
Scope of Data	The population consists of all ICE detention facilities (State and Local, Contracted, Federal) that house undocumented detainees for periods in excess of 72 hours and that have an average daily population of 10 or more detainees. The unit of analysis is a single detention facility. The attribute that makes the facility included in the result is whether the inspection was "completed (e.g., a final inspections report has been published and disseminated to the respective ERO

	field office and other agency and department stakeholders). There are instances in which a facility is only inspected one time during a FY, (e.g., a new facility is added mid-FY and is only inspected once) and these instances are handled on a case-by case basis. These facilities are still included in the results.
Data Source	Data Source is OPR's Office of Detention Oversight, which maintains a count of detention facilities inspected. Completed inspections are only counted once a final inspections report has been published.
Data Collection Methodology	The ODO inspection team lead concludes each inspection with an exit briefing in which the team lead briefs facility and Enforcement and Removal Operations (ERO) leadership on the inspection team's preliminary findings and submits a preliminary report to his/her section chief for review. The section chief reviews the preliminary report and once approved, disseminates the preliminary report to the respective ERO field office and other agency and department stakeholders. Within 60 days after inspection, a final report is generated and disseminated to the respective ERO field office and other agency and department stakeholders -- counted as "inspected." The count of Detention Facility Inspections is divided by double Total Count of Active Detention Facilities with an ADP greater than or equal to 10. A facility may only be inspected one time during a FY on a case-by case basis (e.g., a new facility added mid-FY and is only inspected once) but these are included in the total count.
Reliability Index	Reliable
Explanation of Data Reliability Check	Each Detention Facility is inspected by a team consisting of one or more federal inspectors and four or more contractor subject matter experts. Once a facility has completed the inspection, a report is published and signed off by the ODO Unit Chief formalizing that the inspection has been completed. Once a specific inspection has been completed it is added to the total tabulation of facilities inspected by ODO personnel and validated/matched to the total number of inspection reports for reliability.

Performance Measure	Number of stakeholder engagements related to the DHS civil immigration enforcement and removal priorities (New Measure)
Program	Office of the Principal Legal Advisor
Description	This measure captures all formal stakeholder engagements regarding implementation of the Interim Guidance to OPLA Attorneys Regarding Civil Immigration Enforcement and Removal Policies and Priorities, and any superseding guidance that may be issued related to civil immigration enforcement priorities. Field Locations and Headquarters Divisions schedule formal engagements with stakeholder to ensure these enforcement priorities and expectations for the pursuit of justice and efficient progress of immigration court litigation are understood by affected parties.
Scope of Data	The population includes all formal scheduled stakeholder engagements regarding current enforcement priorities and exercises of discretion during the fiscal year from all OPLA Field Locations and Headquarters Divisions. The unit of analysis is a single stakeholder engagement. The attribute that determines whether the engagement is counted is if the engagement was regarding DHS enforcement priorities and exercises of discretion.
Data Source	The data will be submitted by OPLA Chief Counsel at Field Locations and Headquarters Managers via a spreadsheet located on an internal OPLA SharePoint site. OPLA Chief Counsel and Headquarters Managers will be directed to begin reporting the occurrence of stakeholder engagements regarding current enforcement priorities and exercises of discretion.
Data Collection Methodology	Chief Counsel and Headquarters Managers will be required as part of their performance work plans to report data via a spreadsheet on the OPLA

	SharePoint site. The Chief of the Strategic Management Division will consolidate and report the data cumulatively, from the beginning of the fiscal year until the end of each reporting cycle to determine the total number of engagements and exercises of discretion.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data collected is reviewed quarterly by the Chief of the Strategic Management Division for consolidation and reporting.

Performance Measure	Percent of final administrative orders that result in orders of removal from the United States (Retired Measure)
Program	Office of the Principal Legal Advisor
Description	This measure indicates the percent of total final administrative orders secured by Office of Principal Legal Advisor (OPLA) attorneys that result in removal of those found to be in the United States in violation of the Immigration and Nationality Act (INA). 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 violation of the INA.
Scope of Data	The scope of data will consist of all immigration cases with a final administrative order date (Final Orders are orders where neither party has reserved appeal), including both Immigration Judge and Board of Immigration Appeals (BIA) decisions, occurring during the given reporting period.
Data Source	The data is collected from OPLA attorneys and support personnel and stored in the Principal Legal Advisor's Network (PLAnet) PLAnet is OPLA's case management system that documents and tracks litigation before the Executive Office for Immigration Review (EOIR), advice and guidance provided to ICE's clients, agency taskings, and administrative work performed by ICE's attorney and support personnel. Data stored in PLAnet is input manually and is not verified against the Dept. of Justice EOIR databases. PLAnet is not intended to be a statistical tool. The Office of the Chief Information Officer manages the PLAnet system located at Headquarters. The data retrieved for this measure is only based on what is collected within the PLAnet system, no external system or database are used.
Data Collection Methodology	OPLA Knowledge Management Division analysts export the data directly from PLAnet into Excel to calculate the percent of final administrative orders that result in removal. The following data collection methodology is used for this measure: 1) Obtain all final orders from PLAnet; 2) If the Immigration Judge (IJ) issues an order and there are no subsequent activity, it is included in the final order count; 3) If the IJ issues an order and the case is continuing (meaning that there are hearings, etc. that occur after the date of that order), then we do not count the case as a final order; 4) If the IJ issues an order that is appealed, and the BIA issues a different final order, then we count the BIA's order as final; and 5) If the IJ issues an order, and the BIA upholds the order, then we use the IJ order along with the date it was issued to determine if it should be included in that quarterly report. Based on this information the percent is calculated.
Reliability Index	Reliable
Explanation of Data Reliability Check	OPLA's Knowledge Management Division statisticians review and confirm the accuracy of the data presented on a quarterly basis. For quality control purposes, statisticians independently process and analyze the data using the defined criteria of the request. Upon completion, the statisticians compare results to ensure consistency. If the results differ, i.e. an error is found, the statisticians review the criteria used to derive the statistical results to confirm accuracy of the measure. Once the accuracy of the criteria has been confirmed, the statisticians individually re-run the analysis to determine whether the same results are

	obtained as a method of measuring the validity and reliability of the data output. If the results differ after re-running the analysis, the statisticians review the criteria and the data to determine the reason for the differing results and come to a consensus on the correct criteria to apply.

Performance Measure	Percent of removal orders secured that support current enforcement priorities (New Measure)
Program	Office of the Principal Legal Advisor
Description	This measure gauges progress in implementing the Interim Guidance to OPLA Attorneys Regarding Civil Immigration Enforcement and Removal Policies and Priorities, and any superseding guidance that may be issued related to civil immigration enforcement priorities by measuring the percentage of total final administrative removal orders secured by OPLA attorneys for those noncitizens found to be in the United States in violation of the Immigration and Nationality Act (INA) that support current enforcement priorities. Final Orders are orders where neither party has reserved appeal, an appeal is not timely filed, or the appeal is dismissed), including both Immigration Judge and Board of Immigration Appeals (BIA) decisions, occurring during the given reporting period. 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 violation of the INA.
Scope of Data	The population consists of all immigration cases with a final administrative removal order (Final Orders are orders where neither party has reserved appeal, an appeal is not timely filed, or the appeal is dismissed), including both Immigration Judge and Board of Immigration Appeals (BIA) decisions, occurring during the given reporting period. The unit of analysis is a single final administrative removal order. The attribute that makes the order eligible to be reported in the result is whether the case met the DHS enforcement priorities.
Data Source	The population consists of all immigration cases with a final administrative removal order (Final Orders are orders where neither party has reserved appeal, an appeal is not timely filed, or the appeal is dismissed), including both Immigration Judge and Board of Immigration Appeals (BIA) decisions, occurring during the given reporting period. The unit of analysis is a single final administrative removal order. The attribute that makes the order eligible to be reported in the result is whether the case met the DHS enforcement priorities.
Data Collection Methodology	Knowledge Management Division analysts export data directly from the PLAnet Sync database and use SQL to identify the final removal orders supporting current enforcement priorities based on: 1) If the Immigration Judge (IJ) issues a removal order and there is no subsequent activity, it is included; 2) If the IJ issues an order and the case is continuing (meaning that there are hearings, etc. that occur after the date of that order), then OPLA does not count the case as a final order; 3) If the IJ issues an order that is appealed, and the BIA issues a different final order, then OPLA counts the BIA's order as final; and 4) If the IJ issues an order, and the BIA upholds the order, OPLA counts the IJ's order as final. Those final administrative orders are assessed through PLAnet data to determine whether they support current enforcement priorities. The percent is calculated by dividing the total that meet the priority criteria divided by the total number of final removal orders.
Reliability Index	Reliable
Explanation of Data Reliability Check	OPLA's Knowledge Management Division statisticians review and confirm the accuracy of the data presented on a quarterly basis. For quality control purposes, statisticians independently process and analyze the data using the defined criteria of the request. Upon completion, the statisticians compare results to

	ensure consistency. If the results differ, i.e., an error is found, the statisticians review the criteria used to derive the statistical results to confirm accuracy of the measure. Once the accuracy of the criteria has been confirmed, the statisticians individually re-run the analysis to determine whether the same results are obtained as a method of measuring the validity and reliability of the data output. If the results differ after re-running the analysis, the statisticians review the criteria and the data to determine the reason for the differing results and come to a consensus on the correct criteria to apply.

Office of Intelligence and Analysis

Performance Measure	Number of finished intelligence products shared with the intelligence community
Program	Analysis and Operations
Description	This measure reflects the DHS contribution of finished intelligence products to the intelligence community and the federal government so as to share the unique information obtained from intelligence officers in the field.
Scope of Data	The scope reflects all raw, unevaluated intelligence (e.g. intelligence information reports, open source information reports, etc.) that is tagged with relevant priority codes and is available to the entire Intelligence Community (numerator) out of the population of all Office of Intelligence and Analysis intelligence information reports that are tagged with the relevant priority codes (denominator).
Data Source	Official federal intelligence repository, the Library of National Intelligence.
Data Collection Methodology	Intelligence officers assigned to headquarters or in the field gather information through their interactions with sources or other assigned duties and then prepare reports that are considered to be raw, unevaluated intelligence. These reports are cataloged and tagged to priorities as they are entered into various dissemination systems, including the Library of National Intelligence. There is significant training and a review process before reports are made permanent in any system. Once made permanent, the reports 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. The number of unique intelligence reports disseminated using DHS raw data is then divided by the total number of raw intelligence reports disseminated.
Reliability Index	Reliable
Explanation of Data Reliability Check	The repositories are designated as the official repositories for the collection of reports across the Intelligence Community and the data are reviewed at least monthly for completeness and accuracy by the Office of Intelligence and Analysis Enterprise Performance and Evaluation Branch and operational analysts. If inaccurate data is reported, processes are in place to adjudicate any issues and correct the record to ensure accuracy

Performance Measure	Percent of finished intelligence products aligned to key intelligence questions
Program	Analysis and Operations
Description	This measure evaluates the extent to which finished intelligence products address Key Intelligence Questions aligned to customer requirements identified in the Program of Analysis. The Program of Analysis is organized around thematic responsibilities and ensures alignment of prioritized planned analytic efforts to customer requirements. Key Intelligence Questions are developed by the intelligence Mission Centers in partnership with the Intelligence Enterprise

	following a Homeland Security Intelligence Priorities Framework process that identifies the most pressing topics for the enterprise. All analytic products must include appropriate metadata tagging, including Homeland Security priority code and alignment against Program of Analysis Key Intelligence Questions. Prioritizing intelligence products around key analytic questions promotes transparency, reduces duplication of effort, and increases the value to customer.
Scope of Data	The population for this measure is based on all finished intelligence products. The numerator includes a subset of finished intelligence products that are aligned to Key Intelligence Questions. A finished intelligence product is a product of analytical judgement applied to address an intelligence question where the analytic conclusions have been drafted, reviewed, and disseminated outside of IA. Key Intelligence Questions are identified and periodically reviewed/ updated in the Program of Analysis.
Data Source	Analysts store their initial 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 appropriate metadata tagging, including Homeland Security priority code and alignment against Program of Analysis Key Intelligence Questions.
Data Collection Methodology	Analysts begin work by initiating a project, tracking its flow through the SARA system, which captures the necessary data and metadata to analyze alignment to identified Key Intelligence Questions. Once the analyst completes their analysis and produces a report of conclusions, it then moves through the work flow to leadership review for analytic tradecraft which validates judgements contained in the report of conclusions. If approved, the report then considered a finished intelligence product, and is disseminated outside the organization depending on classification level. The results for this measure are determined by dividing the number of finished intelligence products aligned to a Program of Analysis Key Intelligence Question by the total number of finished intelligence products.
Reliability Index	Reliable
Explanation of Data Reliability Check	The finished intelligence product information and the numbers themselves are validated monthly by the Performance Measurement and Evaluation and Production staff to ensure completeness and accuracy of the data and metadata in Helix. The information in this check may be cross-referenced with SARA to ensure its accuracy. The number of products aligned to Program of Analysis Key Intelligence Questions and the total number of products are consistently reviewed by senior leadership. If potential errors have been identified in this reliability check, corrections are made to the metadata element in the repository. In the event of differences of opinion, an adjudication process exists to resolve discrepancies over the determination of information that are determined by IA senior leadership.

Performance Measure	Percent of finished intelligence products incorporating DHS and/or state and local originated data
Program	Analysis and Operations
Description	This measure gauges the impact that DHS provides to the intelligence community through disseminated finished intelligence products harnessing DHS and state, local, tribal, and territorial (SLTT) data that is unique. A finished intelligence product 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. Intelligence source data may initiate with DHS or in a partnership with other agencies. The measure highlights the impact of the Department's unique contributions to the intelligence community by demonstrating the value of 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	All analytical products must contain a source citation per Intelligence Community Directive 206 in the report. The scope of the measure reflects the finished intelligence products that source unique intelligence information from DHS or SLTTP partners. The population includes all finished intelligence products. Finished intelligence 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 the finished analytical products and reports are stored in an internal system named HELIX. All analytic products must include sources and metadata associated with those sources.
Data Collection Methodology	Analysts begin work by initiating a project, tracking its flow through the SARA system, which captures the necessary data and metadata to analyze the source information. All analytical products must contain a source citation per Intelligence Community Directive 206 in the report. Analysts also capture the source citations and whether or not a particular DHS source was used. Once the analyst completes their analysis and produces a report of conclusions, it then moves through the work flow to leadership review for analytic tradecraft which validates judgements contained in the report. If approved, the report is then considered a finished intelligence product, and is disseminated outside the organization depending on classification level. The results for this measure are determined by dividing the total number of finished intelligence products into the number that contains DHS originated data.
Reliability Index	Reliable
Explanation of Data Reliability Check	The finished intelligence product information and the numbers themselves are validated monthly by the Enterprise Performance and Evaluation Branch and Production staff to ensure completeness and accuracy of the data and metadata in Helix. The information in this check may be cross-referenced with SARA to ensure its accuracy. The numbers of both DHS and SLTT originated data report and the total number of products are consistently reviewed by senior leadership. If potential errors have been identified in this reliability check, corrections are made to the metadata element in the repository. In the event of differences of opinion, an adjudication process exists to resolve discrepancies over the determination of information that are determined by I&A senior leadership.

Performance Measure	Percent of finished intelligence products shared with state, local, tribal, territorial, and private sector partners
Program	Analysis and Operations
Description	This measure reflects the percent of Office of Intelligence and Analysis (IA’s) finished intelligence production that is considered compliant with Intelligence Community Directive (ICD) 203, and which is shared with its State, Local, Tribal, Territorial, and Private Sector partners. A finished intelligence product is a product of analytical judgement applied to address an intelligence question where the analytic conclusions have been drafted, reviewed, and disseminated outside of IA. This measure ensures that IA is leveraging its unique information sharing role by sharing finished intelligence products with State, Local, Tribal, Territorial, and Private Sector partners.
Scope of Data	The scope reflects finished intelligence products that are considered compliant with Intelligence Community Directive (ICD) 203, and which are shared with State, Local, Tribal, Territorial, and Private Sector partners (numerator) as a

	percent of the total number of ICD 203-compliant finished intelligence products. IA finished intelligence products that are ICD 203-compliant constitute a smaller subset of IA's finished intelligence production, including products, Homeland Intelligence Todays, Intelligence Assessments, and Field Analysis Reports. IA employs a formal review process to verify compliance; reporting restricted to this compliance is predicated by the Office of the Director of National Intelligence's role as IA's funding source.
Data Source	Finished intelligence products are stored in an internal system named HELIX, and entered into various dissemination systems, including the Homeland Security Information Network (HSIN). HSIN is the trusted DHS Information Sharing Environment, and allows trusted partners access to information via controlled community of interest portals (e.g., intelligence, critical infrastructure, and etc).
Data Collection Methodology	Analysts initiate a project and track its flow through the System for Analytic Review and Approval (SARA) system. Once the analyst produces a report of conclusions, it then moves through the work flow to leadership review for analytic tradecraft, validating judgements contained in the product. If approved, the report is then considered a finished intelligence product compliant with Intelligence Directive 203. Finished intelligence products are disseminated outside the organization depending on classification level, and available to properly cleared State, Local, Tribal, Territorial, and Private Sector (SLTT) partners. The results for this measure are determined by dividing the number of finished intelligence products that are compliant with ICD 203 and shared with SLTTP partners by the total number of finished intelligence production, which includes products, Homeland Intelligence Todays, Intelligence Assessments, and Field Analysis Reports.
Reliability Index	Reliable
Explanation of Data Reliability Check	IA employs a formal review process to verify the data for this measure. Data in the SARA and HELIX systems are reviewed at least monthly for completeness and accuracy by the Office of Intelligence and Analysis Enterprise Performance and Evaluation Branch, as well as operational analysts. 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 finished intelligence products shared with the Intelligence Community
Program	Analysis and Operations
Description	This measure reflects the percent of Office of Intelligence and Analysis (IA's) finished intelligence products that are considered compliant with Intelligence Community Directive (ICD) 203, and which are shared with the Intelligence Community. A finished intelligence product is a product of analytical judgement applied to address an intelligence question where the analytic conclusions have been drafted, reviewed, and disseminated. ICD 203-compliant products constitute a smaller subset of finished intelligence production that includes Homeland Intelligence Todays, Intelligence Assessments, and Field Analysis Reports. Providing finished intelligence products equips the Homeland Security Enterprise with the timely intelligence and information it needs to keep the homeland safe, secure, and resilient.
Scope of Data	The scope is finished intelligence production that is considered compliant with Intelligence Community Directive (ICD) 203, and which is shared with the Intelligence Community (numerator) as a percent of the total number of IA's ICD 203-compliant finished intelligence production (denominator). IA finished intelligence products that are ICD 203-compliant constitute a smaller subset of IA's finished intelligence production that includes products, Homeland Intelligence Todays, Intelligence Assessments, and Field Analysis Reports.

Data Source	Finished intelligence products are stored in an internal system named HELIX, and entered into various dissemination systems, including the official federal intelligence repository, the Library of National Intelligence. This is the same system used by the rest of the Intelligence Community to access all intelligence reporting.
Data Collection Methodology	Analysts initiate and track projects through the System for Analytic Review and Approval (SARA) system. Once the analyst produces a report of conclusions, it then moves through the work flow to leadership review for analytic tradecraft which validates judgements contained in the product. If approved, the report is then considered a finished intelligence product compliant with Intelligence Directive 203. Finished intelligence products are disseminated outside the organization depending on classification level. The results for this measure are determined by dividing the number of finished intelligence products that are compliant with ICD 203 and shared with the Intelligence Community divided by the total number of finished intelligence production, which includes products, Homeland Intelligence Todays, Intelligence Assessments, and Field Analysis Reports.
Reliability Index	Reliable
Explanation of Data Reliability Check	IA employs a formal review process to verify the data for this measure. Data in the SARA and HELIX systems are reviewed at least monthly for completeness and accuracy by the Office of Intelligence and Analysis Enterprise Performance and Evaluation Branch, as well as operational analysts. 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 reports rated satisfactory and useful by customers
Program	Analysis and Operations
Description	This measure gauges the extent to which finished intelligence products are satisfying customers’ needs. An intelligence report is a product of analytical judgement applied to address an intelligence question produced by DHS or through partnerships with other agencies where the analytic conclusions have been drafted, reviewed, and disseminated to customers. Responses of "very satisfied" and "somewhat satisfied" are considered to have met the criteria for "satisfactory and useful.” Providing intelligence on topics of concern equips the Homeland Security Enterprise with the timely intelligence and information it needs to keep the homeland safe, secure, and resilient.
Scope of Data	The population of this measure is all customer feedback received from surveys appended to each IA intelligence report. The customer feedback surveys contain a standard question intended to elicit the degree of customer satisfaction with the usefulness of the intelligence report. The question asks customers to rate satisfaction on a five-point rating scale (very satisfied, somewhat satisfied, neither satisfied nor dissatisfied, somewhat dissatisfied, very dissatisfied). Responses of "very satisfied" and "somewhat satisfied" will be considered to have met the criteria for "satisfactory and useful” and are included in the scope of this measure.
Data Source	The data sources for this performance measure will be the Enterprise Performance and Evaluation Branch (EPE) Dashboards located on the unclassified and high-side networks, as well as the unclassified EPE SharePoint site. Note that analysts initiate and track projects 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.
Data Collection Methodology	Once the analyst produces a report, it moves to leadership review, which validates judgements contained in the report. Approved reports are

	disseminated outside the organization depending on classification level. Interactive customer feedback surveys are appended to each intelligence report. Customers enter their responses to the surveys and click a "Submit Feedback" button that automatically generates an email on the appropriate network. The feedback is automatically ingested from the email responses and fed into the dashboards on SharePoint, to include an automated file transfer and consolidation to the high-side. The results for this measure are determined by dividing the total number of those responding they are "very satisfied" or "somewhat satisfied" by the total number of survey responses received.
Reliability Index	Reliable
Explanation of Data Reliability Check	EPE verifies the successful ingest of feedback at least weekly and ensures the removal of any redundant entries through rigorous data cleansing and direct customer follow-up, where necessary. Satisfaction and usefulness metrics are consistently reviewed by senior leadership. If potential errors have been identified in this reliability check, corrections are made to the dashboards and SharePoint site. In the event of differences of opinion, an adjudication process exists to resolve discrepancies over the determination of information that are determined by IA senior leadership.

Office of Operations Coordination

Performance Measure	Percent of Department of Homeland Security Component Emergency Response Group personnel ready to initiate continuity of essential functions and services in the event of a catastrophic disaster
Program	Analysis and Operations
Description	This measure assesses the percent of DHS Component Emergency Response Group (ERG) personnel ready to respond immediately to a continuity event. This measure encompasses select DHS Component ERG personnel that respond to the Department's weekly ERG notification tests and real-world incidents within four hours. This measure directly supports the Department's ability to continue performing DHS Primary Mission Essential Functions (PMEFs). Failure of the select personnel to respond within the 4-hour timeframe would adversely impact the Department's ability to implement continuity operations and continue performing its PMEFs during and after a continuity event. PMEFs are defined by Presidential Policy Directive 40 and Federal Continuity Directive 1 as functions that must be continuously performed to support or implement the uninterrupted performance of the National Essential Functions.
Scope of Data	This measure includes the notification via the Emergency Notification System of select DHS Component ERG personnel. There are over 1200 ERG personnel DHS wide that are tested weekly. ERG personnel are given 4 hours to respond to the test.
Data Source	Data is generated via the Emergency Notification System, an automated tool that compiles real-time responses from Emergency Response Group personnel and provides a consolidated DHS response.
Data Collection Methodology	The Emergency Notification System program team provides this data to the Office of Operations Coordination. The data is compiled from the actual responses from ERG members at the conclusion of the four-hour test timeframe each week. The Office of Operations Coordination (OPS) Continuity Division maintains a record of ERG results on all completed tests throughout the year. The measure reflects the percent of ERG personnel who respond within 4 hours of the notification being released divided by the total number of ERG individuals

	that were notified. The data is collected weekly, reported to OPS leadership, maintained in a database and stored electronically in multiple locations. Quarterly and annual reports are also generated.
Reliability Index	Reliable
Explanation of Data Reliability Check	The Office of Operations Coordination Continuity Division personnel review the data and brief OPS leadership on a weekly basis. Additionally, OPS' reviews the data, coordinates, and ensures accuracy with DHS Components where necessary through the monthly DHS Continuity Working Group.

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 database 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 database 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 three ways; either during the National Special Events Data Call (NSEDC) period, as late NSEDC submissions, 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, by December 31 for late NSEDC submissions, or within 3 business days for submitted short-notice events.
Data Source	The National Special Events Database on 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 National Special Events Database on the Homeland Security Information Network Special Events Working Group Community of Interest (HSIN SWEG COI). Once an event is submitted to the Database, the date of submission establishes the start time for the assessment (if the submission is incomplete or requires contributor followup, the date of receiving the complete entry is the start time). The new event is then adjudicated with the proper SEAR rating by the Special Events Program; and approved in the Database. The date the event is approved in the Database 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. The SEP has a team of full time program analysts responsible for event database management.

Science and Technology Directorate

Performance Measure	Number of SAFETY Act transition (new, highly innovative) technologies awarded (Retired Measure)
Program	Acquisition and Operations Analysis
Description	In order to stay up to date with the continually changing nature of terrorism, the Office of SAFETY (Support Anti-Terrorism by Fostering Effective Technologies) Act Implementation (OSAI) will seek out those evolving technologies that can serve a homeland security mission and provide coverage to enable their transition into the commercial market, at a rate of 20 percent a year. A "transition" technology is defined as any technology that is awarded Developmental Testing and Evaluation (DTE) Designation, or those that can be considered new and innovative (i.e. a new technological application in the homeland security arena).

	These technologies are actively sought out to address the ever-changing nature of terrorism. The SAFETY attempts to help industry transition these developmental technologies into the commercial marketplace.
Scope of Data	The population of data includes the total number of complete SAFETY Act applications received by the Science and Technology Directorate for liability protection of a technology or service that is a new entrant into the homeland security arena and that is emerging from a developmental status toward widespread commercial availability. A "transition" technology is defined as any technology that is awarded Developmental Testing and Evaluation (DTE) Designation, or those that can be considered new and innovative (i.e. a new technological application in the homeland security arena).
Data Source	The source of the data is the www.safetyact.gov website, where all full applications are stored. Applications are submitted electronically and via US mail, and those submitted in hard copy are entered into the application database when they are received. Each application is given a unique identifier and is tracked electronically.
Data Collection Methodology	The data is captured through the www.safetyact.gov website which is designed specifically for application processing and information. Once applications have been submitted, program staff review them to make sure they are complete and valid, and reviewers identify those that are "highly innovative." The program leadership makes the determination whether a technology is a transition technology, taking into consideration inputs from the technical review team. This generally occurs at the end of the evaluation when all relevant facts, including new or innovating aspects of the technology, are known. The website then "feeds" this information to the program's business process management software system, and the output of this system is a report in the form of an excel spreadsheet. The measure result is calculated by counting the cumulative total number of SAFETY Act "transition" technologies approved in a fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	Various weekly reports are generated in hard copy, which are reviewed and verified by the Program Director. The Program Director finalizes the classification of "highly innovative" technologies. OSAI Director reviews the data to ensure accuracy/consistency and submits the data to the Science and Technology's Performance Team within the Finance and Budget Division's Budget and Performance Branch. The ST Performance Team provides a third data reliability review before results are finalized and submitted to DHS.

Performance Measure	Percent of research, development, and innovation program milestones that are met, as established in the fiscal year's budget execution plan
Program	Research, Development, and Innovation
Description	This measure reflects the percent at which S&T meets its research, development, and innovation (RD&I) milestones planned for the fiscal year. A milestone is defined as a scheduled point or event in a project signifying the completion of a major deliverable or a phase of work. The research, development, and innovation (RD&I) program refers to the Program, Project, and Activity (PPA) funding area for the Science and Technology Directorate (S&T) within the DHS Common Appropriations Structure. RD&I provides state-of-the-art technology and/or solutions to meet the needs of DHS Components and the first responder community. Completing these milestones indicate satisfactory progress toward advancing technology within the Department and its stakeholders.
Scope of Data	The research, development, and innovation (RDI) program refers to the Program, Project, and Activity (PPA) funding area for the Science and Technology Directorate (ST) within the DHS Common Appropriations Structure. The scope of

	this measure are the total research, development, and innovation (RDI) milestones planned for the fiscal year from the list of milestones confirmed by program/project managers, approved by ST leadership, and submitted to the ST Performance Team for review and management. RDI includes customer-focused and output-oriented Research, Development, Test and Evaluation (RDTE) programs that balance risk, cost, impact, and time to delivery. A milestone is defined as a scheduled point or event in a project signifying the completion of a major deliverable or a phase of work. These milestones indicate satisfactory progress toward achieving long-term ST performance goals and Department-wide goals and objectives.
Data Source	The system of record is the Science and Technology Analytical Tracking System (STATS). The final list of RDI milestones planned in the fiscal year of execution is compiled outside of STATS, in an Excel file that is then imported into STATS. ST Offices are tasked through the ST Exec Sec process to submit the quarterly status of each RDI milestone planned. ST program/project managers report the quarterly status of each planned milestone. ST leadership review and verify the quarterly status and explanation of each milestone prior to submitting to the ST Performance Team for review and management. Information from STATS may be exported to an Excel file (Milestone Status Report) to assist with calculating and explaining the measure result as well as forecasting if likely or unlikely to meet the fiscal year target.
Data Collection Methodology	Prior to the budget execution of each fiscal year, ST determines milestones to be met. During the fourth quarter of each fiscal year, the ST Performance Team requests program/project managers to confirm milestones planned for budget execution of program/projects. During quarterly performance reporting data calls from the ST Performance Team, program/project managers report the status of each milestone planned for that fiscal year, which are then verified by ST leadership prior to review by the ST Performance Team. For the percent result of this measure, the total number of milestones that are met (numerator) is divided by the total number of milestones planned for the fiscal year (denominator), then multiplied by 100. This information is captured in STATS and submitted by program/project managers with the approval of ST leadership to the ST Performance Team.
Reliability Index	Reliable
Explanation of Data Reliability Check	Science and Technology (ST) leadership supervising program/project managers reviews the data submitted by program/project managers to ensure accuracy and consistency then verifies the status and explanation of milestones prior to submitting the data to the ST Performance Team. The ST Performance Team provides a third data reliability review before results are finalized and submitted to DHS.

Performance Measure	Percent of stakeholder counterdrug related requests fulfilled
Program	Research, Development, and Innovation
Description	This measure reflects the percent at which the Science and Technology Directorate (ST) fulfills requests from its stakeholders for counterdrug-related research and development program outputs and accomplishments. Stakeholder requests are information, data, or technology needs related to the detection, identification, and investigation of narcotics, such as opioids/fentanyl, and trafficking networks. Outputs and accomplishments encompass the delivery, demonstration, transfer, or transition of knowledge or technology products. Knowledge products include, but are not limited to, standards, technology assessments, test and evaluation results, training, data, and documents for decision support. Technology product is a piece of equipment, system, or

	component of a system, such as an algorithm to be embedded into a piece of software. This measure reflects the value that ST provides in delivering capabilities to meet critical needs to support and improve homeland counterdrug missions.
Scope of Data	The population of this measure includes counterdrug requests for counterdrug-related research and development program outputs and accomplishments. The value for this measure is those requests which have been completed. Stakeholders are those who submit requests from Congress, DHS Components, or others across the Homeland Security Enterprise. Requests are defined as knowledge products or technology. Knowledge products include, but are not limited to, standards, technology assessments, test and evaluation results, training, data, and documents for decision support. Technology product is a piece of equipment, system, or component of a system, such as an algorithm to be embedded into a piece of software.
Data Source	ST's Office of Mission and Capability Support (MCS) maintains an intake Excel spreadsheet for counterdrug related requests received from customers or stakeholders and accepted by ST. Requests do not include the high-level "needs" identified through the ST and Component Integrated Product Team (IPT) process but may include the "decomposed" gaps. The Excel file is accessible and edited by program/project managers in a SharePoint site managed by MCS Front Office. After the end of each quarter, the Excel file is sent to the ST Performance Team to verify and validate the quarterly results of the performance measure.
Data Collection Methodology	Throughout the fiscal year, program/project managers collect counterdrug related requests from stakeholders. An intake file is updated with request title, description, date and how received request, customer/stakeholder, and planned/anticipated program deliverable. Requests are reviewed and final adjudication (accept or defer request) is made within 30 business days and documented in writing by ST. Approved requests are given an initial planned completion date. To successfully fulfill a request, planned program outputs, including knowledge or technology products, must be delivered, demonstrated, transferred, or transitioned to the requirement owner. When a request is fulfilled, the file is updated with the date, output/deliverable, delivery method, location of output/deliverable. The total number of stakeholder requests fulfilled is divided by total number of stakeholder requests received and planned by ST to be fulfilled within the fiscal year, then multiplied by one hundred.
Reliability Index	Reliable
Explanation of Data Reliability Check	ST leadership supervising program/project managers reviews and verifies the data entered by program/project managers to ensure accuracy and consistency. The MCS Front Office reviews the measure data, result, and explanation of result prior to submitting the data to the ST Performance Team within the Finance and Budget Division's Budget and Performance Branch. The ST Performance Team provides a third data reliability review before results are finalized and submitted to DHS.

Performance Measure	Percent of technology or knowledge products transitioned to customers for planned improvements in the Homeland Security Enterprise
Program	Research, Development, and Innovation
Description	This measure reflects the percent at which the Science and Technology Directorate (S&T) meets its planned fiscal year transitions of technology or knowledge products for research and development funded programs/projects. A successful transition is the ownership and/or operation of a technology or knowledge product by a customer within the Homeland Security Enterprise. Technology product is a piece of equipment, system, or component of a system,

	such as an algorithm to be embedded into a piece of software. Knowledge products may be assessments, standards, training, or documents for decision support. The transition of technology or knowledge products reflects the value that S&T provides in delivering solutions to secure key assets, enhance operational efficiencies and effectiveness, and enable the Department and first responders to do their jobs safer, better, and smarter.
Scope of Data	The scope of this measure includes the successful transition to ownership and/or operation of a technology or knowledge product by a customer within the Homeland Security Enterprise out of the population of planned technology or knowledge products. Technology product is a tangible product in the form of a piece of equipment, system, or component of a system, such as an algorithm to be embedded into a piece of software. Knowledge product is a document containing conclusions from a study or assessment conducted by a project or service function that is delivered to a customer or released to the public. Knowledge products may be assessments, standards, training, or documents for decision support. Planned program/project milestones that are considered “transitions” start with action verbs such as “deliver,” “complete,” “transfer”, or “transition.”
Data Source	The system of record is the Science and Technology Analytical Tracking System (STATS). The final list of milestones planned, including planned transitions, for research and development (RD) funded program/projects in the fiscal year of execution is compiled outside of STATS, in an Excel file that is then imported into STATS. ST Offices are tasked through the ST Exec Sec process to submit the quarterly status of each RD milestone planned, including planned transitions. ST program/project managers report the quarterly status of each planned milestone. ST leadership review and verify the quarterly status and explanation of each milestone prior to submitting to the ST Performance Team for review and management. Information from STATS may be exported to an Excel file (Milestone Status Report) to assist with calculating and explaining the measure result as well as forecasting if likely or unlikely to meet the fiscal year target.
Data Collection Methodology	During the fourth quarter of the previous fiscal year, program/project managers submit milestones planned for research and development (RD) funded program/projects in the upcoming fiscal year; planned milestones include technology or knowledge products to be transitioned. During quarterly performance reporting data calls from the ST Performance Team, program/project managers report the status of each milestone planned for the fiscal year of execution, which are then verified by ST leadership prior to review by the ST Performance Team. For the percent result of this measure, the total number of technology products and knowledge products transitioned (numerator) is divided by the total number of technology products and knowledge products planned to be transitioned within the fiscal year (denominator), then multiplied by 100. This information is captured in STATS and submitted by program/project managers with the approval of ST leadership to the ST Performance Team.
Reliability Index	Reliable
Explanation of Data Reliability Check	ST leadership supervising program/project managers reviews the data submitted by program/project managers to ensure accuracy and consistency then verifies the status and explanation of milestones (specifically planned transitions) prior to submitting the data to the ST Performance Team. The ST Performance Team provides a third data reliability review before results are finalized and submitted to DHS.

Performance Measure	Percent of university programs milestones that are met, as established in the fiscal year's budget execution plan
Program	University Programs
Description	This measure reflects the percent of university programs milestones that meet the programmatic and technical events, accomplishments, or intermediate goals in the life of programs and projects. A milestone is defined as a scheduled point or event in a project signifying the completion of a major deliverable or a phase of work. The Office of University Programs (OUP) engages the academic community to conduct research and analysis, provides education and training to enhance homeland security capabilities, works closely with its stakeholders to identify requirements, set goals for milestones and deliverables, discuss the status of projects, and plan for the allocation of resources. The percent of milestones met reflects the programmatic and technical events, accomplishments, or intermediate goals in the life of projects and programs. These milestones indicate satisfactory progress toward achieving long-term ST performance goals and Department-wide goals and objectives.
Scope of Data	The percent of milestones met reflects the programmatic and technical events, accomplishments, or intermediate goals in the life of projects and programs for the Office of University Programs (OUP) within the Science and Technology Directorate (ST). A milestone is defined as a scheduled point or event in a project signifying the completion of a major deliverable or a phase of work. These milestones, approved by the OUP Director, indicate satisfactory progress toward achieving long-term ST performance goals and Department-wide goals and objectives. They help identify specific and established criteria for measuring incremental progress associated with long-term activities and program outcomes.
Data Source	The system of record is the Science and Technology Analytical Tracking System (STATS). The final list of OUP milestones planned in the fiscal year of execution is compiled outside of STATS, in an Excel file that is then imported into STATS. ST Offices are tasked through the ST Exec Sec process to submit the quarterly status of each RDI milestone planned. ST program/project managers report the quarterly status of each planned milestone. ST leadership review and verify the quarterly status and explanation of each milestone prior to submitting to the ST Performance Team for review and management. Information from STATS may be exported to an Excel file (Milestone Status Report) to assist with calculating and explaining the measure result as well as forecasting if likely or unlikely to meet the fiscal year target.
Data Collection Methodology	Prior to the budget execution of each fiscal year, ST determines milestones to be met. During the fourth quarter of each fiscal year, the ST Performance Team requests program/project managers to confirm milestones planned for budget execution of program/projects. Project managers update the Directorate's planning/programming milestone data on at least a quarterly basis from project status reports provided by performers that can be objectively corroborated by artifacts such as signed documents. For the percent result of this measure, the total number of milestones that are met (numerator) is divided by the total number of milestones planned for the fiscal year (denominator), then multiplied by 100. This information is captured in STATS and submitted by program/project managers with the approval of ST leadership to the ST Performance Team.
Reliability Index	Reliable
Explanation of Data Reliability Check	Science and Technology (S&T) leadership supervising program/project managers reviews the data submitted by program/project managers to ensure accuracy and consistency then verifies the status and explanation of milestones prior to submitting the data to the ST Performance Team. The ST 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 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 Traveler Redress Inquiry Program (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	The process begins when the 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 timestamp applicable to this metric doesn’t begin until all required documents are received. The process ends when 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 days an application is in pending status. Pending status is when DHS TRIP is waiting for the customer to provide required documentation. 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. For the quarterly submission, Redress program specialists review the data to ensure the report is pulling from the correct fields, that the date range is correct for the reporting quarter, and that the formula is properly formatted to calculate the average. The redress process itself include data quality assurance steps at multiple points to ensure data is input properly, that cases are assigned to components properly, and that cases are closed out properly. 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 canine teams that pass operational training assessments within 45 days of completing basic course at the Canine Training Center
Program	Aviation Screening Operations
Description	This measure gauges the effectiveness of the Canine Training Center's (CTC) basic handler program by measuring the percent of passenger screening canines (PSC) and explosive detection canines (EDC) teams that pass the Training Mission (TM) assessment at their assigned station. Basic training for PSC and EDC teams occurs at the CTC, followed by additional transition training at their respective duty locations. TMs take place approximately 45 days after canine teams' graduate from the basic Handler Courses and transitional training. Once a canine team passes a TM, they can begin working in all operational areas at their assigned station. CTC instructors train and assess PSC and EDC teams for deployment throughout the Nation's transportation system, to provide explosive detection capability, visible deterrence, and a timely and mobile response to security threats. The pass rate on TMs for PSC and EDC teams serves as an indicator of the CTC's training program success.
Scope of Data	The population includes the total number of TM assessments conducted within 45 days after EDC and PSC canine teams return to their duty stations during the year. The unit of analysis is a single TM assessment conducted 45 days after an EDC or PSC team returns to their duty stations. The attribute is whether a TM assessment is included in the result is whether a given EDC or PSC passes the TM assessment 45 days after returning to their duty station. The scope of this measure includes both PSC and EDC teams that have completed the Basic Handler Courses at the CTC and the transition training at their duty locations. Completion of the basic Handler Courses at the CTC is a pre-requisite to additional training conducted at their assigned station.
Data Source	This measure gathers data from TMs conducted by CTC training instructors (TIs) approximately 45 days after the canine team returns to their duty location. Data is stored in an asset management system and Canine Web Site (CWS) that are owned by Domestic Aviation Operations (DAO).
Data Collection Methodology	CTC Training Instructors (TIs) conduct TMs approximately 45 days after the canine teams graduate from the basic Handler Courses at their assigned station. Once the TM is complete, TIs upload the results (pass/fail) to the CWS and run a national report on the canine team's performance. The measure result calculated is the number of assessed canine teams that pass the TM divided by the total number of TMs conducted within the respective year.
Reliability Index	Reliable
Explanation of Data Reliability Check	CTC's evaluation supervisor and scheduler will verify the accuracy of the report by comparing the results, to the number of certification evaluations scheduled, resulting from TM failures. The CTC and Training Center Division leadership team will assess the report and performance on an annual basis to gauge success.

Performance Measure	Percent of checked baggage screened with Explosive Detection Systems
Program	Aviation Screening Operations
Description	The measure tracks the percentage of checked baggage screened by Explosives Detection System (EDS) equipment, and provides an indicator of the deployment and utilization of stand-alone and in-line Next Generation (NextGen) EDS, which are installed at airports to detect threats concealed within checked baggage. Checked baggage that is not screened with EDS is alternatively screened with Explosives Trace Detection units in order to meet the 100% checked baggage

	screening requirement of the Aviation and Transportation Security Act of 2001 (P.L. 107-71).
Scope of Data	The scope of this data includes the total population of bags screened at airports (meaning all bags screened) in relation to those screened using Explosives Detection Systems (EDS) equipment. Checked baggage that is not screened with EDS is alternatively screened with Explosives Trace Detection units in order to meet the 100% checked baggage screening requirement of the Aviation and Transportation Security Act of 2001 (P.L. 107-71).
Data Source	Baggage throughput numbers are retrieved from the Transportation Security Administration (TSA's) Performance Management Information System (PMIS), which includes airport level data related to screening and workforce operations. Throughput information is manually captured and input into the system every 24 hours by airport staff. Measure is calculated by determining the total checked baggage throughput for all TSA airports as compared to actual number of bags screened by EDS.
Data Collection Methodology	The calculation of this measure is the number of bags screened with EDS divided by the total number of bags screened, expressed as a percentage. This data is drawn from PMIS which gathers airport level data. Airport staff at each location input the required information every 24 hours. Data Elements: Number of Bags Screened with EDS; Total Number of Bags Screened. Calculation: (Number of Bags Screened with EDS ÷ Total Number of Bags Screened) x 100 = %.
Reliability Index	Reliable
Explanation of Data Reliability Check	PMIS verification via TSA supervisory responsibilities provide verification of data used for this measure.

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 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 Service Level Agreement (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 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 Transportation Security Officers separating with at least one year experience who selected management as the primary reason for leaving
Program	Aviation Screening Operations
Description	This measure gauges the percent of Transportation Security Officers (TSO) with at least one year of experience selected management as their primary reason when asked in the National Exit Survey their reasons for voluntarily leaving TSA. More detailed information provided from this selection of management allows respondents to indicate if they perceived that there was a lack of management skills, poor communication, and/or unfair practices occurring. Results from surveys from TSOs with less than one year of service are excluded since they

	tend to identify less controllable factors as their primary reason for leaving (i.e., personal reasons, schedule). This measure provides feedback to assist in encouraging conditions that will increase TSO retention.
Scope of Data	The unit of analysis is single National Exit Survey completed by a TSO separating after at least one year of service. The population includes the total number of National Exit Surveys completed by all TSO's with at least one year of service. Results from surveys from TSOs with less than one year of service are excluded since they tend to identify less controllable factors as their primary reason for leaving (i.e., personal reasons, schedule). The attribute for being reported in the results is whether the TSO indicated "management" as the primary reason for leaving. Response rates may be low for a variety of reasons, including the fact that exit surveys are voluntary and completed on an employee's own time.
Data Source	The measure gathers data from the National Exit Survey. The survey is available electronically through HRAccess/HCInsight. Separating employees are provided a link to the Exit Survey and answer the questions presented. Survey results are stored in the Integrated Data Warehouse and SAP Business Objects produces reports using predefined queries. These reports are available through the HRAccess tool. This tool is Human Capital's (HC) personnel action repository and is owned and managed by HC.
Data Collection Methodology	When TSOs are departing the Agency, their human resource official submits a Request for Personnel Action through HR Access and the system emails the employee a request to complete the exit clearance form and provide their contact information (email). Once the clearance form is processed, separating employees are emailed a link to complete the exit survey. Among a series of questions, respondents are asked their primary reason for leaving the organization from a predefined list of choices. To gather the data for this measure, analysts filter the survey responses based onto three questions: "What was your most recent job category?" (TSO); "How long did you work for TSA?" (more than one year); and "What was your primary reason for leaving?" (Management). The measure is calculated as the total number of TSOs who selected management as their primary reason for leaving divided by the total number of TSOs that answered the exit survey within the reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	The results of reports using predefined queries were reviewed by analysts when the procedure was first established to produce the exit survey reports. Analysts in the HC Assessment Branch confirm that the data being reported meet the criteria specified for the period covered and trend data makes sense. Reports are vetted through leadership in HC and also shared in quarterly reviews with senior TSA leadership

Performance Measure	Percent of Transportation Security Officers that achieve a first-time pass rate on the Image Interpretation Test
Program	Aviation Screening Operations
Description	This measure gauges the ability of Transportation Security Officers (TSO) to identify prohibited items such as guns, knives, and improvised explosive devices through X-ray screening during their initial test. The Image Interpretation Test (IIT) is a pass/fail test conducted in a simulated classroom environment that mimics X-ray screening of carry-on baggage at passenger checkpoints. A passing score on the test consists of two elements: 70% detection rate and no more than a 50% false alarm rate. Image interpretation is a key learning objective of TSO-Basic Training Program (TSO-BTP) and a skill required for TSOs to successfully execute the mission in an operational environment. The results of this measure support the goal to counter terrorism and threats to aviation.

Scope of Data	The population of this measure includes all students that undergo TSO-BTP and take the IIT within the designated timeframe. The IIT is a requirement for completing the TSO-BTP. It is a pass/fail test and serves as an indicator that the student is ready to move to the on-the-job training phase where he/she can apply the knowledge acquired from TSO-BTP and further improve his/her image interpretation skills. The unit of analysis is a test result for an individual student. The attribute that indicates whether it is reported in the results is whether a given student achieves a passing score consisting of two elements: 70% detection rate and no more than a 50% false alarm rate.
Data Source	This measure gathers data from the Online Learning Center (OLC), which serves as the system of record for TSO-BTP test results. The data in this report is classified SSI due to the detailed scores by TSO and airport location.
Data Collection Methodology	After completing the TSO-BTP training at the TSA academy, a training simulator is used to deliver the IIT and results are recorded in the OLC automatically. A passing test score consists of two elements: 70% detection rate and no more than a 50% false alarm rate. A member of the OLC team generates ad hoc Item Status Reports using qualifiers to identify which students passed the IIT. In the case of an OLC to IIT data load failure for a student, a Tier 2 OLC Administrator attempts to reload the test for a student. If this fails, the staff may take the IIT on a stand-alone device and the Administrator will record the score into OLC manually. The measure result calculated is total number of students that passed the IIT on their first attempt divided by the total number of students who took the IIT within the measure period.
Reliability Index	Reliable
Explanation of Data Reliability Check	Once the Item Status Report is generated by a member of the OLC team, the IIT data is validated by staff at the TSA Academy and also by program staff at headquarters. The TSA-Academy (TSA-A) Operations Team checks the IIT data to identify and correct any recording errors in OLC. The TSA-A Registrar verifies the student scores recorded against a course “Completion Report” for TSO-BTP to verify that a score was collected for each student on the first attempt. The confirmation of the Pass/Fail status by the TSA-A staff provides the data integrity to conduct reporting of IIT First time pass rates. The headquarters staff also validate the data by comparing the numbers against training plans.

Performance Measure	Percent of travelers who receive TSA Pre Check screening with a Known Traveler Number
Program	Aviation Screening Operations
Description	The measure counts the number of air travelers who received TSA Pre Check security screening based on having a Known Traveler Number (KTN) against the total number of air travelers per day that go through TSA Pre Check lanes at domestic airports due to meeting low risk protocols or otherwise being assessed at checkpoints as low-risk. Individuals enrolled in DHS Trusted Traveler Programs (i.e., TSA Pre Check, Global Entry, etc.), receive a KTN. This number indicates that they are a trusted traveler and of low risk to aviation security, further enabling TSA’s effective and efficient use of security screening resources.
Scope of Data	The results are based on available data related to all traveling passengers transiting through TSA Pre Check lanes at all Federalized airport. The portion of data collected which represents TSA Pre Check throughput only applies to the 214 airports that have TSA Pre Check lanes, and only when the TSA Pre Check lanes are in operation.
Data Source	The systems that are used to collect, report and store the data for this measure include Secure Flight systems and Security Operations systems. This includes information from TSA Pre Check Secure Flight Executive Report, the Secure Flight

	Age and Gender report, and data collected at airport checkpoints by TSA personnel. Performance Measurement Information System (PMIS) is a web-based application created in 2002 to collect TSA metrics and measures. Security Operations owns PMIS and is responsible for all system maintenance and upgrades.
Data Collection Methodology	The data used is based on daily passenger throughput information collected at TSA checkpoints through TSA checkpoint technology, as well as TSA Pre Check data compiled by Secure Flight. After data is entered into PMIS by checkpoint supervisors, managers and/or field coordination center staff, on a daily basis, it is compiled and analyzed by TSA Security Operations Performance Management staff who verify and report the results. The calculation is total number of travelers who received TSA Pre Check security screening on their trip based on having a KTN/total number of passengers within the six month and annual reporting period. The Security Operations SF Breakout Compile Report is the report used to calculate the metric.
Reliability Index	Reliable
Explanation of Data Reliability Check	Throughput is collected directly from checkpoint equipment. The numbers from each machine are recorded every hour and entered into PMIS at the end of the shift. Data entry responsibility depends on the airport—typically either the supervisor or manager of the checkpoint, or the coordination center. Airport personnel review their submissions. Submissions with entries exceeding high/low thresholds undergo mandatory review; other submissions can be reviewed as needed. There are safeguards in place, and the data is complete and reliable. Airport personnel review their submissions. Submissions with entries exceeding high/low thresholds undergo mandatory review; other submissions can be reviewed as needed. Users with the appropriate permissions are able to roll back a submission and make changes for submissions within the past 14 days. Submissions beyond 14 days can be rolled back for editing by the PMIS Help Desk support staff. Any suspect data is not included in the final calculation.

Performance Measure	Average number of international airport assessments and inspections conducted annually per inspector (Retired Measure)
Program	Other Operations and Enforcement
Description	This measure reports the average number of assessments or inspections by Transportation Security Specialists (TSSs) completed each fiscal year at international locations. Airports located outside the territorial boundaries of the U.S. or its protectorates receive on-site assessments to determine whether aeronautical authorities effectively maintain and carry out security measures to support International Civil Aviation Organization standards while TSA regulated entities get inspected to evaluate compliance with TSA regulations beyond the international standards. These entities can include aircraft operators, foreign air carriers, or repair stations. Requiring TSSs to complete a minimum number of regulatory activities assists the program to improve workforce utilization and buy down risk through consistent assessments and inspections. These assessments and inspections identify vulnerabilities and compliance with security standards with the goal of improving overall security posture.
Scope of Data	The population for this measure includes all planned assessments and inspections to be performance by TSSs, along with unexpected assessments/inspections needed due to emerging threats. The value for this measure reflects all assessments and inspections performed by TSSs at international locations. An assessment is an on-site review of a foreign airport that determines whether aeronautical authorities effectively maintain and carry out security measures to support International Civil Aviation Organization

	standards. Inspections of TSA regulated entities evaluate compliance with TSA regulations beyond the international standards. The annual work plan specifies frequencies and targets for assessments and inspections of international airports based on criteria established by Compliance.
Data Source	Data for this measure comes from the annual work plan developed by Compliance. The program uses historical information from the Performance and Results Information System (PARIS) and the Global Risk Analysis and Decision Support (GRADS) System to establish the work plan. Both systems along with the work plan are maintained and managed by the Compliance team within Security Operations.
Data Collection Methodology	The Compliance team in Security Operations extracts information from the PARIS and GRADS database associated with TSA's regulatory assessments and inspections, investigations, security incidents, and enforcement actions. They then establish the annual work plan designating frequencies and targets for assessments and inspections, which are then assigned to TSSs. Once a TSS completes an assessment or inspection, data is recorded in both PARIS and GRADS. GRADS is a tool that streamlines the assessment report writing process and strengthens the agency's data analysis capabilities of its foreign airport assessment results. Program analysts run queries to identify the airports where assessments and inspections occurred and compare it the annual work plan. The measure calculated is the number of completed assessments and inspections divided by the number of TSSs available for all regions and offices.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data reliability is ensured through a series of actions. Global Operations personnel within Security Operations conduct tracking audits and spot checks by followed by a management review and validation process by the Budget and Performance team at Headquarters.

Performance Measure	Number of international airport assessments and regulated entity inspections conducted annually (New Measure)
Program	Other Operations and Enforcement
Description	This measure identifies the total number of international assessments of all last point of departure airports to the United States and inspections of regulated entities across all international regions and offices completed in a fiscal year. An annual workplan is established for inspectors to conduct international inspections at these facilities that are subject to International Civil Aviation Organization (ICAO) Standards and Recommended Practices for international security regulations. Inspection activity is a key indicator that may be predictive of the overall security posture of an airport, air carrier, or other regulated entity. Identifying compliance with the key indicators assesses an entities' vulnerabilities and is part of an overall risk reduction process and is a strong indicator of system security.
Scope of Data	The unit of analysis is a single international last point of departure airport or regulated entity that is inspected at a given location. The population includes all international last point of departure airports and regulated entities that are subject to ICAO Standards and Recommended Practices for international security regulations. The scope of this measure includes all international inspections that are completed at regulated entities and last point of departure airports within the fiscal year.
Data Source	The data source for this measure is obtained from the Master Work plan (MWP), Performance and Results Analysis System (PARIS), and the Global Risk Analysis and Decision Support (GRADS), which serve as the official sources of data repository for Global Compliance's regulatory activities.

Data Collection Methodology	Compliance assessments and inspections are performed in accordance with an annual work plan that specifies frequencies and targets for assessments and inspections of international airports and regulated entities based on criteria established by Compliance. When inspections and assessments are completed, the results are entered into the MWP, PARIS, and GRADS which 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 international airport assessments and regulated entity inspections for all international offices.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data reliability is ensured through a series of actions. There are system record tracking audits and spot checks by HQ personnel, followed by a management review and validation process at the headquarters level.

Performance Measure	Number of security reviews conducted on high risk pipeline systems
Program	Other Operations and Enforcement
Description	This measure gauges the number of Critical Facility Pipeline Security Reviews (CFSR) and Corporate Security Pipeline Reviews (CSR) conducted at the Nation's high-risk pipelines. CSRs are conducted at corporate headquarters and include an extensive review of physical and cyber security policies and practices. CFSRs are conducted at individual pipeline facilities and assess onsite physical and cyber security measures. The onsite security reviews develop firsthand knowledge of security planning and execution of the critical pipeline systems, establish communication with key pipeline security personnel, and identify and share smart practices. As industry wide security gaps are identified through the process, the TSA Surface Division develops programs to address gaps throughout the pipeline industry. Pipeline security reviews assess and elevate the security posture of the pipeline energy transportation mode.
Scope of Data	The scope of this measure reports the number of the CSRs and CFSRs conducted out of the population of the top 200 pipeline companies and pipeline systems as determined by use of the TSA Pipeline Relative Risk Ranking Tool (PRRRT) and the list of critical facilities as reported by the pipeline owners and operators. CSRs and CFSRs are narrowed to approximately 200 systems supporting critical infrastructure throughout the nation out of approximately 3,000 pipeline operators nationwide.
Data Source	Overall results of the total CSRs and CFSRs conducted at both the headquarters and field sites are compiled in a database maintained by TSA's Surface Division.
Data Collection Methodology	CSRs and CFSRs are extensive and include assessments of many areas such as plans, security incident procedures, control measures, training, exercises and outreach. In cases where quantitative methods do not sufficiently determine the relative criticality of a given pipeline system, TSA employs qualitative methods involving subject matter experts to determine criticality of certain systems. Reviews can take a few days up to a few weeks, depending on the size of the pipeline system. Once the review is completed, the pipeline facility is briefed on the outcome. These results lead to the analysis of weak and strong areas, not only of the individual facilities, but also of the collective pipeline mode. Overall results of the total conducted at both the headquarters and field sites are compiled in a database maintained by TSA's Surface Division and reported cumulatively as an aggregate of both headquarters and field site reviews.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data for this measure is verified by TSA's Surface Division and double-checked for accuracy by analysts in the Budget and Performance Division.

Performance Measure	Percent of air carriers operating from domestic airports in compliance with standard security programs
Program	Other Operations and Enforcement
Description	This performance measure gauges the security posture of air carriers operating at domestic airports through compliance with standard security programs issued by the Transportation Security Administration (TSA). Standard Security Programs serve as the security baseline for an operator. Inspectors conduct inspections on an annual basis and can include one or more aspect of operations that an air carrier oversees such as catering, cargo acceptance and aircraft searches. Air carrier compliance to standard security programs enhances the safety of the Nation’s transportation systems and infrastructure.
Scope of Data	The scope of this measure includes all air carrier operations at domestic airports subject to TSA’s Standard Security Programs. Air carrier operations can include cargo screening, ground security coordinator responsibilities and Security Information Display Area Badging responsibilities by both domestic and international carriers. Any inspections conducted and completed that are outside of the work plan will be added in the calculation.
Data Source	Data for this measure comes from the annual work plan developed by Compliance. The program uses historical information from the Performance and Results Information System (PARIS) to establish the work plan. PARIS is a web-based database that serves as the official source repository of all information regarding performance and compliance activities results. It is maintained and managed by the Security Operations-Compliance.
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 Security Operations-Compliance. When inspections are completed, the results are entered into the Performance and Results Information System (PARIS). Performance Management Branch within Security Operations query inspection data from PARIS and conduct an analysis of regulated entities inspected, violations, and assessments to codify performance results. The result calculated for this measure is total completed inspections without standard security program violations divided by the total completed inspections for the reporting period conducted at domestic airports.
Reliability Index	Reliable
Explanation of Data Reliability Check	Program audits are conducted to ensure accuracy of information absorbed from PARIS. As part of oversight, Regional Security Inspectors (RSIs) conduct quarterly quality control reviews (QCR) of PARIS entries to ensure data reliability. Results also receive another layer of validation through the Budget and Performance Division at Headquarters.

Performance Measure	Percent of applicants for security threat assessments to whom TSA sends a response within 30 calendar days
Program	Other Operations and Enforcement
Description	This measure gauges the percent of applicants for a security threat assessment, credential, or endorsement to whom a response is sent within 30 calendar days of receiving a Security Threat Assessment (STA) application. Responses include either a notification stating the completion of an STA or a preliminary determination of ineligibility (PDI) letter, which indicates that something potentially disqualifying was discovered. The adjudication of a PDI letters that require additional information from applicants is not included in the results. Vetting programs include aviation, maritime, and surface populations such as the Alien Flight Student Program, Aviation Workers, General Aviation, Air Cargo, Hazardous Materials Threat Assessment Program, TSA PreCheck®, and the

	Transportation Worker Identification Credential (TWIC®) program. STAs ensure individuals with credentials, expedited screening, or secure access do not pose a threat to national or transportation security.
Scope of Data	The population includes all vetting program applicants from the Alien Flight Student Program, Aviation Workers, General Aviation, Air Cargo, Hazardous Materials Threat Assessment Program, TSA PreCheck®, and the Transportation Worker Identification Credential (TWIC®) program. The unit of analysis is an individual application sent by an applicant for any of the eligible vetting programs. The attribute for inclusion in the results is whether the applicant was sent a notification of approval or a PDI letter within 30 days of receiving the application. The 30-calendar day window is driven by the TWIC® regulation established by Congress.
Data Source	The vetting programs are managed by enrollment and case management applications and systems, including the Universal Enrollment Services system, Consolidated Screening Gateway, Technology Infrastructure Modernization system, Transportation Vetting System, and Vetting and Credentialing System. These systems store and report case management data that can be queried or exported to other data management applications and tools. The Enrollment Services and Vetting Programs (ESVP) and Information Technology (IT) offices are the designated owners for the respective enrollment, case management, and reporting applications and systems, with business owners and representatives from the ESVP and Intelligence and Analysis (I&A) offices.
Data Collection Methodology	Applicants apply to TSA's vetting programs via the various vetting and case management systems that ESVP manages. These systems record the calendar date applications are submitted and the credential/notification/correspondence calendar date that an initial decision is made. ESVP manages and monitors correspondence and notification dates from the respective applications and systems to determine the number of calendar days required to notify individual applications or enrollments. ESVP, IT, and I&A analysts run automated and manual queries and data exports to collect data from each system. For each application, the time between its submission and the time for initial communication of TSA's decision is calculated. These times are then combined across the various vetting application types, and ESVP divides the number of applications where TSA notified applicants of its decision within 30 calendar days by all the applications submitted.
Reliability Index	Reliable
Explanation of Data Reliability Check	ESVP maintains data validation rules and operating procedures, such as standardized requirements for the enrollment of a vetting program applicant, including specific biometric and biographic data fields and identification documentation. These rules provide reasonable assurance that TSA is performing vetting against a known identity and minimize potential data and reporting errors. Data queries and reporting are both automated and manual. ESVP produces several automated reports as well as customized reports. ESVP operates an internal and quality control framework for each STA process. Analysts and staff perform regular control assessments or techniques on components of the STA process to provide reasonable assurance that TSA achieves program objectives. Program offices regularly monitor processing times, and Congress also conducts oversight of TWIC® processing.

Performance Measure	Percent of attended interchanges of rail cars containing rail security sensitive materials transiting into or through high-threat urban areas
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 Rail Sensitive Security Material (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 Rail Sensitive Security Material (RSSM) interchanges inspected 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 and complete an inspection 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 PARIS; 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 deployments met against planned deployments for Visible Intermodal Prevention and Response Operations
Program	Other Operations and Enforcement
Description	This measure reflects the coverage by VIPR teams at prioritized locations based upon risk and assesses how well TSA is deploying its VIPR resources based on the risk levels assigned to deployment locations. The percent is determined by evaluating the deviation of actual coverage from desired coverage. VIPR operations are the deployment of any combination of TSA personnel and equipment for the purpose of enhancing the security of any mode of transportation (aviation, mass transit, highway, maritime, freight rail, and pipeline) with any of TSA's transportation security and law enforcement stakeholders which may include federal, state, tribal, or local authorities. The deployment locations within each transportation mode nationwide have been assigned a risk level based on data from the Transportation Sector Security Risk Assessment (TSSRA). TSSRA also determines the percent of deployment time for each risk level and constitutes the foundation for the risk-based deployment targets.
Scope of Data	The scope of this data includes all VIPR team deployments/operations within the U.S. and its territories.VIPR teams do not deploy internationally. VIPR operations are defined as the deployment of any combination of TSA personnel that may include Transportation Security Inspectors (TSIs), Transportation Security Officers

	(TSOs), Federal Air Marshals (FAMs), Behavioral Detection Officers (BDOs), canine teams, and equipment for the purpose of enhancing the security of any mode of transportation (aviation, mass transit, highway, maritime, freight rail, and pipeline) with any of TSA's transportation security and law enforcement stakeholders which may include federal, state, tribal, or local authorities.
Data Source	The operations data to support this measure is contained in a Joint Coordination Center (JCC) database located in the Transportation Security Operations Center (TSOC). Following deployment of a VIPR team, the VIPR team prepares an Activity Summary Report (ASR), which includes an overview of the deployment, a description of the locality where the operation occurred, and the composition of the VIPR team and other participating authorities. Data from ASRs are entered into the JCC database. The risk categorization data for deployment locations is contained in a separate database that has been developed using historical deployment data, risk knowledge center data, and input from field personnel in each area of responsibility.
Data Collection Methodology	For each VIPR operation, there is a designated TSA team lead who is responsible for preparing the ASR. TSA uses a standard ASR template for collecting and reporting data on all VIPR Operations. Following an operation, the team lead prepares the report and submits it electronically to the JCC. Once at the JCC, the data is entered into an Access database. The operation hours are tracked and calculated using the Access database. The operation hours data is combined with data extracted from the risk categorization data to calculate the measure value for each reporting period. Calculation of the measure involves determining the variation of actual value from the target value for each risk level and then aggregating the results. This aggregation is subtracted from 100% to provide the measure result, indicating what percent of the planned risk-based deployment level was achieved.
Reliability Index	Reliable
Explanation of Data Reliability Check	TSA has dedicated personnel within the JCC to coordinate and monitor operational planning and reporting of VIPR operations. These personnel review each ASR prior to its entry into the database for accuracy, thoroughness, and quality of the data. Data from the ASR is then entered into the database. Data is routinely analyzed and reviewed by TSA managers and supervisors to ensure it is entered accurately into the database. Members of the JCC also interact with field elements to ensure accurate data and reporting.

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 identified vulnerabilities at last point of departure airports addressed through stakeholder engagement and partnerships
Program	Other Operations and Enforcement
Description	This measure gauges the percent of vulnerabilities at last point departure airports (LPD) identified and then discussed through stakeholder engagements and partnerships so as to encourage resolution. An LPD country is a country with at least one port providing direct traffic to a specific destination - usually a foreign airport with direct passenger and/or cargo flights to a U.S. destination airport. Inspectors conduct the security assessments at LPDs based on International Civil Aviation Organization (ICAO) standards and identify vulnerability gaps. The program also identifies vulnerabilities beyond the ICAO requirements through inspections but has limited authority to enforce mitigation activities. Through the identification of vulnerabilities, the sharing of findings and best practices, the program works to mitigate aviation security risks and have them addressed so as to reduce vulnerabilities at foreign LPD airports.
Scope of Data	The population is any vulnerabilities identified by TSA inspectors through assessments and inspections at foreign last point departure airports (LPD) within the reporting period. An assessment is an on-site review that determines whether aeronautical authorities effectively maintain and carry out security measures to support International Civil Aviation Organization standards. Inspections evaluate compliance of aircraft operators and foreign air carriers with TSA regulations beyond the international standards. The value are those vulnerabilities discussed through stakeholder engagements and partnerships and categorized as either closed or being addressed.
Data Source	The data source is the Global Risk Analysis and Decision Support (GRADS) Vulnerability Report. It contains data pertaining to all open and reported closed vulnerabilities at foreign LPD airports, and is maintained by International Operations (IO) within Security Operations (SO).
Data Collection Methodology	The program establishes the standards for assessments and inspections based on International Civil Aviation Organization standards and TSA regulations. Inspectors then conduct on-site assessments and inspections to identify vulnerabilities which are then entered into GRADs. Once a vulnerability is identified and added into GRADS, IO tracks status updates provided by a variety of program staff who regularly engage with stakeholders. Twice a year, IO runs a report and validates that all identified vulnerabilities, both open and reported closed, have a clear description, root cause, and mitigation actions taken to address the specific vulnerability. The measure result calculated is the total number of closed and open vulnerabilities with a corrective action plan or other mitigation strategies divided by the total number of identified vulnerabilities at LPD airports within the reporting period.
Reliability Index	Reliable

Explanation of Data Reliability Check	As part of the Foreign Airport Assessment Program Standard Operating Procedures process, Global Operations 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, Desk Officers and Program Analysts are responsible for conducting validation reports and quality control reports for Global Operations senior leadership to track all identified vulnerabilities and their closure.

Performance Measure	Percent of Indirect Air Carriers found to be compliant with TSA standard security programs
Program	Other Operations and Enforcement
Description	This measure gauges the percent of Indirect Air Carriers that have at least one finding during inspection calculated against the total number of inspections conducted. An Indirect Air Carrier (IAC) is defined as any person, organization, or business within the United States national air system that does not possess a Federal Aviation Administration issued air carrier operation certificate, yet employs the services of licensed air carriers to move cargo from one destination to another. Air carriers leasing and selling space on their aircrafts provide these services to companies for the purpose of shipping items. Examples of an IAC could be a charter vendor, the postal service, or freight forwarder. Standard Security Programs provide detailed guidance to these regulated parties on how to implement regulatory requirements. Continuing education, outreach efforts, and targeting additional resources on IACs identified as noncompliant, will increase the rate of IACs in compliance.
Scope of Data	Data is the collection of Indirect Air Carriers that have at least one finding during inspection, which is calculated against the total number of inspections conducted. Similar to the time needed to conduct initial air cargo inspections, the compliance rate for IACs decreased based on the new and complex air cargo security requirements.
Data Source	Performance & Results Inspection System
Data Collection Methodology	Performance & Results Inspection System (PARIS) Calculation: [# of inspections with no findings / # of inspections]
Reliability Index	Reliable
Explanation of Data Reliability Check	All data is reported in PARIS, HQ coordinator queries the database

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 the largest mass transit, light and passenger rail, bus, and other commuter transportation agencies with security standards and practices related to critical Security Action Items (SAIs) reviewed during Baseline Assessment for Security Enhancement (BASE) assessments. BASE assessments are completed jointly by a team of Transportation Security Inspectors (TSI) and participating mass transit and passenger rail systems. They provide information on key SAIs including established written security programs and emergency management plans; background investigations of employees and contractors; security training; exercises and drills; and public awareness and preparedness campaigns. SAIs are key indicators of the overall security posture of a mass transit and passenger rail transportation system. Measuring implementation of these SAIs assesses transit vulnerabilities and is part of an overall risk reduction process.
Scope of Data	The population for this measure includes the latest ratings for every mass transit and passenger rail system with an average daily ridership of 60,000 or more evaluated by a BASE assessment during the last 20 quarters. Of the 17 SAIs included in BASE, only 5 are counted for this measure which include established written security programs and emergency management plans; background investigations of employees and contractors; security training; exercises and drills; and public awareness and preparedness campaigns. The scope of reported results are systems achieving an 'Effectively Implementing' rating based on a score of 70 or higher in each of these 5 SAIs. The measure uses the latest rating for every agency evaluated during the last 20 quarters to ensure that it's representative of the industry's security posture.
Data Source	The source of data for this measure are BASE assessments completed by a team of TSIs and transit agencies. TSIs document assessment results by manually entering the information and ratings for each SAI in the central database within the TSA computer system owned and managed by Security Operations.
Data Collection Methodology	During a BASE assessment, TSIs conduct interviews, review documents, and assign a score for each of the 17 SAIs based on the level of implementation. Only 5 key SAIs are relevant to this measure. TSIs post their BASE reports in a TSA central database. Transportation Security Specialist (TSS) within Security Operations extract data from completed BASE Assessments for all assessed agencies during the past 20 quarters. To obtain the numerator for this measure, TSS filter the data to get the number of agencies achieving an Effectively Implementing rating with a score of 70 or higher in each of the 5 key SAIs. The denominator is the total number of agencies receiving a base assessment inclusive of all ratings on the 5 key SAIs. The result is the number of mass transit and passenger rail agencies achieving an 'Effectively Implementing' rating for the 5 key SAIs divided by the total number of mass transit and passenger rail agencies rated for the past 20 quarters.
Reliability Index	Reliable
Explanation of Data Reliability Check	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. Final results for this measure are reviewed by headquarters staff prior to submission.

Performance Measure	Percent of transportation sector vetted population submissions that are matched against watch lists using the Transportation Vetting System
Program	Other Operations and Enforcement
Description	This measure indicates the percent of qualified record submissions, received from vetted transportation-sector population data providers, that are matched against existing high-risk watchlists using the Transportation Vetting System (TVS). A qualified submission contains sufficient data to allow the TVS automated vetting system to match individuals against existing high risk watch lists. The transportation sector populations include internationally-flying aircrew; aviation, air cargo, and port workers; HAZMAT drivers; FAA certificate holders; TSA employees; Pre-Check applicants; and alien flight school students. Vetting individuals against high risk watch lists strengthens the security of the transportation system.
Scope of Data	Data is collected detailing the number of new individuals vetted and the number of individuals recurrently vetted for all functional vetting programs. TSA's total defined population receiving a Security Threat Assessment currently includes international flight crews, aviation workers, hazardous material drivers, transportation workers requiring unescorted access to secure areas of MTSA-regulated facilities and vessels, TSA Pre-Check program applicants, and all mariners holding Coast Guard-issued credentials, FAA Certificate holders, individuals involved in transporting cargo on commercial aircraft, and non - U.S. citizens receiving flight instruction at Federal Aviation Administration certified flight schools in the U.S. and abroad.
Data Source	This data source for Vetting Reports and monthly vetting and credentialing data is a secured database maintaining vetting and credentialing monthly report data and assessments.The data source is SLA_RAW_DATA table from the Service Level Agreement database.
Data Collection Methodology	Each TSA program details and reports through TSA's Management Review metrics reporting process the number of qualified records received and the number of qualified records fully processed through the Transportation Vetting System (TVS). Calculation: The percentage of qualified records vetted ttrough TVS out of the total number of records received for vetting in TVS.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data collected reports the number of individuals vetted by each program monthly, and is closely monitored by TSA's Office of Intelligence and Analysis and is reported quarterly in TSA's Management Review metrics report.

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 PARIS which are subsequently used to calculate the results for this measure. The result for this measure is reported annually and is calculated by dividing the total number of entities inspected by the total number of 'inspectable entities' 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 Visible Intermodal Prevention and Response deployments to high-throughput transportation venues during forecasted peak travel times
Program	Other Operations and Enforcement
Description	This measured indicates how often Visible Intermodal Prevention and Response (VIPR) teams deploy to high-throughput transportation venues during forecasted peak travel times. High-throughput transportation venues include Category X/1 commercial airports and large mass transit venues such as Washington D.C.'s Union Station. VIPR operations are defined as the deployment of any combination of TSA personnel that includes Federal Air Marshals (FAMs), personnel from Security Operations, and/or other transportation security and law enforcement stakeholders which may include federal, state, tribal, or local authorities. This measure gauges our deployment of law enforcement to serve as a deterrence and response force as needed to increase surface transportation security.
Scope of Data	The scope of this data includes all Visible Intermodal Prevention and Response (VIPR) team operations within the U.S. and its territories conducted at high-throughput commercial aviation and mass transit venues. VIPR operations are the deployment of Federal Air Marshals (FAMs), Security Operations personnel, and/or other federal, state, tribal, or local transportation security and law enforcement stakeholders. High-throughput transportation venues are derived from risk categorization data from the VIPR Concept of Operation and VIPR implementing instructions. Results for this measure are the VIPR operations conducted within peak travel hours determined by operational start and stop times listed in Activity Summary Reports.
Data Source	The data to support this measure is contained in a Joint Coordination Center (JCC) database located in the Transportation Security Operations Center (TSOC). Data from Activity Summary Reports (ASR) are entered into the JCC database. Forecasted peak travel times are modeled using historical traveler throughput data and information on future systemic changes to venues. Executed peak hours are determined by operational start and stop times listed in the ASR.
Data Collection Methodology	For each VIPR operation, there is a designated TSA team lead who is responsible for preparing the ASR. Prior to the deployment of a VIPR team, the VIPR team

	prepares an ASR, which includes an overview of the deployment, a description of the locality where the operation will occur, and the composition of the VIPR team and other participating authorities. TSA uses a standard ASR template for collecting and reporting data on all VIPR Operations. Prior to an operation, the team lead prepares the report and submits it electronically to the JCC. Once at the JCC, the data is entered into an MS Access database. ASR data is then combined with risk categorization data and forecasted peak time data to determine the VIPR program's percentage of risk-based deployments conducted at high-throughput transportation venues during forecasted peak travel times. The percentage is derived by the number of peak hour operations divided by all high throughput venue operations.
Reliability Index	Reliable
Explanation of Data Reliability Check	TSA has dedicated personnel within the JCC to coordinate and monitor operational planning and reporting of VIPR operations. These personnel review each ASR prior to its entry into the database for accuracy, thoroughness, and quality of the data. Data from the ASR is then entered into the database. Data is routinely analyzed and reviewed by TSA managers and supervisors to ensure it is entered accurately into the database.

U.S. Citizenship and Immigration Services

Performance Measure	Percent of workers determined to be Employment Authorized after an initial mismatch
Program	Employment Status Verification
Description	This measure reports the number of cases in which adjudicating officials in the E-Verify program find a person employment authorized under U.S. law after the program issued the person under examination with a Tentative Non-Confirmation (TNC) of eligibility for employment, and the person in question contested this initial mismatch. In cases when an employee contests an eligibility determination, the program's Legal Instrument Examiners (LIEs) make a final determination of the employee's eligibility for employment and transmits the determination both to the hiring employer and to VIS. Ensuring the accuracy of E-Verify program processing reflects the program's intent to minimize negative impacts imposed upon those entitled to employment in the U.S. while ensuring the integrity of immigration benefits by effectively detecting and preventing cases of unauthorized employment.
Scope of Data	The population of this measure includes all E-Verify cases during the reporting period in which a Tentative Non- Confirmation (i.e. 'initial mismatch') is identified. The scope of the results includes E-Verify cases in which actions following a Tentative Non-Confirmation (i.e. 'initial mismatch') result in a finding of 'Employment Authorized' for the person in question. Tentative Non-Confirmations that result in a finding of 'Not Employment Authorized' are excluded from the calculation.
Data Source	Data for this measure come from records stored in the program's Verification Information System (VIS). This system contains detailed, searchable information regarding all steps taken in resolving E-Verify cases, including whether the program issued a TNC, whether the employee contested the TNC, and the final eligibility determination.
Data Collection Methodology	In cases when an employee contests an eligibility determination, the program's Legal Instrument Examiners (LIEs) make final determination of the employee's eligibility for employment. Upon completing a final determination of eligibility,

	an LIE transmits the determination both to the hiring employer and to VIS. The program has configured VIS to produce a standard quarterly summary of case outcomes, which includes both the number of Tentative Non-Confirmations, and the subset of contested Tentative Non-Confirmations which produce a final finding of 'Employment Authorized.' The result is calculated by dividing the number of all Tentative Non-Confirmations which produce a final finding of 'Employment Authorized' by the all total number of all E-Verify cases for the reporting period as the denominator, and multiplying by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	Each quarter, the contractor managing VIS for the program extracts E-Verify transaction data from VIS. Analysts apply an algorithm to the extracted data, removing all duplicate and invalid queries. The contractor then refers data and performance results to program staff for review and clearance.

Performance Measure	Percent of fraud referrals from adjudicative directorates that are closed or converted into fraud cases within 90 calendar days (Retired Measure)
Program	Fraud Prevention and Detection
Description	This measure gauges the percent of referrals received from adjudicative officers to the Fraud Detection and National Security (FDNS) Directorate that are resolved within 90 days. Adjudication Officers may contact FDNS if they suspect fraudulent activity related to the adjudication of immigration benefits. Fraud referrals that are either declined or administratively returned to adjudications, closed as leads, converted into cases, or linked to existing cases within the time limit of the referral are included in this measure. Performance is measured as the percentage of. Referrals pending with FDNS greater than the time limit will be counted as not meeting the measurement. Ensuring prompt resolution of fraud concerns helps to safeguard the integrity of the nation's lawful immigration system while fostering timely and accurate adjudication of applications.
Scope of Data	This measure’s scope includes all fraud referrals closed or converted from adjudication offices from Field Operations (FOD), Service Center Operations (SCOPS), and Refugee, Asylum, and International Operations (RAIO) Directorates, respectively, entered into the Fraud Detection and National Security Data System (FDNS-DS) or CLAIMS 3. Those referrals declined and returned to the adjudication office; determined to have no basis for continuing the investigation; or determined to involve a reasonable suspicion of fraud exists and converted into an active fraud case are included in the numerator. All active referrals from the above offices. make up the denominator A case record with a “Resolved” flag in the FDNS-DS database or a “Resolved” HAC code in CLAIMS 3 identifies cases closed or converted. This measure does not include system generated fraud referrals or “hits” from law enforcement databases.
Data Source	Adjudicative referral dates, referral declination and administrative return dates, lead closure dates, and case linkage and conversion dates for referrals from FOD and RAIO are derived from the Fraud Detection and National Security Directorate’s system of record, FDNS-DS. Adjudicative referral dates, referral rejection dates, lead closure dates, and case linkage and conversion dates for referrals from SCOPS are derived from CLAIMS 3.
Data Collection Methodology	All fraud referrals “resolved” in the current fiscal year are included. The adjudicative referral date is subtracted from the date of the resolution to derive the total number of days. Adjudication Officers (AOs) vet potential fraud issues with their Supervisors. When supervisors concur with AOs with regard to creating a referral to FDNS, AOs enter a referral in FDNS-DS or CLAIMS3. Subsequently, FDNS officers enter the status of resolved cases in FDNS-DS or update the CLAIMS3 HAC code corresponding to resolution in CLAIMS3. FDNS Statisticians

	conduct a query from FDNS-DS and CLAIMS3 using SAS a statistical analysis software package, to extract data on all referrals closed or converted during the reporting period. SAS is also used to calculate the duration in working days of the time to close or convert referrals. The number of all referrals resolved within 90 days is the numerator and the total number of all referrals resolved for the reporting period is the denominator.
Reliability Index	Reliable
Explanation of Data Reliability Check	FDNS-DS supervisors review the SAS query results to ensure that records to ensure that they contained correct information at the time of closure. Analysts in The Office of the Chief Financial Officer checks performance results for internal leadership reviews and before posting data to the DHS Performance System.

Performance Measure	Percent of Immigration Services Officers, Asylum Officers, and Refugee Officers who receive advanced fraud detection or interview skills enhancement training (Retired Measure)
Program	Fraud Prevention and Detection
Description	This measure reports the overall percent of Immigration Services Officers, Adjudicators, and Asylum and Refugee Officers, including supervisors, who received advanced fraud detection training or training through online courses or instructor-led classes to enhance their interviewing skills. Advanced training and interviewing training is provided to adjudicators who have taken basic fraud detection and interviewing courses to enable them to stay abreast of trends in fraudulent applications. Officers receive advanced training to improve their ability to detect fraudulent applications and/or assess the completeness and truthfulness of responses from applicants when conducting interviews related to applications for immigration benefits. Increasing the officer's ability to detect fraud helps mitigate the risk of applicants receiving fraudulent benefits.
Scope of Data	The scope includes all mandatory advanced fraud and advanced interviewing courses for adjudication staff as defined by Series 1801 (General Inspection and Investigative Enforcement) and 0930 (Hearings and Appeals) delivered via online modules or instructor-led classes for all officers who adjudicate requests for immigration benefits. Basic fraud detection and interviewing techniques training are excluded from the scope of this measure. Employees that separate from adjudication officer positions during the fiscal year are excluded from the measure's denominator.
Data Source	The Table of Organization Position System (TOPS) system contains the information on employees in relevant adjudication positions. The Performance and Learning Management System (PALMS) contains the records of employee completion of online training modules. For initial implementation, Directorate offices can maintain electronic records of attendees of in-person classroom training locally or can record the classroom attendance in PALMS. By the end of FY 2020, all data used for confirming online training completion and classroom attendance will be recorded in the agency Learning Management System (LMS), as required by USCIS Management Directive (MD) 258-006. The Advanced Fraud Detection and Interviewing Training report owned by the Human Capital Directorate will contain the consolidated data for reporting.
Data Collection Methodology	Human Capital and Training (HCT) analysts will query TOPS to determine the total number of employees that are still assigned to relevant adjudication positions during the reporting period. Program offices & Directorates having Series 1801 and 0930 staff who are not responsible for adjudicating requests for immigration benefits will confirm removal of these employees from the TOPS report. HCT analysts will query PALMS to determine the number of completed advanced fraud and interview courses taken in PALMS. Directorates' Training Officers will

	consolidate all instructor-led classroom training on advanced fraud and interviewing into a spreadsheet/report and provide this data to the Human Capital Division who will consolidate the PALMS training data with the Directorate information into the Advanced Fraud Detection and Interviewing Training Report. The consolidated PALMS and Directorate training is the numerator and the TOPS query provides the denominator for this measure.
Reliability Index	Reliable
Explanation of Data Reliability Check	Supervisory HR Analysts validate exclusion of data for basic fraud and interviewing courses prior to submitting the Report to the Office of the Chief Financial Officer (OCFO). OCFO completes subsequent checks of the data during each reporting period, prior to an internal review meeting and before posting data to the Future Years Homeland Security Program System (FYHSP).

Performance Measure	Percent of system generated notifications related to national security, public safety, or fraud triaged on pending cases within 60 calendar days
Program	Fraud Prevention and Detection
Description	This measure gauges the timely resolution of system generated notifications (SGNs) related to national security, public safety, or fraud for immigration benefits in cases pending a decision to approve or deny immigration benefits. SGNs provide continuous vetting capabilities to alert FDNS to investigate potential issues of concern. Program Officers may resolve the notification by determining that there is no basis for continuing the investigation or that a basis exists which warrants the opening of a fraud, public safety, or national security case in the Fraud Detection and National Security Data System (FDNS-DS). Continuous vetting of information helps safeguard the integrity of the nation's lawful immigration system.
Scope of Data	This measure's scope includes most ATLAS system SGNs that are triaged during the fiscal year within 60 calendar days of their creation in FDNS-DS in cases pending a decision to approve or deny immigration benefits. Scope excludes SGNs that pertain to a form type of I-589 (Application for Asylum and for Withholding of Removal) or I-590 (Registration for Classification as Refugee) or forms received in a Refugee, Asylum, and International Operations (RAIO) location. The scope also excludes referrals generated from other sources.
Data Source	Fraud Detection and National Security (FDNS) Reports and Analysis Branch (RAB) uses the SAS system to extract data from FDNS-DS, FDNS' system of record, to report the data. The system generated notices (SGNs) originate from ATLAS, a screening functionality incorporated into FDNS-DS. Records of SGNs reside in a different segment of FDNS-DS. Analysts may identify resolved SGNs in FDNS-DS by searching for records with active identifier flags. Information available in FDNS-DS includes each SGN; the status--pending or complete--of all benefits decisions linked to each SGN; and time stamps for the receipt and disposition of each SGN.
Data Collection Methodology	System generated biometric notifications (SGNs) issued from law enforcement databases require Immigration Officers to record their actions in FDNS-DS. FDNS Statisticians use SAS to conduct a query from FDNS-DS on the date of all SGNs during the reporting period and the date of their resolution. Staff compile reports using SAS--a statistical analysis software package--to extract data from FDNS-DS for all SGNs resolved during the reporting period. Staff use SAS to calculate duration, in working days, of the period from receipt of each SGN to its disposition by FDNS. The number of all in-scope SGNs triaged within 60 or fewer calendar days for disposition in a given reporting period provides the numerator. The total number of all relevant SGNs in a given reporting period is the

	denominator. The percentage of these two quantities is the result for the reporting period and is cumulative throughout the fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	The programs used to calculate the measures are quality checked before implementation by an independent FDNS RAB staff member or contractor. Additionally, as end users also monitor the data, they are likely to identify any potential data issues that can be corrected as they arise, if necessary. Additionally, supervisors in FDNS review the data to ensure exclusion of post-adjudicative forms from this measure's data. The Office of the Chief Financial Officer checks results per reporting period for internal leadership review meetings and before posting data to the DHS Performance System.

Performance Measure	Accuracy rate of USCIS's processing of manual verifications for Systematic Alien Verification for Entitlements referrals
Program	Immigration Services
Description	This measure tracks the accuracy of manual verifications conducted for the Systematic Alien Verification for Entitlements (SAVE) program. A SAVE verification involves federal, state, tribal, or local government agency which grants licenses or benefits verifying an applicant's immigration status. If SAVE cannot match an applicant's data to a database record from U.S. Government systems used to adjudicate immigration benefits in the initial search, customer agencies pursue further verification if requested by the applicant. Status Verifiers (SV) perform these additional queries manually to determine the applicant's immigration status. SAVE referrals are sampled monthly to verify the work provided by SV correctly reflects the immigration status on record for persons seeking benefits from other Government agencies. Conducting accurate SAVE verifications ensures that federally funded benefits are awarded correctly to non-citizen applicants and recipients.
Scope of Data	The scope of this measure's results includes manual 'second step' and 'third step' queries by SV's that are verified as correct from a sample out of the total population of second and third step manual queries. Each month, the program assembles a random sample of completed SAVE manual referrals consisting of second step or third step cases at a sample sized to achieve a confidence level of 95 percent.
Data Source	SAVE draws from U.S. Government systems used to adjudicate immigration benefits. Records from SAVE verifications stored in the program's Status Verification System (SVS) provides all data required for the SVO Quarterly Quality Review Report, used to produce the result for this measure, including designators for second step verifications and third step verifications, as well as the final outcome of each verification.
Data Collection Methodology	SVs conduct manual queries on second and third step referrals and enter data on verifications in the SVS. Quality Assurance analysts select sample sizes based on expected monthly volumes for each audit and historical data to achieve the desired 95 percent confidence interval. Analysts then construct a random sample of completed cases from the SVS database and forward it to SVs for re-verification. Analysts report results to the Quality Assurance (QA) section for analysis, then share results with supervisors. Program and QA staff confer about the results, and then draft a consensus summary of findings.
Reliability Index	Reliable
Explanation of Data Reliability Check	QA staff conduct secondary review and vetting of data and results to ensure the accuracy of the findings. Program staff also review findings with supervisors from the appropriate unit to ensure accurate reporting. Immigration Records and

	Identity Services' (IRIS) Verification Division reports results to the program's OCFO, through IRIS's front office.

Performance Measure	Number of asylum determinations (New Measure)
Program	Immigration Services
Description	This measure gauges the total number of asylum determinations to approve, deny, refer to an Immigration Judge, or administratively close cases related to refugee and asylum. Individuals physically present in the U.S. may apply for asylum, regardless of their country of nationality or current immigration status, if they were persecuted or have a fear that they will be persecuted because of their race, nationality, religion, membership in a particular social group, or political opinion. The processing of asylum determinations advances the objective to adjudicate protection, humanitarian, and other immigration benefits.
Scope of Data	The population includes all applications for asylum received within entire population of all available case data (no sampling). The unit of analysis is a single application for asylum. The attribute that makes an application eligible to be counted in the result is whether the Asylum Officer made a determination to approve, deny, refer to an Immigration Judge, or administratively close the case.
Data Source	The source for data is the Global case management system. Data is extracted from Global and analyzed in the Standard, Measurement, and Analysis, Reporting Tool (SMART) environment using consolidated in reports (in Excel or pdf format) using a web-based reporting tool.
Data Collection Methodology	The data begins with the receipt of a case, interview request and scheduling, and ends with the delivery of the Asylum Officer's determination. When a determination is made, the decision is recorded as an approval, denial, administrative close, or referral in Global. The data is exported from Global and analyzed in the Standard, Measurement, and Analysis, Reporting Tool (SMART) environment using the codes for these types of transactions. Historical information and data is collected using data collection and gathering techniques, filters, and sorting. Data is collected from the beginning of the fiscal year through the end of the most current reporting cycle to determine the cumulative number of asylum determinations made.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data reliability checks consist of supervisory controls and checks, reviewing, sampling, verification, the use of Standard Operating Procedures, and Quality Assurance reviews and analysis. Checks are conducted randomly and systematically, and scheduled and unscheduled. Data reliability reviews are also integrated as controls within most processes. Refugee and Asylum program managers double-check the data reported each quarter to ensure accurate results.

Performance Measure	Percent of actionable refugee interviews conducted (New Measure)
Program	Immigration Services
Description	This measure assesses the progress in conducting refugee interviews needed to feed the pipeline of individuals eligible for refugee admission to the US. Interview results are used to verify identity and make eligibility recommendations to immigration officers that inform adjudication decisions on refugee applications. Refugee interviews are considered actionable if there are no external factors preventing officers from interviewing cases presented by the Department of State, Bureau of Population, Refugees, and Migration (PRM). The main purpose of the refugee interview is to elicit and provide information related to eligibility

	for refugee status. Each interview may involve multiple individuals connected to a single refugee case.
Scope of Data	The Population is the total number of refugee interviews presented by PRM. The unit of analysis is a single actionable refugee interview conducted in person (face to face) or those completed via Video Teleconferencing (VTEL). A refugee interview is considered actionable if there are no external factors preventing officers from interviewing a when officers arrive at an interview location. Examples of external factors include the inability to secure visas or country clearance for officers to travel to a processing location, the security situation in a processing location preventing officers from travelling to perform interviews, or the inability to supply sufficient cases ready for interview when officers have travelled to a processing location. The attribute that makes a refugee interview eligible to be included in the results is that it was an actionable interview that was actually conducted.
Data Source	The total number of actionable interviews will be pulled from two case management systems: Global, a USCIS case management system, and the Department of State’s Worldwide Refugee Admissions Processing System (WRAPS). WRAPS data is available through a Tableau data source that IRAD has access to. Global interview data is accessed through Databricks and Tableau and can be blended with the WRAPS data. All interview data will be available from just Global by the end of fiscal year 2022.
Data Collection Methodology	PRM requests a refugee interview and the request is logged in the WRAPS or Global system. When the officer completes the interview, the completion is entered in the system. If the interview is not completed due to external factors, it is tracked in the system by checking a box. USCIS analysts run queries from Global and/or WRAPS to extract the total number of actionable interviews and how many actionable interviews are actually conducted. The total number of actionable interviews actually conducted are divided by the total number of actionable interviews to get a final percentage.
Reliability Index	Reliable
Explanation of Data Reliability Check	Supervisors regularly review the queries of Global and/or WRAPS to ensure accuracy and consistency before data is reported. In addition, this data, the required calculations, and trend analysis will be checked by analysts to ensure reliability of the data.

Performance Measure	Percent of applications for immigration benefits digitally processed via the Electronic Immigration System (Retired Measure)
Program	Immigration Services
Description	This measure gauges the degree to which immigration applications, petitions, and other requests are fully digitally processed through the Electronic Immigration System (ELIS). ELIS is a digital platform of services providing program staff all of the digital products and tools needed to complete case processing and adjudicative tasks. ELIS offers end-to-end digital case processing, supporting digital ingestion (data and images) of applications, petitions, and other requests filed through both the e-filing (online) and paper (Lockbox) intake channels. ELIS also enables streamlined digital processing of task-based workflow; systematic data harvesting automated workload distribution; on-demand and automated background checks; case examination and disposition; tablet-based interviewing and exams; and production of benefits. Digital processing through ELIS reduces case processing times, improves adjudication rates, increases data quality, and enhances the customer experience.
Scope of Data	The population of this measure is the case workload digitally processed through the ELIS platform, and includes all applications, petitions, and other requests--

	known as 'forms', referred to as 'cases', 'filings', or 'receipts'. The scope is 'closed' cases that are approved, denied, or withdrawn. ELIS digitally ingests filings (data and images) from both the e-filing and paper intake (Lockbox) channels: Regardless of intake channel, ELIS digitally processes all filings received, from the point of ingestion through closure for those forms that have been brought into the ELIS digital environment.
Data Source	The National Performance Report (NPR) includes total case workload data, which includes all filings received through both the e-filing and paper intake channels. The NPR draws data for the total case workload—receipts for applications, petitions, and other requests—from the Enterprise Citizenship and Immigration Services Centralized Operation Repository (eCISCOR), CLAIMS3 systems, ELIS, and the Standard Management Analysis Reporting Tool (SMART). The Office of Performance and Quality (OPQ) manages the National Performance Report (NPR), and the Office of Information Technology (OIT) manages reporting of this measure.
Data Collection Methodology	OIT analysts extract data from the NPR to gather the total number of applications, petitions, and other benefit requests the received during the reporting period. Analysts extract ELIS case workload data from the ELIS database using an automated query in SMART. Analysts enter data extracted from both the NPR and ELIS into the ELIS Receipts Processed Report to calculate the percentage of total closed cases digitally processed through the ELIS platform during a reporting period. The sum of all closed cases digitally processed in ELIS is the numerator, and the sum of the total filings is the denominator for this calculation.
Reliability Index	Reliable
Explanation of Data Reliability Check	Program analysts in the Office of Performance and Quality review the NPR to ensure its accuracy. Supervisors in the Office of Information Technology (OIT) review the query results for the ELIS Receipts Processed Report to ensure accuracy and completeness. The Office of the Chief Financial Officer (OCFO) checks performance results for internal leadership review meetings and before posting data to the Future Years Homeland Security Program System (FYHSP).

Performance Measure	Percent of approved applications for naturalization that were appropriately decided
Program	Immigration Services
Description	This measure assesses the validity of final decisions by program adjudicators to approve all electronic N-400 Naturalization Forms received through USCIS Electronic Immigration System (ELIS) by reporting the findings of regular quality reviews of these decisions by experienced subject matter experts (SMEs). The program conducts quality reviews by drawing a statistically valid random sample of approved N-400s on a quarterly basis. Insuring that the program provides immigration services accurately and with full documentary support through quality reviews identifies opportunities to improve training and business processes and enhances confidence in the legal immigration system.
Scope of Data	The scope of this measure includes all approved and oathed (sworn and signed) electronic N-400 Forms received through USCIS Electronic Immigration System (ELIS). The program conducts quality reviews of these cases, drawing a statistically valid random sample of approved N-400s on a quarterly basis. For a typical quarterly total of roughly 171,600 N-400s, the program constructs a sample of roughly 139 files, which provides accuracy with a ±5% margin of error. Quarterly reviews draw on approvals completed in the preceding quarter. Year-end results from a stratified sample, with each quarterly review providing one stratum of data.

Data Source	After creation of a quality review sample, teams of SMEs review records for each of the approved N-400s selected to complete Decisional Quality Review (DQR) checklists, with data entered into an online database. Program headquarters staff in the Office of Performance and Quality, Office of the Chief Data Officer, Data Quality Branch has access to this database. These HQ staff members maintain the information from each review and integrate it into a consolidated spreadsheet, which serves as the data source for this measure.
Data Collection Methodology	SMEs use original applicant requests to complete their quality reviews of the sample of approved N-400s, documenting their work using DQR checklists. A SME sets aside cases when the SME determines that documentation does not support the original adjudication. After the SME has reviewed all files, at least two other SMEs review flagged applications. If any of the additional reviewers question a decision, that file goes back to the original adjudicating office to resolve discrepancies. The original office must submit to a SharePoint site documented resolution of discrepancies within 10 business days. The result is calculated by dividing the number of files returned to original offices by the review's sample size, subtracting this quantity from 1 and multiplying by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	Layers of subject matter experts review and concur on correct or questionable decisions to ensure data reliability. The program obtains a valid random sample to conduct this audit, compile results, and develop corrective action plans to address any deficiencies noted.

Performance Measure	Percent of approved applications for permanent residence that were appropriately decided
Program	Immigration Services
Description	This measure assesses the validity of final decisions by program adjudicators to approve Form I-485 applications to register for permanent residence or to adjust status by reporting the findings of regular quality reviews of these decisions by experienced subject matter experts (SMEs). The program conducts quality reviews of these cases, drawing a statistically valid random sample of approved I-485s on a quarterly basis. Insuring that the program provides immigration services accurately and with full documentary support through quality reviews identifies opportunities to improve training and business processes and enhances confidence in the legal immigration system.
Scope of Data	The scope of this measure includes all I-485 Forms approved nationwide and received at the program's National Records Center. To validate the I-485, the program conducts quality reviews of such cases, drawing a statistically valid random sample of approved I-485s on a quarterly basis. For a typical quarterly total of roughly 103,600 I-485s, the program constructs a sample of roughly 139 files, which provides accuracy with a ±5% margin of error. Quarterly reviews draw on approvals completed in the preceding quarter. Year-end performance results from a stratified sample, with each quarterly review providing one stratum of data.
Data Source	After creation of a quality review sample, teams of SMEs review records for each of the approved I-485s selected to complete Decisional Quality Review (DQR) checklists, with data entered into an online database. Program headquarters staff in the Office of Performance and Quality, Office of the Chief Data Officer, Data Quality Branch has access to this database. These HQ staff members maintain the information from each review and integrate it into a consolidated spreadsheet, which serves as the data source for this measure.
Data Collection Methodology	SMEs use original applicant requests to complete their quality reviews of the sample of approved I-485s, documenting their work using DQR checklists. A SME

	sets aside cases when the SME determines that documentation does not support the original adjudication. After the SME has reviewed all files, at least two other SMEs review flagged applications. If any of the additional reviewers question a decision, that file goes back to the original adjudicating office to resolve discrepancies. The original office must submit to a SharePoint site documented resolution of discrepancies within 10 business days. The result is calculated by dividing the number of files returned to original offices by the review's sample size, subtracting this quantity from 1 and multiplying by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	Layers of subject matter experts review and concur on correct or questionable decisions to ensure data reliability. USCIS is able to obtain a valid random sample to conduct this audit, compile results, and develop corrective action plans to address noted deficiencies.

Performance Measure	Percent of approved refugee and asylum applications that were appropriately decided (Retired Measure)
Program	Immigration Services
Description	This measure assesses the ability of officers to process Form I-589 and Form I-590 refugee and asylum applications in a fully supportable and accurate manner. A panel of subject matter experts are convened to review a sample of approved applications to determine whether the final decision was appropriately supported and legally sufficient. The panel may sustain the decision to grant asylum, recommend denial, or send the file back to the appropriate field office for correction or more information if it is determined that procedures were not correctly followed, or the case is lacking sufficient interview evidence. This measure helps ascertain the accuracy of decisions and to improve the training and processes used in conducting asylum and refugee adjudications.
Scope of Data	The scope of this measure includes those Forms I-589 and I-590 which met legal sufficiency and evidence criteria among all Forms I-589 and I-590 sampled by the program to determine the accuracy rate. Cases varying from standard asylum or refugee adjudications due to adherence to a different set of legal, procedural, or administrative guidelines, as well as cases requiring urgent travel or lacking supervisory review are excluded. The confidence level for each review (90% to 95%) is set to accommodate the underlying purpose and resource requirements of each review at the given time. The sample size of total cases reviewed is the denominator for the calculation.
Data Source	Application and screening decision data are recorded and stored in RAIO case management systems, e.g. Global and CAMINO. Decisional review check sheets completed by decision reviewers are consolidated in a database. The RAIO Performance Management and Planning Program owns the final reporting database.
Data Collection Methodology	A team of subject matter experts conducts reviews of a sample of the asylum and refugee decisions, and documents these reviews using a checklist. The review team uses consensus panels, two-tiered review, or limited two-tiered review with discussion groups to analyze the appropriateness of decisions. Cases found to be inappropriately decided are returned the responsible field office for correction. Reviews are made periodically throughout the year using a sample size to reach a confidence level of 90% to 95% and the annual result is determined by aggregating these samples as the final annual sample for that year. The percentage is calculated by dividing the number of approved cases in the sample that do not require correction by changing the decision outcome by the total number of approved cases in the sample.
Reliability Index	Reliable

Explanation of Data Reliability Check	To ensure accuracy of the checklist and panel decision, multiple layers of subject matter experts review and concur on correcting applications by changing decisions to approve. The results are double-checked by supervisors before the results are submitted to Office of the Chief Financial Officer for submission. OCFO completes subsequent checks of the data during each reporting period, prior to an internal review meeting and before posting data to the Future Years Homeland Security Program System (FYHSP).

Performance Measure	Percent of eligible immigration benefit requests processed electronically end-to-end (New Measure)
Program	Immigration Services
Description	This measure gauges the degree to which immigration applications, petitions, and other eligible requests are electronically processed end to end. USCIS provides a digital platform of services used to complete intake, case management, and adjudicative tasks. Ultimately, end-to-end electronic processing reduces case processing times, improves adjudication rates, increases data quality, and enhances the customer experience. The targets for this measure also reflect the reality that USCIS will maintain a degree of paper/manual processing for those benefits that represent a very small portion of filings.
Scope of Data	The population of this measure is the case workload digitally processed through USCIS immigration systems, and includes all applications, petitions, and other requests--known as “forms”, referred to as “cases”, “filings”, or “receipts”. The scope is “closed” cases that are approved, denied, or withdrawn. USCIS digitally ingests filings (data and images) from both the e-filing and paper intake (Lockbox) channels: Regardless of intake channel, USCIS digitally processes filings received, from the point of ingestion through decision and communication to applicant.
Data Source	The National Performance Report (NPR) includes total case workload data, which includes all filings received through both the e-filing and paper intake channels. The NPR draws data for the total case workload—receipts for applications, petitions, and other requests—from the Performance Analysis System (PASEXEC). The source of the PASEXEC is the Enterprise Citizenship and Immigration Services Centralized Operation Repository (eCISCOR) which is the enterprise reporting and repository platform. NPR collects relevant data from eCISCOR. The Office of Performance and Quality (OPQ) manages the National Performance Report (NPR), and the Office of Information Technology (OIT) manages eCISCOR.
Data Collection Methodology	OIT and OPQ analysts extract data from eCISCOR to gather the total number of applications, petitions, and other benefit requests received during the reporting period using an automated query. OPQ analysts enter PASEXEC receipts data extracted from eCISCOR into the NPR to calculate the total number of applications received during a reporting period, then subtract the number of cases not processed electronically. This difference represents the total number of cases electronically processed. The sum of all cases electronically processed is the numerator, and the sum of the total filings is the denominator for this calculation. The result is the percentage of eligible applications, petitions and other requests processed electronically end-to-end.
Reliability Index	Reliable
Explanation of Data Reliability Check	Business Analysts and IT Specialists in OIT review the NPD to ensure its accuracy. OPQ Program analysts review the query results for the total number of Receipts Processed Report to ensure accuracy and completeness. The Office of the Chief Financial Officer (OCFO) checks performance results for internal leadership

	review meetings and before posting data to the OneStream Performance Management (PM) system.

Performance Measure	Percent of Immigration Officers who are trained to perform their duties within six months of entry on duty
Program	Immigration Services
Description	This measure includes Immigration Services Officers who complete BASIC training within six months of their entry on duty date. BASIC training is typically held at residential training facility. At the completion of their required BASIC training, officers are then considered certified to performance their duties. Ensuring officers are adequately trained and certified before performing their job duties protects the integrity of the immigration system.
Scope of Data	The population included in this measure are all newly hired Immigration Officers in the fiscal year. The scope for this measure is those officers who have completed the required BASIC training. The attribute that makes a unit from the population eligible to be in the scope is whether the training was completed within six months of their entry on duty date. Officers who are deferred attendance due to deferments allowed under published USCIS policy, as well as students that fail to achieve a passing grade, or withdraw will be excluded from the results.
Data Source	The data sources for training attendance records include the Basic Training Dashboard Summary spreadsheet. The Table of Organization Position System (TOPS) managed by the Human Capital Directorate will provide the data to the Entry on Duty (EOD) date and the current date.
Data Collection Methodology	Using the report data from the BASIC database, an automated excel formula computes the individual EOD to basic times and number of attendees from the start of the fiscal year until the end of the current reporting cycle. The denominator is the number of officers who have reached 6 months from their EOD date within the reporting quarter (minus deferments, failures, and withdrawals allowed under policy). The numerator is the number of officers from that group who have completed BASIC by 6 months from their EOD date. The results are calculated from the start of each fiscal year until the end of the most recent reporting period for a cumulative result.
Reliability Index	Reliable
Explanation of Data Reliability Check	USCIS HCT is responsible for validating the accuracy of the completed training reports, and the calculations made regarding how many Officers met their training requirements within six months. They also confirm that the list of Officers is accurate and those who are on deferred attendance, or failed the course, have not been included in the numbers. The Office of the Chief Financial Officer checks performance results for internal leadership review meetings and before posting data to the DHS Performance System.

Performance Measure	Percent of naturalization cases where derogatory information was identified and resolved prior to taking the oath of allegiance
Program	Immigration Services
Description	This measure gauges the rate at which derogatory information is identified and resolved before N-400 Form naturalization applicants take the final the Oath of Allegiance at a naturalization ceremony. Taking the oath at a ceremony completes the process of becoming a U.S. citizen for approved applicants. USCIS employs continual vetting of applicants and a final check for derogatory information close to the oathing ceremony to ensure that ineligible applicants are not naturalized due to criminal activity, national security, or public safety

	concerns. Continuous vetting ensures the integrity of the immigration system and protects our national security.
Scope of Data	The scope of the measure includes cases that have been 'oathed' (sworn and signed) with derogatory information identified and resolved out of the population of all N-400 Forms/cases received through USCIS' Electronic Immigration System (ELIS) with an indication of identified derogatory information. N-400 cases with no derogatory information are excluded from the calculation of this measure.
Data Source	ELIS is the system that contains all records of N-400 cases with derogatory information identified and resolved. Derogatory information is identified in ELIS by a Derogatory Information and Resolved flags. The Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR) business intelligence tool is used to extract the data for N-400 cases oathed with a derogatory information flag identified in ELIS.
Data Collection Methodology	Derogatory information identified by adjudicators or the Fraud Detection and National Security Directorate is entered in ELIS by checking a flag. Adjudicators record the resolution of this information checking a resolved flag in the ELIS system before scheduling an oathing ceremony. The USCIS Office of Performance and Quality (OPQ) will export data from eCISCOR via SAS statistical analysis software program a week following the end of the quarter to ensure all N-400 cases oathed during the reporting period with a derogatory information flag are included in the calculation. The calculation is the number of cases where derogatory information was resolved before the oathing ceremony divided by the total number of cases where there was derogatory information identified before or after oathing. Data is calculated from the beginning of the fiscal year until the end of the reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	After the results have been generated, a second OPQ data analyst will conduct a peer-review of the data to ensure completeness, reliability and accuracy. Prior to submission of the final results to OCFO, an Office of Performance and Quality manager will conduct a final quality check of the data. The Report is subsequently checked by the Office of the Chief Financial Officer during each reporting period prior to an internal review meeting and before posting data to the Future Years Homeland Security Program System (FYHSP).

Performance Measure	Percent of refugee and asylum adjudications that were legally sufficient (New Measure)
Program	Immigration Services
Description	This measure assesses the ability of officers to adjudicate asylum and refugee determinations for Forms I-589 and Form I-590 in a legally sufficient manner. An adjudication is legally sufficient if the analysis breaks down the determination that an applicant does or does not qualify for asylum or refugee status into explanations and conclusions that makes clear to the reviewer the rationale behind the final determination. A panel of subject matter experts are convened to review a sample of refugee and asylum adjudications. The panel may sustain the decision to grant, recommend denial, or send the file back to the appropriate field office for correction or more information if it is determined that procedures were not correctly followed, or the case is lacking sufficient interview evidence. This measure helps ascertain the quality of decisions and to improve the policy and procedural guidance, training, and processes used in conducting asylum and refugee adjudications.
Scope of Data	The population includes all adjudication decisions for standard cases that received supervisory review, were documented in case files, and recorded and

	stored in RAIO case management systems. Samples are pulled in sufficient quantities to reach a confidence level for each review of 90% to 95% from the population based on refugee and asylum priorities articulated by leadership such as the distribution of the countries of origin of applicants to reflect current refugee flows. Cases varying from standard asylum or refugee adjudications due to adherence to a different set of legal, procedural, or administrative guidelines, as well as cases requiring urgent travel, are typically excluded. The unit of analysis is a single adjudication decision. The attribute for it to be reported in the results is whether those determinations met legal sufficiency and evidence criteria among all adjudications sampled by the program.
Data Source	Application and screening decision data are recorded and stored in Refugee, Asylum and International Operations (RAIO) case management systems, such as the Global system. Decisional review check sheets completed by decision reviewers are consolidated in a custom database prepared for the review. The RAIO Performance Management and Planning Program owns the final reporting database.
Data Collection Methodology	A team of subject matter experts conducts reviews of a sample of the asylum and refugee decisions documented in case files and then records the results of these reviews using a checklist. The review team uses consensus panels, two-tiered review, or limited two-tiered review with discussion groups to analyze the appropriateness of decisions. Cases found to be not legally sufficient are returned the responsible field office for correction. Reviews are made periodically throughout the year using a sample size to reach a confidence level of 90% to 95% and the annual result is determined by aggregating these samples as the final annual sample for that year. The percentage is calculated by dividing the number of legally sufficient cases by the total number of cases in the sample.
Reliability Index	Reliable
Explanation of Data Reliability Check	To ensure accuracy of the checklist and panel decision, multiple layers of subject matter experts review and concur on correcting adjudications. The results are double-checked by supervisors before the results are submitted to Office of the Chief Financial Officer (OCFO) for submission. OCFO completes subsequent checks of the data during each reporting period, prior to an internal review meeting and before entry in the DHS performance reporting tool.

Performance Measure	Percent of respondents satisfied with the citizenship and immigration-related support received from the USCIS Contact Center (New Measure)
Program	Immigration Services
Description	This measure gauges the overall satisfaction of support received from the USCIS Contact Center based on accuracy of information, responsiveness to public inquiries, and accessibility to information. The Qualtrics Automated Omnichannel Survey Tool captures live feedback after customers complete their interaction with the contact center through the IVR, telephony, virtual assistant, live chat agent, myUSCIS account experience, and/or website. The survey question that pertains to this measure is: “I am satisfied with the service I received from the USCIS Contact Center,” rated on a scale of 1 to 5, with 1 being “strongly disagree” and 5 being “strongly agree”. Scores of 4 and 5 are included in the results of this measure. Providing quality customer service helps to ensure applicants receive the information they need and increases trust in the Federal government.
Scope of Data	The population includes all email surveys completed by customers distributed through the Qualtrics Automated Omnichannel Survey Tool once a Service Item is closed after the customer interaction through IVR, telephony, virtual assistant, live chat agent, myUSCIS account experience, and/or website. The customer has the ability to accept or decline the survey. The unit of analysis is an individual

	survey completed by a customer. The attribute that determines whether a survey is included in the result is whether the customer rates the question as a 4 or a 5, indicating that they agree or strongly agree with the statement "I am satisfied with the service I received from the USCIS Contact Center." Data is collected and reported for the entire fiscal year.
Data Source	Data is captured via Qualtrics a Software as a Service (SaaS) subscription basis tool. USCIS Contact Center uses the Qualtrics Automated Omnichannel Survey Tool to capture live feedback from our multichannel operations, after customers complete their interaction with the contact center through the IVR, telephony, virtual assistant, live chat agent, myUSCIS account experience, and/or website. The Qualtrics tool is integrated with the Contact Center telephony's Customer Relationship Management (CRM) tool, which provides an email survey to the customer once a Service Item is closed after the customer interaction. The data is deleted every 90 days by our vendor. No PII is used and only ANI-data (telephone number data) is scrubbed.
Data Collection Methodology	The Qualtrics Automated Omnichannel Survey Tool offers USCIS Contact Center customers the ability to provide their feedback automatically through a survey. There are seven questions asked aligned with reporting requirements for OMB A-11 for High Impact Service Providers that cover customer satisfaction across all contact center tiers. All USCIS Contact Center calls are recorded for quality assurance purposes. The survey question that pertains to this measure is: "I am satisfied with the service I received from the USCIS Contact Center." The question is rated based on a scale of 1 to 5, with 1 being "strongly disagree" and 5 being "strongly agree". Data is captured from the survey sample on a daily basis. The calculation to support the measure is a Numerator divided by a Denominator to get a percentage. The Numerator is the number of survey respondents who responded with a 4 or 5 on the satisfaction scale and the Denominator is the total number of survey respondents.
Reliability Index	Reliable
Explanation of Data Reliability Check	The survey is performed automatically by the Qualtrics survey and analyzed by Management and Program Analyst at the USCIS Contact Center. Data and reports are pulled from the Qualtrics Dashboard using standard statistical practices to ensure the appropriate level of confidence.

Performance Measure	Percent of students enrolled in civics-based English as a Second Language classes under the Citizenship and Integration Grant Program that show educational gains (New Measure)
Program	Immigration Services
Description	This measure reports on the success of grant recipients to increase knowledge of English necessary for permanent resident students receiving services under the program to pass the naturalization test. Students receive specialized civics-based English as a Second Language (ESL) training on vocabulary and grammar needed to know in order to successfully navigate the naturalization test and interview. 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 civics-based English as a second language (ESL) classes who demonstrate a one point or greater increase in score. The classes equip immigrants with the tools they need to be successful throughout their journey to become new U.S. citizens.
Scope of Data	The population includes all cumulative civics-based English language proficiency (ESL) test results for Q1-Q3 of the current fiscal year and Q4 of the prior fiscal year. This measure is reported with a one quarter lag because the source data are found in grant recipient quarterly reports are due to USCIS 30 days after the

	close of the quarter. The unit of analysis is a student that received civics-based ESL services from a grant recipient that was pre-and post-tested. The attribute of whether a student is counted in the results is a student who demonstrates a one point or greater increase in score on English language proficiency tests from the pre- to the post-test.
Data Source	The data source is the Grant Book tool owned by the USCIS/External Affairs Directorate. Grant Book is located on a USCIS-owned platform called STARS. The measure will be tracked using quarterly grant recipient performance reports submitted through Grant Book.
Data Collection Methodology	Grant recipients complete and submit quarterly reports via Grant Book on each permanent resident who receives civics-based ESL classes on the services provided, including dates of enrollment, and pre and post-test scores, within 30 days of the conclusion of each quarter. Data contained in each quarterly report is then reviewed, transferred to the SAS Enterprise server, and analyzed by Office of Citizenship program officers. Staff in the Office of Citizenship extracts the data from Grant Book, uploads to the SAS Enterprise server, and runs a query developed by USCIS SAS analysts that calculates student test results from Q4 of the prior fiscal year to the end of the current reporting cycle. The calculation is the total number of students who were pre- and post-tested and scored at least one point higher on the post-test divided by the total number of students who were pre- and post-tested through Q3 of the current fiscal year and Q4 of the prior fiscal year.
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 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 time that U.S. Citizenship and Immigration Services mission essential systems are available for service to end users
Program	Immigration Services
Description	This measure reports the percent of time in during which users in core adjudication related positions and analysts have access to critical systems needed for immigration case processing. The program designates an information technology system as a Mission Essential System (MES) based on these systems' critical role in functions supporting adjudication case processing. The program's information technology policies specify that MES must have a validated recovery not exceeding four hours. The uninterrupted availability of Mission Essential Systems enables the processing of immigration benefits.
Scope of Data	This measure's scope includes--for every information technology (IT) system designated as an MES during a particular reporting period--the web tier, application tier, data tier, and the network segment which makes the mission essential application available to the enterprise. Any failure in any of these elements which affects the performance of the mission essential system counts as an outage. Specifically, this measure's scope includes the number of minutes

	per outage for all outages reported. The measure's scope excludes authorized outages, i.e. planned and coordinated periods for system maintenance. The population of mission essential systems will change as systems migrate to the cloud or the program decommissions them.
Data Source	Program analysts draw for this measure from two key sources of data regarding detection and measurement of an MES outage. The program has licensed a commercial monitoring tool (New Relic) configured to detect anomalies in the performance of Mission Essential Services and when an outage occurs. First, the New Relic reporting tool includes automated reporting functionality, which generates outage reports aggregated in an MES Report. Direct reporting from users when disruptions in Mission Essential Systems occur provides the second source for information on MES performance and outages. The program's IT staff record users' reports of MES outages in an electronic trouble ticket. The program's Enterprise Operations Center assesses the tickets to classify the user report as a single user level, site level, or enterprise level occurrence, escalating the report for action as appropriate.
Data Collection Methodology	Program analysts measure the duration of any Mission Essential Services (MES) outage in minutes. To allow for maintenance, the program authorizes up to two four-hour outage windows for each MES each week, scheduled for low-traffic periods. The program's IT staff will determine the duration, in minutes, of an outage for each disruption of service. For each reporting period—roughly 90 days or 129,600 mins—analysts will subtract two authorized four-hour outage windows each week, roughly 5,760 minutes. Analysts will calculate the difference between total and outage minutes, producing an availability total. The result is calculated as the summed duration of all unplanned outages as the numerator, and the availability total for the reporting period as the denominator, multiplied by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	Supervisory analysts in the Office of Information Technology review the results for accuracy. In coordination with the Enterprise Operations Center, analysts in the program's Office of the Deputy Chief Information Officer resolve discrepancies between user reported data and the New Relic reporting tool. The program's Office of the Chief Financial Officer checks the MES Report during each reporting period, prior to an internal review meeting and before posting data to the Future Years Homeland Security Program System (FYHSP).

U.S. Coast Guard

Performance Measure	Fishing regulation compliance rate
Program	Maritime Law Enforcement
Description	This measure gauges the percent of all fishing vessels boarded and inspected at sea by the U.S. Coast Guard, which had no documented violations of domestic fisheries regulations. The U.S. Coast Guard boards and inspects U.S. commercial and recreational fishing vessels in the waters of the United States; U.S. commercial and recreational fishing vessels in the U.S. Exclusive Economic Zone (EEZ); and U.S. commercial and recreational fishing vessels outside the U.S. EEZ. Compliance to fishing regulations impact the health and well-being of U.S. fisheries and marine protected species.
Scope of Data	The population includes all boardings and inspections of U.S. commercial and recreational fishing vessels in the waters of the United States; U.S. commercial and recreational fishing vessels in the U.S. Exclusive Economic Zone (EEZ); and

	U.S. commercial and recreational fishing vessels outside the U.S. EEZ. The U.S. does not permit foreign vessels to fish within the U.S. EEZ. Vessels without any documented violations are reported for this measure.
Data Source	Boardings and violations of domestic fisheries regulations are documented by U.S. Coast Guard Boarding Forms and entered into the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database. The MISLE database has a specific LMR Violation Action box to facilitate identifying, sorting, and filtering vessels with violations.
Data Collection Methodology	U.S. Coast Guard units document violations of domestic fisheries regulations in U.S. Coast Guard Boarding Forms and enter them into the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database after completion of fisheries enforcement boardings. The data is extracted by a manual query in MISLE conducted by Coast Guard headquarters staff in the Office of Maritime Law Enforcement. The calculated results for a given year are the number of boarded fishing vessels with no documented violations of domestic fisheries regulations divided by the number of fishing vessels boarded and inspected at sea by the U.S. Coast Guard, multiplied by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	MISLE data consistency and integrity is controlled through program logic and pull-down menus that require key elements, prohibit the inappropriate, and limit choices to pre-determined options. Reliability is further ensured by comprehensive training and user guides, and the application itself has embedded Help screens. District, Area and Headquarters staffs review, validate and assess the data on a quarterly basis as part of the U.S. Coast Guard's Standard Operational Planning Process; and Program managers review and compare MISLE data to after-action reports, message traffic and other sources of information.

Performance Measure	Interdiction rate of foreign fishing vessels violating U.S. waters
Program	Maritime Law Enforcement
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	Maritime Law Enforcement
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 undocumented migrants who attempt to enter the U.S. via maritime routes that are interdicted
Program	Maritime Law Enforcement
Description	This measure is the total number of all undocumented migrants who are attempting to enter the U.S. by maritime means and who are interdicted by the U.S. Coast Guard and other law enforcement agencies. The other agencies include Customs and Border Protection, and foreign entities partnering with the U.S. Coast Guard for migrant interdiction operations.

Scope of Data	The measure includes migrants from all nationalities attempting direct entry by maritime means into the United States, its territories, and possessions who are interdicted by the Coast Guard.
Data Source	Data obtained from U.S. Coast Guard and Customs and Border Protection.
Data Collection Methodology	Interdiction information is obtained through the U.S. Coast Guard Marine Information for Safety and Law Enforcement (MISLE) database, and Bureau of Customs and Immigration records. Data collection is managed by the Migrant Interdiction Program Manager (CG-5313).
Reliability Index	Reliable
Explanation of Data Reliability Check	Data is actual number of migrants interdicted by the Coast Guard and other law enforcement agencies. These numbers are entered into MISLE upon completion of interdiction event or cutter patrol.

Performance Measure	Removal rate for cocaine by the U.S. Coast Guard from non-commercial vessels in maritime transit zone
Program	Maritime Law Enforcement
Description	This measure reports the amount of cocaine removed plus the estimated amount jettisoned or destroyed during interdiction efforts by the U.S. Coast Guard on non-commercial vessels based on a three-year average annual maritime flow of cocaine. Removing cocaine from non-commercial vessels helps ensure effective maritime law enforcement and border control.
Scope of Data	The measure includes the amount of cocaine physically seized by the U.S. Coast Guard from non-commercial vessels in the maritime domain, which is weighed and assigned a Federal Drug Identification Number. Also included is cocaine not physically recovered that is jettisoned or destroyed during interdiction operations, which is typically determined from pursuit video or other intelligence analysis. The amount of cocaine removed is expressed as a percentage of the 3-year average annual maritime flow of cocaine on non-commercial vessels over the previous 36-month period. Cocaine seized by other law enforcement partners and from commercial vessels is excluded from the calculation.
Data Source	Cocaine flow and removal data is from the consolidated counter-drug database (CCDB) maintained by the United States Interdiction Coordinator, Office of National Drug Control Policy. CCDB source data includes interdiction reports provided by the U.S. Coast Guard—as well as other Joint Interagency Task Force South (JIATF-S) members, intelligence reports from U.S. Coast Guard LANT and PAC Maritime Intelligence Fusion Centers, and other authoritative sources for cocaine production, trafficking and consumption information. Seizure data is tracked and verified by Federal Drug Identification Numbers.
Data Collection Methodology	U.S. Coast Guard inputs data on cocaine seized or physically recovered that is jettisoned or destroyed as determined from pursuit video or other intelligence analysis into the CCDB. Members from the Coast Guard Office of Law Enforcement quarterly meet with its partners to verify and validate the data. The numerator for this measure is the total metric tons of cocaine seized, observed or determined jettisoned or destroyed during the current 12-month period divided by the unweighted 3-year average annual maritime flow of cocaine on non-commercial vessels over the previous 36-month period.
Reliability Index	Reliable
Explanation of Data Reliability Check	Both the physically seized and jettisoned or destroyed components of this measure are tracked, collected, and analyzed by the U.S. Coast Guard Office of Maritime Law Enforcement (CG-MLE). Consolidated Counter-drug Database (CCDB) source data is verified and validated quarterly by representatives from the agencies involved in transit zone interdiction, who meet and review the data

	for each source event and resolve any discrepancies. Seizure data is also tracked and verified by Federal Drug Identification Numbers.

Performance Measure	Annual Maritime Transportation Security Act Facility compliance rate with Transportation Worker Identification Credential regulations
Program	Maritime Prevention
Description	This measure reports the percent of Maritime Transportation Security Act (MTSA) regulated facilities that are found to be in compliance with the Transportation Worker Identification Card (TWIC) regulations during CG inspections. The Security and Accountability for Every (SAFE) Port Act of 2006 requires the Coast Guard to conduct at least two MTSA security inspections on regulated facilities each year; one announced and one unannounced. CG Inspectors randomly sample different areas of a facility (admin staff, security staff, dock workers, etc.) to check for TWIC compliance by ensuring workers have a valid and current TWIC card. Some infractions can be corrected on the spot, e.g., a trucker forgot his TWIC in his truck cab. Depending on the number and severity of TWIC infractions, the inspector/Capt of the Port may find the facility not in compliance. Statistical guidelines have been developed based on the size of the facility to aid inspectors, and to ensure random sampling.
Scope of Data	Results are based on all available data. All inspections conducted at MTSA regulated facilities.
Data Source	Inspection results are collected and maintaned in the Marine Information for Safety and Law Enforcmeent (MISLE).
Data Collection Methodology	U.S. Coast Guard field inspectors enter the results of TWIC compliance during a MTSA facility inspection into the MISLE database. Headquarters level program managers will download the data from MISLE and determine the TWIC compliance rate by dividing the number of TWIC compliant facility inspection by the total number of inspections in the fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	Field level Sectors report their data to their regional Coast Guard Districts for first review, who in turn reports the data to each of the two Area Commanders (for 3-Star review). Final review occurs at the headquarters level Coast Guard program office (CG-544) which compares trend data across the organization. Data inconsistencies found during the review process are investigated and resolved prioir to reporting final data.

Performance Measure	Number of breaches at high-risk maritime facilities
Program	Maritime Prevention
Description	This measure reports the number of security breaches 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. As such, they pose a greater risk for significant loss of life, environmental damage, or economic disruption if attacked. MTSA regulated facilities constitute more than 3,400 high-risk subset of all waterfront facilities. They are facilities that handle certain dangerous cargoes, liquid natural gas, transfer oil, 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	Three-year average number of chemical discharge incidents in the maritime environment per 100 million short tons shipped
Program	Maritime Prevention
Description	This measure is an indicator of the U.S. Coast Guard Program's impact on chemical discharge incidents. It is a moving average of U.S. Coast Guard investigated chemical discharge incidents into navigable waters of the United States for the past 36 months, divided by the 3-year average annual foreign and domestic short tons (100 million) of chemical and chemical products shipped in U.S. waters.
Scope of Data	This measure includes Cchemical spills exceeding reportable quantities in U.S. navigable waters from sources subject to U.S. Coast Guard jurisdiction. A 3-year average is used to show the near-term trend. The U.S. Coast Guard has jurisdiction for spills into or upon navigable waters of the U.S, adjoining shorelines, the contiguous zone, Deepwater Ports, the Continental Shelf, and other areas. 40 CFR 300 requires Vessel or facility operators to report any discharge of any hazardous substance that equals or exceeds reportable quantities listed in 40 CFR 302. Because some reports are delayed in reaching the U.S. Coast Guard, published data is subject to revision with the greatest impact on recent quarters. Shipping statistics are from the Army Corps of Engineers, and not generally available until December following the calendar year. Current values are projected from three years of past data.
Data Source	Investigations of reportable chemical discharge incidents are recorded in the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database. Shipping data is obtained from the U.S. Army Corps of Engineers, from information they use to compile their annual report of the Waterborne Commerce of the United States.
Data Collection Methodology	In FY 2015 this measure changed from a five year average to a three year average. This change does not materially affect the trends or targets. Only investigations recorded in the U.S. Coast Guard's MISLE database of reportable chemical discharge incidents into U.S. waters from maritime sources subject to U.S. Coast Guard jurisdiction are counted. Discharges onto land, into the air, or into enclosed spaces are excluded. Discharges from non-maritime sources such

	as aircraft, trucks and other vehicles, rail cars and rail equipment, U.S. Navy and other public vessels, fixed platforms, and pipelines are excluded. Discharges from unspecified, unclassified, and unknown sources are also excluded. Shipping statistics from the Army Corps of Engineers are not generally available until December following the end of a calendar year. Current values are a forecast, based on a simple least-squares projection of the most recent three years of data.
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.

Performance Measure	Three-year average number of commercial mariner deaths and significant injuries
Program	Maritime Prevention
Description	This is a measure of the average annual number of reportable commercial mariner deaths and significant injuries over the past 12 quarters. It is an indicator of the long-term performance impact of the Coast Guard's Maritime Prevention Program on commercial mariner fatalities and injuries.
Scope of Data	This is a measure of reportable commercial mariner deaths and significant injuries. 46 CFR 4.05-1 requires the owner, agent, master, operator, or person in charge to notify the Coast Guard of any loss of life or injury that requires professional medical treatment beyond first aid. Commercial mariner deaths and significant injuries encompass crewmembers or employees aboard U.S. commercial vessels, with 'significant injuries' defined as those that meet or exceed the level of a 'serious injury', which is an injury that requires significant medical/surgical management, but for which the person was not hospitalized for more than 48 hours within 5 days of the injury. A 3-year average is used to indicate the near term trend.
Data Source	Notices of Mariner casualties are recorded in the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database
Data Collection Methodology	For Mariner deaths and significant injuries, only investigations recorded in the MISLE database with casualties of crewmembers or employees aboard U.S. commercial vessels are counted. Casualties aboard foreign flag or government vessels are excluded. Deaths, disappearances, or injuries determined to be the result of natural causes or intentional acts such as heart attack, altercation, or the like are excluded. The three-year average for a given year is calculated by taking the average of the deaths and significant injuries for the most recent 12 quarters. 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.

Performance Measure	Three-year average number of commercial passenger deaths and significant injuries
Program	Maritime Prevention
Description	This is a measure of the average annual number of reportable commercial passenger deaths and significant injuries over the past 12 quarters. It is an indicator of the long-term performance impact of the Coast Guard's Maritime Prevention Program on commercial passenger fatalities and injuries.
Scope of Data	This is a measure of reportable commercial passenger deaths and significant injuries. 46 CFR 4.05-1 requires the owner, agent, master, operator, or person in charge to notify the Coast Guard of any loss of life or injury that requires professional medical treatment beyond first aid. Commercial passenger deaths and significant injuries encompass commercial passengers aboard U.S. vessels and foreign vessels in U.S. waters, with 'significant injuries' defined as those that meet or exceed the level of a 'serious injury', which is an injury that requires significant medical/surgical management, but for which the person was not hospitalized for more than 48 hours within 5 days of the injury. A 3-year average is used to indicate the near-term trend.
Data Source	Notices of Passenger casualties are recorded in the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database
Data Collection Methodology	Only investigations recorded in the MISLE database with passenger casualties associated with U.S. vessels or foreign vessels operating in U.S. waters are counted; passenger deaths, disappearances or injuries associated with diving activities are excluded. Deaths, disappearances, or injuries determined to be the result of natural causes or intentional acts such as heart attack, altercation, or the like are also excluded. The three-year average for a given year is calculated by taking the average of the deaths and significant injuries for the most recent 12 quarters. 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.

Performance Measure	Three-year average number of oil spills in the maritime environment per 100 million short tons shipped
Program	Maritime Prevention
Description	This measure is an indicator of the U.S. Coast Guard Prevention Program's impact on significant oil spills. It is a moving average of U.S. Coast Guard investigated oil spills greater than 100 gallons discharged into navigable waters of the United States for the past 36 months, divided by the 3-year average annual foreign and domestic short tons (100 million) of oil and oil products shipped in U.S. waters.
Scope of Data	This measure includes oil spills exceeding 100 gallons in U.S. navigable waters from sources subject to U.S. Coast Guard jurisdiction. A 3-year average is used to

	show the near-term trend. The U.S. Coast Guard has jurisdiction for spills into or upon navigable waters of the U.S, adjoining shorelines, the contiguous zone, Deepwater Ports, the Continental Shelf, and other areas. 40 CFR 300 requires Vessel or facility operators to report any discharge of oil or oil products that cause a sheen, discoloration, sludge, or emulsion. Because some reports are delayed in reaching the U.S. Coast Guard, published data is subject to revision with the greatest impact on recent quarters. Shipping statistics are from the Army Corps of Engineers, and not generally available until December following the calendar year. Current values are projected from three years of past data.
Data Source	Investigations of reportable oil discharge incidents are recorded in the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database. Shipping data is obtained from the U.S. Army Corps of Engineers, from information they use to compile their annual report of the Waterborne Commerce of the United States.
Data Collection Methodology	In FY 2015 this measure changed from a five year average to a three year average. This change does not materially affect the trends or targets. Only investigations recorded in the U.S. Coast Guard's MISLE database of reportable chemical discharge incidents into U.S. waters from maritime sources subject to U.S. Coast Guard jurisdiction are counted. Discharges onto land, into the air, or into enclosed spaces are excluded. Discharges from non-maritime sources such as aircraft, trucks and other vehicles, rail cars and rail equipment, U.S. Navy and other public vessels, fixed platforms, and pipelines are excluded. Discharges from unspecified, unclassified, and unknown sources are also excluded. Shipping statistics from the Army Corps of Engineers are not generally available until December following the end of a calendar year. Current values are a forecast, based on a simple least-squares projection of the most recent three years of data.
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 inappropriate entries, 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 Coast Guard Office of Investigations and Casualty Analysis.

Performance Measure	Three-year average of recreational boating deaths
Program	Maritime Prevention
Description	This measure reports the three-year average of recreational boating deaths and removes the inclusion of injuries in the scope. Injuries tend to be larger in number but less meaningful in terms of reflecting meaningful maritime prevention efforts.
Scope of Data	The measure reports the 3-year average annual number of recreational boating deaths on waters subject to U.S. jurisdiction, and on the high seas for vessels owned in the U.S. 33 CFR 173.55 requires operators of vessels used for recreational purposes to file a Boating Accident Report when a person dies, is injured and requires medical treatment beyond first aid or disappears under circumstances that indicate death or injury. Deaths or disappearances determined to be the result of natural causes or intentional acts are excluded.
Data Source	Boating Accident Reports are recorded in the U.S. Coast Guard's Boating Accident Report Database (BARD) System, which is maintained by the Coast Guard Office of Auxiliary and Boating Safety. The majority of data originates from State marine agencies; some data may come from other federal agencies if an accident

	occurred on waters subject to federal jurisdiction; and a limited amount of data may be sourced from news media if a report was not received for an incident that appears to meet federal reporting requirements.
Data Collection Methodology	Results for a given fiscal year are the average number of all applicable recreational boating deaths for the most recent three years. Only casualties recorded in the BARD database are counted.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data is reliable with respect to discoverable information; prior to submitting an accident report, State reporting agencies are required to ensure the completeness and accuracy of the data. To ensure boating casualties are accurately captured, the Coast Guard Office of Auxiliary and Boating Safety crosschecks BARD data with incidents reported in the Coast Guard Marine Information for Safety and Law Enforcement database, other federal sources, and recreational boating casualties reported in media announcements and articles provided by a news clipping service.

Performance Measure	Percent of people in imminent danger saved in the maritime environment
Program	Maritime Response
Description	This measure gauges the lives saved by the U.S. Coast Guard on the oceans and other waterways expressed as a percentage of all people in imminent danger at the time the Service received notification. The measure excludes persons lost prior to notification and single incidents with 11 or more people.
Scope of Data	The measure encompasses all maritime distress incidents reported to the U.S. Coast Guard, which are judged by U.S. Coast Guard operational commanders as valid enough to order a response. The measure includes lives recorded as saved, lost after notification, or unaccounted. Single incidents with 11 or more people saved, lost, or unaccounted are excluded so as not to skew results or impede trend analysis.
Data Source	All maritime distress incidents reported to the U.S. Coast Guard judged by U.S. Coast Guard operational commanders as valid enough to order a response—and associated response data—are recorded in the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database. Data is extracted from MISLE using a CG Business Intelligence (CGBI) cube.
Data Collection Methodology	Data related to maritime distress incidents reported to the U.S. Coast Guard judged by operational commanders as valid enough to order a response are recorded in the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database A CGBI cube is then used to extract the data. The CGBI cube is formulated to only look at cases with 0-10 lives impacted. The results for a given fiscal year are the total number of lives recorded as saved expressed divided by the total number of lives recorded as saved, lost after notification, or unaccounted, multiplied by 100. Single incidents with 11 or more people saved, lost, or unaccounted are excluded from the calculation.
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, limit choices to pre-determined options, and flag data not conforming to expectations. Comprehensive training and user guides help ensure reliability and the application itself contains embedded Help screens. Search and rescue data are also reviewed at multiple levels, and discrepancies reviewed and corrected as necessary.

Performance Measure	Percent of time rescue assets are on-scene within 2 hours
Program	Maritime Response

Description	Time on scene is calculated from the earliest time a Search and Rescue Unit (SRU) is requested to proceed until the earliest time of arrival on scene of an SRU. This includes readiness time, the 30 minutes of preparation time, that provides for underway preps (i.e. engine warm-ups, underway checklist, risk management evaluation, and mission planning) and the transit time, the 90 minutes from underway to on scene based on moderate environmental conditions which allow for operation of the SRUs at their top cruise speeds. To calculate the response times used in the measure, the Coast Guard uses the following equation: Time On Scene = First Sortie On Scene Time minus First Resource Requested Time. The Coast Guard established the 2-hour On Scene Standard in the 1970's and conducted a full review of the standard in 1992. The standard is based on survival expectations in the average weighted water temperatures. The weighting factors into the varying number of incidents occurring regionally.
Scope of Data	One hundred percent of the maritime distress incidents reported to the Coast Guard are collected in the Marine Information for Safety and Law Enforcement (MISLE) database. Data accuracy is limited by human error during data entry.
Data Source	Marine Information for Safety and Law Enforcement (MISLE) database.
Data Collection Methodology	Since FY 2003, operational units have input SAR data directly into the MISLE database. Program review and analysis occurs at the Districts, Area, and Headquarters levels.
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 SAR 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	Three-year average number of serious marine incidents
Program	Maritime Response
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.

Performance Measure	Percent of coordinated anti-terrorism activities contained in Port Tactical Activity Plans that were executed
Program	Maritime Security Operations
Description	This measure gauges the percent of all planned Maritime Security and Response Operations (MSRO) contained in the 37 Captain of the Port (COTP) zone Port Tactical Activity Plans were executed by U.S. Coast Guard or federal, state, and local partners. Quarterly, COTPs use Risk-Based Maritime Security and Response Operations (RBMSRO) calculations of assessed vulnerabilities, historical maritime activity, and asset availability to produce their Tactical Activity Plans to specify the types of operations that will optimize reducing the risk to ports by terrorism and other criminal acts in the maritime domain. Operations include conducting vessel security boardings, providing vessel escorts, enforcing fixed security zones, and conducting surface and land patrols around ports based on available hours and assets. Security risks in the maritime environment include waterborne explosive device attacks, hijacked large vessel attacks, hostage taking, and terrorist assault teams.
Scope of Data	The population includes all MSRO associated with Tactical Activity Plans for the 37 Captain of the Port (COTP) zones. These MSRO occur at vessels, facilities, key assets, and other critical infrastructure at maritime ports. Tactical Activity Plans include only MSRO that impact addressable risk, which is risk the U.S. Coast Guard can address with its current capabilities and authorities. The scope of the results includes information about MSRO from the Tactical Activity Plans that were actually executed by U.S. Coast Guard assets and/or federal, state, and local partners.
Data Source	MSRO data comes from the Marine Information for Safety and Law Enforcement (MISLE) database that is managed by Office of C4 & Sensors Capability (CG-761). MSRO executed by federal, state, and local partners are collected in a formatted spreadsheet and entered into MISLE by the relevant COTP. The Maritime Security Risk Analysis Model (MSRAM), managed by the Office of International and Domestic Port Security (CG-PSA), contains the data that is used to calculate the addressable risks to the 37 COTP zones using a variety of data such as port subject matter experts' judgements of vulnerabilities, actual port activity data, and intelligence. The U.S. Coast Guard Business Intelligence (CGBI) and associated data tools are used to pull data from MISLE and MSRAM to populate Risk-Based Maritime Security and Response Operations (RBMSRO) tools. These

	tools are used for both creating the 37 COTP Tactical Activity Plans and for conducting the actual calculations for this measure.
Data Collection Methodology	The 37 COTPs gather a variety of data annually to update risk estimates for their zones. This information informs Ports' Tactical Activity Plans to optimize risk reduction with the hours and assets available. Coast Guard units that perform MSRO enter that data directly into MISLE. Anti-terrorism MSRO performed solely by federal, state, and local partners are recorded on a formatted spreadsheet and collected by the relevant COTPs. Using CGBI, each COTP pulls their MISLE data for their respective zones to populate RBMSRO. The Coast Guard's Headquarters Maritime Security Operations Program Office then sums these values to determine the total MSRO performed and the total MSRO specified in the Tactical Activity Plans. To calculate the result for this measure, the number of MSRO in Port's Tactical Activity Plans actually executed is divided by the total number of MSRO in the 37 Port's Tactical Activity Plans.
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 inappropriate entries, and limit choices to pre-determined options. Comprehensive training and user guides help ensure reliability and the MISLE application itself contains embedded Help Screens. MISLE records also get verification and validation through regular records review by District, Area, and Headquarters staffs. Annual risk exposure and risk reduction parameters are determined and annually validated in MSRAM by CG-PSA.

Performance Measure	Percent risk reduction of coordinated anti-terrorism activities throughout the maritime transportation system
Program	Maritime Security Operations
Description	This measure gauges risk reduction impact of maritime security and response operations (MSRO) conducted in and around ports in the 37 Captain of the Port (COTP) zones by the U.S. Coast Guard or federal, state, and local partners. MSRO include conducting vessel security boardings, providing vessel escorts, enforcing fixed security zones, and conducting surface and land patrols around ports based on available hours and assets. Security risks in the maritime environment include waterborne explosive device attacks, hijacked large vessel attacks, hostage taking, and terrorist assault teams. Executing planned MSRO helps detect, deter, prevent, disrupt, and recover from terrorist attacks and other criminal acts in the maritime domain.
Scope of Data	The population includes all MSRO associated with Tactical Activity plans for the 37 COTP zones. These MSRO occur at vessels, facilities, key assets, and other critical infrastructure at maritime ports. Tactical Activity Plans include only MSRO that impact addressable risk, which is risk the U.S. Coast Guard can address with its current capabilities and authorities. The scope of the results includes information about MSRO from the Tactical Activity Plans that were actually executed by the U.S. Coast Guard and/or federal, state, and local partners.
Data Source	MSRO data comes from the Marine Information for Safety and Law Enforcement (MISLE) database what is managed by Office of C4 & Sensors Capability (CG-761). MSRO executed by federal, state, and local partners are collected in a formatted spreadsheet and entered into MISLE by the relevant COTP. The Maritime Security Risk Analysis Model (MSRAM) system managed by the Office of International and Domestic Port Security (CG-PSA) contains the data that is used to calculate the addressable risks to the 37 COTP zones using a variety of data such as port subject matter experts' judgements of vulnerabilities, actual port activity data, and intelligence. The U.S. Coast Guard Business Intelligence (CGBI) and

	associated data tools are used to pull data from MISLE and MSRAM to populate Risk-Based Maritime Security and Response Operations (RBMSRO) tools. These tools are used for both creating the 37 ports Tactical Activity Plans and for conducting the actual calculations for this measure.
Data Collection Methodology	The 37 COTPs gather a variety of data annually to update risk estimates for their zones. This information informs Ports' Tactical Activity Plans to optimize risk impact with the hours and assets available. Coast Guard units that perform MSRO enter that data directly into MISLE. MSRO performed solely by federal, state, and local partners are recorded on a formatted spreadsheet and collected by the relevant COTPs. Using CGBI, each COTP pulls their MISLE data for their respective zones to populate RBMSRO. The Coast Guard's Headquarters Maritime Security Operations Program Office sums these values for the risk reduction MSRO completed to determine the numerator for this measure. The same office calculates the addressable risk by summing the risk estimates for the 37 COTP Zones for the denominator. The result is calculated by dividing the sum of all MSRO completed by the addressable risk score across all 37 COTP Zones.
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 inappropriate entries, and limit choices to pre-determined options. Comprehensive training and user guides help ensure reliability and the MISLE application itself contains embedded Help Screens. MISLE records also get verification and validation through regular records review by District, Area, and Headquarters staffs. Annual risk exposure and risk reduction parameters are determined and annually validated in MSRAM by CG-PSA.

Performance Measure	Availability of maritime navigation aids
Program	Maritime Transportation System Management
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 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	Five-year average number of navigational accidents
Program	Maritime Transportation System Management
Description	This measure evaluates the long-term trend of U.S. Coast Guard Waterways Management Program in preventing collisions, allisions (vessels striking fixed objects), and groundings.
Scope of Data	The measure is the sum of all distinct Collision, Allision, and Grounding events involving commercial vessels operating on U.S. navigable waters. A 5-year average is used to show the long-term trend. 46 CFR 4.05-10 requires the owner, agent, master, operator, or person in charge to notify the U.S. Coast Guard of any occurrence involving a vessel that results in a Collision, Allision, or Grounding (CAG). Because some reports are delayed in reaching the U.S. Coast Guard, published data is subject to revision the greatest impact on recent quarters.
Data Source	Notices of Marine casualties are recorded in the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database.
Data Collection Methodology	Only Investigations recorded in the U.S. Coast Guard's MISLE database of reported collision, allision, and grounding incidents in U.S. waters involving commercial vessels are counted. Collision, allision, and grounding incidents not involving a commercial vessel such as a collision between two recreational vessels are excluded. Only distinct events are counted. A collision incident in U.S. waters between two or more vessels, at least one of which is not a recreational boat, is counted as a distinct collision event. An allision incident involving one or more commercial vessels, as might be the case for a tug and several barges in tow, is counted as a distinct allision event. A grounding incident involving one or more commercial vessels, as might be the case for a tug and several barges in tow, is counted as a distinct grounding event.
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 the application itself contains embedded Help screens. MISLE system quality control, and data verification and validation, is effected through regular review of records by the U.S. Coast Guard Office of Investigations and Analysis.

Performance Measure	Percent of time high priority waterways in the Great Lakes and along the eastern seaboard are open during ice season
Program	Maritime Transportation System Management
Description	This measure is the percent of time Tier One Waterways, in the Great Lakes and along the eastern seaboard, are open to vessel transits during the icebreaking season as a percentage of the total. Tier One Waterways are those connecting waterways of the Marine Transportation System that waterways managers at Coast Guard District commands determine are highest-priority due to geographical location or importance of cargo to public health and safety.
Scope of Data	Domestic icebreaking operations are generally conducted during a January to April icebreaking season in the Great Lakes and waterways along the eastern seaboard from New England to the Mid-Atlantic States. Tier One waterways are those identified and categorized as such by waterways managers at Coast Guard District commands due to their geographical location or importance of cargo to public health and safety. A closure is defined as an event or condition preventing

	vessels from transiting a waterway due to a Captain of the Port safety zone, regulated navigation area or other vessel traffic controls, or an environmentally imposed closure without Coast Guard actions, including extreme ice conditions or a vessel beset in ice blocking the safe passage of other vessels.
Data Source	Data is obtained from U.S. Coast Guard field units, validated at the U.S. Coast Guard District level, and recorded in end-of-season reports submitted to U.S. Coast Guard Headquarters by 01 July each year.
Data Collection Methodology	Measure results are total icebreaking season hours by District for all Tier One waterways less total hours Tier One waterways were closed, expressed as a percentage of the total icebreaking season hours. Total icebreaking season hours by District are: total ice season days x 24 hours. Total hours Tier One waterways were closed include: Ice-related Tier One waterway closures reported in days x 24, plus ice-related Tier One waterway closures reported in hours, plus total number and duration of Tier One ice-related waterway restrictions or Captain of the Port limitations.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data verification and validation is conducted through review of U.S. Coast Guard unit reports by U.S. Coast Guard Districts, and the Mobility and Ice Operations Division in the Office of Waterways and Oceans Policy at U.S. Coast Guard Headquarters.

U.S. Secret Service

Performance Measure	Amount of cyber-financial crime loss prevented (in billions)
Program	Field Operations
Description	This measure is an estimate of the direct dollar loss to the public prevented due to cyber-financial investigations by the U.S. Secret Service. The dollar loss prevented is based on the estimated amount of financial loss that would have occurred had the offender not been identified nor the criminal enterprise interrupted. The measure reflects the U.S. Secret Service's efforts to reduce financial losses to the public attributable to cyber financial crimes.
Scope of Data	This measure reports an estimate of the direct dollar loss prevented due to Secret Service intervention/interruption of a cyber-financial crime. It includes all investigations by the Secret Service (authorized under 18 USC 3056) which were closed in the fiscal year being reported. Potential error is due to lag time in data entry or corrections to historical data.
Data Source	The Cyber 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. This system is owned and maintained internally by the U.S. Secret Service.
Data Collection Methodology	Data is input to FIRS via Secret Service personnel located in field offices throughout the United States and overseas. Field personnel entering the data have already estimated the loss prevented using standards from the Federal Sentencing Guidelines. These values are extracted from FIRS by cyber financial crime codes (case 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	The scope of this measure includes all cyber mitigation response data and is based on the number of cyber mitigation responses conducted by the USSS within the given reporting period.
Data Source	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	The scope of this measure includes 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 hours of cyber crime training provided to law enforcement both domestically and overseas
Program	Field Operations
Description	This measure represents the number of cyber crime training hours provided 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 represents the number of cyber crime training hours provided by the Secret Service in cyber crime and cyber forensics. This includes both internal agents and external law enforcement partners.
Data Source	Data on training hours provided 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.
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	Number of law enforcement individuals trained in cybercrime and cyberforensics 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	The scope of this measure is the number of individuals trained by the Secret Service in cybercrime and cyber forensics. This includes both internal agents and external law enforcement partners.
Data Source	Data on individuals trained by the USSS is currently collected through internal tracking devices. An enterprise solution is contemplated 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 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 information and systems. 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	The scope of this measure includes the total U.S. dollars in circulation (reported from the US Department of the Treasury). 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. Past audits indicate that overall error rates are less than one percent. Some error is due to lag time in data entry or corrections to historical data.

Performance Measure	Percent of National Center for Missing and Exploited Children 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	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	The scope of this measure includes all data forensically analyzed for criminal investigations 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.

Performance Measure	Number of information sharing events with the law enforcement and intelligence community
Program	Protective Operations
Description	This measure gauges the number of information sharing events with both internal entities and external partner agencies as an assessment of the effectiveness of information dissemination. Information sharing elements include both internal and external briefings and intelligence products. Information sharing events include: Targeted Violence Information Sharing System (TAVISS) briefings, agency alerts, specialty desk briefings and other training, spot reports, suspicious activity reporting, advisories, permanent protectee threat assessments, major events assessments, and certain other assessment products. Sharing information about threats, hazards, and protective actions will allow for the internal and external coordination needed to prevent successful attacks.
Scope of Data	The scope of this measure includes information sharing events with both internal entities and external partner agencies. Information sharing events include both internal and external briefings and intelligence products such as: Targeted Violence Information Sharing System (TAVISS) briefings, agency alerts, specialty desk briefings and other training, spot reports, suspicious activity reporting, advisories, permanent protectee threat assessments, major events assessments, OSB trip reports (open source intelligence relating to protectee travel) and certain other assessment products. It does not include NTAC events.
Data Source	Data on information sharing events provided by the Secret Service are manually collected on an internal Excel spreadsheet.
Data Collection Methodology	Data is entered manually in an Excel document by authorized Secret Service personnel. Data from multiple spreadsheets are consolidated into a single report by headquarters personnel that sum all information sharing events. Quarterly data will be aggregated and the total reported at the end of the quarter/year.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data reliability for this measure includes a review process conducted by program managers. They verify and validate each event with the instructor before entering the results. The performance metrics advisor in the Analytics Division at U.S. Secret Service Headquarters also reviews the results and identifies any inconsistencies and/or data outliers.

Performance Measure	Number of National Threat Assessment Center trainings and briefings
Program	Protective Operations
Description	This measure quantifies the information sharing sessions communicating information conducted by the National Threat Assessment Center (NTAC) to law enforcement, interested stakeholders, and others with a role in public safety. NTAC conducts research, training, consultation, and information sharing on threat assessment and the prevention of targeted violence. In addition to attacks on K-12 schools, colleges, and universities, NTAC studies violence directed at government officials and agencies, workplaces, and public spaces. The sharing of information from NTAC studies about threats, hazards, and protective actions will allow for the internal and external coordination needed to prevent successful attacks.
Scope of Data	This scope of this measure includes all NTAC trainings and briefing events delivered to Secret Service personnel (e.g., new special agent recruits), external federal/state/local law enforcement, K-12 school/college/university personnel,

	and others with a role in public safety. The result excludes NTAC training for those newly detailed to the Protective Intelligence and Assessment Division (PID) as those are captured in the information sharing events performance measure.
Data Source	This measure gathers data from all NTAC trainings and briefings. The numbers are compiled in a Microsoft Access database that is maintained by NTAC staff.
Data Collection Methodology	NTAC trainings and briefings are entered into the NTAC Training Database by the NTAC Training Coordinator. Once an event is complete, the event and all of its relevant data (e.g., location, number of attendees, etc. is entered into the database by the Coordinator. The number includes external trainings and briefings delivered by NTAC and does not include training delivered by other U.S. Secret Service programs.
Reliability Index	Reliable
Explanation of Data Reliability Check	Staff members who delivered the training verify and validate that the information entered into the NTAC Training Database is accurate. The performance metrics advisor in the Analytics Division at U.S. Secret Service Headquarters also reviews all results and identifies any inconsistencies, data outliers, or training within PID.

Performance Measure	Percent of days with incident-free protection at the White House Complex and Vice President's Residence
Program	Protective Operations
Description	This measure gauges the percent of instances where the Secret Service provides incident free protection to the White House Complex and the Vice President's Residence. An incident is defined as someone who is assaulted or receives an injury from an attack while inside the White House Complex or Vice President's Residence.
Scope of Data	The scope of this measure is all activity throughout the entire year for all 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	Percent of instances protectees arrive and depart safely (campaign protectees)
Program	Protective Operations
Description	This measure represents the percent of travel stops where the protectee safely arrives and departs. The security of protectees is the ultimate priority of the Secret Service; therefore, all necessary resources are utilized before and during a protective assignment in order to provide the highest-quality protection the Secret Service demands for all protectees.

Scope of Data	Performance data capture the activities of major Presidential and Vice Presidential candidates and nominees and their spouses, and President-elect and Vice President-elect and their immediate families. There is no error rate for this measure.
Data Source	This program measure originates from every protective event or visit. 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.
Reliability Index	Reliable
Explanation of Data Reliability Check	Program management and the Management and Organization division 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 instances protectees arrive and depart safely (domestic protectees)
Program	Protective Operations
Description	The percent of travel stops where our Nation's leaders and other protectees arrive and depart safely. The security of protectees is the ultimate priority of the Secret Service; therefore, all necessary resources are utilized before and during a protective assignment in order to provide the highest-quality protection the Secret Service demands for all protectees.
Scope of Data	Performance data capture the protection of domestic leaders consisting of the President and Vice President and their families, former Presidents and their spouses, and other designated individuals. There is no error rate for this measure.
Data Source	This program measure originates from every protective event or visit for domestic protectees. 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.
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 instances protectees arrive and depart safely (Foreign Dignitaries)
Program	Protective Operations
Description	The percent of travel stops where visiting world leader protectees safely arrive and depart. The security of protectees is the ultimate priority of the Secret Service; therefore, all necessary resources are utilized before and during a protective assignment in order to provide the highest-quality protection the Secret Service demands for all protectees.

Scope of Data	Performance data captures the protection of visiting heads of state, heads of government, and their spouses and other distinguished visitors to the United States as directed by the President. Data also capture external security to foreign diplomatic embassies and missions in the Washington, D.C., area (and other limited areas, consistent with statute). There is no error rate for this measure.
Data Source	This program measure originates from every protective event or visit. 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.
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 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 scope of this measure is every NSSE where the Secret Service has a role in the protection or planning of the NSSE.
Data Source	This program measure originates from the protective event or visit and all data is available through After-Action Reports.
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. Protectees include the President and Vice President of the United States and their immediate families, former presidents, their spouses, and their minor children under the age of 16, major presidential and vice presidential candidates and their spouses, and foreign heads of state. The performance target is always 100%.

Scope of Data	The scope of this measure is the total number of protective stops. Protectees include the President and Vice President of the United States and their immediate families, former presidents, their spouses, and their minor children under the age of 16, major presidential and vice presidential candidates and their spouses, and foreign heads of state.
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 instances protectees arrive and depart safely (campaign protectees)
Program	Protective Operations
Description	This measure represents the percent of travel stops where the protectee safely arrives and departs. The security of protectees is the ultimate priority of the Secret Service; therefore, all necessary resources are utilized before and during a protective assignment in order to provide the highest-quality protection the Secret Service demands for all protectees.
Scope of Data	Performance data capture the activities of major Presidential and Vice Presidential candidates and nominees and their spouses, and President-elect and Vice President-elect and their immediate families. There is no error rate for this measure.
Data Source	This program measure originates from every protective event or visit. 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.
Reliability Index	Reliable
Explanation of Data Reliability Check	Program management and the Management and Organization division 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 instances protectees arrive and depart safely (domestic protectees)
Program	Protective Operations
Description	The percent of travel stops where our Nation's leaders and other protectees arrive and depart safely. The security of protectees is the ultimate priority of the

	Secret Service; therefore, all necessary resources are utilized before and during a protective assignment in order to provide the highest-quality protection the Secret Service demands for all protectees.
Scope of Data	Performance data capture the protection of domestic leaders consisting of the President and Vice President and their families, former Presidents and their spouses, and other designated individuals. There is no error rate for this measure.
Data Source	This program measure originates from every protective event or visit for domestic protectees. 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.
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 instances protectees arrive and depart safely (Foreign Dignitaries)
Program	Protective Operations
Description	The percent of travel stops where visiting world leader protectees safely arrive and depart. The security of protectees is the ultimate priority of the Secret Service; therefore, all necessary resources are utilized before and during a protective assignment in order to provide the highest-quality protection the Secret Service demands for all protectees.
Scope of Data	Performance data captures the protection of visiting heads of state, heads of government, and their spouses and other distinguished visitors to the United States as directed by the President. Data also capture external security to foreign diplomatic embassies and missions in the Washington, D.C., area (and other limited areas, consistent with statute). There is no error rate for this measure.
Data Source	This program measure originates from every protective event or visit. 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.
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 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 scope of this measure is every NSSE where the Secret Service has a role in the protection or planning of the NSSE.
Data Source	This program measure originates from the protective event or visit and all data is available through After-Action Reports.
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. Protectees include the President and Vice President of the United States and their immediate families, former presidents, their spouses, and their minor children under the age of 16, major presidential and vice presidential candidates and their spouses, and foreign heads of state. The performance target is always 100%.
Scope of Data	The scope of this measure is the total number of protective stops. Protectees include the President and Vice President of the United States and their immediate families, former presidents, their spouses, and their minor children under the age of 16, major presidential and vice presidential candidates and their spouses, and foreign heads of state.
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.

This Page Intentionally Left Blank

Homeland
Security

Homeland
Security