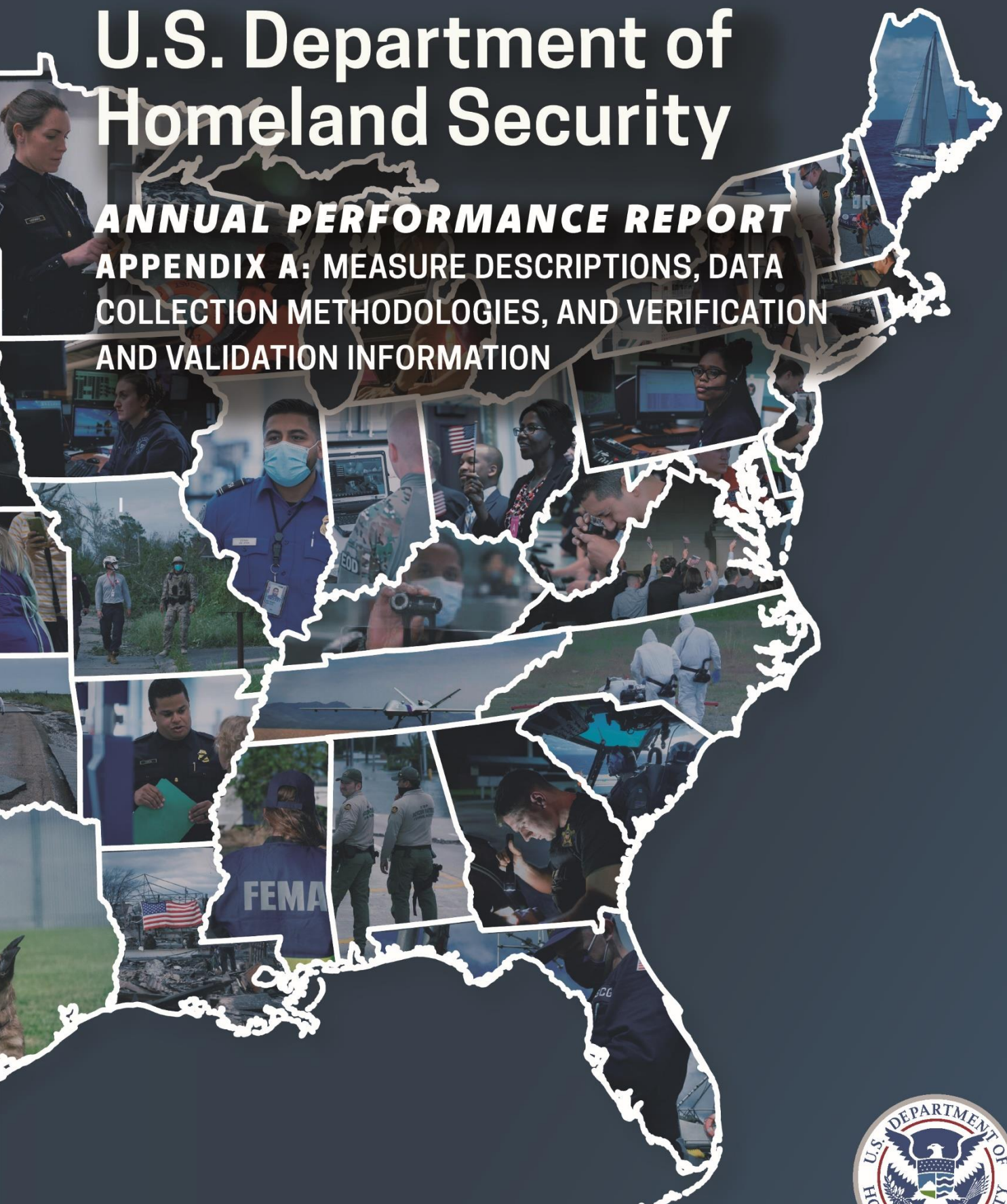


# U.S. Department of Homeland Security

## ***ANNUAL PERFORMANCE REPORT***

### **APPENDIX A: MEASURE DESCRIPTIONS, DATA COLLECTION METHODOLOGIES, AND VERIFICATION AND VALIDATION INFORMATION**



**FY 2022 – FY 2024**



# About this Report

The U.S. Department of Homeland Security (DHS) Annual Performance Report (APR) for Fiscal Years (FY) 2022-2024 presents the Department's mission programs, progress summaries, performance measure results, and FY 2023 and FY 2024 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. Appendix B provides a list of the more significant DHS program evaluations conducted in FY 2022 by the GAO and DHS OIG.

For FY 2022, the Department's Performance and Accountability Reports consist of the following three reports:

- DHS Agency Financial Report | Publication date: November 15, 2022
- DHS Annual Performance Report | Publication date: March 13, 2023
- DHS Report to our Citizens (Summary of Performance and Financial Information) | Publication date: April 11, 2023

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 .....2**

*Performance Data Verification and Validation Process .....2*

*Management Assurance Process for GPRAMA Performance Measure Information.....4*

**Measure Descriptions, Data Collection Methodologies, and Verification and Validation Information .....5**

*U.S. Customs and Border Protection (CBP).....5*

*Countering Weapons of Mass Destruction Office (CWMD)..... 17*

*Cybersecurity and Infrastructure Security Agency (CISA) ..... 19*

*Federal Emergency Management Agency (FEMA) ..... 30*

*Federal Law Enforcement Training Centers (FLETC)..... 61*

*Office of Intelligence and Analysis (I&A) ..... 63*

*U.S. Immigration and Customs Enforcement (ICE)..... 68*

*Office of Homeland Security Situational Awareness (OSA) ..... 77*

*Science and Technology Directorate (S&T)..... 79*

*Transportation Security Administration (TSA)..... 81*

*U.S. Citizenship and Immigration Services (USCIS)..... 99*

*U.S. Coast Guard (USCG)..... 120*

*U.S. Secret Service (USSS)..... 129*



## 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.<sup>1</sup>

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 following 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.

#### **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

---

<sup>1</sup> 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.



quality.<sup>2</sup> 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 DHS 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 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 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 annual assessment of its performance measure data with the support of 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

---

<sup>2</sup> In their report, *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.



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

### *U.S. Customs and Border Protection (CBP)*

Performance Measure	Percent of detected conventional aircraft incursions resolved along all borders of the United States
Program	Air and Marine Operations (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	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	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



	<p>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 awareness and ability to secure the border.</p>
<p>Scope of Data</p>	<p>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.</p>
<p>Data Source</p>	<p>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). GAs, TBs, and NAs 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.</p>
<p>Data Collection Methodology</p>	<p>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 GAs, NAs, or TBs 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)</p>



	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, GAs, NAs, and TBs. 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	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	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 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



	<p>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.</p>
Scope of Data	<p>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.</p>
Data Source	<p>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&amp;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.</p>
Data Collection Methodology	<p>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</p>



	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 $[1 - (\text{Estimated Revenue Gap} / \text{Total Collectable Revenue})] \times 100$ .
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



	<p>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.</p>
Reliability Index	Reliable
Explanation of Data Reliability Check	<p>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.</p>

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	<p>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.</p>
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	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.
--	---

**Countering Weapons of Mass Destruction Office (CWMD)**

Performance Measure	Percent of Acquisition programs to counter CBRN threats that meet their Acquisition Program Baseline (APB) schedule, cost, and performance thresholds (New Measure)
Program	Capability and Operational Support
Description	This metric will assess two things: (1) programs having APB schedule thresholds which remain to be achieved, and programs that have completed their final baselined key event during the current annual evaluation period and (2) programs that have not yet reached FOC and those that have reached FOC during the current annual evaluation period, defined as CWMD and all supported Component(s) having signed an FOC Achievement Memorandum.
Scope of Data	This metric will be calculated for programs beginning at Acquisition Decision Event (ADE)-2C or ADE-3, whichever occurs earlier; and ending at Post-Implementation Review or FOC achievement, whichever occurs later. Programs achieving one or more of these milestones during the current annual evaluation period will be included in the calculation.
Data Source	The sources of the data are: APBs, Acquisition Decision Memoranda (ADM) granting Acquisition Decision Event approval, Component Acquisition Review Board (CARB) results, Technical Review Board (TRB) reports, other written documentation of schedule key event completion (as applicable, varies by program and key event) APBs, FOC achievement reporting memoranda, Financial obligation and execution data, DHS INVEST data (for MAOL programs)
Data Collection Methodology	Program managers provide written evidence of performance against APB and cost, schedule, and performance thresholds. The data collected on an ongoing basis. The data is collected via monthly ACQ Division Issue papers, Quarterly Performance Reviews, status of funds, and spend plans.
Reliability Index	Reliable
Explanation of Data Reliability Check	Reviewed at semi-annual 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 technology or knowledge products transitioned to customers for planned improvements in the Homeland Security Enterprise (New Measure)
Program	Capability and Operational Support
Description	<p>This measure reflects the percent at which the Countering Weapons of Mass Destruction (CWMD) meets its planned fiscal year transitions of technology or knowledge products for research and development funded programs/projects. A successful transition is the transition/transfer of ownership and/or operation of a technology or knowledge product from CWMD to a customer within the Department of Homeland Security or industry. 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 CWMD 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.</p>
Scope of Data	<p>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.”</p>
Data Source	<p>Input is gathered by the responsible person/party involved in technology transition for CWMD. Data is recorded quarterly in the NDAA Tech Transition and the RDD Project Database spreadsheet as TTAs are approved. 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. CWMD Offices are tasked through the CWMD Exec Sec process to submit the quarterly status of each RD milestone planned, including planned transitions. CWMD program/project managers report the quarterly status of each planned milestone. CWMD leadership review and verify the</p>





	quarterly status and explanation of each milestone prior to submitting to the CWMD Performance Team for review and management. Information from the Excel file (Milestone Status Report) is used for calculating and explaining the measure result as well as forecasting if it is 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 CWMD Performance Team, program/project managers report the status of each milestone planned for the fiscal year of execution, which are then verified by CWMD leadership prior to review by the CWMD 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 and submitted by the tech transition team with the approval of CWMD leadership to the Performance Team.
Reliability Index	Reliable
Explanation of Data Reliability Check	CWMD 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 CWMD Performance Team. The CWMD Performance Team provides a third data reliability review before results are finalized and submitted to DHS.

**Cybersecurity and Infrastructure Security Agency (CISA)**

Performance Measure	Percent of agencies for which a Continuous Diagnostic and mitigation dataset, measured to be at the established acceptable quality target and supporting the agency risk score, can be provided for assets reporting to the federal dashboard (New Measure)
Program	Cybersecurity
Description	This measure reports the percent of participating Federal Civilian Executive Branch (FCEB) agencies that have completed a series of required engineering reviews conducted with CDM engineers, demonstrated that the agency’s CDM Asset Management



	<p>solution set is ready for a data quality assessment, and then been assessed as having achieved an acceptable level of data quality to support a reliable AWARE score. The AWARE scoring uses numerical scales to quantify the severity of identified vulnerabilities present on a system, how long they have been present, and the potential risk to the system. Using AWARE scores provides useful information to agencies and serves as a mechanism to prioritize and remediate system vulnerabilities. This measure is an indicator of a federal agency's ability to provide reliable asset management information to the Federal Dashboard and its subsequent use to determine cyber risk.</p>
Scope of Data	<p>The total possible population of this measure is the 23 federal civilian CFO Act agencies and the 79 mid- to small-sized agencies that have a signed Memorandum of Agreement (MOA) with CDM indicating participation in the program. To be counted in the measurement, an agency must have a working end-to-end CDM Asset Management solution, have implemented the new CDM Agency Dashboard Ecosystem, and have established a data exchange providing valid data to the Federal Dashboard. The agency must also participate in a series of systems engineering reviews with the CDM program office to verify that key Asset Management functions are working properly; the agency must then indicate it is prepared to participate in a scheduled DQM assessment cohort. The value being counted is whether any one of the agencies' organizations is providing valid data to the Federal Dashboard that then allows for the calculation of the automated AWARE score.</p>
Data Source	<p>The CDM Project Management Office is responsible for maintaining all the data used for this measure. Data is captured during the DQM quality assessment process and via the CDM Federal Dashboard, and entered into the FY22-23 APG Data Collection Instrument spreadsheet stored on the CDM IPT SharePoint site.</p>
Data Collection Methodology	<p>The CDM Program Office will track progress of agencies' ability to provide valid data to the Federal Dashboard and the subsequent automated calculation of an AWARE score for that organization. CDM Program analysts perform a manual review in coordination with agencies and CDM systems integrators to assess quality of data collected and reported to the agency dashboard. Data is considered of acceptable quality based on tests using the published CDM data consistency protocol. The focus for this validation includes ensuring proper configuration of agency's CDM tools and sensors, ensuring resolution of missing/duplicative data, and that data transfer between agency and federal dashboards is functioning properly, allowing for the calculation of an AWARE score. This measure is calculated by</p>



	dividing the number of agencies where any organization in that agency has a valid AWARE score by the total possible participating agencies.
Reliability Index	Reliable
Explanation of Data Reliability Check	Upon collection and calculation of the quarterly data, the CDM Program Manager, CDM Deputy Program Managers, CDM Portfolio Management Section Chief, the CB Director, and the CB Deputy Director will review the data to verify its validity as compared to other authoritative sources (e.g., agency FISMA reporting), and review collected data from previous quarters and the quality of the data provided, to ensure accuracy of reporting. The Cybersecurity Division’s Performance Management Branch will also review the results and accompanying explanations to ensure accuracy.

Performance Measure	Percent of agencies that have developed internal vulnerability management and patching procedures by the specified timeline (New Measure)
Program	Cybersecurity
Description	This measure tracks compliance with CISA’s Managing Unacceptable Risk Vulnerabilities Binding Operational Directive (BOD) that was released in November 2021. The first requirement from the directive is for agencies to develop or update internal vulnerability management procedures. The requirement to develop or update comes into effect 60 days from issuance. The BOD includes details on scope for these procedures, including establishing a process for ongoing remediation of vulnerabilities that CISA identifies to carry unacceptable risk, assigning roles and responsibilities, establishing validation and enforcement procedures, and setting tracking and reporting requirements. Internal vulnerability patching procedures will reduce the number of vulnerabilities across the Federal Civilian Executive Branches.
Scope of Data	The scope is all Federal Civilian Executive Branch (FCEB) agencies, which will be required to comply with the BOD. The denominator will be all FCEB agencies. The numerator will be the percent of Federal Executive Branch agencies that have developed internal vulnerability management and patching procedures.
Data Source	Initially agencies may submit quarterly reports through CyberScope submissions or report through the CDM Federal Dashboard. Starting on October 1, 2022, agencies that have not migrated reporting to the CDM Federal Dashboard will be



	<p>required to update their status through CyberScope bi-weekly. Upon request agencies will provide a copy of these policies and procedures to CISA. The following data sources are compiled and managed by the CISA CyberDirectives Team: 1) Agency Self Reporting via CyberScope Platform – quarterly deadlines and 2) Continuous Diagnostics and Mitigation (CDM) Federal Dashboard – automated platform pulling scan data from agency networks. The CyberDirectives team consolidates this data into an excel dashboard and reports on agency compliance. The numerator will be the percent of Federal Executive Branch agencies that have developed internal vulnerability management and patching procedures.</p>
Data Collection Methodology	<p>Initially agencies may submit quarterly reports through CyberScope submissions or report through the CDM Federal Dashboard. Starting on October 1, 2022, agencies that have not migrated reporting to the CDM Federal Dashboard will be required to update their status through CyberScope bi-weekly. These metrics will be captured quarterly until October 2022, then will be captured bi-weekly. The denominator for compliance percentage would be the total number of FCEB agencies that have developed internal vulnerability management and patching procedures. The numerator will be the % of Federal Executive Branch agencies that have developed internal vulnerability management and patching procedures.</p>
Reliability Index	Reliable
Explanation of Data Reliability Check	<p>CISA will ingest and validate the data from CyberScope each quarter, until October 2022, at which point CISA will review and validate the data reporting via CDM Federal Dashboard bi-weekly. CISA will also reach out to select agencies for added validation if reporting warrants, for example an agency reports not updating portions of their policy or procedures. The CDM dashboard will be an authoritative data source, directly scanning agency networks and will enable quick response and less cycles on validation.</p>

Performance Measure	Percent of Federal Civilian Executive Branch agency Domain Name System egress traffic bypassing CISA’s Domain Name System filtering capabilities (New Measure)
Program	Cybersecurity
Description	<p>This measure assesses CISA’s ability to manage risk to Federal Civilian Executive Branch (FCEB) entities using CISA’s DNS filtering capabilities. The program impacts the results by working with Agencies to improve integrated network defense services through analyst-to-analyst discussions and reduction of false positive results. Results will be used to determine if</p>



	<p>improvements to supporting suite of IT systems [specifically protective DNS (pDNS)] improve FCEB risk posture by escalating the percent of DNS traffic that uses CISA DNS filtering capabilities. This measure aligns to agency goal of deploying needed visibility capabilities (CSD AOP 1.1.2), which is important to manage risk to FCEB entities. External factors such as intentional Agency manual bypass of DNS filtering will impact results.</p>
Scope of Data	<p>The scope of this measure is limited to DNS egress traffic from FCEB entities. The scope includes traffic which uses CISA's DNS filtering capabilities, and traffic which bypasses CISA's DNS filtering capabilities, due to both automatic or manual DNS filtering bypass, so that the complete picture of which traffic is using the filtering capability, and which is not, is established for purposes of measurement. CISA's inability to distinguish between automatic or manual DNS filtering bypass makes the specific reason for bypass difficult to discern at scale. Both IPv4 and IPv6 traffic are in scope for this metric. The unit of analysis is a single DNS over Transport Layer Security (DOT), DNS over HTTPS (DOH) outbound query packet. The population includes all DOT and DOH outbound query packets. The attribute is whether a DNS packet transits CISA DNS filtering capabilities.</p>
Data Source	<p>The data for the measure are stored in NCPS (EINSTEIN) systems. Packet transit information is compiled automatically in the course of standard Integrated Network Defense operations. The results are then transferred to the CSD Metrics Platform by a Threat Hunting/Adversary Pursuit analyst.</p>
Data Collection Methodology	<p>Daily statistics are entered for all DNS, DOT and DOH outbound queries for all FCEB entities. Outbound queries, which are not directed at CISA authorized DNS filtering infrastructure are known to be bypassing CISA DNS filtering capabilities. A Threat Hunting/Adversary Pursuit analyst retrieves the data to calculate the result. The number of DNS packets directed at CISA authorized DNS filtering infrastructure are divided by the total number of DNS packets and multiplied by 100 to derive the percentage routed through CISA DNS filtering capabilities.</p>
Reliability Index	<p>Reliable</p>
Explanation of Data Reliability Check	<p>The data collection methodology is sufficiently reliable to derive the percentage of FCEB entities with DNS egress traffic, which bypasses DNS filtering capabilities. DNS queries may be sent multiple times but counted only once and TCP DNS numbers will include packets which are not directly related to queries (overhead packets), but these outliers are not estimated to make a substantial difference in the percentage of FCEB entities bypassing DNS filtering capabilities.</p>





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 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 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 Organizational Interagency Security Committee Benchmarks Reported at Fully Compliant (New Measure)
Program	Infrastructure Security
Description	This measure demonstrates progress agencies are making towards achieving the Interagency Security Committee (ISC)'s identified benchmarks related to its policies and standards. Additionally, this measure showcases Domestic Violent Extremism (DVE) mitigation/prevention activities conducted by CISA. Executive Branch organizations submit benchmark data, including DVE activities, which is reviewed and scored on a scale from 1 to 5 (fully compliant) to ensure relevant policies and standards are met. The results are used by the program to make recommendations for areas of noncompliance.
Scope of Data	The results of the measure are based on all available data within the ISC-CS (Interagency Security Committee Compliance System). The unit of analysis is an individual benchmark submitted from a



	<p>member organization. The population is the total number of organizational benchmarks (which includes DVE activities) received from Executive Branch organizations. The attribute is whether the benchmark received a score of 5 (fully compliant). The numerator, or what is counted in the results, is the total number of benchmarks, across the total number of member organizations reporting, that have a score of 5, defined as fully compliant, on a scale of 1-5. The denominator, or population, is the total number of benchmarks reported on, across the total number of member organizations reporting.</p>
Data Source	<p>The data is sourced from ISC-CS, which is operated by the ISC program office and provides a summary of each organization's submission, thereby indicating that a successful submission has been completed.</p>
Data Collection Methodology	<p>The compliance benchmark data is provided by ISC-CS Administrators, Uploaders and/or Data POC's. These individuals, who represent Executive Branch organizations, are responsible for submitting data, ensuring its accuracy, and validating it in the ISC-CS. While data upload privileges are granted by departments/agencies as they see fit, only the organization administrator can validate the data as correct. Once the data is input into the ISC-CS, analysts within the program generate a report from the system annually. The numerator, or what is counted in the results, is the total number of benchmarks, across the total number of member organizations reporting, that have a score of 5, defined as fully compliant, on a scale of 1-5. The denominator, or population, is the total number of benchmarks reported on, across the total number of member organizations reporting. The numerator is dividing by the denominator to calculate the percentage of total reported benchmarks that are fully compliant.</p>
Reliability Index	<p>Reliable</p>
Explanation of Data Reliability Check	<p>The ISC-CS, which serves as the primary data source, has the capability to create reports for organizations who have submitted compliance data. Once all Agencies have submitted their data, the ISC creates a report and spot checks the results with the data located in the ISC-CS to ensure that there are no anomalies or inconsistencies with the reported data submissions. The ISC keeps a record of all Agencies providing compliance data, ensuring that all organizations are accounted for and properly identified. The data and results 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.</p>





Performance Measure	Total number of election stakeholders reached through strategic engagements (New Measure)
Program	National Risk Management Center
Description	This measure demonstrates the capacity of the CISA/NRMC Election Security and Resilience (ESR) Sub-division to engage state and local jurisdictions to ensure awareness and to promote the use of election information services and cybersecurity assessment services. This measure counts individual stakeholders responsible for executing election activity. The CISA/NRMC election security team engages state and local jurisdictions through various outreach engagements, (e.g., conferences, meetings, summits) to promote CISA/NRMC services, the process for requesting services, and the value these services provide to help stakeholders better understand and manage risk that is unique to their respective jurisdictions and election infrastructure.
Scope of Data	The population of the data encompasses all election security stakeholders (e.g., state/local jurisdictions and entities) reached through strategic engagements in a fiscal year as recorded in the CISA/NRMC state and local jurisdictions election security stakeholder engagement meeting calendar/database. The unit of analysis is a single election security stakeholder reached through strategic engagements in a fiscal year as recorded in the CISA/NRMC state and local jurisdictions election security stakeholder engagement meeting calendar/database This includes in-person engagements such as conferences and meetings and virtual engagements including webinars and teleconferences where ESI has a participatory role.
Data Source	The CISA/NRMC ESR team will maintain a fiscal year’s state and local jurisdictions election security stakeholder engagement meeting calendar/database. The meeting calendar/database serves as the source of data for the measure. The meeting calendar/database will contain the list of state and local jurisdictions that have invited ESI to attend, or ESI has requested to attend, election security related engagements/meetings. The CISA/NRMC ESI team will update the meeting calendar/database on a regular basis.
Data Collection Methodology	The CISA/NRMC performance analyst conducts a quarterly state and local jurisdictions election security stakeholder engagement data call. The CISA/NRMC election security office will use the state and local jurisdictions election security stakeholder engagement meeting calendar/database to provide the total number of election stakeholder engagements completed by ESR during the reporting period.



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 (FEMA)**

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



	<p>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.</p>
--	---

Performance Measure	Benefit to cost ratio of the Hazard Mitigation Grants
Program	Grants
Description	<p>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.</p>
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	<p>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.</p>
Data Collection Methodology	<p>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</p>



	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 capabilities where community capability is far less than national goal (New Measure)
Program	Grants
Description	This measure assesses the effectiveness of the Homeland Security Grant program. The Homeland Security Grant Program is a suite of risk-based grants to assist state, local, tribal, and territorial efforts in preventing, protecting against, mitigating, responding to, and recovering from acts of terrorism and other threats. This measure compares the combined community capability to national capability targets and presents a snapshot of the general state of preparedness at the national level. A capability is considered to have far less than the national goal if affected communities report capability of less than 30% of the national goal necessary to manage catastrophic scenarios. Because the national capabilities required to be reported each year may change, it may be necessary to provide additional context on the number of national capabilities included in the reported measure score each year.
Scope of Data	The unit of analysis is a single capability reported in the Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) by states, territories tribes and urban areas against relevant national capability goals. The population is the total capabilities reported by communities who complete the THIRA and SPR. Each national capability is specific to a catastrophic scenario that affects a subset of states, territories, and urban areas. For each national capability target, all communities are identified as either directly impacted by the scenario or as a non-scenario community. Therefore, only a subset of communities contribute towards each scenario-specific capability. The attribute is whether the community capability is below 30% for each standardized impact of national goal achievement The capabilities used in this measure are the



	national capabilities that states, territories, and urban areas are required to report in that year.
Data Source	For community capabilities, the data is derived from the Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR). The THIRA is a three-step risk assessment process that helps communities understand their risks and what they need to do to address those risks. The outputs from this process lay the foundation for determining community’s gaps as part of the SPR. THIRA/SPR data for each community is submitted through the online FEMA Preparedness Toolkit. For National goals the data is derived from the National Risk and Capability Assessment (NRCA) and the National THIRA (NTHIRA). The National THIRA is a process that assesses the impacts of the most catastrophic threats and hazards to the Nation and establishes capability targets to manage them. The information from this process is published in the National Preparedness Reports.
Data Collection Methodology	Communities submit their THIRA/SPR data through the online FEMA Preparedness Toolkit. NPAD will calculate community capability gaps in relation to National goals for each required standardized impact by dividing aggregated community-level capability assessments from the SPR by National Capability Targets set in the National Risk and Capability Assessment (NRCA). NPAD will then count the number of required standardized impacts with a national target achievement below 30% for each standardized impact. The count of all standardized impacts below 30% of national goal achievement is the numerator. The denominator is the total number of standardized impacts states, territories, and urban areas are required to report in the measurement year. The measurement score is calculated by dividing the numerator by the denominator.
Reliability Index	Reliable
Explanation of Data Reliability Check	FEMA’s National Preparedness Assessments Division (NPAD) aggregates Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) data on an annual basis, reviews each submission for errors, and works with communities to correct issues.

Performance Measure	Percent of communities in high-risk areas for earthquake, flood, and wind hazards, adopting current or next most recent hazard-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 through 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 United 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 nationwide.
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 assesses the effectiveness of FEMA’s commitment to increase public understanding of flood risks while working with insurance agents and companies nationally to encourage the purchase of flood insurance. This measure counts the number of flood insurance policies in force (PIF). Flood insurance policies are issued by private insurance carriers who participate in the “Write Your Own” segment of FEMA’s National Flood Insurance Program (NFIP), as well as policies sold by independent insurance agents through NFIP Direct. This measure aligns to the 2022-2026 FEMA Strategic Plan Goal 2: Lead Whole of Community in Climate Resilience which aims to build a climate resilient nation through risk reduction. Individual’s lack of awareness of flood risk they face, lack of awareness of flood damage not covered in homeowner policies, and price of flood insurance could adversely impact the results.
Scope of Data	The unit of analysis is the number of flood insurance policies in force. The population includes all flood insurance policies in force issued by private insurance carriers that participate in National Flood Insurance Program’s (NFIP) 'Write Your Own' (WYO) Program or sold by independent insurance agents and serviced by the NFIP Direct. The attribute is the policies are in force.
Data Source	Data for this measure is stored in the NFIP System of Record, Pivot. The transactions come into the Pivot system through daily/monthly reporting from the NFIP Write Your Own companies and NFIP Direct. Federal Insurance Directorate under Federal Insurance and Mitigation Agency (FIMA) is responsible for the Pivot and reporting the results.



Data Collection Methodology	NFIP Write Your Own companies and independent insurance agents enter policy information into Pivot. Analysts within FIMA use a .SQL file to retrieve the number of policies in force from Pivot. The measure is a total count of the number of flood insurance policies in force at the time of reporting.
Reliability Index	Reliable
Explanation of Data Reliability Check	FEMA’s Financial Control Plan and the Pivot Use Procedures set out the reporting requirements of insurance companies, both Write Your Own and NFIP Direct, which includes transactions for new business, renewals, endorsements, and cancellations. The system of record will validate policy submissions by either accepting or rejecting each transaction. Rejected policies must be corrected and resubmitted with time standards set out in FEMA procedures. Write Your Own companies and NFIP Direct must also reconcile individual policy transactions on a monthly basis.

Performance Measure	Percent of adults that have set aside money for emergencies (Retired Measure)
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





<p>Explanation of Data Reliability Check</p>	<p>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 <a href="https://www.census.gov/programs-surveys/popest/technical-documentation/methodology.html">https://www.census.gov/programs-surveys/popest/technical-documentation/methodology.html</a>. The program itself maintains a list of non-federal public authorities registered to use the Integrated Public Alert &amp; 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.</p>
--	---

<p>Performance Measure</p>	<p>Average annual percentage of administrative costs for major disaster field operations, as compared to total program costs</p>
<p>Program</p>	<p>Regional Operations</p>
<p>Description</p>	<p>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).</p>
<p>Scope of Data</p>	<p>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.</p>
<p>Data Source</p>	<p>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.</p>
<p>Data Collection Methodology</p>	<p>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</p>



	<p>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</p>
Reliability Index	Reliable
Explanation of Data Reliability Check	<p>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.</p>

Performance Measure	Average number of the incident staff to support small federally-declared disasters (Retired Measure)
Program	Response and Recovery
Description	<p>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.</p>
Scope of Data	<p>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</p>



	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	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 managers 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	Applicants' confidence rate for FEMA's Individuals and Households Program application process (New Measure)
Program	Response and Recovery
Description	This measure assesses the program's ability to assist people before, during, and after disasters by measuring applicants' satisfaction with the service they received. The application process is the first step in providing disaster assistance through specific FEMA Individual Assistance programs. The measure utilizes data from responses to a question in the FEMA Customer Experience Survey (OMB Control Number: 1601-0029) administered electronically to applicants with an email address. Respondents rate how strongly they agree with the statement "I am satisfied with the service I received from FEMA". All responses are included in the results. The insights derived from survey results will help drive improvements for FEMA policies and programs. However, the results will not be used to generalize the data beyond the scope of the sample.
Scope of Data	The unit of analysis is a single completed survey from a disaster survivor who applied for FEMA disaster assistance and has an e-mail address. The population is the total number of completed surveys from a random sample of disaster survivors who registered for assistance, indicated their preference of electronic communication, and provided a valid email address. Survey results are calculated using all available data from completed electronic surveys. The confidence interval for this survey is 95% +/- 5%. However, the results will not be used to generalize the data beyond the scope of the sample. The attribute is all



	<p>responses to the question. The average score is then used to calculate a normalized percentage to move from a 1-5 Likert scale to a 0-100% scale to accurately relay the applicant’s confidence based on their response to the question, “This interaction increased my confidence in FEMA” on a Likert Scale of 1-5 (1 strongly disagree, 5 strongly agree).</p>
Data Source	<p>The OMB filing for this survey was made under OMB Circular A-11 Section 280 which specifies “No attempt will be made to generalize the findings from these three groups of activities to be nationally representative or statistically valid”. Furthermore, the OMB Circular A-11 Section 280 implementation guidelines states, “Results will not be used to make statements representative of the universe of study, to produce statistical descriptions (careful, repeatable measurements), or to generalize the data beyond the scope of the sample.” We are in full compliance of this guidance. The FEMA Recovery Reporting and Analytics Division’s (RRAD) Customer Survey and Analysis Section (CSAS) uses the Medallia tool to administer the FEMA Customer Experience Survey (OMB Control Number: 1601-0029) electronically to disaster survivors who have applied for FEMA assistance and provided an email address. The question used for this measure is question one “I’m satisfied with the service received from FEMA”.</p>
Data Collection Methodology	<p>CSAS sends the FEMA Customer Experience survey to a random sample of disaster survivors via email two weeks after the disaster registration period begins and continues until the registration period closes. They export the results from the Medallia tool into the Enterprise Data Warehouse (EDW) / Organizational Data Store (ODS) database for storage every two weeks. Quarterly, CSAS generates reports and raw data from EDW and ODS and sends it to the RRAD Performance Measurement and Analysis Team (PMAT). PMAT then loads the raw data into PowerBi for automatic calculation of a normalized percentage using the average of all responses. The numerator is the average of all responses - 1. The denominator is 4.</p>
Reliability Index	<p>Reliable</p>
Explanation of Data Reliability Check	<p>CSAS monitors surveyors to control quality, and ensure data provided by applicants is recorded correctly. CSAS supervisors provide training and coaching to mitigate reliability issues during the recording of applicant answers. CSAS program analysts and statisticians review data after the surveys are complete to ensure data accurately reflects what the surveys captured. After accuracy is ensured, data are provided in an Excel format for performance measurement and uploaded to the Enterprise Data Warehouse (EDW) / Organizational Data Store (ODS) database for storage. The Performance Measurement and Analysis Team</p>



	(PMAT) compares the raw data to the CSAS results summary. These results are then peer reviewed and then a supervisor reviews the calculations. These steps ensure that the data are complete, accurate, and thoroughly reviewed.
--	--

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 (Retired Measure)
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



	<p>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.</p>
<p>Scope of Data</p>	<p>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.</p>
<p>Data Source</p>	<p>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.</p>
<p>Data Collection Methodology</p>	<p>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.</p>





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 applicants satisfied with the Public Assistance process and customer service (New Measure)
Program	Response and Recovery
Description	This measure assesses the program’s ability to evaluate Public Assistance (PA) applicants’ satisfaction with the PA program and customer service. The PA Assessment survey collects satisfaction information from applicants after they received an award. These applicants have progressed from requesting assistance to developing projects and then obtaining the award. The measure utilizes data from responses to a question in the FEMA Customer Experience Survey (OMB Control Number: 1601-0029) administered electronically to applicants with an email address. Respondents rate how strongly they agree with the statement “I am satisfied with the service I received from FEMA”. All responses are included in the results. The insights derived from survey results will help drive improvements for FEMA policies and programs. However, the results will not be used to generalize the data beyond the scope of the sample.
Scope of Data	The unit of analysis is a single completed survey from a disaster survivor who applied for FEMA disaster assistance and has an e-mail address. The population is the total number of completed surveys from a random sample of applicants who registered for assistance, indicated their preference of electronic communication, and provided a valid email address. Survey results are calculated using all available data from completed electronic surveys. The confidence interval for this survey is 70% of applicants with awards. However, the results will not be used to generalize the data beyond the scope of the sample. The attribute is applicants that have complete the project development process. Applicants that have not received an



	award are excluded from the Assessment survey and therefore from the measure. In the Assessment survey applicants will rate how strongly they agree with the statement “I am satisfied with the...” on a scale of 1 – 5 (1 being strongly disagree, 5 being strongly agree).
Data Source	The OMB filing for this survey was made under OMB Circular A-11 Section 280 which specifies “No attempt will be made to generalize the findings from these three groups of activities to be nationally representative or statistically valid”. Furthermore, the OMB Circular A-11 Section 280 implementation guidelines states, “Results will not be used to make statements representative of the universe of study, to produce statistical descriptions (careful, repeatable measurements), or to generalize the data beyond the scope of the sample.” We are in full compliance of this guidance. The FEMA Recovery Reporting and Analytics Division’s (RRAD) Customer Survey and Analysis Section (CSAS) uses the Medallia tool to administer the FEMA Customer Experience Survey (OMB Control Number: 1601-0029) electronically to disaster survivors who have applied for FEMA assistance and provided an email address. The question used for this measure is question one “I’m satisfied with the service received from FEMA”.
Data Collection Methodology	CSAS sends the FEMA Customer Experience survey to a random sample of disaster survivors via email two weeks after the disaster registration period begins and continues until the registration period closes. They export the results from the Medallia tool into the Enterprise Data Warehouse (EDW) / Organizational Data Store (ODS) database for storage every two weeks. Quarterly, CSAS generates reports and raw data from EDW and ODS and sends it to the RRAD Performance Measurement and Analysis Team (PMAT). PMAT then loads the raw data into PowerBi for automatic calculation of a normalized percentage using the average of all responses. The numerator is the average of five specific survey responses - 1. The denominator is 4.
Reliability Index	Reliable
Explanation of Data Reliability Check	CSAS monitors surveyors to control quality and ensure responses provided by applicants is recorded correctly. CSAS supervisors provide training and coaching to mitigate reliability issues during the recording of applicant answers. CSAS program analysts and statisticians review data after the surveys are complete to ensure data accurately reflects what the surveys captured. After accuracy is ensured, data are provided in an Excel format for performance measurement and uploaded to the Enterprise Data Warehouse (EDW) / Organizational Data Store (ODS) database for storage. The Performance Measurement and Analysis Team



	(PMAT) compares the raw data to the CSAS results summary. These results are then peer reviewed and then a supervisor reviews the calculations. These steps ensure 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 applicant’s confidence in FEMA (New Measure)
Program	Response and Recovery
Description	This measure assesses the program’s ability to assist people before, during, and after disasters by measuring an applicant’s confidence in FEMA after applying for disaster assistance. The application process is the first step in providing disaster assistance through specific FEMA Individual Assistance programs. The measure utilizes data from responses to a question in the FEMA Customer Experience Survey (OMB Control Number: 1601-0029) administered electronically to applicants with an email address. Respondents rate how strongly they agree with the statement “This interaction increased my confidence in FEMA”. All responses are included in the results. The insights derived from survey results will help drive improvements for FEMA policies and programs. However, the results will not be used to generalize the data beyond the scope of the sample.
Scope of Data	The unit of analysis is a single completed survey from a disaster survivor who applied for FEMA disaster assistance and has an e-mail address. The population is the total number of completed surveys from a random sample of disaster survivors who registered for assistance, indicated their preference of electronic communication, and provided a valid email address. Survey results are calculated using all available data from completed electronic surveys. The confidence interval for this survey is 95% +/- 5%. However, the results will not be used to generalize the data beyond the scope of the sample. The attribute is all responses to the question. The average score is then used to calculate a normalized percentage to move from a 1-5 Likert scale to a 0-100% scale to accurately relay the applicant’s



	confidence based on their response to the question, “This interaction increased my confidence in FEMA” on a Likert Scale of 1-5 (1 strongly disagree, 5 strongly agree).
Data Source	The OMB filing for this survey was made under OMB Circular A-11 Section 280 which specifies “No attempt will be made to generalize the findings from these three groups of activities to be nationally representative or statistically valid”. Furthermore, the OMB Circular A-11 Section 280 implementation guidelines states, “Results will not be used to make statements representative of the universe of study, to produce statistical descriptions (careful, repeatable measurements), or to generalize the data beyond the scope of the sample.” We are in full compliance of this guidance. The FEMA Recovery Reporting and Analytics Division’s (RRAD) Customer Survey and Analysis Section (CSAS) uses the Medallia tool to administer the FEMA Customer Experience Survey (OMB Control Number: 1601-0029) electronically to disaster survivors who have applied for FEMA assistance and provided an email address. The question used for this measure is question 2 “This interaction increased my confidence in FEMA”.
Data Collection Methodology	CSAS sends the FEMA Customer Experience survey to a random sample of disaster survivors via email two weeks after the disaster registration period begins and continues until the registration period closes. They export the results from the Medallia tool into the Enterprise Data Warehouse (EDW) / Organizational Data Store (ODS) database for storage every two weeks. Quarterly, CSAS generates reports and raw data from EDW and ODS and sends it to the RRAD Performance Measurement and Analysis Team (PMAT). PMAT then loads the raw data into PowerBi for automatic calculation of a normalized percentage using the average of all responses. The numerator is the average of all responses - 1. The denominator is 4.
Reliability Index	Reliable
Explanation of Data Reliability Check	CSAS monitors surveyors to control quality, and ensure data provided by applicants is recorded correctly. CSAS supervisors provide training and coaching to mitigate reliability issues during the recording of applicant answers. CSAS program analysts and statisticians review data after the surveys are complete to ensure data accurately reflects what the surveys captured. After accuracy is ensured, data are provided in an Excel format for performance measurement and uploaded to the Enterprise Data Warehouse (EDW) / Organizational Data Store (ODS) database for storage. The Performance Measurement and Analysis Team (PMAT) compares the raw data to the CSAS results summary. These results are then peer reviewed and then a supervisor





	reviews the calculations. These steps ensure that the data are complete, accurate, and thoroughly reviewed.
--	---

Performance Measure	Percent of Public Assistance project obligations completed within targeted timeframes (Retired Measure)
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)



	<p>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.</p>
Data Collection Methodology	<p>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.</p>
Reliability Index	<p>Reliable</p>
Explanation of Data Reliability Check	<p>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.</p>

**Federal Law Enforcement Training Centers (FLETC)**

Performance Measure	<p>Percent of Partner Organizations satisfied with Federal Law Enforcement Training Centers' training</p>
Program	<p>Law Enforcement Training</p>
Description	<p>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</p>



	<p>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.</p>
Scope of Data	<p>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.</p>
Data Source	<p>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.</p>
Data Collection Methodology	<p>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.</p>
Reliability Index	<p>Reliable</p>
Explanation of Data Reliability Check	<p>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</p>



	<p>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.</p>
--	---

**Office of Intelligence and Analysis (I&A)**

Performance Measure	Percent of finished intelligence products aligned to key intelligence questions
Program	Analysis and Operations
Description	<p>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.</p>
Scope of Data	<p>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 I&amp;A. Key Intelligence Questions are identified and periodically reviewed/ updated in the Program of Analysis.</p>
Data Source	<p>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.</p>
Data Collection Methodology	<p>Analysts begin work by initiating a project, tracking its flow through the SARA system, which captures the necessary data</p>



	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 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 (I&A'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 I&A. This measure ensures that I&A 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. I&A finished intelligence products that are ICD 203-compliant constitute a smaller subset of I&A's finished intelligence production, including products, Homeland Intelligence Todays, Intelligence Assessments, and Field Analysis Reports. I&A 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 I&A'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	I&A 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 (I&A'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 I&A's ICD 203-compliant finished intelligence production (denominator). I&A finished intelligence products that are ICD 203-compliant constitute a smaller subset of I&A'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



<p>Explanation of Data Reliability Check</p>	<p>I&amp;A 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.</p>
--	--

<p>Performance Measure</p>	<p>Percent of intelligence reports rated satisfactory and useful by customers</p>
<p>Program</p>	<p>Analysis and Operations</p>
<p>Description</p>	<p>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.</p>
<p>Scope of Data</p>	<p>The population of this measure is all customer feedback received from surveys appended to each I&amp;A 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.</p>
<p>Data Source</p>	<p>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.</p>
<p>Data Collection Methodology</p>	<p>Once the analyst produces a report, it moves to leadership review, which validates judgements contained in the report.</p>



	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 I&A senior leadership.

***U.S. Immigration and Customs Enforcement (ICE)***

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	Percent of detention facilities found in compliance with the national detention standards by receiving a final acceptable inspection rating (Retired Measure)
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 detention facilities that meet the subsequent 180-day reinspection (New Measure)
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 on their 180-day reinspection 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 non-citizens in immigration proceedings or awaiting removal to their countries do so in accordance with the Performance Based National Detention Standards.
Scope of Data	The unit of analysis for this measure is an adult facility on the Authorized Facility's List authorized to house ICE detainees through ERO Detention Management Control Program (DMCP) with an ADP greater than 10 that received a 180-day reinspection during the reporting period. The population is all adult facilities on the Authorized Facility's List authorized to house ICE detainees through ERO Detention Management Control Program (DMCP) that received a 180-day reinspection during the reporting period. Family residential centers, or ERO juvenile facilities, staging facilities, or holding rooms that may temporarily hold ICE detainees are not included. The attribute for each unit of analysis is whether or not the facility received an "acceptable" inspection rating.
Data Source	The 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 are compiled to determine the agency-wide percentage of facilities receiving acceptable or above rating.
Data Collection Methodology	Data for this measure is collected and evaluated by ERO inspectors. These 180-day reinspections 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. The percent is calculated by dividing those



	facilities that passed the 180-day reinspection by the total population those receiving a 180-day reinspection during the reporting period.
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	Number of human trafficking and child exploitation victims rescued or assisted
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 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.

Performance Measure	Number of stakeholder engagements conducted (New Measure)
Program	Office of the Principal Legal Advisor
Description	This measure assesses OPLA’s efforts to engage intra-governmental and external stakeholders relating to changes in its policies and the importance of its missions, including its efforts to preserve limited government resources to achieve just and fair outcomes in individual immigration cases, and reduce the backlog of cases pending before EOIR. Ensuring stakeholder alignment in addressing immigration enforcement provides opportunities to improve the transparency of OPLA’s actions and identify docket efficiency initiatives to improve case processing in immigration court. This measure aligns with the DHS objective to enforce U.S. immigration laws. External factors and changes in policies and regulations may lower the results independent of program actions.
Scope of Data	The unit of analysis is a planned stakeholder engagement. The population is all planned stakeholder engagements for the fiscal year. The attribute is whether a planned stakeholder engagement is conducted. All OPLA Field Locations and Headquarters leadership can initiate or participate in an intra-governmental or an external stakeholder engagement.
Data Source	Data from OPLA’s Field Legal Operations is collected on Excel spreadsheets and are submitted and maintained on the OPLA SharePoint site. The Strategic Management Division (SMD) Chief collects information regarding HQ leadership’s engagements through OPLA’s HQ leaders and their Special Counsel. At the end of each reporting period, the SMD Chief combines and tabulates the information to report the results.
Data Collection Methodology	OPLA Field Location Managers and Headquarters Leadership will be requested to report the results of intra-governmental and



	external stakeholder engagements. Then, the SMD Chief will extract all engagement files from OPLA HQ leadership and Field Location reporting and report quarterly and year-to-date results. The total of all completed stakeholder engagements will be aggregated and counted to get the result.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent data entry and retrieval errors, the Field Legal Operations Excel files are templated to include formatted fields. In addition, all relevant data are called out on the Excel template to ensure all data are provided. The SMD Chief collects additional information regarding HQ leadership engagements and reports that with the Field Location data. The SMD Chief and Field Legal Operations Special Counsel review each submission of completeness and accuracy. Any errors or omissions are requested to be completed by the submitting party. The SMD Chief will review collected data for consolidation and quarterly reporting prior to release.

Performance Measure	Number of stakeholder engagements related to the DHS civil immigration enforcement and removal priorities (Retired Measure)
Program	Office of the Principal Legal Advisor
Description	This measure captures OPLA's 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 by measuring the number of stakeholder engagements. Due to recent court rulings, this measure will not report FY 2022 results.

Performance Measure	Percent of removal orders secured that support current enforcement priorities (Retired Measure)
Program	Office of the Principal Legal Advisor
Description	This measure captures OPLA's success 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. Due to recent court rulings, this measure will not report FY 2022 results.





### Office of Homeland Security Situational Awareness (OSA)

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 (Retired Measure)
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 (NSED) period, as late NSED 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 NSED 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 <a href="https://hsin.dhs.gov">HTTPS://hsin.dhs.gov</a> . 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 follow-up, 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 (S&T)**

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.



### Transportation Security Administration (TSA)

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 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 Passengers whose Overall Satisfaction with TSA Screening was Positive (New Measure)
Program	Aviation Screening Operations
Description	This measure assesses effectiveness on how satisfied passengers are with TSA screening and is a gauge of both the trust and confidence that passengers have in TSA screening and the level of professionalism that passengers experience from the TSA workforce. This measure will represent the percentage of passengers who were surveyed and indicated “agree” or “strongly agree” (from the Likert scale) to the question of “I am satisfied with the service I received from TSA” or similar. All passengers must successfully complete security screening at a TSA passenger screening checkpoint before entering the sterile area of an airport and boarding a commercial flight. This



	includes the screening of their person and their accessible property. This measure aligns to the agency goal of maintaining a positive customer experience.
Scope of Data	The unit of analysis is a single passenger that completes checkpoint screening and an on-the-spot survey which a representative will request passengers to complete after checkpoint screening has been concluded, using live surveyors located at the checkpoint or via a website advertised to passengers. The population includes all passengers that successfully complete security screening at any TSA passenger screening checkpoint that are sampled when live surveyors are utilized. When sampling is used, only Category X, I, and II airports will be sampled, as Category III and IV airport do not have sufficient passenger throughput for a statistically significant sample (i.e., different regions, sizes, etc.). The attribute is whether the passenger had a positive experience by indicating “agree” or “strongly agree” (from the Likert scale) to the question of “I am satisfied with the service I received from TSA” or similar.
Data Source	The source of the data will be passenger responses to the passenger experience survey. The data will be initially captured and stored in non-TSA data storage systems associated with the live surveyors and/ or website contracted to conduct the surveys. The data will be exported each month and stored on TSA data storage systems (network drives and/ or SharePoint), which are managed by the Customer Service Branch. The data will be retained in accordance with established TSA record retention policies. The data will be used by the Customer Service Branch at monthly, quarterly, and yearly intervals for reports to agency senior leadership.
Data Collection Methodology	The process begins when a passenger completes TSA screening. The passenger will be offered the passenger experience survey either directly by a live surveyor or indirectly via checkpoint signage with a referral to a website. The passenger completes the passenger experience survey in one of the two methods described above. The passenger will complete the survey via a tablet when live surveyors are utilized; otherwise, the passenger will use a website-based survey to complete the survey. The completed passenger experience surveys will be exported to a compatible Excel spreadsheet format or CSV file. The Customer Service Branch will retrieve data from the spreadsheet functionalities to calculate the measure.
Reliability Index	Reliable
Explanation of Data Reliability Check	The passenger experience survey uses a standardized set of questions (all Paper Reduction Act approved) and responses (i.e., Likert scale) to collect passenger sentiment. The questions are



	<p>tailored to the TSA screening experience that the passenger just completed. The responses are limited to the five responses of the Likert scale. The Customer Service Branch will use spreadsheet functionalities to scrub the data for anomalous entries. These automated processes will flag anomalous entries for review and exclude them from calculations until such time as the anomalies are resolved. All calculations are automated by utilizing verified formulas.</p>
--	---

Performance Measure	Percent of Transportation Security Officers that achieve a first-time pass rate on the Image Interpretation Test
Program	Aviation Screening Operations
Description	<p>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.</p>
Scope of Data	<p>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.</p>
Data Source	<p>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.</p>
Data Collection Methodology	<p>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%</p>



	<p>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.</p>
Reliability Index	Reliable
Explanation of Data Reliability Check	<p>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.</p>

Performance Measure	Percent of air carriers operating from domestic airports in compliance with standard security programs
Program	Other Operations and Enforcement
Description	<p>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.</p>
Scope of Data	<p>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</p>





	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 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 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 Information 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



	<p>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.</p>
Scope of Data	<p>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.</p>
Data Source	<p>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).</p>
Data Collection Methodology	<p>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.</p>
Reliability Index	<p>Reliable</p>
Explanation of Data Reliability Check	<p>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,</p>



	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 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.



<p>Data Collection Methodology</p>	<p>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.</p>
<p>Reliability Index</p>	<p>Reliable</p>
<p>Explanation of Data Reliability Check</p>	<p>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.</p>

<p>Performance Measure</p>	<p>Percent of surface operations cybersecurity workforce personnel completing required cybersecurity training (New Measure)</p>
<p>Program</p>	<p>Other Operations and Enforcement</p>
<p>Description</p>	<p>This measure assesses the completion percentage of surface transportation operations personnel achieving annual cybersecurity-related training requirements. The composition of the Surface Operations workforce includes a variety of Headquarters, Regional and Field Personnel—Information Technology Specialists (IT), Transportation Security Specialists, Program Analysts, Surface Transportation Security Inspectors (TSIs) in both supervisory and non-supervisory roles that perform cybersecurity-related assignments. These assignments may include program management/reviews, assessments, inspections, and supporting engagement with stakeholders. Completion of cybersecurity training creates a cybersecurity</p>



	enriched surface operations workforce, improving staffing, education, and retention capabilities. Due to schedules, seasonal requirements, and training frequency, this measure will be reported on an annual basis.
Scope of Data	The unit of analysis is a single individual within TSA Surface Operations that supports cybersecurity related program, projects, assignments, and engagements. Training requirements are determined on an annual basis by TSA Surface Operations leadership based on operational needs and are assigned to employees via their Learning Plans. The population includes approximately 300 surface operations personnel that support cybersecurity related program, projects, assignments, and engagements. The total workforce number may vary from year to year based on staffing needs and funding constraints. The attribute is whether an individual has completed all required annual cybersecurity training.
Data Source	This measure gathers data employee learning plans and completion rates which are tracked in TSA’s Online Learning Center (OLC). OLC tracks learning requirements, due dates, and completion rates for both courses internally and externally. Internal trainings can be assigned to employees with a due date for completion. External training is captured in OLC by submission and approval of a SF-182. The SF-182 is submitted by the employee through the OLC for approval by the employee’s supervisor and added to the employee’s OLC Learning Plan. External trainings are also verified via course rosters or certificates of completion. All completed courses are available in an employee’s OLC record. OLC is managed by the Office of Training and Development, with Surface Operations maintaining an OLC Training Point of Contact (TPOC) for record entry, data management, and reporting.
Data Collection Methodology	TSA Surface Operations (SO) maintains written and electronic training records related to cybersecurity training completion and in OLC tracking. Analysts in the Surface Operations Exercises and Training Branch maintain an excel spreadsheet containing the names of personnel requiring cybersecurity training to ensure those individuals are registered for any required virtual OLC courses and external trainings. Upon completion of external training courses, the SO TPOC inputs course completion information into the OLC. This process permits tracking in the OLC by attendee name or class code. The TPOC can/will retrieve an OLC report, and the name rosters are then compared to SO staffing records to ensure accurate recording and to assist with determining future training needs.
Reliability Index	Reliable



<p>Explanation of Data Reliability Check</p>	<p>To prevent observation and assessment errors, OLC tracks assignment and completion of all courses within the online course library by employee. For external trainings, the SO TPOC runs an OLC report, and the name rosters are then compared to SO staffing records to ensure accurate recording and to assist with determining future training needs. Additionally, as an internal control/audit measure, SO compares class rosters with the class records maintained by external training vendors.</p>
--	---

<p>Performance Measure</p>	<p>Percent of TSA regulated entities inspected per fiscal year by Transportation Security Inspectors</p>
<p>Program</p>	<p>Other Operations and Enforcement</p>
<p>Description</p>	<p>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 entity's 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.</p>
<p>Scope of Data</p>	<p>The scope of this measure includes all U.S. regulated entities only that are subject to Transportation Security Administration transportation rules and regulations.</p>
<p>Data Source</p>	<p>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.</p>
<p>Data Collection Methodology</p>	<p>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.</p>
<p>Reliability Index</p>	<p>Reliable</p>



Explanation of Data Reliability Check	Data reliability is ensured through a series of actions. There are system record tracking audit trails and spot audit checks, followed by a management review and validation process at the headquarters level.
---------------------------------------	---

### ***U.S. Citizenship and Immigration Services (USCIS)***

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



	<p>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.</p>
Reliability Index	Reliable
Explanation of Data Reliability Check	<p>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.</p>

Performance Measure	Percent of system generated notifications related to national security, public safety, or fraud reviewed and addressed for pending applications within 60 days
Program	Fraud Prevention and Detection
Description	<p>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.</p>
Scope of Data	<p>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.</p>
Data Source	<p>The FDNS Reports and Analysis Branch (RAB) uses SAS –a statistical analysis software package—to extract data from FDNS-</p>





	DS, FDNS' system of record, to report the data. The SGNs originate from ATLAS screening. Records of SGNs reside in FDNS-DS. Information available in FDNS-DS includes each SGN and time stamps for the creation and disposition of each SGN.
Data Collection Methodology	The triage of SGNs requires 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 triaged or pending for more than 60 calendar days during the reporting period, and the dates of their creation and resolution. Staff compile reports using SAS to extract data from FDNS-DS. Staff use SAS to calculate duration, in calendar 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 in-scope SGNs in a given reporting period, excluding untriated SGNs 60 or fewer calendar days from creation, is the denominator. The percentage of these two quantities is the result for the reporting period and is cumulative across the FY.
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. 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	Average processing time for adjustment of status to Permanent Resident Applications (I-485) (in months) (New Measure)
Program	Immigration Services
Description	This measure assesses the ability of the Field Operations Directorate (FOD) to meet adjudication processing goals for the Form I-485, Application to Register Permanent Residence or Adjust status. This measure supports the DHS Strategic Goal Objective of Administering the Immigration System to ensure it is administered efficiently and fairly. External factors such as immigration policies, economic security, and issues like the COVID-19 pandemic could have a negative impact on the results for this measure.
Scope of Data	The unit of analysis is a single I-485 application that has been adjudicated. The application could have been received before the reporting period, but an application is only included if it is



	completed during the reporting period. The population is all I-485 applications that were adjudicated during the reporting period. The measure is the processing time each application takes to be adjudicated. Processing time is defined as the elapsed time between the received date and the decision date for completed applications.
Data Source	Data for this measure are stored in the system of record, Electronic Immigration System (ELIS) and in the Computer Linked Adjudication Information Management System (CLAIMS 3).
Data Collection Methodology	The data for each application is entered into the ELIS and CLAIMS 3 data systems. The USCIS Office of Performance and Quality (OPQ) exports data via SAS statistical analysis software a week following the end of the quarter to ensure all actions taking place in the reporting quarter have been recorded. Data is pulled if an application has been adjudicated within the time period being assessed. The average processing time calculation is calculated by taking the processing time for all applications included in the reporting period and dividing by the total number applications completed during the time period. This results in a number of days and is converted to months.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data will be provided one week after the quarter ends to ensure that all electronic systems have been completely updated. An OPQ data analyst will be assigned to provide the data on a quarterly basis. After the data have been produced a second OPQ data analyst will conduct a peer-review of the data to ensure completeness, reliability, and accuracy. In addition, an OPQ manager conducts a final quality check of the performance measure data.

Performance Measure	Average processing time for detainees claiming Credible Fear (in days) (New Measure)
Program	Immigration Services
Description	This measure assesses how quickly the program processes the credible fear claims of individuals held in ICE-operated detention centers. Specifically, for individuals claiming persecution or a well-founded fear of persecution or harm on account of his or her race, religion, nationality, membership in a particular social group, or political opinion if returned to their country. This measure reports the average number of days between individuals expressing their fear and the program completing the case. By evaluating how quickly the credible fear claims of detained individuals are completed, the program can assess the



	effectiveness of a critical element of the agency's goal to secure borders through effective use of detention capacity.
Scope of Data	The unit of analysis is the amount of time (in days) from when USCIS receives the completed packet transferring jurisdiction for an individual who expresses their claim of persecution or a well-founded fear of persecution or harm on account of their race, religion, nationality, membership in a particular social group, or political opinion if returned to their country and when the program completes processing their claim. The population only includes individuals who are placed in ICE-operated detention facilities. The average processing time for the population is 14 days or less.
Data Source	Data for this measure is stored in the Global case management system. The system contains data on when a credible fear case is initiated and when the final determination when the case is made. Global is maintained by USCIS and data is extracted and consolidated into Excel and PDF formats. The Standard, Management Analysis and Reporting Tool (SMART), and Tableau data visualization and business analysis tools are two web-based performance analysis tools used to create dashboards and reports of the data.
Data Collection Methodology	The data for each credible fear case is entered into Global from the time that USCIS receives the completed packet transferring jurisdiction for the individual who made the credible fear claim until the credible fear claim determination is made. USCIS exports data from Global using SMART and Tableau to create dashboards and reports. Data collection using these tools can be fully automated once the reports and/or dashboards are created. The average processing time calculation adds the processing time for all completed credible fear cases included in the reporting period, and this number is then divided by total number of cases in the data set.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent data entry and retrieval errors, Global uses formatted fields and dropdown menus. Standardized reporting scripts help prevent errors in downloading the data from Global to dashboards and reports. To prevent analysis and calculation errors, standard and repeatable reporting templates are used. Data for performance reporting are typically provided no later than 15 days after the quarter ends to ensure that all electronic systems have been completely updated. The reported data is reviewed by at least two analysts for completeness, reliability, and accuracy. 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. Data reliability reviews are also integrated as controls within most processes.
--	---

Performance Measure	Average processing time for naturalization applications (N-400) (in months) (New Measure)
Program	Immigration Services
Description	This measure assesses the ability of the Field Operations Directorate (FOD) to meet its published adjudication processing goals for the Applications for Naturalization (N-400). An N-400 is filed by an individual applying to become a United States citizen. This measure supports the DHS Strategic Goal Objective of Administering the Immigration System to ensure it is administered efficiently and fairly. External factors such as immigration policies, economic security, and issues like the COVID-19 pandemic could have a negative impact on the results for this measure.
Scope of Data	The unit of analysis is a single N-400 application that has been adjudicated. The application could have been received before the reporting period, but an application is only included if adjudication is completed during the reporting period. The population is all N-400 applications that were adjudicated during the reporting period. The measure population includes naturalization applications based on eligibility from service in the Armed Forces of the United States. The attribute is the processing time each application takes to be fully adjudicated. Processing time is defined as the elapsed time between the received date and the decision date for completed applications.
Data Source	Data for this measure are stored in the system of record the Electronic Immigration System (ELIS).
Data Collection Methodology	The data for each application is entered into the ELIS System from the time the application starts until the application is adjudicated and a decision has been made. The USCIS Office of Performance and Quality (OPQ) exports data via SAS statistical analysis software program a week following the end of the quarter to ensure all actions taking place in the reporting quarter have been updated. The average processing time calculation adds the processing time for all applications included in the reporting period, and this number is then divided by total number applications in the set. This result is then converted to months.
Reliability Index	Reliable



<p>Explanation of Data Reliability Check</p>	<p>Data will be provided one week after the quarter ends to ensure that all electronic systems have been completely updated. An OPQ data analyst will be assigned to provide the data on a quarterly basis. After the data have been produced a second OPQ data analyst will conduct a peer-review of the data to ensure completeness, reliability, and accuracy. Prior to delivery to OCFO, an OPQ manager will conduct a final quality check of the performance measure data.</p>
--	---

<p>Performance Measure</p>	<p>Average processing time to adjudicate form I-129 (Petition for Nonimmigrant Worker) (in months) (New Measure)</p>
<p>Program</p>	<p>Immigration Services</p>
<p>Description</p>	<p>This measure assesses the ability of the Service Center Operations Directorate (SCOPS) to meet its published adjudication processing goals of Form I-129, Petition for a Nonimmigrant Worker. An I-129 is filed on behalf of a nonimmigrant worker to come to the United States temporarily to perform services or labor, or to receive training, as an E-1, E-2, E-3, H-1B, H-2A, H-2B, H-3, L-1, O-1, O-2, P-1, P-1S, P-2, P-2S, P-3, P-3S, Q-1, R-1, or TN nonimmigrant worker. This process time information will help determine if the organization has the capability and capacity to process petitions and will also be used to make operational decisions. This measure supports the DHS Strategic Goal Objective of Administering the Immigration System to ensure it is administered efficiently and fairly. External factors such as immigration policies, economic security, and issues like the COVID-19 pandemic could have a negative impact on the results for this measure.</p>
<p>Scope of Data</p>	<p>The unit of analysis is a single I-129 petition that has been adjudicated. The petition could have started adjudication before the reporting period, but a petition is only included if it is completed during the reporting period. The population is all I-129 petitions that were adjudicated during the reporting period. Eligible categories include E-1, E-2, E-3, H-1B, H-2A, H-2B, H-3, L-1, O-1, O-2, P-1, P-1S, P-2, P-2S, P-3, P-3S, Q-1, R-1, or TN nonimmigrant worker. The measure excludes premium processing petitions. The attribute is the processing time each petition takes to be adjudicated. Processing time is defined as the elapsed time between the received date and the decision date for completed petitions.</p>
<p>Data Source</p>	<p>Data for this measure are stored in the system of record, Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR), for petitions adjudicated in the Electronic Immigration System (ELIS). The eCISCOR system</p>



	contains data on when a petition is initiated and when it has been adjudicated. The system is maintained by the Office of Information Technology. On an hourly basis, data from ELIS is, consolidated into the eCISCOR system.
Data Collection Methodology	The data for each petition is entered into the ELIS System from the time the petition starts until the petition is adjudicated and a decision has been made. The USCIS Office of Performance and Quality (OPQ) exports data from eCISCOR via SAS statistical analysis software program a week following the end of the quarter to ensure all actions taking place in the reporting quarter have been updated in eCISCOR. Data is pulled if a petition has been adjudicated within the time period being assessed. The average processing time calculation adds the processing time for all petition included in the reporting period, and this number is then divided by total number petition in the set. This result is then converted to months.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent data entry and retrieval errors, the ELIS System uses formatted fields and dropdown menus. An HQ analyst conducts automated reviews of the entered data looking for missing or anomalous entries. Standardized reporting scripts and the use of SAS commands help prevent errors in downloading the data from eCISCOR. To prevent analysis and calculation errors, standard and repeatable reporting templates are used. Data will be provided one week after the quarter ends to ensure that all electronic systems have been completely updated. An OPQ data analyst will be assigned to provide the data on a quarterly basis. After the data have been produced a second OPQ data analyst will conduct a peer-review of the data to ensure completeness, reliability, and accuracy. Quarterly and annual results are subjected to a multi-level review that checks for anomalies or discontinuities. Prior to delivery to OCFO, an OPQ manager will conduct a final quality check of the performance measure data.

Performance Measure	Average processing time to adjudicate form I-140 (Immigrant Petition for Alien Worker) (in months) (New Measure)
Program	Immigration Services
Description	This measure assesses the ability of Service Center Operations (SCOPS) to meet its published adjudication processing goals for the Immigrant Petition for Alien Worker (I-140). An I-140 is filed on behalf of an immigrant worker to come to the United States permanently to perform services or labor as an E11, E12, E13, E21, E31, E32, or EW3 immigrant worker. This measure supports the DHS Strategic Goal Objective of Administering the





	Immigration System to ensure it is administered efficiently and fairly. External factors such as immigration policies, economic security, and issues like the COVID-19 pandemic could have a negative impact on the results for this measure.
Scope of Data	The unit of analysis is a single I-140 petition that has been adjudicated. The petition could have started adjudication before the reporting period, but a petition is only included if it is completed during the reporting period. The population is all I-140 petitions that were adjudicated during the reporting period. Eligible categories include E11, E12, E13, E21, E31, E32, or EW3 immigrant workers. The measure population excludes premium processing petitions. The attribute is the processing time each petition takes to be fully adjudicated. Processing time is defined as the elapsed time between the received date and the decision date for completed petitions.
Data Source	Data for this measure are stored in the system of record, Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR), for petitions adjudicated in the Electronic Immigration System (ELIS). The eCISCOR system contains data on when a petition is initiated and when it has been fully adjudicated. The system is maintained by the Office of Information Technology. On an hourly basis, data from ELIS is, consolidated into the eCISCOR system.
Data Collection Methodology	The data for each petition is entered into the ELIS System from the time the petition starts until the petition is adjudicated and a decision has been made. The USCIS Office of Performance and Quality (OPQ) exports data from eCISCOR via SAS statistical analysis software program a week following the end of the quarter to ensure all actions taking place in the reporting quarter have been updated in eCISCOR. Data is pulled if a petition has been adjudicated within the time period being assessed. The average processing time calculation adds the processing time for all petitions included in the reporting period, and this number is then divided by total number petitions in the set. This result is then converted to months.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent data entry and retrieval errors, the ELIS System uses formatted fields and dropdown menus. An HQ analyst conducts automated reviews of the entered data looking for missing or anomalous entries. Standardized reporting scripts and the use of SAS commands help prevent errors in downloading the data from eCISCOR. To prevent analysis and calculation errors, standard and repeatable reporting templates are used. Data will be provided one week after the quarter ends to ensure that all electronic systems have been completely updated. An OPQ data



	<p>analyst will be assigned to provide the data on a quarterly basis. After the data have been produced a second OPQ data analyst will conduct a peer-review of the data to ensure completeness, reliability, and accuracy. Quarterly and annual results are subjected to a multi-level review that checks for anomalies or discontinuities. Prior to delivery to OCFO, an OPQ manager will conduct a final quality check of the performance measure data.</p>
--	--

Performance Measure	Number of asylum determinations
Program	Immigration Services
Description	<p>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.</p>
Scope of Data	<p>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.</p>
Data Source	<p>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 reports (in Excel or pdf format) using a web-based reporting tool.</p>
Data Collection Methodology	<p>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</p>



	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 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 $\pm 5\%$ 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 Immigration Officers who are trained to perform their duties within six months of entry on duty (Retired Measure)
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 pending cases that are considered backlog (New Measure)
Program	Immigration Services





<p>Description</p>	<p>The measure assesses the proportion of pending cases considered as backlog. Backlog is defined as the number of cases pending within the government’s control that exceed target processing time for each form. This measure will help senior leadership assess the effectiveness of the agency’s multiple initiatives for reducing the backlog. These initiatives include strategic staffing, technology enhancements, regulatory and policy changes, and the use of overtime. This measure supports the DHS Strategic Goal Objective of Administering the Immigration System to ensure it is administered efficiently and fairly. External factors such as immigration policies, economic security, and issues like the COVID-19 pandemic could have a negative impact on the results for this measure.</p>
<p>Scope of Data</p>	<p>The unit of analysis is a pending case for a major form type. Major form types, and their target processing times are located at this link: <a href="https://www.uscis.gov/newsroom/news-releases/uscis-announces-new-actions-to-reduce-backlogs-expand-premium-processing-and-provide-relief-to-work">https://www.uscis.gov/newsroom/news-releases/uscis-announces-new-actions-to-reduce-backlogs-expand-premium-processing-and-provide-relief-to-work</a>. The population is all pending cases for major form types. For a pending case to be considered in the backlog, its current processing time must exceed the publicly posted processing time at the URL above. Current processing time is defined as the elapsed time between the received date and the date the of reporting.</p>
<p>Data Source</p>	<p>Data for this measure are stored in the system of record, Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR), for applications adjudicated in the Electronic Immigration System (ELIS). The eCISCOR system contains data on when an application is initiated and when it has been fully adjudicated. The system is maintained by the Office of Information Technology. On an hourly basis, data from ELIS is, consolidated into the eCISCOR system. From this system, the USCIS National Performance Report (NPR) is produced by the Office of Performance and Quality (OPQ). The NPR is a monthly report that displays by each form type, the number of forms received, completed, and pending, and calculates the backlog by form type. The NPR utilizes system of record data. The NPR is recognized as the official USCIS source for the number of monthly receipts, completions, and backlog.</p>
<p>Data Collection Methodology</p>	<p>The data for each form is entered into the ELIS System from the time the application starts until the application is fully adjudicated and a decision has been made. The USCIS Office of Performance and Quality (OPQ) exports data from eCISCOR eight weeks following the end of the quarter to ensure all actions have been properly captured and updated, which is then used to create the NPR. From this information, the total backlog of cases</p>



	is divided by the total population of pending cases to calculate the percent of pending cases that are considered backlog.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent data entry and retrieval errors, the ELIS System uses formatted fields and dropdown menus. An HQ analyst conducts automated reviews of the entered data looking for missing or anomalous entries. Standardized reporting scripts and the use of SAS commands help prevent errors in downloading the data from eCISCOR. To prevent analysis and calculation errors, standard and repeatable reporting templates are used. OPQ conducts monthly quality checks during the creation of the NPR report. OPQ maintains a standard operating procedure that outlines the requirements of the quality review process for the NPR. As part of the process one analyst creates the NPR, a second senior analyst reviews the NPR for anomalies and finally a supervisor reviews the quality check and signs off on the report prior to publication on an internal USCIS webpage. An external auditing firm conducts an audit of the NPR to ensure the OPQ process for validation is appropriate and to ensure accuracy of the data.

Performance Measure	Percent of refugee and asylum adjudications that were legally sufficient
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



	<p>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.</p>
Data Source	<p>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.</p>
Data Collection Methodology	<p>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.</p>
Reliability Index	<p>Reliable</p>
Explanation of Data Reliability Check	<p>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.</p>
Performance Measure	<p>Percent of respondents satisfied with the citizenship and immigration-related support received from the USCIS Contact Center</p>



Program	Immigration Services
Description	<p>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.</p>
Scope of Data	<p>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.</p>
Data Source	<p>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.</p>
Data Collection Methodology	<p>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</p>



	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 with increased test scores after attending courses funded through USCIS Grant Programs
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	Total number of attendees at USCIS naturalization sessions (New Measure)
Program	Immigration Services





<p>Description</p>	<p>This measure assesses the effectiveness of the program’s effort toward public engagement. These engagements include, but are not limited to, presentations by leadership, webinars, trainings, stakeholder events, conference presentations, summits, panel discussions, meetings, roundtables, and serving as guest speakers. Information sessions will include scheduled engagements, both virtual and in-person, conducted for the public under the coordination of the USCIS Office of Citizenship, Partnerships, and Engagement (OCPE). This measure supports the DHS Strategic Goal Objective of Administering the Immigration System to ensure it is administered efficiently and fairly. External factors such as immigration policies and issues like the COVID-19 pandemic could have a negative impact on the results for this measure.</p>
<p>Scope of Data</p>	<p>The unit of analysis for this measure is a completed naturalization engagement. Naturalization engagements include, but not limited to, presentations by leadership, webinars, trainings, stakeholder events, conference presentations, summits, panel discussions, meetings, roundtables, and serving as guest speakers. The population is all completed naturalization engagements within the period being reported. The attribute to be measured are the number of attendees at USCIS naturalization sessions. An attendee will be included in the count if they attend all or part of an engagement/event designed for a specific audience. In the case of a multi-day or multi-session event intended for a single audience/population and with a single, specific purpose, each attendee will only be counted once. In the case of a multi-session event/engagement intended for multiple audiences and each session with a distinct purpose, attendees will be counted separately for each session.</p>
<p>Data Source</p>	<p>Data for this measure are collected and stored in a SharePoint database currently containing all field- and headquarters-reported engagement information. The system contains data entered by field and headquarters Community Relations staff into a form in the SharePoint Engagement Calendar and includes numbers of attendees, focus area of the engagement, and engagement notes. The Office of Citizenship, Partnership, and Engagement (OCPE) maintains the SharePoint site and manages the data fields to capture current data and new filed for future data needs. OCPE also manages the report generation to report the results quarterly.</p>
<p>Data Collection Methodology</p>	<p>Following each event/engagement, the office or sub-office coordinating the event will be required to complete the OCPE Engagement Report Form in SharePoint. Onsite staff at each event/engagement will take attendance utilizing standard sign-in sheets. In cases where this is not possible, onsite staff will take a</p>



	<p>headcount of attendees. For virtual engagements, the attendance logs will be pulled by staff from the hosting office. The data for each engagement is entered into the SharePoint database from the field offices (local engagements) and by headquarters staff (national engagements). The Public Engagement staff consolidates the data into a monthly report. Quarterly, an Analyst from OCPE will run a query in the SharePoint database and download the data into an Excel file. The number of attendees is calculated by adding together the reported number of attendees from all engagements during the reporting period.</p>
Reliability Index	Reliable
Explanation of Data Reliability Check	<p>To prevent data entry and retrieval errors, the SharePoint database uses formatted fields and dropdown menus. Senior staff from each of the divisions within OCPE review the reported results from all of the engagements under their division on a quarterly basis to ensure that the numbers are all being accurately reported for the events/engagements for which they are responsible. Standardized reporting scripts help prevent errors in downloading the data from the SharePoint database. To prevent analysis and calculation errors, standard and repeatable reporting templates are used. Final numbers will go from OCPE through the Office of External Affairs' clearance process prior to being reported to the Office of the Chief Financial Officer.</p>

**U.S. Coast Guard (USCG)**

Performance Measure	Availability of maritime navigation aids
Program	Marine Transportation System Management
Description	<p>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.</p>
Scope of Data	<p>The measure is the hours short range Aids to Navigation were available as a percent of total hours they were expected to be available.</p>
Data Source	<p>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.</p>



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	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



	<p>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.</p>
Reliability Index	Reliable
Explanation of Data Reliability Check	<p>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.</p>

Performance Measure	Number of breaches at high-risk maritime facilities
Program	Maritime Prevention
Description	<p>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 subsets 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.</p>





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 serious marine incidents
Program	Maritime Prevention
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 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 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,



	<p>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.</p>
Scope of Data	<p>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.</p>
Data Source	<p>MSRO data comes from the Marine Information for Safety and Law Enforcement (MISLE) database what is managed by Office of C4 &amp; 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.</p>
Data Collection Methodology	<p>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</p>



	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.

**U.S. Secret Service (USSS)**

Performance Measure	Amount of cyber-financial crime loss prevented (in billions) (Retired Measure)
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



	<p>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.</p>
Reliability Index	Reliable
Explanation of Data Reliability Check	<p>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.</p>

Performance Measure	Financial Crime Loss Recovered (in billions) (New Measure)
Program	Field Operations
Description	<p>The measure includes recovered financial loss attributed to the investigation of the crime. The recovered amount is the sum of asset forfeiture, returned payment transactions, and loss recovered through a criminal investigation.</p>
Scope of Data	<p>The calculation of the loss recovered amount is based on a sum of the amount recovered through an asset forfeiture process (administrative or judicial), returned payments to victims, and the amount recovered through criminal financial investigations.</p>
Data Source	<p>Data is recorded in FIRS by personnel assigned to the Office of Investigations (INV), which encompasses domestic and foreign field offices and headquarters divisions. The data is based on loss recovered attributable to a crime.</p>
Data Collection Methodology	<p>The calculation of the loss recovered amount is based on the sum value recovered through the asset forfeiture process (administrative or judicial), returned payments to victims, and the amount recovered through criminal financial investigations. The asset forfeiture process requires precise calculations of the assets seized and forfeited either administratively or through a judicial process, and their value in USD. This amount is reported by investigative personnel and validated by CID Asset Forfeiture Branch personnel. The amount recovered other than through asset forfeiture includes assets returned via financial</p>





	transactions, or other means which do not require forfeiture. This amount is calculated as part of the investigation and reported by investigative personnel. The sum of these amounts is calculated and reported after closure of the case in FIRS as Crime Loss Recovered.
Reliability Index	Reliable
Explanation of Data Reliability Check	There are numerous checks in place to ensure reliable reporting of this information. In addition to supervisory reviews and approvals of the case records associated with this measure, the asset forfeiture process is a multi-step process controlled and validated by the CID Asset Forfeiture Branch and attorney-advisors. The amount recovered separate from the asset forfeiture process requires corresponding documentation, such as financial transactions.

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) (Retired Measure)
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 cybercrime case violation codes and the dates these cases were closed. The data is then aggregated up to the highest levels by month, year, office, and Service-wide. This information is then reported through various management and statistical reports to Secret Service headquarters program managers, field offices, and the Department of Homeland Security.
Reliability Index	Reliable
Explanation of Data Reliability Check	FIRS has many features built into it in order to provide the most accurate data possible. Along with the mainframe security features, there are many edit checks built into the applications to ensure the accuracy and validity of the data. Only authorized headquarters and field personnel have access to the applications, and they are governed by specific procedures to input case and arrest data. An annual audit is conducted and recurring verification reports are generated and reviewed to reduce errors and ensure data accuracy.



Performance Measure	Number of law enforcement individuals trained in cybercrime and 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 cybercrime.
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	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 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.



