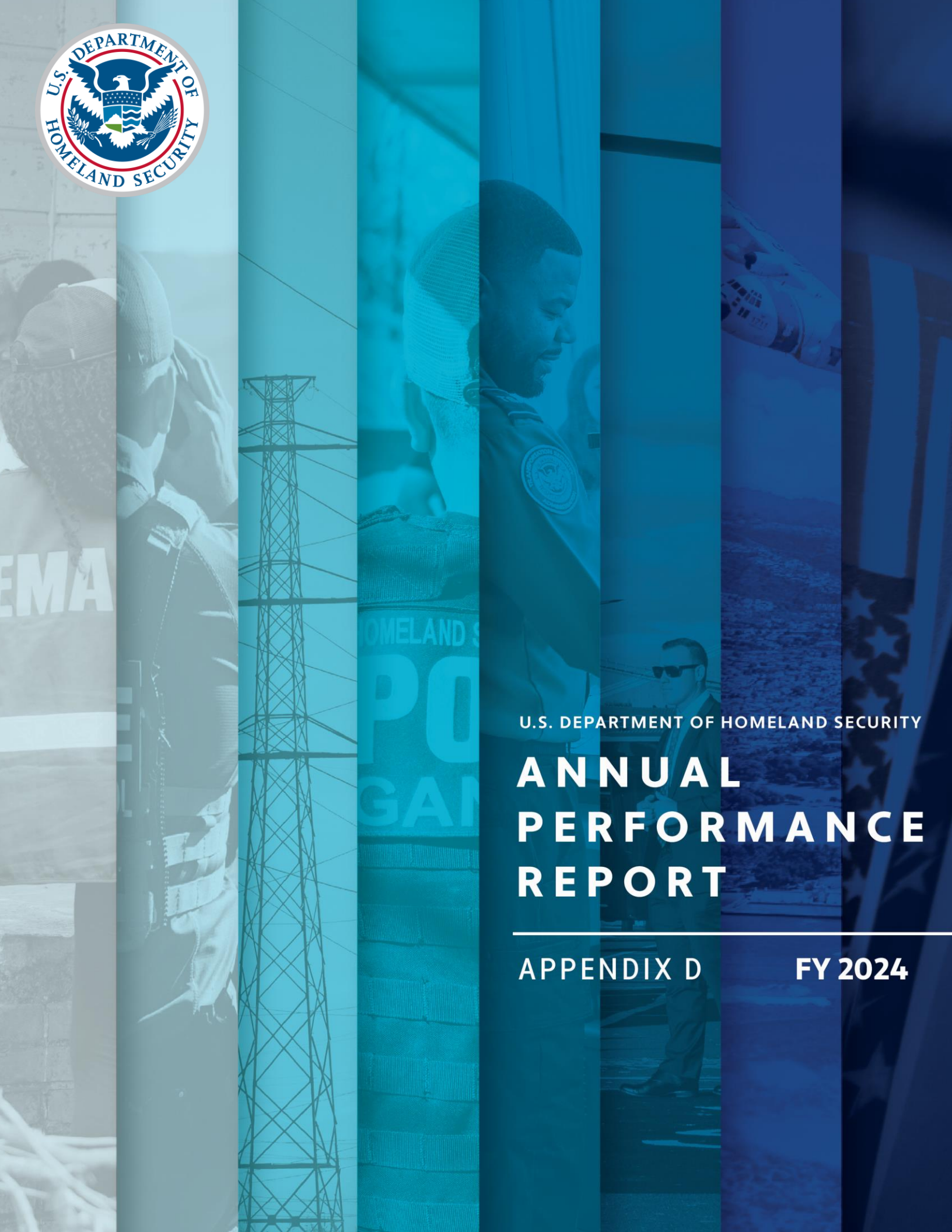

U.S. DEPARTMENT OF HOMELAND SECURITY

ANNUAL PERFORMANCE REPORT

APPENDIX D **FY 2024**

APPENDIX D: MEASURE DESCRIPTIONS, DATA COLLECTION METHODOLOGIES, AND COMPLETENESS AND RELIABILITY INFORMATION

About This Section

The U.S. Department of Homeland Security's (DHS) Annual Performance Report for fiscal year (FY) 2024 provides a comprehensive assessment of the Department's performance throughout the year. This report includes key performance measure results and insights into our strategic initiatives, reflecting our commitment to enhancing the safety and security of our Nation.

For FY 2024, the Department's Performance and Accountability Reports consist of the following three reports:

- DHS Agency Financial Report (AFR) | Publication Date: November 15, 2024
- DHS Annual Performance Report (APR) | Publication Date: January 17, 2025
- DHS Annual Performance Plan (APP) | Publication Date: March 2025[1]

Appendix D of the APR provides a detailed, tabular listing of all performance measures included in the report. Before the measure listing, the appendix provides an overview of the Department's performance data verification and validation process.

Each measure listed includes its description, scope of data, data source, collection methodology, reliability index, and an explanation of the data reliability check. The appendix also shows the alignment between each measure and the corresponding strategic objective from the Department's 2023 Quadrennial Homeland Security Review (QHSR). Learn more about the QHSR here: https://www.dhs.gov/publication/2023-quadrennial-homeland-security-review-qhsr

The next page includes a table of contents for easy navigation. The appendix is organized by the Department's Operational Components: U.S. Customs and Border Protection (CBP); the Cybersecurity and Infrastructure Security Agency (CISA); the Federal Emergency Management Agency (FEMA); U.S. Immigration and Customs Enforcement (ICE); the Transportation Security Administration (TSA); U.S. Coast Guard (USCG); U.S. Citizenship and Immigration Services (USCIS); and U.S. Secret Service (USSS). The appendix concludes with measures listed for the Department's Support Components and key DHS Management Directorate (MGMT) lines of business, including: the Countering Weapons of Mass Destruction Office (CWMD); the Federal Law Enforcement Training Centers (FLETC); DHS MGMT's Federal Protective Service (FPS) and Office of the Chief Human Capital Officer (OCHCO); the Office of Intelligence and Analysis (I&A); the Office of Homeland Security Situational Awareness (OSA); and the Science and Technology Directorate (S&T).

[1] Please note that the above dates for Department's FY 2026 APP is subject to change. The APR and APP are generally published as a single, consolidated document. However, in years where there is a transition in Presidential Administration, performance is reported under the outgoing Administration, while planning activities are conducted under the incoming Administration. Thus, performance targets are not reported in the FY 2024 AFR or APR, but will be included in the FY 2026 APP, which we anticipate being published concurrently with the first full President's Budget of the new Administration. See Office of Management and Budget, Circular A-11, Part 6, *The Federal Performance Framework for Improving Program and Service Delivery*, Section 210.4

Table of Contents

Performance Data Verification and Validation Process

DHS 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 Office of Management and Budget (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.[2]

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 Performance Measure Definition Form (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

DHS has used an annual continuous improvement process as a means to mature the breadth and scope of our publicly reported set of measures. This process employs a tool known as the PMDF, which provides a structured format to describe every measure we

[2] Note: OMB Circular A-11, Part 6, *The Federal Performance Framework for Improving Program Service Delivery*, Section 240.26. 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.

publicly report in our performance deliverables. The PMDF provides instructions to DHS Components on completing all data fields and includes elements such as the measure name, description, scope of data, where the data is collected and stored, a summary of the data collection and computation process, and what processes exist to ensure the accuracy and reliability of the data. These data fields on the form reflect the U.S. Government Accountability Office's (GAO's) recommended elements regarding data quality.[3] 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 an appendix to our APR.

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 information technology (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 like 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 Performance Improvement Officers (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 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 Component Head assurance statements attesting to the completeness and reliability of performance data.

[3] 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.

Independent Assessment of the Completeness and Reliability of Performance Measure Data

DHS 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 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 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 DHS Office of the Chief Financial Officer, 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 AFR 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.

U.S. Customs and Border Protection

Performance Measure	Percent of detected conventional aircraft incursions resolved along all borders of the United States
Program	Air and Marine Operations
Description	This measure represents the percent of conventional aircraft detected visually or by sensor technology, suspected of unauthorized or 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 U.S, was continuously visually or electronically monitored while over the U.S., and has exited U.S. airspace and is no longer a threat to national security.
Strategic Alignment	Objective 2.1: Secure and Manage Air, Land, and Maritime Borders
Scope of Data	The unit of analysis is an individual unauthorized or illegitimate airspace incursions by conventional aircraft. The population is all unauthorized or illegitimate airspace incursions by conventional aircraft along all borders of the US. The scope of data excludes reporting of unconventional aircraft, such as ultra-light aircraft or small unmanned aircraft systems/drones, etc. The incursion is considered resolved when: 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. The incursion is considered unresolved when the aircraft is not located by responding or other authorities and has presumably remained within the US.
Data Source	Validated air incursions are entered and maintained in the Air & Marine Operations Surveillance System (AMOSS) and the Tasking Operations and Management Information System (TOMIS), owned by the program and maintained by the Component Office of Information and Technology. Program Managers at the AMOC are responsible for retrieving the data

	from AMOSS, which houses the data, every quarter to calculate the air incursion rate.
Data Collection Methodology	After an incursion is established, information is transmitted to the appropriate air branch for a response. 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. The results are then entered into and tracked in the AMOSS, a system of record, and summarized on a monthly basis. Program Managers at the AMOC are responsible for retrieving the data from AMOSS each quarter. 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. Initial incursion reports are documented in the AMOSS and reviewed for accuracy by the line Supervisor. The data is validated by a second level Supervisor or the Operations' Supervisor. Data is pulled quarterly for further review by the responsible Program Manager who verifies the accuracy and compiles the quarterly findings. If errors are found during any phase of the review process, the report is sent back to the original author for updating/correcting and resubmitted as necessary. Excel spreadsheets are maintained and reviewed periodically for updates or changes throughout the reporting FY.

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 removable individuals who have entered the U.S. illegally and been apprehended or encountered multiple times by the U.S. Border Patrol along the Southwest Border. It serves as an indicator of the potential impact of the Border Patrol's application of consequence on affecting future illegal crossing activity into the United States. Those crossing the border illegally, from first-time offenders to people with criminal records, face an array of available consequences. Efficient application of effective consequences

	for illegal border crossers intends, over time, to reduce overall recidivism. The measure factors in border crossing activity within a rolling, 12-month period.
Strategic Alignment	Objective 2.1: Secure and Manage Air, Land, and Maritime Borders
Scope of Data	The unit of analysis is an individual deportable illegal entrant who has or receives a Fingerprint Identification Number (FIN). The population includes only those apprehensions or encounters that occur within the U.S. Border Patrol's nine sectors along the Southwest Border. Fingerprints are not taken and FINs are not generated for some individuals younger than age 14, older than age 86, and some humanitarian cases. Those without a FIN are not included in calculating the data for this measure. The attribute counted is whether a deportable illegal entrant has been apprehended under Title 8 or encountered under Title 42 multiple times within a rolling, 12-month rolling period.
Data Source	Apprehension and encounter data are captured by Border Patrol agents at the station level and entered in the e3 Processing (e3) system at the time of processing. All data entered via e3 updates automatically after entry and it 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) Division. Source data is collected within e3 as apprehended/encountered subjects are processed at U.S. Border Patrol stations. Analysts within SDI query that data as needed. The physical database is owned and maintained by ICE.
Data Collection Methodology	Apprehended/encountered subjects are processed, including collection of detailed facts related to the event and subjects, as well as biometrics (fingerprints, facial/retinal scans, etc.). Data relating to apprehensions are entered into e3 by Border Patrol agents at the station level as part of standard processing procedures. With that data and biometrics, a subject-exclusive FIN is generated. Data input can be made by any agent who knows the details of the event. This data is typically reviewed regularly at the station, sector, or Headquarters level to note trends and provide feedback to the field on operational activity. The calculation is completed by SDI at Border Patrol Headquarters with a data query of FINs for a time period under examination (rolling 12 months in this measure) to determine the number of individuals apprehended multiple times, then dividing it by the total number of individuals apprehended/encountered during the same duration.

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.
Strategic Alignment	Objective 2.1: Secure and Manage Air, Land, and Maritime Borders
Scope of Data	The unit of analysis is an individual response to a geospatial intelligence-informed report of potential illicit activity in remote areas along the Southern and Northern land border (excluding Alaska) that U.S. Border Patrol sectors have determined to be low flow and low risk. Response is defined as the time when U.S. Border Patrol Agent arrives at the coordinates for a site determined to have shown potential indication of illicit activity, as designated and communicated by CBP's Office of Intelligence (OI). The population for this measure encompasses all geospatial intelligence-informed reports of potential illicit activity

	in remote areas along the Southern and Northern land border that U.S. Border Patrol sectors determined to be low flow and low risk. This measure does not include the maritime domain. The attribute counted in this measure is when a U.S. Border Patrol agent arrives at the site and investigates evidence of potentially illicit activity within 24 hours of the OI alert.
Data Source	Data for this measure is stored in CBP's Intelligence Reporting System – Next Generation (IRS-NG) and maintained by CBP's Office of Information Technology. A U.S. Border Patrol Assistant Chief assigned to OI extracts the Field Information Reports (FIR) data into an Excel spreadsheet, calculates the response times, and then determines the percentage of all notifications that agents reached the designated coordinates within 24 hours. The IRS-NG contains all data relevant to this measure. The results are then provided to analysts in the Strategic Planning and Analysis Directorate's Performance Reporting and Evaluation Division, which reports the results to U.S. Border Patrol leadership and to other relevant parties.
Data Collection Methodology	Using outputs from unmanned systems or other U.S. Government collection platforms, OI analysts alert appropriate U.S. Border Patrol sectors to the indication of potential illicit activity. Sectors deploy U.S. Border Patrol agents to respond to the site and investigate for evidence of 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. A U.S. Border Patrol Assistant Chief assigned to OI extracts the data from FIRs into an Excel spreadsheet, calculates the response times, and then determines the percentage of all notifications in which agents reached the site within 24 hours.
Reliability Index	Reliable
Explanation of Data Reliability Check	In the field, the Sector Intelligence Unit (SIU) Patrol Agent In Charge reviews and considers approval on all FIR documentation prior to submission to the OI. After the result is calculated, it is then transmitted to the Performance Reporting and Evaluation Division with sector specific information, including number of notifications and the percent of responses within 24 hours. Analysts review the data over quarters to identify trends and any potential anomalies. The aggregate information, as well as the data itself, is shared with the Border Patrol Chief and the Chief of the Law Enforcement Operations Directorate to confirm awareness and determine any needs for sector planning 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 interdicted (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 compares interdictions to the total of detected illegal entrants, which adds those determined to have evaded apprehension. Border Patrol achieves desired results by maximizing the apprehension of detected illegal entrants, confirming that illegal entrants return to the country from which they entered, and by minimizing the number of persons who evade apprehension and can no longer be pursued (a Got-Away Border Zone [GA-b] in zones contiguous to the international border or a Got-Away Interior Zone [GA-i] in enforcement zones having no direct nexus to the international border). This measure is a key indicator of the Border Patrol's law enforcement response and resolution impact.
Strategic Alignment	Objective 2.1: Secure and Manage Air, Land, and Maritime Borders
Scope of Data	Scope is subjects detected entering illegally in Southwest Border areas that are south of the northernmost checkpoint within a given area of responsibility. In border zones, it includes all Apprehensions (App), Encounters, Turn-Backs (TB), and GA-b. In non-border zones, GA-i replaces GA-b. An App 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-b is a subject associated with a Tracking Sign-cutting and Modeling (TSM) event initiated within a border zone who is a) classified as being involved in illicit, cross-border activity; b) not turned back; and c) no longer being actively pursued by agents. A GA-i is a subject associated with a TSM event initiated within an interior zone who is: a) classified as being involved in illicit, cross-border activity; and b) no longer being actively pursued by agents. A TB is a subject who, after making an illegal entry on the Southwest Border of the United States, returns to Mexico.
Data Source	Border Patrol agents capture Apprehension, Encounters, GA-b, GA-i, and TB data at the station level in several systems. Apprehensions and encounters are entered into the e3 Processing (e3) system. All data entered via e3 resides in EID, the official system of record for this data, which is under the purview of the Border Patrol Headquarters SDI Unit. The physical

	database is owned and maintained by ICE. GA-b, GA-i, and TB are recorded in the Intelligent Computer Assisted Detection (ICAD) TSM application, which resides with the U.S. Border Patrol. TSM is under the purview of and is owned by the U.S. Border Patrol's Enforcement Systems Unit.
Data Collection Methodology	Data relating to apprehensions and encounters are entered into e3 by Border Patrol Agents (BPAs) at the station level as part of the standardized processing procedure. BPAs use standard definitions for determining when to report a subject as a GA-b, GA-i, or TB in the TSM system. Some subjects can be observed directly as evading apprehension/encounter or turning back; others are acknowledged as GA-b, GA-i, or TB after agents 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 SDI Unit; the numerator is the sum of apprehensions and encounters and TBs, divided by the total entries, which is the sum of apprehensions, encounters, TB, GA-b, and GA-i.
Reliability Index	Reliable
Explanation of Data Reliability Check	Patrol Agents in Charge ensure all agents at their respective stations are aware of and use proper definitions for apprehensions, encounters, GA-b's, GA-i's, and TB's. They also ensure the necessary communication takes place between and among sectors and stations to ensure accurate documentation of subjects who may have crossed more than one station's area of responsibility. In addition to station-level safeguards, SDI validates data integrity by using various data quality reports. The integrity of TB, GA-b, and GA-i 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 the Customs Trade Partnership Against Terrorism (CTPAT) as a share of the total value of all cargo imported. CBP works with the trade community through this 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.
Strategic Alignment	Objective 2.2: Expedite Lawful Trade and Travel
Scope of Data	The unit of analysis is an individual cargo shipment and the attribute counted is its monetary value imported through CTPAT. The population of this measure includes all cargo imported through CTPAT. A variety of trade actors participate in this program such as importers, carriers, brokers, consolidators/third-party logistics providers, marine port-authority and terminal operators, and foreign manufacturers. Each CTPAT partner is assigned a unique identification number that is entered in the Automated Targeting System (ATS) and the Automated Commercial Environment (ACE) with each unique import-entry shipment.
Data Source	CBP stores relevant data on cargo imports in two CBP information technology systems, ATS and ACE. The systems contain data on import-entry number, including individual lines with a Harmonized Tariff Schedule of U.S. numbers and monetary line values. Reports for this measure are extracted from the ACE Reports module and the ATS Analytical Selectivity Program. CBP's Office of Field Operations National Targeting Center and the Office of Information and Technology (OIT) manage ATS and the Office of International Trade (OT) and the OIT manage ACE. OT extracts data on all shipments from ATS and ACE on a quarterly basis.
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. 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 and multiplying by 100 to convert to a percentage.
Reliability Index	Reliable

Explanation of Data Reliability Check	Both field-level and headquarters (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. The data entry in ATS and ACE is automated and also includes some screens that contain drop downs menus and specialized field formatting. The retrieval of data is automated through routines built from extract queries which included drop down menus and specific fields.

Performance Measure	Percent of import revenue successfully collected
Program	Trade Operations
Description	This measure assesses the effectiveness of ensuring that the importers pay the proper amount of taxes and duties owed on imports. Importers must deposit the revenue owed, which they estimate based on type of import, declared value, country of origin, and quantity being imported. CBP impacts the results by implementing enforcement actions and providing guidance and estimation tools that serve to reduce importer fraud, negligence, and misunderstanding in estimating revenue owed. Results are used to determine the need for additional or changed policies, enforcement actions, and guidance. This measure aligns to the goal of protecting national economic security, facilitating fair trade, supporting the health and safety of the American people, and ensuring a level playing field for U.S. industry. External factors such as foreign governments that support importer noncompliance and unforeseen changes in policy and trades laws may result in underpayment of import revenue.
Strategic Alignment	Objective 2.2: Expedite Lawful Trade and Travel
Scope of Data	The unit of analysis is an import (i.e., a commodity or set of merchandise being imported) as defined by an entry line on the CBP Entry Summary Form 7501 that describes the import (e.g., type, value, origin, etc.). The attribute is the net of importers' over- and under-payments of duties and taxes owed on the import. The population includes all of the imports for a given time period, excluding non-electronic informal entries. Each year, the Trade Compliance Measurement (TCM) program creates a stratified sample based on sampling rules (aka user defined rules) that account for changes in the import population and risk factors. A post-entry review of the selected sample is used to identify the amount of over-/underpayment for each import (entry line) in the sample. The net total under/overpayment across imports is known as the revenue

	gap. The revenue gap for the sample is used to estimate the revenue for the population with a 95 percent confidence level.
Data Source	Data resides in CBP's ATS with User Defined Rules (UDR) that help identify the sample. Program staff record findings from the TCM review in CBP's ACE information technology system, using ACE's Validation Activity (VA) function. On a monthly basis, a TCM analyst download the data from ATS into a local MS Access datafile for analysis. The CBP Performance Management and Analysis Division (PMAD) within the Office of Accountability is responsible for preparing a report of the measure results, provided by TCM, to CBP leadership and reporting them to PA&E. Since the post-entry reviews of the samples are not completed until January 31 of the following fiscal year, the annual result reported at the end of the current fiscal year is an estimate. The estimate is updated in the one-number system once the final result is available.
Data Collection Methodology	The determination of the under/overpayment of revenues owed on the import in the sample is carried out by teams of import entry specialists located in the CBP field offices. Each office is responsible to review entry lines for imports under their jurisdiction. After receiving a sample of entry lines via ACE VA, each review team checks the importer's estimate of validate the duties, taxes, and fees owed for each import and records the amount of under-overpayment with a Validation Activity Determination (VAD) stored in ACE. A TCM statistician retrieves the VAD data in ACE using SQUEL, transfers it to an MS Access datafile, uses standardized Statistical Analysis System (SAS) commands to calculate the measure result for a given period. The statistician sends the measure results for a given period to PMAD. The calculation is [1-(Estimated Revenue Gap/Total Collectable Revenue)] x100.
Reliability Index	Reliable
Explanation of Data Reliability Check	HQ staff host quarterly conference calls with field locations for open discussion of any issues and provides reports to field locations in the event requiring remediation. Analysts document this oversight, sharing this documentation annually with outside auditors as evidence of program control.

Performance Measure	Percent of imports compliant with U.S. trade laws
Program	Trade Operations
Description	This measure gauges the results of an annual CBP review of imports into the U.S., which assesses imports' compliance with U.S. trade laws, including laws related to customs revenue.

	CBP's 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. A statistically valid random sample of transactions are reviewed to ensure that imports remain legally compliant and free of major discrepancies.
Strategic Alignment	Objective 2.2: Expedite Lawful Trade and Travel
Scope of Data	The unit of analysis is each entry summary line found on Form 7501 via ACE. When an import enters the United States, it must have an "Entry Summary" (Form 7501). This is used by CBP to verify the accuracy of information about the imported commodity. The Entry Summary is submitted electronically and includes entry summary lines. The population consists of all entry summary lines from the reporting period, limited to those with certain entry type codes. The entry type code is a two-digit code where the first digit indicates the general category of the entry (e.g., consumption = 0, informal = 1) and the second digit specifies the processing type within that category. The attribute under examination is whether an entry summary line passes a major discrepancy (e.g., clerical error, illegal transshipment, etc.) review by an import specialist. Each entry summary line is rated as pass or fail and passes (is compliant) if no major discrepancy is found.
Data Source	CBP stores relevant data on imports in two CBP information technology systems, ACE and ATS. ACE is the system of record for import Entry Summaries and contains pertinent data on imports such as carrier, country of origin, manufacturer, importer number, description of merchandise, and merchandise value. An automated process passes entry summary lines from ACE to the ATS Import Targeting module where a random sample is selected for review. The import specialists review the entry summary lines and record the review results in the ATS Entry Summary Findings (ESF) module. CBP's Office of International Trade (OT) and OIT manage ACE; the Office of Field Operations' National Targeting Center and OIT manage ATS. Each quarter the OT Operations Directorate mathematician using the TCM program, extracts the results from the ATS ESF dashboard and projects the population statistics.
Data Collection Methodology	Import specialists continuously review entry summary lines selected for TCM review. Each fiscal year, program staff define rules in ATS to randomly select incoming imports for review. Import specialists record their findings in the ATS Entry Summary Findings module. An OT Operations Division mathematician processes exam results by labeling import-entry records containing major discrepancies. Examples include a

	discrepancy in value or a clerical error producing a revenue loss exceeding $1,000, an intellectual property rights violation, or a country-of-origin discrepancy for an item with a value in the top two thirds for the product class. The mathematician then determines the share of the sample which includes a major discrepancy under criteria for each sampling component. The overall discrepancy rate is computed as a weighted sum of the component discrepancy rates. This Major Transactional Discrepancy rate is subtracted from 1 and multiplied by 100 to determine the result.
Reliability Index	Reliable
Explanation of Data Reliability Check	Based on user defined rules, the ATS Import Targeting module selects a random sample of entry summary lines from incoming goods for review. This opens a review order in the ATS entry summary dashboard. Each CBP field office reviews the identified summary line transaction for compliance and records their findings in the ATS Entry Summary Findings module. A mathematician resident in OT's Operations Division extracts the Entry Summary Findings data from ATS monthly and computes preliminary statistics monthly as well as final statistics at year end.

Performance Measure	Percent of inbound cargo identified as potentially high-risk that is assessed or scanned prior to departure or arrival at a U.S. port of entry
Program	Trade Operations
Description	This measure reports the percent of international cargo coming to the U.S. via air, land, and sea, which CBP identified as potentially high-risk and then assessed or scanned prior to departure from a foreign port of origin or upon arrival at a U.S. port of entry to address security concerns. CBP assesses risk associated with a particular cargo shipment using 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.
Strategic Alignment	Objective 2.2: Expedite Lawful Trade and Travel

Scope of Data	The unit of analysis is an individual shipment firing to a National Security Hot List (NSHL) at a U.S. port of entry (POE) and has been identified as potentially high-risk using CBP's ATS scenario-based modeling and algorithms. The population is all shipments identified as potentially high-risk. Shipments include all cargo from international mail to a palletized commercial shipment of packaged items in the land, sea, or air environments destined for a POE. The attribute counted is whether an inbound cargo identified as potentially high-risk was assessed or scanned prior to departure or at arrival at a U.S. port of entry. A shipment is considered assessed or scanned when a final disposition status is determined.
Data Source	Data is stored in Borderstat, the primary reporting tool managed by the CBP Office of Field Operations. The system includes data such as 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 POE. CBP continuously collects and maintains shipment information on systems of record owned by CBP, including the Automated Commercial System (ACS), the Automated Export System (AES), ACE, TECS, and systems owned by partner governments and the private sector. All systems feed data in real time to ATS. The ATS Exam Findings Module (EFM) contains the data used by the program to determine the disposition of cargo flagged as potentially high-risk. Officers enter findings into these systems as cargo is processed. The National Targeting Center Cargo Division reports the results.
Data Collection Methodology	All data sources and systems stated above feed data in real time to ATS, which assesses the security risk associated with each shipment. When a shipment is identified by ATS as high risk CBP officers continuously review and assess information in ATS on high-risk shipments; resolve or mitigate security concerns; determine cases requiring further examination; and record findings from this review in ATS EFM. Review occurs prior to departure, during transport, and at arrival at a U.S. port of entry. When a case's final disposition is determined by a CBP officer, the status is noted in the shipments record and the case is closed.
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

	Headquarters 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.
Strategic Alignment	Objective 2.2: Expedite Lawful Trade and Travel
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.

Cybersecurity and Infrastructure Security Agency

Performance Measure	Number of targeted hunts of Federal Civilian Executive Branch agencies leveraging Endpoint Detection and Response Persistent Access Capability under CISA's National Defense Authorization Act authorities
Program	Cybersecurity Division
Description	This measure counts the number of Federal Civilian Executive Branch (FCEB) targeted hunts leveraging Endpoint Detection and Response Persistent Access Capability (EDR PAC), with an overall goal of uncovering unknown anomalous and/or malicious activity. Agencies are chosen through operational priorities set by CSD's Threat Hunting Chief of Operations. Targeted Hunt operations include a comprehensive (host, network, and cloud telemetry) review, triage, and baselining of an agency's corporate environment to identify technology/services patterns and trends. These operations also include industrial control systems and operational technology environments. Outputs from hunts are utilized by tactical and operational staff; and senior leaders to inform mission resources and actions, Operational Visibility investments, and external outreach (Binding Operational Directives, Emergency Directives, Cybersecurity Alerts). These hunts lessen the impact of or prevent national service degradation, theft of proprietary and/or intellectual property, and prevent harm to the public.
Strategic Alignment	Objective 4.1: Support the Cybersecurity of Federal Civilian Networks
Scope of Data	Operations will establish the prioritization list for targeted hunts, these efforts will be limited to agencies that have been onboarded to EDR PAC. Unit of analysis is a completed targeted hunt. A targeted hunt is deemed complete once there is a finalized operations report, which is shared only with the targeted agency. Other operational artifacts include documented/updated operational tickets, playbooks, and knowledge articles.
Data Source	Data for these operations will be stored in the CISA ticketing system of record – TARDIS. Artifacts associated with the activity will be stored within CSD's operational networks meant for storing customer data.

Data Collection Methodology	At the end of each quarter, a Threat Hunting (TH) analyst from the Targeted Hunt team runs a query for 'completed targeted hunts' from TARDIS (ServiceNow is replacement system). The TH Analyst retrieves and calculates the total number each quarter and inputs this as the measure 'Quarterly Result' for reporting.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent observation and assessment error, the Targeted Hunt Lead reviews the 'Quarterly Result' data prior to reporting. To prevent data entry and retrieval errors, the data entry screen for TARDIS includes formatted fields and dropdown menus. To prevent analysis and calculation errors, the TH Analyst uses formula-based spreadsheet calculations where necessary to assist in arriving at the result and reflects this within the 'Quarterly Result'. The number is reviewed by multiple staff prior to final submission.

Performance Measure	Percent of vulnerable systems notified under the Ransomware Vulnerability Warning Pilot that have been mitigated
Program	Cybersecurity Division
Description	This measure reports the percent of stakeholders that have mitigated vulnerable systems after notification under the Ransomware Vulnerability Warning Pilot (RVWP). Through RVWP, CISA leverages existing authorities and technology to proactively identify systems that contain security vulnerabilities associated with ransomware attacks. Once affected systems are identified, regional cybersecurity personnel notify system owners of identified vulnerabilities. CISA encourages system owners to mitigate identified vulnerabilities in a timely manner and conducts regular follow-up to determine whether system owners are mitigating identified vulnerabilities after notification under RVWP. Measure results are used by CISA senior leadership to inform decision making and by RVWP team members and collaborating CISA divisions to inform operations. The primary external factor that affects measure results is stakeholder capacity and capability to mitigate vulnerabilities identified under RVWP.
Strategic Alignment	Objective 4.1: Support the Cybersecurity of Federal Civilian Networks
Scope of Data	The unit of analysis is a single Internet Protocol (IP) address belonging to a system participating in RVWP and the population is all IP addresses participating in the pilot. The attribute for the measure is whether the port of a vulnerable device associated with a given IP address is later found by CISA to be "closed" or

	"open." After system owners have been notified regarding vulnerabilities identified under RVWP, CISA conducts follow-up to determine if the vulnerability has been mitigated. If the port of the device associated with a given IP address and system is closed, the vulnerability is considered mitigated. If the port is open, the vulnerability is not considered mitigated.
Data Source	CISA RVWP analysts gather data regarding RVWP notifications, associated IP addresses, identified vulnerabilities, and associated mitigation statuses from ServiceNow primarily through Shodan. Managed by the CISA Joint Cyber Defense Collaborative (JCDC), the entity notification platform in ServiceNow is a cloud-based information management system that supports a range of push and pull communications with RVWP partners, from general document sharing to the distribution of notifications regarding potential vulnerabilities. RVWP also collects data from Shodan, a search engine primarily used by cybersecurity professionals, law enforcement agencies, and other researchers to identify publicly accessible internet connected devices. CISA leverages an Application Programming Interface (API) to consolidate the needed raw data from Shodan to ServiceNow and into an Excel file that is then used for additional analysis and calculation of measure results.
Data Collection Methodology	CISA RVWP analysts leverage the Shodan API to streamline data collection. CISA leverages a custom script to compare relevant data between the systems and identify vulnerabilities which have been successfully mitigated. The API helps CISA analysts efficiently consolidate the raw information from their review of Shodan data into an Excel file that uses formulas to automate the calculation of measure results and the results are uploaded into ServiceNow. This measure is calculated by comparing the number of system vulnerabilities mitigated under RVWP to the total number of IP addresses and associated devices included in the pilot, expressed as a percentage.
Reliability Index	Reliable
Explanation of Data Reliability Check	Both ServiceNow and Shodan have controls in place to ensure reliability and mitigate data entry or extraction errors, such as drop-down menus, required fields, and automated checks for duplicate information. The Excel file that houses the raw data utilized by CISA RVWP to calculate measure results also has data controls such as drop-down menus to mitigate data entry or extraction errors. Data in ServiceNow related to the pilot program is monitored regularly, and while measure results are calculated automatically through use of an API and Excel

	formulas, results are also manually reviewed several times and then approved by program leadership before reporting.

Performance Measure	Percent of all state and territory emergency communications interoperability markers assessed at the highest levels
Program	Emergency Communications Division
Description	This measure identifies the current maturity level of emergency communications interoperability components across the nation, as assessed against best practices known as "interoperability markers" defined by CISA and the National Council of Statewide Interoperability Coordinators (NCSWIC). Each state and territory self-assess the maturity of their emergency communications interoperability components against all markers, which cover a range of factors. States and territories with a marker identified as "defined" or "optimized" are operating at the highest levels of interoperability for that marker. In FY 2025, CISA and NCSWIC are implementing the next generation of markers (Version 2.0), which will help to improve emergency communications capabilities and interoperability throughout the nation. Performance targets will be adjusted in FY 2025 to give states and territories the time to enhance capabilities and adopt best practices established in the next generation of interoperability markers.
Strategic Alignment	Objective 4.2: Strengthen the Security and Resilience of Critical Infrastructure
Scope of Data	The unit of analysis is a single state or territory self-assessment of the maturity level of a single emergency communications interoperability component, as assessed against best practices known as interoperability markers established by the CISA and NCSWIC. The population includes all states and territories' self-assessments for all markers. States and territories evaluate their interoperability capability along one of three maturity ratings for each of the assessed markers: initial, defined, or optimized. "Initial" indicates little to no maturity reached on a particular marker, "defined" indicates a sufficient level of maturity, and "optimized" indicates the highest level of maturity. The attribute for this measure is whether the state or territory's interoperability capability was self-assessed as "defined" or "optimized" for each of the markers.
Data Source	CISA staff, including the Performance Management Team from CISA's Emergency Communications Division (ECD) and Emergency Communications Coordinators from the Integrated Operations Division (IOD), coordinate with the Statewide Interoperability Coordinator (SWIC) for each state and territory to

	support their annual self-assessment. Following the assessment, CISA consolidates its findings using a Power BI tool, capturing data related to the maturity levels for emergency communications interoperability markers (i.e., initial, defined, or optimized), as well as other contextual information generated during the self-assessment. ECD staff manage the Power BI tool and the overall dataset.
Data Collection Methodology	Each quarter, the ECD Performance Management Team will extract the data needed for this measure from the Power BI dashboard using a query that filters for defined and optimized ratings for all the markers assessed or updated during the reporting period. Power BI functionalities automatically calculate measure results by comparing the number of defined and optimized ratings to the total number of ratings for the reporting period, expressed as a percentage.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data is self-reported by SWICs with assistance and guidance from ECD's Performance Management Team and IOD's Emergency Communications Coordinators to ensure consistency. These CISA personnel review and validate information with SWICs on a regular basis to ensure the latest data is being tracked to measure progress. The Power BI tool in which this information is stored has controls to mitigate data entry and extraction errors, such as drop-down menus and mechanisms to identify potentially duplicate information. While measure results are calculated automatically using Power BI functionalities, they are also reviewed manually and approved by relevant program leadership prior to reporting to CISA, DHS, or other stakeholders.

Performance Measure	Percent of landline priority calls successfully connected using the Government Emergency Telecommunications Service Landline Network
Program	Emergency Communications Division
Description	This measure assesses the reliability and effectiveness of the Government Emergency Telecommunications Service (GETS) by reflecting the call completion rate (CCR) made through the service. The CCR is the percent of calls that authorized GETS subscribers successfully complete via the landline telephone network to their intended audience (e.g., person, location, system) as compared to the total number of attempted calls. GETS is accessible to authorized users, such as public safety and critical infrastructure partners, at any time and is considered a resilience tool for users to ensure interoperability

	through priority calls completed during times of network congestion caused by all-hazard scenarios, including natural or manmade disasters.
Strategic Alignment	Objective 4.2: Strengthen the Security and Resilience of Critical Infrastructure
Scope of Data	The unit of analysis is a single GETS call attempt, regardless of it being connected or not, and the population for the measure is all GETS call attempts for the reporting period. GETS can be leveraged 24/7 by authorized users for all-hazard scenarios, including during designated "Code Red" events, National Level Exercises (NLEs), natural or manmade disasters, and other scenarios that might contribute to increased network congestion. Again, the population includes all attempted GETS calls for the reporting period. The attribute for this measure is whether or not an authorized GETS subscriber successfully connects and completes their call with their intended audience (e.g., person, location, system).
Data Source	Data is obtained though contractually required Monthly Performance Reports (MPRs) provided by AT&T, Sprint, and Verizon. These reports contain information on daily GETS call attempts including, but not limited to, 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 (e.g., answered, busy, no answer). When a "Code Red" event or other significant all-hazard scenario occurs, each carrier also provides an Emergency Performance Report (EPR) within 24 hours of the event. An EPR contains the same information as an MPR and enables ECD to rapidly leverage GETS data for analysis and decision-making purposes. While carriers maintain source data on MPRs and EPRs, this data is also internally stored and managed by ECD's Priority Communication Services (PCS) Subdivision. Measure results are reported as needed to CISA and DHS leadership.
Data Collection Methodology	Each quarter, ECD's PCS Subdivision analyzes all MPRs and EPRs for the reporting period to calculate overall and event-specific call completion rates, the latter of which becomes part of the population for determining the overall completion rate. PCS consolidates this information in an Excel spreadsheet that uses filter and formula functions to automatically calculate measure results. Measure results are calculated as the number of GETS calls successfully completed during the reporting period, compared to the total number of attempted GETS calls during the reporting period, expressed as a percentage. If one or more "Code Red" events or other scenarios that would cause network congestion occurs during the reporting period,

	additional narrative description is provided alongside the overall completion rate for additional context on the event-specific call completion rates.
Reliability Index	Reliable
Explanation of Data Reliability Check	Carrier data is recorded, processed, and shared with CISA based on contractual and industry standards that carriers must work to meet. Once the data is received, processed, and stored by CISA, and to prevent data entry and retrieval errors, the PCS Subdivision uses an Excel spreadsheet with data validation functions to require key data elements, prohibit inappropriate data entries, and limit choices to pre-determined options. To that end, the Subdivision also manages access to the Excel spreadsheet using SharePoint permissions. To prevent data analysis and calculation errors, the Excel spreadsheet leverages filter and formula functions to automatically calculate measure results, which are reviewed several times by Subdivision staff prior to submitting for final review and approval. To prevent observation and assessment error, ECD and PCS leadership review and approve all measure results prior to reporting.

Performance Measure	Percent of wireless priority calls successfully connected using the Wireless Priority Service
Program	Emergency Communications Division
Description	This measure assesses the reliability and effectiveness of the Wireless Priority Service (WPS) by reflecting the call completion rate made through the service. The call completion rate is the percent of calls that authorized WPS subscribers successfully complete to their intended audience (e.g., person, location, system) as compared to the total number of attempted calls. WPS provides subscribers, such as public safety and critical infrastructure partners, with priority access to wireless networks at any time and is considered a resilience tool for users to ensure interoperability through priority calls completed during times of network congestion caused by all-hazard scenarios, including natural or manmade disasters.
Strategic Alignment	Objective 4.2: Strengthen the Security and Resilience of Critical Infrastructure
Scope of Data	The unit of analysis is a single WPS call attempt, regardless of it being connected or not, and the population for the measure is all WPS call attempts for the reporting period. WPS can be leveraged 24/7 by authorized users for all-hazard scenarios, including during designated “Code Red” events, National Level Exercises (NLEs), natural or manmade disasters, and other

	scenarios that might contribute to increased network congestion. Again, the population includes all attempted WPS calls for the reporting period. The attribute for this measure is whether or not an authorized WPS subscriber successfully connects and completes their call with their intended audience (e.g., person, location, system).
Data Source	Data is obtained though contractually required Monthly Performance Reports (MPRs) provided by AT&T, Sprint, and Verizon. These reports contain information on daily WPS call attempts including, but not limited to, 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 (e.g., answered, busy, no answer). When a "Code Red" event or other significant all-hazard scenario occurs, each carrier also provides an EPR within 24 hours of the event. An EPR contains the same information as an MPR and enables ECD to rapidly leverage WPS data for analysis and decision-making purposes. While carriers maintain source data on MPRs and EPRs, this data is also internally stored and managed by ECD's PCS Subdivision. Measure results are reported as needed to CISA and DHS leadership.
Data Collection Methodology	Each quarter, ECD's PCS Subdivision analyzes all MPRs and EPRs for the reporting period to calculate overall and event-specific call completion rates, the latter of which becomes part of the population for determining the overall completion rate. PCS consolidates this information in an Excel spreadsheet that uses filter and formula functions to automatically calculate measure results. Measure results are calculated as the number of WPS calls successfully completed during the reporting period, compared to the total number of attempted WPS calls during the reporting period, expressed as a percentage. If one or more "Code Red" events or other scenarios that would cause network congestion occurs during the reporting period, additional narrative description is provided alongside the overall completion rate for additional context on the event-specific call completion rates.
Reliability Index	Reliable
Explanation of Data Reliability Check	Carrier data is recorded, processed, and shared with CISA based on contractual and industry standards that carriers must work to meet. Once the data is received, processed, and stored by CISA, and to prevent data entry and retrieval errors, the PCS Subdivision uses an Excel spreadsheet with data validation functions to require key data elements, prohibit inappropriate data entries, and limit choices to pre-determined options. To that end, the Subdivision also manages access to the Excel

	spreadsheet using SharePoint permissions. To prevent data analysis and calculation errors, the Excel spreadsheet leverages filter and formula functions to automatically calculate measure results, which are reviewed several times by Subdivision staff prior to submitting for final review and approval. To prevent observation and assessment error, ECD and PCS leadership review and approve all measure results prior to reporting.

Performance Measure	Percent of organizational Interagency Security Committee benchmarks reported as fully compliant
Program	Infrastructure Security Division
Description	This measure demonstrates progress agencies are making towards achieving the Interagency Security Committee's identified benchmarks related to its policies and standards for facility security. Led by CISA, the Interagency Security Committee (ISC) establishes policies, monitors compliance, and works to enhance the security and protection of federal facilities, ensuring that federal facilities, the people that work at them, and those who visit are safe and secure throughout the country. The capacity and capability of federal facilities to implement security countermeasures that meet ISC benchmarks is the primary external factor that can affect measure results.
Strategic Alignment	Objective 4.2: Strengthen the Security and Resilience of Critical Infrastructure
Scope of Data	The unit of analysis is an individual benchmark assessment that is self-reported by an ISC member organization, and the population is the total number of benchmark assessments received by CISA from ISC member organizations. Federal facilities self-report their compliance with ISC benchmarks on a scale from non-compliant (1) to fully compliant (5), and the attribute for the measure is whether an ISC benchmark is reported by a member organization as fully compliant with ISC standards and policy (5).
Data Source	ISC member organizations and stakeholders report their benchmark scores into the ISC Compliance System (ISC-CS). ISC manages all aspects of ISC-CS, which is used for both internal functions (e.g., analysis, reporting) and external functions (e.g., push and pull communications with critical infrastructure stakeholders). ISC leverages the ISC-CS to extract the data needed and calculate measure results, which are reported annually to DHS Program Analysis and Evaluation and as requested by CISA leadership.

Data Collection Methodology	ISC member organizations are responsible for submitting data regarding their compliance benchmarks to the ISC through ISC-CS. Once the data is received, ISC analysts leverage ISC-CS to automatically calculate measure results and generate any needed reports. This measure is expressed as a percentage, and compares the number of ISC member organizations that rated a given ISC benchmark as being fully compliant (5), to the total number of benchmark assessments completed by ISC member organizations for a given reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	ISC-CS has a series of controls to mitigate data entry and extraction errors, such as drop-down menus, required fields, and mechanisms to identify potentially duplicate information. Because of the large number of users in ISC-CS, ISC provides training to ensure data management standards are understood and met by all system users. ISC member organizations are responsible for the completeness and reliability of the data they submit through ISC-CS regarding their benchmark assessments, with ISC analysts conducting subsequent review and follow-up on data provided by member organizations to correct identified issues as needed. Once data has been reviewed and verified by ISC analysts for a given reporting period, measure results are reviewed further and then approved by relevant program leadership prior to reporting.

Performance Measure	Percent of respondents stating cyber and physical security exercises enhanced individual or organizational preparedness
Program	Infrastructure Security Division
Description	This measure demonstrates the effectiveness of CISA's cyber and physical exercises in enhancing the security, preparedness, and resiliency of critical infrastructure partners both at the individual and organizational level. Exercises include but are not limited to those conducted under the National Cyber Exercise Program and in support of the Joint Cyber Defense Collaborative. Following a CISA exercise, a survey is distributed to participants to rate the degree to which participating in the exercise enhanced their individual or organizational preparedness to execute their role(s) in preventing, protecting against, responding to, or mitigating threats to critical infrastructure.
Strategic Alignment	Objective 4.2: Strengthen the Security and Resilience of Critical Infrastructure

Scope of Data	The unit of analysis is a single response to a voluntary survey distributed to participants at the conclusion one of CISA's cyber and physical exercises, and the population is all such responses for the reporting period. The attribute of assessment is whether the respondent selects "Agree" or "Strongly Agree" in their response to the statement, "Based upon participation in this exercise, I or my organization are better prepared to execute our role in preventing, protecting against, responding to, and/or mitigating threats or incidents." Responses of "Strongly Disagree," "Disagree," and "Neither Agree nor Disagree" are included in the measure population but do not count toward measure results. Additionally, participants that do not return the survey, return a blank survey, or return a survey without a response to the subject question are not included in the calculation.
Data Source	Data for this measure is obtained using a voluntary, follow-up survey, distributed and collected using a variety of formats depending on whether the exercise was in-person or virtual. These formats include hard copy, electronic (.pdf), and/or an online Microsoft Form that are passed out, emailed, and/or posted online for participants at the conclusion of the exercise. The CISA Exercises Program Management Office (PMO) is responsible for collecting, tracking, and reporting the results, and leverages a SharePoint database to manage all related data. CISA encourages survey feedback be returned promptly; however, in some cases, surveys are returned after reporting deadlines have passed. In those cases, CISA Exercises calculates results for the current period using the data available and will provide updated results at the next reporting milestone if needed.
Data Collection Methodology	If hard copy forms are used for the post-exercise survey, they are collected at the end of the exercise by the CISA team running the event and turned over to the CISA Exercises PMO for processing. Electronic (.pdf) forms are returned via email and processed directly by the PMO. If Microsoft Forms is used, the PMO directly processes the results via the application. Information from these survey results is consolidated into a master SharePoint database that automatically calculates measure results through its built-in formula and filter functionalities. Measure results are calculated as the number of respondents who select "Strongly Agree" or "Agree" to the statement, "Based upon participation in this exercise, I or my organization are better prepared to execute our role in preventing, protecting against, responding to, and/or mitigating threats or incidents," compared to the total number of

	responses to the survey question for the reporting period, expressed as a percentage.
Reliability Index	Reliable
Explanation of Data Reliability Check	CISA Exercises employs a multi-step data reliability process. First, once processed by the PMO Data Analyst, survey results for individual exercises are checked for accuracy by the responsible CISA Exercises Team Lead. Second, the CISA Exercises PMO Branch Chief, who is responsible for overseeing and administering the process for data collection and processing, conducts periodic spot checks of survey data for individual exercises as well as cumulative survey results. Any anomalies in the data receive an additional review by the responsible Brach Chief. Finally, results are reported to the CISA Exercises Associate and Deputy Associate Directors who conduct a review of the data on a quarterly basis prior to reporting results to relevant stakeholders.

Performance Measure	Percent of facilities that are likely to integrate vulnerability assessment or survey information into security and resilience enhancements
Program	Integrated Operations Division
Description	This measure demonstrates the percent of facilities that are likely to enhance their security and resilience by integrating IOD's 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.
Strategic Alignment	Objective 4.2: Strengthen the Security and Resilience of Critical Infrastructure
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	Number of Committee on Foreign Investment in the United States (CFIUS) related cases reviewed, analyzed, and processed
Program	National Risk Management Center
Description	This measure demonstrates the number of CFIUS related cases reviewed, analyzed, and processed. CISA relies on the Foreign Investment Risk Branch (FIRB) within the National Risk Management Center's (NRMC) Analysis Division to manage the CFIUS process and foreign risk review on behalf of CISA. The review for CFIUS cases includes each CFIUS Notified Transaction, Supplemental Threat Information Reporting for each case, and full risk analysis for those transactions with

	equities where CISA is the designated Sector Risk Management Agency (SRMA). FIRB performs an initial review of Declarations (short form filings) and provides full risk analysis where CISA as the SRMA has potential equities. FIRB also provides a bi-weekly analysis of the Non-Notified Transaction Digest. Non-Notified transactions are potential CFIUS cases that did not go through the CFIUS filing process. The digest provides early warning of and information about foreign acquisitions of U.S. businesses and similar transactions that may impact DHS CISA equities.
Strategic Alignment	Objective 4.3: Assess and Counter Evolving Cyber and Emerging Technology Risks
Scope of Data	The unit of analysis is one CFIUS related case. The population includes all CFIUS related cases within the reporting period. The attribute is whether the CFIUS case was reviewed, analyzed, and processed. Included is the review of each CFIUS Notified Transaction, and full risk analysis for those transactions with equities where CISA is the SRMA; full analysis of Declarations which are short form CFIUS submissions; and bi-weekly analysis of the Non-Notified Transaction Weekly Digest that provides early warning of and information about foreign acquisitions of U.S. businesses and similar transactions that may impact DHS CISA equities where CISA is the SRMA.
Data Source	Data source is the case information received from DHS Policy Foreign Investment Risk Management Division via email contact and a SharePoint site. Case information is entered into the NRMC Modeling Capability Transition Environment (MCTE), which allows FIRB to manage CFIUS cases, and the accompanying analysis of each case, as well as Supplemental Information Reporting for every CFIUS Case. Within MCTE, NRMC can run and produce reports, and extractions of various data sets related to CFIUS such as CFIUS case by CI sector, Acquiree (Country), Acquirer (Country), Calendar Year (CY) and FY, and Case Disposition, to name a few.
Data Collection Methodology	The FIRB has all case information located in the MCTE. It contains case information for all CFIUS cases which include notified, declarations, and notified CFIUS transactions. as well as Supplemental Information Reporting, and subject matter expert (SME) input with final Risk Analysis. The CFIUS application in MCTE allows FIRB to pull CFIUS related numbers by FY, CY, Critical Infrastructure Sector, Acquiree, Acquirer, Type of CFIUS Case, CISA Co-lead cases, etc. This data is used to do a simple count of the number of CFIUS related cases that meet the requirement of being reviewed, analyzed, and processed.
Reliability Index	Reliable

Explanation of Data Reliability Check	All CFIUS related cases are recorded, reviewed, processed, and summarized as they are received. At any point in the Calendar Year a current number of cases can be accessed and further reviewed by Country, Sector Specific Agency, Case Type, CY/Month, and assigned case number. The number of CFIUS cases and ensuing reviews can be verified through the MCTE. Further clarification of the number and/or type of CFIUS cases can be verified with DHS PLCY/Foreign Investment Risk Management Division. Cases are reviewed by NRMC FIRB analysts and CISA equities for clarity and before sending to CISA SME for vulnerability and consequence input. SME results are reviewed for clarity and consistency by NRMC FIRB analysts before submission to DHS PLCY/Foreign Investment Risk Management Division.

Performance Measure	Number of unique election infrastructure stakeholders reached through Election Security & Resilience strategic engagements
Program	National Risk Management Center
Description	This measure demonstrates the capacity of the NRMC's Election Security and Resilience (ESR) Subdivision to engage election infrastructure stakeholders. ESR ensures that election infrastructure stakeholders have the information they need to manage risk to elections, coordinating across the Federal government and with election partners to engage, assist, and prepare the election community for an ever-evolving risk landscape. CISA is committed to working collaboratively with those on the front lines of elections, such as state and local governments, election officials, federal partners, and private sector partners. By reaching more unique election stakeholders through strategic engagements, ESR is able to drive greater awareness and better promote the use of CISA's services to manage risks to the Nation's election infrastructure.
Strategic Alignment	Objective 4.3: Assess and Counter Evolving Cyber and Emerging Technology Risks
Scope of Data	The unit of analysis for this measure is a single ESR strategic engagement and the population is all ESR strategic engagements for a given reporting period. The attribute is whether a unique stakeholder was reached through a given ESR strategic engagement, meaning multiple unique stakeholders may be reached through a single ESR strategic engagement. Strategic engagements include in-person events such as conferences and meetings and virtual engagements including webinars and teleconferences where ESR has a participatory role.

Data Source	ESR personnel maintain Outlook calendars with records of all strategic engagements, including date and time of event, and distribute a quarterly request to election infrastructure stakeholders to obtain the number of unique stakeholders reached through ESR strategic engagements. Calendar information is manually extracted by ESR personnel from Outlook and is consolidated in an Excel spreadsheet that is archived on an internal SharePoint site. ESR personnel leverage filter and formula functions in Excel to automatically calculate measure results, which are reported quarterly to DHS Program Analysis and Evaluation and as requested by CISA leadership.
Data Collection Methodology	ESR personnel use Outlook calendar capabilities to manually obtain the number of strategic engagements conducted for a given reporting period. The number of unique stakeholders reached through ESR strategic engagements is obtained from a quarterly data call to election infrastructure stakeholders. These two sets of information are consolidated in an Excel spreadsheet that leverages filter and formula functions to automatically calculate the number of unique election infrastructure stakeholders reached through ESR strategic engagements for a given reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	To mitigate potential errors in data entry and extraction, ESR personnel leverage Excel functions like drop-down menus and data validation mechanisms to identify potentially duplicate information. SharePoint permissions are used to manage access to the Excel spreadsheet. Measure results are calculated automatically in Excel and are reviewed and approved by relevant program leadership prior to reporting.

Performance Measure	Number of Stakeholder Relationship Management user adoptions
Program	Stakeholder Engagement Division
Description	This measure assesses the growth, by quarter, in the adoption of the Stakeholder Relationship Management (SRM) tool across CISA by staff who conduct direct engagements with agency stakeholders, or who use the data in the SRM to plan or analyze stakeholder engagements. This measure sub-divides user adoptions by organizational category at the Division, Region, and Mission Enabling Office levels to support stakeholder engagement analysis and planning. This measure serves as a proxy to evaluate the utility and effectiveness of the SRM as a

	stakeholder engagement data collection and analysis tool within CISA.
Strategic Alignment	Objective 4.2: Strengthen the Security and Resilience of Critical Infrastructure
Scope of Data	The unit of analysis is a single Stakeholder Relationship Management tool adoption. The population includes the total number of users across CISA (including both federal employees and contractors) that have access to the SRM tool. The total number of SRM users cannot exceed the total user license count of 1,500. A "user" is any CISA staff member, federal or contractor. The attribute is whether the user, who has not previously accessed or used SRM, has adopted or accessed SRM to record a discrete stakeholder engagement or to view SRM data for analysis or planning purposes. This measure can be further broken out and report numbers based on users within a specific Division, Region, or Mission Enabling Office.
Data Source	The data source is the Stakeholder Relationship Management tool which enables the use of Power BI Premium dashboard connected to analyze the data. The SRM Technology Solution provides a license management capability that allows reporting of license issuances to users, as well as the date of issuance.
Data Collection Methodology	CISA's Stakeholder Engagement Division (SED) conducts a quarterly data query of SRM Technology Solution new user adoptions directly through the linked Power BI Premium dashboard. The dashboard generates on-demand reports on numerous system and system user characteristics. The increase in the number of SRM users is calculated by counting the number of newly enabled users from the start of a quarter to the end of that quarter.
Reliability Index	Reliable
Explanation of Data Reliability Check	On-demand SRM Technology Solution reports generated through the PowerBI Premium dashboard pull data directly from the system and do not require manual reviews or validation. User access to the SRM Technology Solution is captured in system logs, which serve as the authoritative data source for this measure.

Federal Emergency Management Agency

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	This measure assesses the effectiveness of National Fire Academy (NFA) courses by assessing the increase in the knowledge, skills, and abilities of students trained as reported by individual first-line supervisors. Course graduates and their supervisors are asked to evaluate the impact of the training on both individual job performance and the performance of the fire and emergency response department where the student works. NFA senior management uses this information to update existing NFA course materials and to develop new courses that reflect the emerging issues/needs of the Nation's fire service. The lack of responses to the Kirkpatrick Level 3 survey can impact results.
Strategic Alignment	Objective 5.4: Enhance Training and Readiness of First Responders
Scope of Data	The unit of analysis is a first line supervisor who responded to the National Fire Academy Long-Term Evaluation Survey. Surveys are circulated to all first line supervisors of students who have attended an NFA course within the last 120 days. The population is all first line supervisors who responded to the survey. this measure assesses the survey response ratings of how strongly first line supervisors agree with the statement "Course has improved student's job performance." The survey produces results using the five-point Likert scale, therefore the attribute is the numeric rating. All survey ratings for the specified question are included in the calculation. The measure's scope includes all valid responses within the reporting period.
Data Source	The data are stored in an oracle database. Reports are pulled from the database where the results are automatically calculated.
Data Collection Methodology	Supervisors of students trained who have completed NFA training are sent a link which enables them to complete the questionnaires online. Responses are stored in an oracle database. Reports are pulled from the database where the

	results are automatically calculated. The numerator is the number of respondents who indicated strongly agree or agree to the question. The denominator is the number respondents who answered the question.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent data entry errors, NFA uses a standardized from approved by OMB to capture responses. Data are retrieved directly from the system using programmed reports. All reports are formula based and tested prior to implementation. Once retrieved, all data is review ty the National Fire Academy's Training, Administration, Planning and Analysis branch staff for completeness.

Performance Measure	Benefit to cost ratio of the Hazard Mitigation Grants
Program	Grants
Description	This measure reports the estimated annual benefit to cost ratio (BCR) of grants provided by the FEMA Hazard Mitigation Assistance (HMA) 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, local, tribal, and territorial (SLTT) 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 SLTT grant requests. The FEMA team verifies that applicants used approved Benefit Cost Analysis (BCA) tools and methodology and confirms the BCR is greater than or equal to one.
Strategic Alignment	Objective 5.2: Strengthen National Resilience
Scope of Data	The scope of this measure includes all grants on an annual basis provided by the FEMA Hazard Mitigation Assistance program.
Data Source	The systems primarily used for the data collection includes FEMA's Enterprise Data Warehouse (EDW) which consolidates data from Hazard Mitigation Grant Program - National Emergency Management Information System (HMGP-NEMIS) and Mitigation Electronic Grants Management System (MT-eGrants) systems. Data is collected and consolidated into an Excel spreadsheet where the calculations for aggregate Benefit to cost ratio will be performed.
Data Collection Methodology	The total project cost and the benefits are calculated by the applicant for each of the projects. The estimated benefits are derived based on benefit-cost analysis methodologies

	developed by FEMA. These are proven methodologies and have been in use for the past 10 years. To determine the cost effectiveness of an 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 Mitigation Electronic Grants Management System (MT-eGrants) by FEMA HMA staff. Quarterly reports will be generated utilizing FEMA's EDW which will be utilized for the data reporting.
Reliability Index	Reliable
Explanation of Data Reliability Check	Each sub-grant obligation and total project cost is captured in the HMGP-NEMIS or MT-eGrants system. This information is electronically consolidated in FEMA's EDW. FEMA HMA staff download relevant data from the EDW, and after making the calculations for an aggregate Benefit to cost ratio generate Quarterly excel based reports. These calculations go through a series of staff reviews before being reported on FEMA's performance system of record – the Performance Hub.

Performance Measure	Percent of capabilities where community capability is far less than national goal
Program	Grants
Description	This measure assesses effectiveness of the Homeland Security Grant program, which is a suite of risk-based grants to assist SLTT 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; it presents a snapshot of the general state of national preparedness. A capability is far less than the national goal if affected communities report capability of less than 30% of the national goal needed to manage catastrophic scenarios. National capabilities required to be reported each year may change, so it may be necessary to provide additional context on the number of national capabilities included in the reported measure score. Information about how national capability targets are identified and determined is at https://www.fema.gov/sites/default/files/2020-06/fema_national-thira-overview-methodology_2019_0.pdf
Strategic Alignment	Objective 5.2: Strengthen National Resilience
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 THIRA and 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 NTHIRA 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. FEMA's National Preparedness Assessments Division (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 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 yet. The measurement score is calculated by dividing the numerator by the denominator.
Reliability Index	Reliable
Explanation of Data Reliability Check	FEMA's NPAD aggregates THIRA and SPR data on an annual basis, reviews each submission for errors, and works with communities to correct issues.

Performance Measure	Percent of capability building Homeland Security Grant Program dollars that align to closing state, territory, and urban area identified capability gaps
Program	Grants
Description	This measure assesses the effectiveness of FEMA efforts to close capability gaps through the Homeland Security Grant Program (HSGP). Capability gaps are identified by states, territories, and urban areas in recipients annual SPR. FEMA's Comprehensive Preparedness Guide (CPG) 201 3rd Edition defines "capability built" projects as those that deliver new capabilities. A project is considered to align to the SPR when it funds a Planning, Organizing, Equipping, Training, and Exercising (POETE) area in a core capability for Prevent, Protect, and Response mission areas and the state, territory, or urban area indicated having a gap in that POETE area in that year's SPR. FEMA uses the results to make sure HSGP recipients are aligning FEMA-funded investments with self-identified capability gaps.
Strategic Alignment	Objective 5.2: Strengthen National Resilience
Scope of Data	The unit of analysis is a dollar reported in the Biannual Strategic Implementation Report (BSIR). The population is funds for State Homeland Security Program and Urban Area Security Initiative projects reported in the June submission of the BSIR that are for POETE area. The funds also must be for core capability targets for Prevent, Protect, and Response mission areas that were required in the THIRA for the relevant reporting year. Projects exclude Management and Administration projects, projects marked as addressing a National Priority Area (NPA) as defined in the Homeland Security Grant Program Notice of Funding Opportunity, projects intended to sustain capabilities, or projects with funds from a grant year that is not the same as the current SPR. The attribute of the funds is they must be for projects that align to capability gaps identified in the SPR.
Data Source	The data for the measure is from two sources: The BSIR and the SPR. The BSIR is maintained within the Grants Reporting Tool (GRT) by the FEMA Grant Programs Directorate (GPD). The SPR is managed by the Risk and Capability Assessments Division in the Risk Analysis, Planning and Information Directorate. The BSIR is a report from grant recipients that collect project-level. The BSIR is submitted twice a year [a summer BSIR (typically in June) and a winter BSIR (typically in December)]. Through FY 2023 data were submitted through the GRT. From FY 2024 onwards, data will be submitted through FEMA GO. GPD owns the BSIR data source. The SPR is an annual capability

	assessment that helps jurisdictions identify their current capability relative to the targets outlined in their THIRA. Communities submit their data by completing the online FEMA Preparedness Toolkit (Prep Toolkit) by December 31 each year. The Resilience Evaluation and Analysis Division (READ) owns the THIRA/SPR data source.
Data Collection Methodology	GPD retrieves the BSIR data from GRT by running a query twice per year. READ retrieves the SPR data from the toolkit by running a query. READ requests BSIR data from GPD and combines it with SPR data into a separate Excel spreadsheet. The data is cleaned and analyzed to include only the applicable projects and funds and designate projects as aligned or not aligning to capability gaps identified in the SPR.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent observation and assessment errors, the BSIR and SPR use standardized forms for data collection. To prevent data entry and retrieval errors, all data is monitored for quality, accuracy and reliability by experienced analysts. To prevent analysis and calculation error, after the measure results are calculated, a second analyst independently replicates the analysis to ensure accuracy of the results. After this check, senior managers in NPAD review the findings and cases where state, territory, or urban area projects and gaps do not align. If confirmed, a Memorandum is issued to the relevant State or territory regarding the discrepancy of the alignment information. Through these communications States, territories, and urban areas may offer clarifying information that offers a second reliability check on the accuracy of the project alignment information to capability gaps.

Performance Measure	Percent of dollars from FEMA Justice40 covered programs flowing to disadvantaged communities
Program	Grants
Description	This measure assesses FEMA's ability to meet the Justice40 initiative EO 14008 goal that 40% of the overall benefits of certain federal investments flow to disadvantaged communities. This measure annually tracks the overall percentage of financial dollars from FEMA's Justice40 covered programs (Building Resilient Infrastructure and Communities [BRIC], Flood Mitigation Assistance [FMA], Risk Mapping, Assessment, and Planning [RiskMAP], and Regional Catastrophic Preparedness Grant Program [RCPGP]) project selections that flow to disadvantaged communities. The purpose of FMA is to reduce/ eliminate the risk of repetitive flood damage to buildings insured

	by the National Flood Insurance Program (NFIP). The target population for this measure are those insured by NFIP in a disadvantaged community. Disadvantaged communities are defined using the Climate and Economic Justice Screening Tool (CEJST).
Strategic Alignment	Objective 5.2: Strengthen National Resilience
Scope of Data	The unit of analysis for BRIC, FMA, and RCPGP is grant dollars announced. For RiskMAP it is the funds allocated. The population is the total grants dollars announced for the BRIC, FMA, and RCPGP programs and the total funds allocated for RiskMAP activities within the fiscal year. The data included are only data associated to the four current Justice40 covered programs, BRIC, FMA, RiskMAP, and RCPGP as follows 1) BRIC and FMA: all grant dollars announced in a fiscal year with the exception of projects that do not include specified jurisdictions 2) RiskMAP: all RiskMAP projects for the fiscal year; 3) RCPGP: all grant dollars announced in the fiscal year with the exception of Management and Administration project-related costs. The attribute is the specified jurisdiction for the funds identified as a disadvantaged community through the CEJST.
Data Source	The data source for BRIC and FMA is the FEMA Grants Outcomes (FEMA Go) platform and Geographic Information Systems (GIS) data attachments from the Notice of Funding Opportunity (NOFO). The data source to determine the projects for RiskMAP is Coordinated Needs Management Strategy (CNMS) and FEMA's Mapping Information Platform (MIP). Once the projects are determined, they are tracked in excel. The data source for RCPGP is the Non-Disaster Grants System. The data source to determine disadvantaged communities is CEJST. Each program owns their own data. The data are collected once a year.
Data Collection Methodology	For the overall measure, the numerator is calculated by adding the numerators of each program, adding the denominator of each program, and then dividing the numerator by the denominator. The numerator for each program is 1) BRIC and FMA, the total dollars announced that flow to the disadvantaged communities; 2) For RiskMAP, the total amount of funding allocated to disadvantaged communities; 3) For RCPGP, the total dollars announced for disadvantaged communities multiplied by the impact score. The denominator for each program is 1) For BRIC, FMA and RCPGP, the denominator is the total dollars announced in the fiscal year excluding the dollars that is not for specified jurisdictions; 2) For RiskMAP, the denominator is the total amount of funding allocated for all RiskMAP activities for the fiscal year. Office of Resilience

	Strategy will collect and compile the data from each program on an annual basis and calculate the overall measure results.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent data entry errors, FEMA GO, the Non-Disaster Grants System, CNMS and MIP has controls such as date validation, the use of dropdown fields rather than free text when possible, and the use of database fields formatted for specific purposes (numbers, dates, etc.). Benefitting areas and communities are intersected on census tracts in CEJST. This manual process is reviewed and validated by supervisors. Additionally, for RCPGP, FEMA staff manually collect impact score data associated with each RCPGP-funded project to determine the percentage and associated dollar benefit to disadvantaged communities. The results are reviewed and validated by supervisors. Once the Office of Resilience Strategy receives the data from the program, staff members validate the total funds against original data sources and validate the disadvantaged communities are correctly identified through CEJST. Measure calculations are done manually and validated by supervisors.

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 five 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.
Strategic Alignment	Objective 5.2: Strengthen National Resilience
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 ISO through their BCEGS

	database and research. The two most recent building code editions, covering a time frame of six years of code development, are used to determine if a community has adopted disaster-resistant codes.
Data Source	The source of data for this measure is ISO's BCEGS database which tracks data on building codes adopted by participating jurisdictions from the BCEGS questionnaire. The BCEGS survey data is completed by communities electronically in the BCEGS database. BCEGS database is updated daily to include the latest surveys taken.
Data Collection Methodology	ISO collects data from the BCEGS survey daily and tracks building code adoption. ISO populates the BCEGS database with the survey results. The Mitigation program receives raw data from ISO through their BCEGS database.
Reliability Index	Reliable
Explanation of Data Reliability Check	FEMA relies on ISO to manage the completeness and reliability of the data provided thought their BCEGS database to the program; however, the data are reviewed by FEMA's Mitigation program to ensure results are consistent over time. If significant fluctuations in quarterly and annual results occur, the program will work with ISO to address issues with data reliability.

Performance Measure	Percent of U.S. population (excluding territories) covered by planned mitigation strategies
Program	Mitigation
Description	This is a point in time metric that determines the percent of U.S. population (excluding territories) covered by approved or approvable local Hazard Mitigation Plans. The population of each community with approved or approvable local Hazard Mitigation Plans is used to calculate the percentage of the national population. The FEMA Mitigation program gathers and analyzes critical data to aid in future mitigation efforts and enable communities to be better informed and protected. FEMA Mitigation helps communities reduce risk through sound land-use planning principles (such as planned mitigation strategies), floodplain management practices, and financial assistance.
Strategic Alignment	Objective 5.2: Strengthen National Resilience
Scope of Data	The scope of this measure includes all Unites States jurisdictions excluding territories.
Data Source	Data are derived from Regional Reports and are entered into a Microsoft Excel spreadsheet, which is maintained on redundant network drives. A Headquarters master spreadsheet is

	populated monthly by FEMA Regional Risk Analysis staff that record, report, and store the names and locations of the jurisdictions that have received FEMA approval of mitigation plans.
Data Collection Methodology	FEMA regional staff review each mitigation plan based on the regulations found in 44 CFR Part 201. Plans are not approved until they demonstrate that the affected jurisdiction(s) engaged in a planning process, identified and evaluated their risks from natural hazards, create overarching goals, and evaluate a range of specific actions that would reduce their risk, including a mitigation strategy that describes how the plan will be implemented. Data on the approved plans is stored by FEMA 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. FY 2019 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.
Strategic Alignment	Objective 5.2: Strengthen National Resilience
Scope of Data	This measure includes data from FEMA as well as data provided by non-FEMA entities that invest in mitigation. Such investments encompass risk-management actions including prevention, property protection, public education/awareness, natural-resource protection, and structural projects. This measure includes the direct Grant amounts provided by the Federal Government and the accumulation of labor and other non-monetary investment not funded by grants and its equivalent monetary value. FEMA expects to incorporate data on private-sector investments between FYs 2022 and 2023, explaining the expected year-on-year target increase of 65 percent.
Data Source	Data for this measure will come from MitInvest, an online database within SharePoint which serves as the sole method for FEMA Headquarters and Regional Offices to record information on the status of FEMA's external engagements, partnerships, and investment data related to investments in mitigation.
Data Collection Methodology	For each mitigation investment, FEMA staff complete an internal data-collection instrument (DCI), which provides staff with instructions for documenting how the investment in question supports the recommendations of FEMA's National Mitigation Investment Strategy; the budget obligation of each fiscal year's mitigation investments; and details about how the investment mitigates risk/harm. FEMA transfers this data from DCIs to the MitInvest database. Staff at FEMA headquarters will confirm the investment with submitting Regional or HQ staff, and with any non-FEMA entity involved to validate a connection between the investment and the National Mitigation Investment Strategy. Upon confirmation, staff will add the investment in question to the total monetary amount included in this measure. FIMA will report annually on the status of mitigation investments nation-wide.
Reliability Index	Reliable
Explanation of Data Reliability Check	The MitInvest database is a SharePoint document repository, available via controlled access exclusively through FEMA's intranet. MitInvest staff use documents separate from DCIs submitted to cross-check information about non-FEMA entities and investments. Information saved to MitInvest will inform management decisions, which will motivate effort to ensure the reliability of MitInvest data in addition to requirements to validate this measure's reliability.

Performance Measure	Number of properties covered with flood insurance (in millions)
Program	National Flood Insurance Fund
Description	This measure 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 NFIP, as well as policies sold by independent insurance agents through NFIP Direct. Individuals' 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.
Strategic Alignment	Objective 5.2: Strengthen National Resilience
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 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 total floodplain mileage mapped with improved engineering standards
Program	National Flood Insurance Fund
Description	This measure assesses the effectiveness of FEMA's Risk MAP Program maintaining the currency of the regulatory flood map inventory with new, validated, or updated engineering flood hazard data. FEMA is required to assess on a 5-year cycle the need to revise and update all floodplain areas and flood risk zones, based upon an analysis of all natural hazards affecting flood risks. This assessment is important because, over time, manmade development and natural processes can alter the land and hydraulic characteristics for a given area, resulting in changes to the flood risk. This measure is used to monitor data quality by ensuring that flood hazard data are new, have been updated, or are deemed to still be valid through a continuous review and update process.
Strategic Alignment	Objective 5.2: Strengthen National Resilience
Scope of Data	The unit of analysis is a mile of riverine and coastal waterways or shorelines in the regulatory flood map inventory. The population is all riverine and coastal waterways or shorelines charted in regulatory flood map inventory. To be considered part of the regulatory inventory, the flood hazard information must be reflected and delivered through a Flood Insurance Rate Map (FIRM). A FIRM is the official map of a community on which defines both the special flood hazard areas and the flood zones applicable to the community. The attribute is if a mile is mapped with new, validated, or updated engineering (NVUE) flood hazard data (CNMS Validation Status = Valid). To be considered mapped, the preliminary Flood Insurance Rate map must be issued to the community for review (Flood studies Attained).
Data Source	The data for this measure are stored in the Coordinated Needs Management Strategy (CNMS) database. On a quarterly basis, each of the 10 regional databases are consolidated into a national database and a geospatial analysis is conducted by a contractor. It is comprised of processes and data for tracking: NVUE; unverified study reaches with the identified change characteristics; and requests for the flood mapping program. The regulatory flood map inventory within CNMS database is built from a network of stream centerlines and coastal shorelines that represent where FEMA regulatory information exists. Assessment results, validation status, and locations of regulatory information are entered as attributes to the network of lines. On an annual basis, new and updated regulatory

	models and maps initiated by the ten regional offices are added to the CNMS database.
Data Collection Methodology	Risk MAP Program uses the CNMS assessment process where NVUE studies are initiated and then attained. The databases are updated by Production and Technical Service providers that support FEMA Regional Offices and FEMA HQ. Automated calculations produce a National Risk MAP summary sheet which includes regional summaries of validation status and miles initiated. The geospatial results are shared to a public facing viewer/website. CNMS Map Viewer (arcgis.com). The numerator is the total number of riverine and coastal waterways or shorelines regulatory flood map inventory miles mapped with new, validated, or updated engineering flood hazard data. The denominator is the total number of riverine and coastal waterways or shorelines regulatory flood map inventory miles.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent observation and assessment errors, the CNMS validation and update process is detailed in the Coordinated Needs Management Strategy Technical Reference document. This technical document outlines assessment and performance criteria for acceptance. To prevent retrieval errors, any updates to the regional databases must clear a CNMS QA/QC tool prior to upload. Additionally, the regional database must also clear the CNMS QA/QC tools prior to upload to the National Database. To prevent analysis and calculation errors, the calculations are automated in the CNMS database. Contractors perform a geospatial analysis and provide to FEMA HQ for final review and approval.

Performance Measure	Number of lives lost per year due to fire in the U.S.
Program	Preparedness and Protection
Description	This measure assesses FEMA's effectiveness in reducing the number of civilian and firefighter lives lost from fire-related events. Though the U.S. Fire Administration (USFA) does not have direct control over the results of this measure, they do have influence through the USFA programs and fire prevention efforts. This measure serves as a proxy metric to indicate how USFA can improve on its programs and fire prevention efforts to continue to address the nation's fire problem.
Strategic Alignment	Objective 5.4: Enhance Training and Readiness of First Responders
Scope of Data	The unit of analysis is one civilian or firefighter. The attribute is fatality due to fire. Fire death is defined as a civilian or firefighter

	fatality resulting from a structure fire or wildland fire event. The population is all civilian and firefighter fire deaths in the U.S. The population currently does not include fire deaths that occur in U.S. territories and Tribal areas.
Data Source	The data source is a combination of submitted and curated data residing at USFA. Curated data will include data selected, organized, and presented using professional or expert knowledge. For years 2023-2025, the National Fire Incident Reporting System (NFIRS) will be the main data source. Beyond 2025, the National Emergency Response Information System (NERIS) data system will be used as source data with internal validation.
Data Collection Methodology	The USFA NFIRS data system receives civilian and firefighter fire death data from local fire departments and state fire marshal offices throughout the United States, excluding territories and Tribal. The data including number of deaths, geolocation, gender, race, ethnicity, and age are collected from NFIRS using structured query language (SQL) to generate a report. USFA staff also manually scrapes nationwide media for fire deaths capturing geolocation, gender, race, ethnicity, and age of fire fatalities. Civilian data collected through internet data searches are maintained and searchable year-round on the USFA home fire fatality webpage. Staff of the Nation Fire Data and Research Center combine the data collected from the NFIRS data system and the internet data searches together and store them in an excel file annually. The measure calculation methodology is a straight count of the number of lives lost due to fire events.
Reliability Index	Reliable
Explanation of Data Reliability Check	Verification: Fire Death data reported to the NFIRS are compiled and reviewed by the USFA National Fire Data Center staff. USFA National Fire and Emergency Medical Services Division staff also search and verify civilian deaths reported in the media and firefighter deaths reported directly from fire departments. Validation: The number of fire deaths will be validated against external data sources including the National Fire Protection Association's (NFPA) National Fire Experience Survey (NFPA Survey) for a given calendar year. Estimates from the NFPA Survey are generally available in Sept. for the preceding year (e.g., fatality estimates for Calendar Year 2006 were available in Sept 2007). Data are analyzed to produce estimates of fire related civilian fatalities which will be used as validation of USFA results.

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.
Strategic Alignment	Objective 5.2: Strengthen National Resilience
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 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 assesses the effectiveness of recruiting Alerting Authorities to send alert and warnings to the public through the Integrated Public Alert and Warning System (IPAWS). IPAWS provides authenticated emergency and life-saving information to the public through mobile phones using Wireless Emergency Alerts, to radio and television via the Emergency Alert System and on the National Oceanic and Atmospheric Administration's Weather Radio. IPAWS seeks to maintain current alerting authority access by providing assistance and training, and to expand the number of local alerting authorities by identifying population coverage gaps and engaging with public safety agencies with jurisdiction in those areas. The continued access and use of IPAWS is contingent on authorized Alerting Authorities completing a mandatory Monthly Proficiency Demonstration each month.
Strategic Alignment	Objective 5.2: Strengthen National Resilience
Scope of Data	The unit of analysis is individuals in the United States. The population is all individuals in the United States based upon the 2020 census Federal Information Processing Standards (FIPS) code. The attribute is if the individual lives within a FIPS code served by local Alerting Authorities authorized to send alerts and warnings to the public using IPAWS.

Data Source	The data are stored in the Local Alerting Authority Population Coverage Workbook (an excel spreadsheet). The data source for the U.S. population is provided by the Commerce Department's Census Bureau. Alerting Authorities authorized to send alerts and warnings to the public using the IPAWS is maintained in the IPAWS Division and posted on fema.gov. The data includes the IPAWS Alerting Authority ID, name, and FIPS code. The spreadsheet is maintained in the IPAWS Division.
Data Collection Methodology	For each period of performance, the program will have 1) a list of Alerting Authorities registered to use IPAWS, last updated no earlier than the preceding fiscal quarter; 2) data on total U.S. population, decomposed by FIPS. The data is manually populated into the Local Alerting Authority Population Coverage Workbook for calculation. The numerator is the population based on the FIPS Code areas served by all authorized Local Alerting Authorities. The denominator is the total U.S. population.
Reliability Index	Reliable
Explanation of Data Reliability Check	For population data, the program uses Census Bureau data, which the Bureau verifies and validates: See the Census Bureau's data verification and validation process at https://www.census.gov/programs-surveys/popest/technical-documentation/methodology.html. The program itself maintains a list of non-federal public authorities registered to use IPAWS, updated quarterly. As the sole grantor of IPAWS access to public authorities, the Office of National Continuity Programs (ONCP) can validate data for this measure as ONCP extends or rescinds IPAWS access to public authorities. To prevent analysis and calculation errors, ONCP uses a Microsoft Excel application to calculate the performance measures results for consistency. The results are peer reviewed before submitting.

Performance Measure	Average annual percentage of administrative costs for major disaster field operations, as compared to total program costs
Program	Response and Recovery
Description	This measure gauges FEMA's efficiency in providing disaster assistance by indicating what share of its disaster expenditures are administrative costs compared to the share disseminated as grants to survivors as assistance. It helps FEMA know if the agency is being efficient in the way it provides disaster assistance. This measure is for FEMA's most common disasters of less than $50 million (Level III).
Strategic Alignment	Objective 5.1: Coordinate Federal Response to Incidents

Scope of Data	The results are based on all available data and not a sample of data for Major Disasters under $50M. The measure only applies to Major Disasters (DRs). It does not apply to Emergency Declarations (EMs), Fire Management Assistance Grants (FMAGs) or any other administrative costs in the disaster relief fund. Administrative Costs are those costs which are classified in IFMIS (Integrated Financial Management Information System) as 'Administrative' in FEMA's system of record, EDW reports and Financial Information Tool (FIT) reports. Examples include but are not limited to salaries and benefits, travel, facilities.
Data Source	The data is collected and stored in IFMIS. It is reported via FIT reports, in addition, the disaster administrative cost percentage for specific disasters is reported on in the Automated Common Operating Picture (COP), which also pulls data from IFMIS. FEMA Office of the Chief Financial Officer (OCFO) owns IFMIS and the FIT reports. ORR owns the Automated COP.
Data Collection Methodology	The data is collected via IFMIS and reported in FIT reports. The remaining steps are conducted by an analyst using data from a FIT report. The data is organized so that disasters are first separated by their size which is determined by the total actual federal dollars obligated. Small disasters have total actual federal obligations less than $50M. An administrative cost percentage is calculated for each disaster and is the (Total Administrative Costs for that disaster)/ (Total Obligations for that disaster). To create the score for each year, the analyst groups all disasters declared in that year of the same size and calculates the average administrative cost percentage across all those disasters (Sum of Admin Cost Percentages of Each Disaster)/Total Number of Disasters). This results in three scores per year, one each for small, medium, and large disasters. Note: Because the data is organized by declaration year, all of the previously reported numbers will need to be updated
Reliability Index	Reliable
Explanation of Data Reliability Check	The data is collected via IFMIS and reported in FIT reports. The remaining steps are conducted by an analyst using data from a FIT report. The data is organized so that disasters are first separated by their size which is determined by the total actual federal dollars obligated. An administrative cost percentage is calculated for each disaster and is the (Total Administrative Costs for that disaster)/(Total Obligations for that disaster). To create the score for each year, the analyst groups all disasters declared in that year of the same size and calculates the average administrative cost percentage across all those disasters (Sum of Admin Cost Percentages of Each

	Disaster)/Total Number of Disasters). This results in three scores per year, one each for small, medium, and large disasters.

Performance Measure	Average 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 Individuals and Households Program provides first financial assistance to qualified individuals and households. The first financial assistance refers to the first financial assistance received by an Individuals and Households Program applicant for the disaster in which they applied. FEMA provides financial assistance to qualified individuals and households who have applied for FEMA assistance. The processes may include application review, casework, and inspections. The results are used by leadership to monitor program delivery and identify gaps and opportunities for improvement. The results are impacted by a number of external factors such as scale of the disaster, volume of applicants, correctness of the completion of the application for assistance, and type of assistance.
Strategic Alignment	Objective 5.3: Support Equitable Community Recovery
Scope of Data	The unit of analysis is the first individuals and households' financial assistance award received by an Individuals and Households Program (IHP) applicant for the disaster in which they applied. Each financial assistance is stamped with an award date for each applicant. The assistance with the earliest award date is used for this measure. The population is all first IHP financial assistance awards received by applicants from all active disasters. If the first award falls in the reporting period, it is included. The measure will include all types of first IHP financial awards. The attribute is the number of days from when the application can first be reviewed ("applied date") to receipt of the first award "first award date". Applicants may apply for assistance before their county has been declared a major disaster. However, the application can't be reviewed until after their county has been declared. The date used for the calculation is the first date the application can be reviewed.
Data Source	Data for this measure is stored in the National Emergency Management Information System (NEMIS) and is the system of record. NEMIS contains all program-pertinent information for registered individuals and households, their current and damaged dwelling locations, inspection results, correspondence, 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. The NEMIS data is replicated to the Organizational Data Storage (ODS) Oracle database every 15 minutes and is identical to the data in NEMIS. The ODS database allows for users to extract NEMIS data separate from the live NEMIS production server. Extracting data separate from a live production server is a best practice to ensure 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) retrieves data from ODS into Tableau (a business intelligence tool used across the agency for data analysis and visualization) using a query that captures a reporting period. Therefore, each quarter the query is modified to include data from the recent quarter. The retrieved dataset contains award type, registration ID, disaster number and code, region, declaration date, Covid or Non-Covid related assistance, award date, designated date, expected applied date, program code, eligibility code and amount. The results are calculated using tableau formulas. The average days is calculated by summing the days between the applied date and the date of the first award and then dividing by the number of applicants that received a first award in that reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	For consistency, a standard definition of “applied date” is used. To prevent data entry errors, NEMIS has controls such as date validation, the use of dropdown fields rather than free text when possible, and the use of database fields formatted for specific purposes (numbers, dates, etc.). To prevent retrieval errors, RAD analysts extract data using a validated and approved SQL query to pull data into Tableau, which then cleans the data and checks for anomalous entries. To prevent calculation and analysis errors, the calculations are automated using Tableau. Initial findings from RRAD analysts are shared between the RRAD Analysis Branch, Reporting Branch, and Director to double-check counts and analysis results. Findings are then shared with the Individual Assistance director and their SMEs for verification and review before submitting to senior leadership. Questions and discrepancies are reviewed and corrected, if necessary.

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 SME 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.
Strategic Alignment	Objective 5.1: Coordinate Federal Response to Incidents
Scope of Data	The scope of the data includes statistics of all incident management employees during the year of reporting. The performance measure is a composite measure made up of two components: force strength and force qualification. The scope of data for force strength is the number of IM workforce on board, or hired, at FEMA. The scope of data for force qualification is based on statistics collected for each member of the IM workforce. These statistics include the associated percentages of required trainings and tasks completed by position.
Data Source	The foundational inputs for the measure are recorded, reported, and stored in FEMA's Deployment Tracking System (DTS). DTS is an SQL database which is accessed and managed by FEMA's Field Operations Directorate (FOD) staff. Planning factors are informed by the Cumulative Distribution Function (CDF) outputs of Event Staffing Models, which relate workloads from expected disaster scenarios to the number of personnel required to manage the workload.
Data Collection Methodology	Data computed for force qualification level begins with taking an individual's overall qualification level based on training and completion percentage. Task completion weighs 75% while training completion weighs 25%. To determine the qualification level of the entire IM workforce, sum all qualification values together then divide the total staff qualification level by the qualification planning factor of 13,605. To calculate force strength, take the total number of IM workforce and divide by the force strength planning factor of 17,670. Lastly, to obtain the composite number, multiple both force strength and qualification results by 0.5 and sum the numbers together.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data used to compile this measure resides on information systems subject to control and maintenance by the programs' subject-matter experts, who use this same data to inform and

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

Performance Measure	Percent of applicants satisfied with simplicity of the Individuals and Households Program
Program	Response and Recovery
Description	This measure assesses the disasters survivors' impressions about the simplicity of the procedures required to receive disaster relief from the Individuals and Households Program. The Individuals and Households Program provides direct and financial assistance through procedures related to disaster information, financial assistance, completing the application and the inspection. Managers will use insights derived from survey results to help drive customer experience improvements.
Strategic Alignment	Objective 5.3: Support Equitable Community Recovery
Scope of Data	The unit of analysis is a survey response rating of how strongly disaster survivors agree with five survey questions from three different surveys (Initial Survey, Contract Survey, and Assessment Survey). Questions included in the measure are 1) FEMA providing easy to understand disaster assistance information, 2) FEMA financial assistance helping to meet disaster related needs, 3) Simplicity of completing application for FEMA assistance, 4) FEMA financial assistance arriving in a reasonable about of time and 5) overall inspection experience. The survey population is a random sample of disaster survivors from active disasters. The confidence interval for these surveys is 95% and the margin of error is +/- 5%. The measure's scope includes all valid responses to the telephone and electronic surveys. The surveys produce results using the five-point Likert scale, therefore the attribute is the numeric rating. All survey ratings for the specified questions are included to obtain an average.
Data Source	The data are stored in the Enterprise Customer Survey System (ECSS) which is an integrated system for both CATI and electronic distribution of survey links. Survey results are then uploaded into the EDW using a Secure File Transfer Protocol (SFTP) process for easy retrieve for statistical analysis and reporting. ECSS contains all survey responses. In addition, it contains information associated with survey administration such as survey disposition, queuing management,

	scheduling/assignment, etc. that assist the surveyor performance metrics and survey research. RRAD manages ECSS.
Data Collection Methodology	Disaster survivors with email preference noted in their disaster assistance application can click on electronically distributed survey links to complete questionnaires, and staff can access survey links within ECSS to complete surveys for phone respondents. RRAD Data Services Sections use SQL file to retrieve data from EDW. The SQL creates a file that is then uploaded into PowerBI by the Measurement and Monitoring Unit. Automated standard calculations within PowerBI are used to generate the results. An average score for each question results is calculated. The average is then converted into a normalized percentage by subtracting 1 from the average score and dividing the result by 4. The formula requires a subtraction of 1 to adjust the lowest score from a 1 to a 0. The percentage scores of each of the 5 questions are then multiplied by a weight of 20%. The weighted scores are added for the final composite score.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent observation and assessment and data entry errors, a quality control section monitors 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 disaster survivors' answers. All surveys use a standard form approved through OMB. To prevent retrieval errors, standard automated SFTP processes and approved SQL scripts are used. To prevent analysis and calculation errors, automated calculations using PowerBI are used.

Performance Measure	Percent of applicants satisfied with the Public Assistance process and customer service
Program	Response and Recovery
Description	This measure evaluates 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.
Strategic Alignment	Objective 5.3: Support Equitable Community Recovery
Scope of Data	The Customer Survey and Analysis Section (CSAS) within the RRAD conducts two surveys for Public Assistance Assessment

	survey quarterly. CSAS delivers the Initial and Assessment surveys to applicants via e-mail. Applicants who do not start or complete the survey will receive a phone call from CSAS to complete the survey. CSAS delivers the survey to applicants by declaration. All applicants receive the survey when their declaration has at least 70% of applicants with awards. Applicants that have not received an award are excluded from the Assessment survey and therefore from the measure. Only applicants that have complete the project development process are include in 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 FEMA RRAD CSAS conducts the survey to collect the data for this measure. They use the Medallia tool for data collection and survey administration. They import, results into the EDW / ODS database for storage. The Recovery Reporting and Analysis Division is the owner of the customer survey data.
Data Collection Methodology	RRAD created an Oracle SQL query to extract the survey data. The Oracle SQL query is saved in a Power BI model stored on a RRAD server folder. The Power BI model is refreshed manually, as needed, to update data in the Power BI model. Any necessary data cleaning is performed in Power BI. Data in the ODS database is updated monthly. The Power BI model is updated, as needed, but at least once a month. This measure calculates the average score for five specific survey questions. The average is then normalized to a scale between 0 and 1. It is normalized by subtracting 1 and dividing the result by 4. The formula requires a subtraction of 1 to adjust the lowest score from a 1 to 0.
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 EDW / 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 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 measure assesses the effectiveness of the Office of Response and Recovery Logistics Management Directorate, Transportation Management Division to deliver lifesaving (Tier 1) and life-sustaining (Tier 2) commodities and key initial response resources from FEMA Distribution Centers (DCs), Incident Support Bases (ISBs), or logistics partners by the validated and agreed upon delivery date. FEMA coordinates the delivery of shipments with contractors and carriers. Senior leaders utilize the information to identify problems with the supply chain, transportation contracts and carriers as well as internal personnel or equipment issues. External factors that impact this measure include availability of Standard Tender of Service (STOS) carriers, as well as the status of the supply chain.
Strategic Alignment	Objective 5.1: Coordinate Federal Response to Incidents
Scope of Data	The unit of analysis is a FEMA responsible shipment. The population is all FEMA responsible shipments. A FEMA responsible shipment is defined as shipment of Tier 1 (Life Saving) or Tier 2 (Life-sustaining) commodities and key initial response resources from FEMA DCs, ISBs, or logistics partners. The attribute is the shipment must arrive by the validated and required delivery date (RDD). The RDD is the established date that both supplier (logistics) and customer (operations) have determined best meets the needs of the situation. The RDD must be within the quarterly reporting period.
Data Source	Data for this measure are stored in the Logistics Supply Chain Management System (LSCMS) as a system of record. The data includes customer order number, required delivery data, order status, in transit visibility, financial status, carrier information, departure and arrival information, distribution orders (authorized payment) and bill of ladings (given to carriers). Requests for assets are entered into LSCMS by the Logistics Management Center (LMC) or the National Assets Logistics Specialist during National Response Coordination Center (NRCC) activation.
Data Collection Methodology	FEMA LMD personnel use LSCMS to track shipment departures and arrivals at forward staging areas FEMA DCs / ISBs. DCs and ISBs fulfill orders, receive shipments, verifies the time received

	and condition of the shipment in LSCMS. Transportation Managers responsible for shipments record in transit visibility status and/or issues during steady state or NRCC activation. If the ISB is not the final destination, Carriers are responsible for entering any information pertaining to their move in LSCMS. (e.g., non carrier delays, breakdowns). LSCMS Supply Chain Intelligence (SCI) reports are exported to excel for analysis and calculation. The numerator is all Tier 1 and Tier 2 shipments delivered within the agreed upon date. The denominator is the total number of Tier 1 and Tier 2 shipments.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent observation and assessment errors, data is verified for accuracy and completeness by the LMC and/or the NRCC Resource Support Section (RSS) when customer orders are submitted. As an additional step, the Transportation Management Division provides in transit visibility through coordination with the Transportation Service Providers and contractors. To prevent data entry and retrieval errors, the Logistics Analysis Office (LAO) validates data with the Transportation Management Division (TMD) for accuracy of the inbound shipment provided by LSCMS to ensure there are no discrepancies. To prevent analysis and calculation errors, TMD maintains a daily log of all orders throughout the year which is used to clarify any questions or discrepancies. LAO conducts monthly validation meetings to check the accuracy of automated data.

U.S. Immigration and Customs Enforcement

Performance Measure	Number of convicted criminal and pending criminal charge arrests
Program	Enforcement and Removal Operations
Description	This measure assesses the effectiveness of efforts to identify, locate, and arrests noncitizen immigrants with criminal convictions or pending criminal charges. Senior leadership will be able to use the results of this metric to evaluate agency performance and inform critical programmatic decision-making, particularly regarding the efficient use and distribution of resources. A noncitizen's status as Convicted Criminal or Pending Criminal is determined at the point of the individual's booking into custody according to their criminal history record in EID.
Strategic Alignment	Objective 3.2: Enforce U.S. Immigration Laws
Scope of Data	The unit of analysis is a single ICE Arrest. The attribute that determines whether an arrest is counted in the results is if the individual is a noncitizen and the individual's criminal history status in EID, specifically, whether the individual is recorded as "convicted criminal" or "pending criminal charge." If an individual's status changes from "convicted criminal" or "pending criminal charge" to another status after their arrest, that change will not be reflected in this metric's data. The population includes all ICE Arrests recorded during the fiscal year. The final result is recorded as the sum of all arrests meeting the above criteria.
Data Source	Data for this measure is stored in EID. This database stores and maintains data relating to the investigation, arrest, booking, detention, and/or removal on non-citizens encountered during immigration and law enforcement activities. This database is managed by EID, under Office of the Chief Human Capital Officer (OCIO) of ICE. Law Enforcement and Systems Analysis (LESA) Statistical Tracking Unit (STU) is the office that gathers, analyzes, and reports this data.
Data Collection Methodology	Arrests and noncitizen criminality are derived and calculated from data recorded in the EID database. ICE personnel input this information into the individual's EID record as part of administrative processing for individuals during and immediately after their arrest by an ICE officer. An ETL (extract, transform,

	load) process then takes data from EID to a data warehouse called the ICE Integrated Decision Support (IIDS) System. An analyst uses spreadsheet functionality to calculate the result. Number of convicted criminal and pending criminal charge arrests is calculated by taking the sum of all arrests for which the subject meets the criteria of "convicted criminal" or "pending criminal charge."
Reliability Index	Reliable
Explanation of Data Reliability Check	Headquarters staff validate the completeness and accuracy of the data entered by field offices into the EID through trend analysis. Data is cross-referenced between field office reports, 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. Any inaccuracies will need to be sent to the Unit Chief, who will make the necessary corrections to the tasking query. Systematic features are in place within both the EID and the ENFORCE Alien Removal Module EARM to mitigate manual data entry errors. Where applicable drop-down lists provide users with a set list of values from which to choose. In addition, required fields must be completed for the information to be submitted to the EID. If these fields are not completed an error message will appear.

Performance Measure	Number of convicted criminal and pending criminal charge noncitizen returns and removals from the U.S.
Program	Enforcement and Removal Operations
Description	This measure assesses the effectiveness of efforts to extricate from the U.S. noncitizens with criminal convictions or pending criminal charges. A noncitizen's status as Convicted Criminal or Pending Criminal is determined at the point of the individual's booking into custody according to their criminal history record in EID. Increases in the number of criminal arrests is likely to be representative of improvements and efficiencies achieved in Enforcement and Removal Operations (ERO) processes, particularly regarding the identification, location, and apprehension of noncitizens with criminality who are more likely to pose threats to U.S. public safety. Senior leadership will be able to use the results of this metric to evaluate agency performance and inform critical programmatic decision-making, particularly regarding the efficient use and distribution of resources.
Strategic Alignment	Objective 3.2: Enforce U.S. Immigration Laws

Scope of Data	The unit of analysis is a single ICE Return or Removal. The population includes all ICE Returns and Removals recorded during the fiscal year. The attribute that determines whether a return or removal is counted in the results is the individual's criminal history status in EID, specifically, whether the individual is recorded as "convicted criminal" or "pending criminal charge." If an individual's status changes from "convicted criminal" or "pending criminal charge" to another status after their return/removal, that change will not be reflected in this metric's data. The final metric is recorded as the sum of all returns and removals meeting the above criteria.
Data Source	Data for this measure is stored in EID. This database stores and maintains data relating to the investigation, arrest, booking, detention, and/or return/removal of non-citizens encountered during immigration and law enforcement activities. This database is managed by EID, under OCIO of ICE. LESA is the office that gathers, analyzes, and reports this data.
Data Collection Methodology	Returns/removals and noncitizen criminality are derived and calculated from data recorded in the EID database. ICE personnel input this information into the individual's EID record as part of administrative processing for individuals during and immediately after their return or removal is conducted by an ICE officer. An ETL process then takes data from EID to a data warehouse called the IIDS System. An analyst uses spreadsheet functionality to calculate the result. Number of convicted criminal and pending criminal charge returns and removals from the U.S. is calculated by taking the sum of all returns and removals for which the subject meets the criteria of "convicted criminal" or "pending criminal charge."
Reliability Index	Reliable
Explanation of Data Reliability Check	Headquarters staff validate the completeness and accuracy of the data entered by field offices into EID 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. Data is then cross-referenced between field office detention facility reports of the number of removals, and data entered the database. LESA 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 STU

	Unit Chief, who will make the necessary corrections to the tasking query.

Performance Measure	Percent of detention facilities that meet the National Detention Standards Program during their full annual inspection
Program	Enforcement and Removal Operations
Description	This measures ICE's effectiveness in ensuring all adult detention facilities, with an Average Daily Population (ADP) greater than 1, meet the ICE National Detention Standards Program. ERO juvenile facilities, staging facilities, or holding rooms that may temporarily hold ICE detainees are not included in this metric. The program ensures facilities used to house noncitizens in immigration proceedings or awaiting removal do so in accordance with their contractually obligated ICE National Detention Standards. The program assesses results through conducting annual facility inspections, imposing penalties for noncompliance and providing guidance to facilities in reaching compliance. Life and safety deficiencies are immediately addressed upon receiving a preliminary report.
Strategic Alignment	Objective 3.2: Enforce U.S. Immigration Laws
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 under the ERO Detention Management Control Program (DMCP) with an ADP greater than 1 during the reporting period. The population consists of all adult facilities on the Authorized Facility's List authorized to house ICE detainees under the ERO DMCP that received a full inspection 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 in this metric. The attribute for each unit of analysis is whether the facility was found in compliance with their contractually obligated ICE national detention standard by receiving an overall rating of acceptable/adequate or higher. An overall rating of acceptable/adequate or higher reflects the facility has passed the inspection.
Data Source	Data for this measure is stored in the Office of Detention Oversight's (ODO) Inspection Management System (IMS). The IMS contains data including the date of annual inspection, location of the inspection, the line items for each standard, if it was compliant or noncompliant, and the overall rating. The rating is contained in formal inspection reports provided by ODO and is further reviewed by the Detention Oversight Unit (DOU). The reports and results of the inspections are automatically uploaded and stored in IMS. Data from the IMS is used to

	generate a detailed Compliance Inspection Final Report. The final report is electronically ingested into ERO's Facility Management System (FMS) from the IMS.
Data Collection Methodology	During annual compliance inspections, subject matter experts (SMEs) enter their determination for each line item of compliant or deficient along with a written description of what they observed that justifies that determination on whether detention facilities are compliant with detention standards. SMEs record their assessment of each standard, along with any comments, in real time on the 3-in-1 tablets that contain a standardized inspection worksheet which automatically uploads to IMS. Life/safety deficiencies are immediately addressed upon receiving a preliminary report. ERO uses an automated query in FMS to produce the quarterly results and inspection data for annual inspections across all field offices or facilities that is imported into the DHS OneNumber system. The calculation is the number of facilities passing the annual inspection divided by the number of facilities inspected.
Reliability Index	Reliable
Explanation of Data Reliability Check	The standardized inspection worksheet is programmed into tablets used onsite. The use of IMS algorithms eliminates inspection rating and other system errors. ODO meets annually to review the weighting factors and rules used in the algorithm. Facility inspection reports undergo multiple levels of review to ensure accuracy, including Team Lead, Section Chief and the ODO Unit Chief. The Unit Chief makes the final determination of whether a line item is deficient or not. If the Unit Chief changes the inspector's determination, an explanation and rationale for the change are entered into the IMS system. All final reports are reviewed by ERO and the Inspections and Audit Unit. The error in calculation of results is minimized by the use of automated queries and formatted fields in FMS.

Performance Measure	Total number of noncitizen returns and removals from the U.S.
Program	Enforcement and Removal Operations
Description	This measure assesses ERO effectiveness enforcing immigration law by removing noncitizens without a legal basis to remain in the United States. This measure includes both the return and removal of noncitizens with final orders of removal from the United States by ICE ERO. This measure reflects the program's efforts to enforce immigration law by identifying, apprehending, processing, and removing noncitizen immigrants from the United States.

Strategic Alignment	Objective 3.2: Enforce U.S. Immigration Laws
Scope of Data	The unit of analysis is a noncitizen without proper legal residency authorization within the United States. The population is all noncitizens without proper legal residency authorization an instance of a return or removals of a noncitizen immigrant from within the United States. The attribute to be counted is if a noncitizen was removed or returned.
Data Source	Data for this measure is stored in EID, which tracks all arrests, detentions, and removals. LESA's STU is the office that gathers, analyzes, and submits this data.
Data Collection Methodology	Headquarters staff validate the completeness and accuracy of the data entered by field offices into EID 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.
Reliability Index	Reliable
Explanation of Data Reliability Check	Headquarters staff validate the completeness and accuracy of the data entered by field offices into EID through trend analysis to look for aberrations and unusual patterns. Data is analyzed on a weekly basis and compared to statistics from prior months and the previous year. An additional reliability check occurs when data is cross-referenced between field office detention facility reports of the number of removals, and data entered into the database. The Statistical Tracking unit checks for consistency of the results or measuring instrument through validation, back-end testing, or reproducibility of the data through alternative methodology. Depending upon the degree of consistency between two measures of the same measure allows the statistician to determine whether the data is considered reliable and or stable. Any inaccuracies will need to be sent to the Unit Chief, who will make the necessary corrections to the tasking query.

Performance Measure	Number of disruptions and dismantlements resulting from significant human trafficking, labor exploitation, and child exploitation investigations
Program	Homeland Security Investigations
Description	This measure reports the number of significant investigations of human trafficking, labor exploitation, and child exploitation that resulted in a disruption or dismantlement. To be considered significant, the investigation must involve a high-threat transnational criminal organization (TCO) or individuals engaged in criminal activity related to human trafficking, labor exploitation, 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.
Strategic Alignment	Objective 6.3: Detect, Apprehend, and Disrupt Perpetrators
Scope of Data	The unit of analysis is a Significant Case Review (SCR). The population is all SCRs within the reporting period. The attribute is an SCR that resulted in a disruption or a dismantlement of high-threat domestic or transnational criminal organizations (TCO) or individuals engaged in criminal activity related to human trafficking, labor exploitation, or child exploitation. The following SCR investigative threshold categories are used to identify the investigative population; 01D,01I, 06A, 06B, 06C, 06D, 06E, 06F, 07A, 07B, 07C, and 07D. SCRs consist of three types of submissions: an initial significant investigation, a disruption, and a dismantlement. The scope of results includes cases that were determined by the SCR process to be a disruption, or a dismantlement of high-threat domestic or transnational criminal organizations or individuals engaged in criminal activity related to human trafficking, labor exploitation, or child exploitation.
Data Source	Data is entered in the SCR module located in the Investigative Case Management (ICM) system. ICM serves as Homeland Security Investigation's (HSI) core law enforcement case-management tool. ICM enables program personnel to create an electronic case file that organizes and links all records and documents associated with an investigation, and to record investigative hours. ICM is the official system of record used to initiate cases, identify case categories, and record and report substantive case information during the investigative process, capturing arrest, indictment, conviction, and case closure.

	Management of the SCR program resides with the Domestic Operations Division located at ICE/HSI 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 or individuals engaged in criminal activity approved through the SCR process during the reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent observation and assessment errors, the data is reviewed by the Special Agent's Group Supervisor and the Special Agent in Charge provides the initial reliability check for this data. Confirmation by HQ that the case is significant is another reliability check. A third reliability check is conducted when the results produced by analysts are reviewed by HSI leadership. To prevent data entry and retrieval errors, analysts at headquarters conduct quality control verification on all data received through ICM to ensure performance data are accurate, complete, and unbiased. To prevent analysis and calculation errors, the last reliability check is conducted by the Office of the Chief Financial Officer, Performance Analysis and Evaluation Branch, reviewing the information based on historical trends.

Performance Measure	Number of human trafficking, labor exploitation, and child exploitation victims assisted
Program	Homeland Security Investigations
Description	This measure reports the number of adult or minor victims assisted as a result of human trafficking, labor exploitation, and child exploitation investigations. Human trafficking includes sex trafficking and labor trafficking. Human trafficking, labor exploitation, and child exploitation victims are considered assisted and entered into the Victim Assistance Database (VAD) when a Victim Assistance Program Specialist (VAPS) or Victim Assistance Coordinator (VAC) 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.
Strategic Alignment	Objective 6.2: Identify, Protect, and Support Victims
Scope of Data	The unit of analysis is a victim assisted by HSI. The population includes all victims assisted by HSI. The attribute is if an assisted victim is connected to human trafficking, labor exploitation, and child exploitation. Victims of human trafficking, labor exploitation, and child exploitation, as well as other identified victims who receive assistance, as described in the Measure Description, are recorded in the VAD.
Data Source	The Data is stored in VAD. The HSI VAP maintains the VAD to capture victims assisted by VAPS and VACs in the field. Victims are identified in the VAD by investigative category, to include, but not limited to, human trafficking, labor exploitation, and child exploitation victims. The VAD database also identifies victims by categories, such as the type of victimization, age range, gender ID, citizenship, country of origin.
Data Collection Methodology	Upon the identification of a victim in a human trafficking case (forced labor or sex trafficking) or child exploitation through an HSI led investigation or partnering non-governmental organizations or other law enforcement agencies, the VAPS informs the victim of the rights accorded to them by law and connect them to services and resources. The action of informing victims of their rights and connecting them to needed individual services/resources is recorded in the VAD, i.e., housing, therapy, immigration attorney, medical services. On a quarterly basis, Analysts at Headquarters request VAP personnel to extract and aggregate data from the VAD by querying and counting the number of victims identified in human trafficking, labor exploitation, and child exploitation investigations. HSI HQ analysts compile and export the data to DHS PA&E where it is entered into the PM System for quarterly reporting.
Reliability Index	Reliable
Explanation of Data Reliability Check	VAPS and VACs receive recurring training on the proper entry into the VAD of the victims that receive information about the rights accorded to them by law and that are connected to needed services and resources. VAP Program Manager, Supervisory VAPS, and Unit Chiefs regularly review VAD data for accuracy and completeness. Reports from the VAD can only be generated by the VAP Program Managers, which increases accuracy and minimizes data manipulation by giving too many individuals access to retrieve data from the VAD. To prevent observation and assessment error the VAPS, Supervisory VAPS, and Unit Chiefs provide the initial data reliability check. To

	prevent data entry and retrieval errors a second reliability check is conducted when the results produced by analysts are reviewed by HSI leadership. To prevent analysis and calculation errors analysts at headquarters conduct quality control verification on all data received to ensure performance data are accurate, complete, and unbiased.

Performance Measure	Number of human trafficking, labor exploitation, and child exploitation victims assisted
Program	Homeland Security Investigations
Description	This measure reports the number of training and outreach programs provided by the HSI VAP, the Center for Countering Human Trafficking (CCHT), the Child Exploitation Investigations Unit (CEIU), and Labor Exploitation Program to advance HSI's nationwide public awareness effort, and any other awareness efforts as needed, to encourage victim identification and reporting to law enforcement and preventing crimes of human trafficking, labor exploitation, and child exploitation. Trainings and events are provided to critical partners such as local, state, national, and international law enforcement, prosecutors, judges, forensic interviewers, nongovernmental organizations, social service programs, victim advocates, and survivors.
Strategic Alignment	Objective 6.1: Enhance Prevention through Public Education and Training
Scope of Data	The unit of analysis is a planned outreach or training session to be presented by HSI related to human trafficking, labor exploitation, and child exploitation. The population includes all planned outreach and training sessions to be presented by HSI related to human trafficking, labor exploitation, and child exploitation. The attribute measured is a completed program or presentation of human trafficking, labor exploitation, child exploitation, and victim assistance outreach or training sessions conducted by each respective HSI Division and/or Program.
Data Source	The HSI Cyber Crimes Center (C3), the Victim Assistance Program (VAP), the CCHT, and the Document, Benefit, and Labor Exploitation Unit (DBLEU) maintains documentation and records to capture the number of outreach or training programs presented by their respective personnel in their respective systems of record, such as HSI's ICM System, VAD, and Forensic Interview Program System. Presentations or outreach programs are identified by investigative category, to include human trafficking, labor exploitation, and child exploitation presentations. On a quarterly basis, HSI HQ analysts request and aggregate data from each Division/Program and export the

	data to CFO PA&E where it is entered into the PM System for quarterly reporting.
Data Collection Methodology	The C3, VAP, CCHT, and DBLEU provide outreach and training programs to various entities, as described in the Measure Description. After each completed presentation the program reports the event into their respective system of record and identify and designate presentation type, e.g., human trafficking. HSI HQ analysts request and aggregate data from each Division/Program. Analysts count the total number of outreach or training programs conducted during the reporting period. This allows HSI to accurately determine the total number of human trafficking, labor exploitation, child exploitation, and victims assistance outreach or training sessions provided.
Reliability Index	Reliable
Explanation of Data Reliability Check	C3, VAP, CCHT, and DBLEU personnel receive guidance on the proper entry of outreach and training sessions given and must enter the data within five days of the activity. To prevent observation and assessment error, Program Managers provide the initial data reliability check. To prevent data entry and retrieval errors, a second reliability check is conducted when the results produced by analysts are reviewed by HSI leadership. To prevent analysis and calculation errors, analysts at headquarters conduct quality control verification on all data received to ensure performance data are accurate, complete, and unbiased.

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 TCO engaged in criminal activity related to illicit trade, travel, or finance (both drug-related or non-drug-related); counterterrorism; 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.
Strategic Alignment	Objective 2.3: Counter Transnational Criminal Organizations and Other Illicit Actors

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 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 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 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	Client satisfaction based on the annual OPLA Voice of the Client Survey
Program	Office of the Principal Legal Advisor
Description	This measure assesses the effectiveness of the Office of the Principal Legal Advisor (OPLA) at providing high quality and timely legal advice and training to our clients. Client feedback provided through responses to the annual Voice of the Client Survey will provide insight into the effectiveness and efficiency of those efforts and provide actionable data on which OPLA will be able to identify gaps and adapt to better serve our clients' needs.
Strategic Alignment	Objective 3.2: Enforce U.S. Immigration Laws
Scope of Data	The unit of analysis is a submitted survey from the annual OPLA Voice of the Client Survey. The population is all surveys submitted during the reporting period. For a survey to be counted, the survey response to the question of whether "OPLA is a valuable partner in my ability to achieve the mission of ICE" must either "agree" or "strongly agree." Survey results are a subjective response provided by clients responding to the Voice of the Client Survey. Any OPLA client (including non-supervisory) may complete the Voice of the Client Survey.
Data Source	Data for this measure is collected via survey responses to the annual Voice of the Client Survey, which is publicized to and solicited from OPLA's HQ and field location clients. The survey is completed utilizing Survey Monkey and responses are collected by OPLA's Knowledge Management Division, for analysis by OPLA contract statisticians.
Data Collection Methodology	A survey link (currently through Survey Monkey) is distributed to OPLA clients through individual outreach, publication in the ICE Breaker, and an ICE broadcast message from the Office of the Director. Clients submit their responses using the provided Survey Monkey link, which are then collected, analyzed, and reported by OPLA contract statisticians in OPLA's Knowledge Management Division. Each substantive question has response

	options on a five-point Likert scale (strongly disagree, disagree, undecided, agree, and strongly agree) and a "not applicable" option. OPLA's statisticians provide both a total number of responses and a corresponding percentage of responses to each question. Each respondent can answer each question for multiple HQ divisions or field locations, which are counted separately. OPLA's statisticians will report the combined percentage for "agree" and "strongly agree" results to the question "OPLA is a valuable partner in my ability to achieve the mission of ICE."
Reliability Index	Reliable
Explanation of Data Reliability Check	Survey respondents complete a standardized questionnaire and submit responses only directly accessible by OPLA's Knowledge Management Division. To prevent data entry errors, Survey Monkey does not allow one person to answer the same question more than once for the same location or division. In addition, answers are selected from a list. Statisticians within the Knowledge Management Division conduct ongoing analysis.

Performance Measure	Number of case actions that contribute to the management and reduction of the backlog of cases on the Executive Office for Immigration Review docket at the start of the fiscal year
Program	Office of the Principal Legal Advisor
Description	This measure captures OPLA's efforts to pursue just outcomes and docket efficiencies, as reflected through actions that contribute to cases being removed, or not added-to, the active Executive Office for Immigration Review (EOIR) docket. Qualifying case actions include, but are not limited to, grants of relief, removal orders, dismissals, administrative closures, declining to file a Notice to Appear (NTA), and any other similar action taken as a result of a docket efficiency initiative, in which OPLA did not reserve appeal.
Strategic Alignment	Objective 3.2: Enforce U.S. Immigration Laws
Scope of Data	The unit of analysis is a case with a pending NTA. The population is all cases with a pending NTA. The attribute is whether a case action was taken by the program to manage or remove the case as a part of the EOIR docket backlog. The program's case actions include, but are not limited to, grants of relief, removal orders, dismissals, administrative closures, declining to file an NTA, or any other similar action taken as a result of a docket efficiency initiative.
Data Source	The Principal Legal Advisor's Network (PLAnet) system is OPLA's case management system that documents and tracks litigation

	before EOIR, advice and guidance provided to OPLA's clients, agency taskings, and administrative work performed by OPLA's attorney and support personnel. Data stored in PLAnet is input manually by OPLA attorneys and support staff. EOIR is the official recordkeeper of proceedings for administrative immigration cases; however, PLAnet data is not validated against EOIR records. The Office of the Chief Information Officer manages the PLAnet system located at ICE Headquarters. The data retrieved for this measure is based solely on what is collected within the PLAnet system.
Data Collection Methodology	Once a case action is completed, OPLA attorneys and support staff enter the results in PLAnet. OPLA's Knowledge Management Division (KMD) will use SQL to run a report for the reporting period to identify the number of qualifying cases from data that is exported from PLAnet. The qualifying cases will be identified using specific combinations of current and future PLAnet case criteria, as defined by any applicable OPLA standard operating procedures or PLAnet tracking guidance. The calculation is the number of case actions that contributed to the more effective management and reduction of the docket backlog of the Executive Office for Immigration Review.
Reliability Index	Reliable
Explanation of Data Reliability Check	KMD statisticians review and confirm the accuracy of the data presented on a quarterly basis. For quality control purposes, statisticians independently process and analyze the data using the defined criteria of the request. Standardized SQL commands help prevent errors in downloading the data from PLAnet. To prevent analysis and calculation errors, the KMD statisticians compare results to ensure consistency. If errors are found, the statisticians review the criteria used to derive the statistical results to confirm accuracy of the measure. Once the accuracy of the criteria has been confirmed, the statisticians individually re-run the analysis to determine whether the same results are obtained as a method of measuring the validity and reliability of the data output. Where possible, PLAnet utilizes formatted fields and dropdown menus to prevent data entry errors.

Performance Measure	Number of stakeholder engagements conducted
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. External factors and changes in policies and regulations may lower the results independent of program actions.
Strategic Alignment	Objective 3.2: Enforce U.S. Immigration Laws
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 templatized 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.

Transportation Security Administration

Performance Measure	Average number of days for DHS Traveler Redress Inquiry Program redress requests to be closed
Program	Aviation Screening Operations
Description	This measure describes the average number of days for the processing of traveler redress requests, excluding the time for the traveler to submit all required documents. Travelers can be any individuals who have inquiries or seek resolution regarding difficulties they experience during their travel screening at transportation hubs, such as airports, or crossing U.S. borders. Travelers can be passengers, pilots, or individuals applying for Visas and Passports. 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. 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.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
Scope of Data	The unit of analysis for this measure is a complete redress application, one that includes all required documents. The attribute is the number of calendar days it takes to close a case, which is measured from the time an application is completed (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 population of this measure is all closed cases for each reporting period. The amount of time does not include the number of days that 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 TRIP Service Console, a Salesforce 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. The system has a report that is automatically updated with each closed case that tracks the Average Age of Case closure. Individuals with PMO Manager and/or TRIP Administrator access can look at the report any time they want. When there is a data call the report is pulled for the FY YTD Case closures and the information is submitted for review. The report shows Case Number, Date Opened, Date Closed, Days in Info Needed, and Case Age. The report can be exported in an Excel spreadsheet, or it can be viewed in the Salesforce system.
Data Collection Methodology	The data collection process begins when the traveler submits their application to the DHS TRIP System. Then a redress program specialist (RPS) reviews the case; if more information is needed the applicant is notified. Once all necessary information is provided, a RPS adjudicates it. When all work is complete, the RPS reviews the work and closes the case with a Final Determination Letter. When cases are closed, they are added to the Case Closed Report which pulls data from the TRIP Service Console using existing reports of closed cases that show the average amount of time it is taking to close a case. The amount of time does not include the days an application is in Info Needed status. To calculate this measure, the total number of days to close for all cases closed in the reporting period are divided by the number of cases closed in the reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent observation and assessment errors DHS TRIP the system tracks the date the case was submitted, the date the case was closed, and any days the case was in Info Needed. The days between case open and case closed are calculated and the number of days in info needed are subtracted from that number to come up with the case age at closure. PMO Managers and System Administrators review the data provided by the Case Age Report for consistency and accuracy. To prevent data entry and retrieval errors, DHS TRIP utilizes a report that has formatted fields. PMO Managers and System Administrators review to check for anomalies or discrepancies. To prevent analysis and calculations errors, DHS TRIP uses a Salesforce report functionality to calculate the Average Case Age. Monthly and quarterly results are subjected to multi-level review to check for anomalies or discrepancies.

Performance Measure	Number of respondents for Passenger Experience Survey
Program	Aviation Screening Operations
Description	This measure assesses compliance with an established baseline requirement for the number of respondents for the passenger

	experience survey at the security screening checkpoints. The passenger experience survey collects passenger feedback at the security screening checkpoint. Such feedback impacts strategic customer experience (CX) improvement initiatives and drives the evolution of CX roadmaps towards increased customer satisfaction and trust in government. The measure aligns to the agency goal to advance the customer experience and aligns to the strategy to standardize customer feedback methodology.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
Scope of Data	The unit of analysis is any one passenger who responds to the passenger experience survey. A unit is included once a passenger completes the passenger experience survey. The population includes any and all passengers who voluntarily and anonymously consent to participating in the passenger experience survey at any airport where TSA provides support. There are no limits of the population. The sample population of respondents is selected at random. The attribute/characteristic the unit of analysis must possess to be counted in the results is consent to participate in the survey. The range of scores that may be given on the attribute is consent/non-consent and the scores are assigned to the units of analysis by written documentation on the survey.
Data Source	Data for this measure are stored in Survey Monkey. Survey Monkey is the DHS approved survey data collection platform. The system contains data on passenger feedback from the Paperwork Reduction Act approved passenger experience survey. On an annual basis, the agency will administer the passenger experience survey and begin collecting respondent data for a period of no more than 2 weeks during a Paperwork Reduction Act approved timeframe. At the conclusion of the survey the DHS survey administrator executes a query that compiles the data from the Survey Monkey platform. The DHS survey administrator manages the Survey Monkey system and downloads data into the excel spreadsheets and transfers the spreadsheets to the office reporting the results.
Data Collection Methodology	Upon voluntary and anonymous consent, a passenger will respond to the passenger experience survey at the conclusion of their screening experience. At that time, the unit of analysis will formally be included as a respondent for data collection purposes. Data is retrieved through the compilation of all units collected in Survey Monkey. Analysis on this measure is the addition of all respondents to obtain a total number of respondents (x) and compare it against the baseline

	requirement (7000) to assess the measurement differential (7000-x=measurement differential).
Reliability Index	Reliable
Explanation of Data Reliability Check	Error mitigation procedures specifically applied to the assessment of the unit of analysis include using a standardized form that defines the standards being assessed. Also, a standardized script is used by survey administrators to ensure consent is received both verbally and in written form. The honor system is used to mitigate false respondent survey entries in Survey Monkey by survey administrators. Primary external factors that could adversely impact the results include Transportation Security Officer attrition which may decrease organic manpower support to administer the passenger experience survey and preventing a baseline measurement from being met. Likewise, a catastrophic event at any airport could adversely impact the results by creating an environment whereby passengers do not feel comfortable providing feedback on their experience at the screening checkpoint.

Performance Measure	Number of states with International Organization of Standardization-compliant mobile driver's licenses accepted at the TSA checkpoint
Program	Aviation Screening Operations
Description	This measure assesses States with International Organization of Standardization (ISO)-compliant mobile driver's licenses (mDLs) that are accepted at the TSA checkpoint. 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. One of the first steps in the security screening process is identification verification and boarding pass verification.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
Scope of Data	The unit of analysis is a single U.S. state, federal district, or territory. Each state, federal district, and territory is counted separately and only counted once regardless of the number of technology platforms they partner with. The population includes all U.S. states, federal districts, and territories that issue driver's licenses. The attribute is whether TSA accepts a state, federal district, or territory's ISO-compliant mDL at the TSA checkpoint. A state, federal district, or territory's mDL is considered publicly launched and accepted by TSA if the state is listed on tsa.gov/digital-id. The state, federal district, or territory may or

	may not publish a press release. A state, federal district, or territory is scored as accepted or not accepted.
Data Source	TSA enters into Cooperative Research and Development Agreements (CRADAs) with mDL state-issuing authorities. When a state has met the requirements of the CRADA, residents with a state-issued mDL are able to participate in operational assessments at airports. At TSA checkpoints, after a passenger consents, Credential Authentication Technology (CAT-2) will securely receive digital identity information from the mDL at the airport checkpoint and verify the passenger's identity. When a passenger's identity is verified by CAT-2 only the necessary information is requested. Passengers will control the access to and use of the mDL kept in their mobile devices. TSA does not copy or store the mDL unless it is done in a limited testing environment for evaluation of the effectiveness of the operational assessment. In that instance, TSA informs the passenger through PIAs, signage, and other means.
Data Collection Methodology	Once a State launches an eligible mDL solution that complies with the foundational international standard (ISO/IEC 18013-5), that State communicates with TSA's Requirements and Capabilities Analysis (RCA) Office on the development and implementation of the solution. The calculation is a count.
Reliability Index	Reliable
Explanation of Data Reliability Check	During identify verification at the checkpoint, the passenger presents the mDL and the CAT-2 verifies the legitimacy of the mDL. CAT-2 verifies the passenger's identity by authenticating the mDL, matching the mDL information against information provided when they made the flight reservation, and matching the live photo captured against the photo on the mDL. Data shared between a passenger's mobile device and a TSA checkpoint is always passed through secure, encrypted channels. TSA's ID authentication occurs offline by design; neither TSA nor the passenger's device requires an internet connection or communication back to an ID issuer which prevents tracking by any ID issuer. TSA deliberately chose this design to enhance passenger privacy, data protection, and cybersecurity.

Performance Measure	Percent of canine teams that pass operational training assessments within 60 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 60 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.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
Scope of Data	The unit of analysis is a single TM assessment conducted approximately 60 days after an EDC or PSC team returns to their duty stations. The population includes the total number of TM assessments conducted approximately 60 days after EDC and PSC canine teams return to their duty stations during the year. The attribute is whether a TM assessment is included in the result and is whether a given EDC or PSC passes the TM assessment approximately 60 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	Data is stored in an asset management system and Canine Web Site (CWS) that are owned by Security Operations, Domestic Aviation Operations (DAO). This measure gathers data from TMs conducted by CTC Training Instructors (TIs) approximately 60 days after the canine team returns to their duty location. CWS records training records, utilization and canine teams' annual evaluation results to include pass/fail TMs entered by CTC training instructors who conducted the event.
Data Collection Methodology	CTC TIs conduct TMs approximately 60 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.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
Scope of Data	The unit of analysis is a passenger screened by TSA. The population is the total nationwide airport passenger throughput. The attribute is receiving expedited screening based on assessed low risk through TSA PreCheck or some other form of eligible expedited screening population. Such as known crew members, active-duty service members, members of Congress and other trusted populations. Known Suspected Terrorists are always ineligible, as well as those listed on the PreCheck Disqualification Protocol. Expedited passengers are anyone that's TSA Pre✓® eligible, passengers 12 and under or over 75 years of age, SIDA badge holders, Members of Congress, Global Entry, SENTRI, and NEXUS who are U.S. Citizens and Elite Frequent Flyers with additional rules applied, CBP Trusted

	Travelers, TSA Trusted Travelers, and military and flight crew in uniform.
Data Source	Data is stored in the TSA's Performance Measurement Information System (PMIS) and the Known Crew Member (KCM) Systems. PMIS captures and analyzes daily operational information to achieve performance goals, including information related to passenger throughput, wait times, airport resource maintenance for checkpoints, baggage, and screening equipment, etc. The hourly data submissions are manually entered by the airport designees on a daily basis. The data is then imported into the enterprise-level business intelligence tool used for reporting and analysis. PMIS generates a nightly job that runs at 3:45AM, making the data available for real-time reports. The system owner is Jae Oh in Performance Management. The daily KCM reported data is received by email subscription kcmsupport@arinc.com, owned by RCA, which includes the previous days KCM totals broken out by airport at the checkpoint level for each hour of the day.
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 airline flight and cabin crew personnel is collected automatically within the KCM system and reported to be input into PMIS. Daily data runs are completed by 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 assessed low risk. 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. The quarterly measure report is run using PIMS by inserting the identified quarter time-frame using two administrator created metrics defined as total expedited screened throughput divided by the total customer throughput.
Reliability Index	Reliable
Explanation of Data Reliability Check	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 daily. Missing information is immediately flagged using a PMIS Data Quality Assurance Report created in the PIMS BI Tool. Performance Management staff sends the report to each airport POC and the Airport Operations Center (AOC) who governs the airports performance ensuring flags are addressed.

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. This measure relates to all covered flights operated by aircraft operators who fly into, out of and over the United States that are required to have a Model Security Program (MSP), Aircraft Operator Standard Security Program (AOSSP) or Twelve-Five Standard Security Program (TFSSP). 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.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
Scope of Data	The unit of analysis is an individual credential and privileged access application presented to TSA Enrollment Services Vetting Programs (ESVP) for biographic-based counter-terrorism, criminal, public health, or immigration vetting during the quarter. An application may include domestic and international aircrew members, aviation workers, air cargo, and maritime port workers, HAZMAT drivers, Federal Aviation Administration (FAA) certificate holders; Pre-Check applicants, and non-citizen flight school students. The population is all credential and privileged access applications presented to TSA ESVP for biographic-based counter-terrorism, criminal, public health, or immigration vetting. The attribute is whether passenger submissions by aircraft operators are evaluated and analyzed for timeliness, completeness and accuracy per regulations and applicable security programs on monthly and quarterly basis.
Data Source	This data source for Aviation Screening data is captured and processed in a secured database. 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
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.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
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 Paperwork Reduction Act approved) and responses (i.e. Likert scale) to collect passenger sentiment. The questions are 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.

Performance Measure	Percent of Transportation Security Officers that achieve a first-time pass rate on the Job Knowledge Test
Program	Aviation Screening Operations

Description	This measure gauges the knowledge retention of new hire Transportation Security Officers (TSOs) on skills learned during TSO Basic Training Program (TSO-BTP), including security screening skills, procedures, policies, and information needed to successfully perform the duties of a TSO. TSOs are assessed with the Job Knowledge Test (JKT). Scores outside the passing range give trainers indicators there may be issues that need to be reviewed and remediated. This measure will ensure new hire students return to their airports with the knowledge needed to successfully complete on-the-job training. It is essential that TSOs retain and apply this knowledge to ensure the respectful treatment and safety of the traveling public.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
Scope of Data	The unit of analysis is a student that undergoes TSO-BTP and takes the JKT for the first time. The population reflects all students that undergo TSO-BTP and take the JKT within the designated timeframe. The JKT is a requirement for completing the TSO-BTP. The attribute is whether a student passes the test on the first attempt. It is a pass/fail test and serves as an indicator 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 skills. A passing score consists of answering 80% of questions correctly on a 50-question examination.
Data Source	This measure gathers data from the Online Learning Center (OLC), which serves as the system of record for TSO-BTP test results. The data in this report is classified Sensitive Security Information (SSI) due to the detailed scores by TSO and airport location.
Data Collection Methodology	The test is delivered through the TSA OLC learning management system. The results are recorded in the OLC automatically. A member of the OLC team generates ad hoc Item Status Reports using qualifiers to identify which students passed the JKT. The measure result calculated is the total number of students that passed the JKT on their first attempt divided by the total number of students who took the JKT for the first time within the measure period.
Reliability Index	Reliable
Explanation of Data Reliability Check	The JKT data is validated at least twice before any reporting is conducted in the OLC. The TSA-A Operations Team checks the JKT 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. This process validates the data recorded twice before course completion is marked for a student. In the case of an OLC to JKT data load failure for a student, a Tier 2 OLC Administrator attempts to reload the test for a student. If the systems will not connect a student may take the JKT on paper or digitally with a Test Administrator and the score will be entered into OLC manually. This score will be included in the general verification process noted above. The confirmation of the Pass/Fail status by the TSA-A provides the data integrity to conduct reporting of JKT First time pass rates.

Performance Measure	Percent of air carriers operating from domestic airports in compliance with standard security programs
Program	Other Operations and Enforcement
Description	This performance measure gauges the security posture of air carriers operating at domestic airports through compliance with Standard Security Programs issued by TSA. Standard Security Programs serve as the security baseline for an air carrier. 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.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
Scope of Data	The unit of analysis for this measure includes all inspections conducted by Transportation Security Inspectors at U.S. domestic airports that regularly serve operations of an air carriers as described in 49 CFR Parts 1544 and 1546.
Data Source	The data to support this measure is contained in the Performance and Results Information System (PARIS), which serves as the official repository for TSA. The repository is owned by the office of Information Technology and managed by Security Operations - Compliance Directorate.
Data Collection Methodology	Domestic Air Carrier Inspections are performed in accordance with an annual Compliance Work Plan (CWP) and the National Inspection Standards (NIS). The CWP specifies frequencies of inspections while the NIS specifies the specific methodology required to establish compliance for each set of regulation prompts which are derived from the requirements of 49 CFR Parts 1544 and 1546. When inspections are completed, the results of each are entered into PARIS with an outcome of “In Compliance, Not in Compliance, or Not Applicable.” If the prompts are found to be “Not in Compliance” a finding is

	recorded. This data collected for this measure pulls all inspections with or without findings from PARIS. The total percentage reported represents the total number of 1544 and 1546 inspections without findings divided by the total number of 1544 and 1546 inspections.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data reliability is ensured through a series of actions. Entering a record into PARIS requires review and approval by a TSA official who has been delegated that authority (e.g., a first line supervisor or designee). No record can be approved by the same individual who created the record. All regulations required by the Aviation NIS are pre-populated in PARIS. Inspectors utilize a drop down menu to select if the regulation prompt was "In Compliance, Not in Compliance, or Not Applicable." The approval process requires the approver to review the record based on the prompt's methodology set forth in the NIS. PARIS inspection records are audited quarterly by Compliance headquarters personnel through the National Quality Control Program. This system of checks and balances provides for improved quality and data integrity. This measure is calculated using spreadsheet functionalities focusing only on approved inspections and associated findings within approved inspections.

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 (inspections) of shippers based on cargo regulations 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.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
Scope of Data	The unit of analysis for this measure includes all inspections conducted by Transportation Security Inspectors of all cargo

	screening facilities to the security standards that are specified in Title 49 Code of Federal Regulations Part 1544.
Data Source	The data to support this measure is contained in PARIS, which serves as the official repository for TSA. The repository is owned by the office of Information Technology and managed by Security Operations - Compliance Directorate.
Data Collection Methodology	Domestic Cargo Screening Inspections are performed in accordance with an annual CWP and the NIS. The CWP specifies frequencies of inspections while the NIS specifies the specific methodology required to establish compliance for each set of regulation prompts which are derived from the requirements of 49 CFR Part 1500 Series. When inspections are completed, the results of each are entered into PARIS with an outcome of "In Compliance, Not in Compliance, or Not Applicable." If the prompts are found to be "Not in Compliance" a finding is recorded. This data collected for this measure pulls all inspections with or without findings from PARIS. The total percentage reported represents the total number of cargo screening inspections without findings divided by the total number of cargo screening inspections.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data reliability is ensured through a series of actions. Entering a record into PARIS requires review and approval by a TSA official who has been delegated that authority (e.g., a first line supervisor or designee). No record can be approved by the same individual who created the record. All regulations required by the Cargo NIS are pre-populated in PARIS. Inspectors utilize a drop down menu to select if the regulation prompt was "In Compliance, Not in Compliance, or Not Applicable." The approval process requires the approver to review the record based on the prompt's methodology set forth in the NIS. PARIS inspection records are audited quarterly by Compliance headquarters personnel through the National Quality Control Program. This system of checks and balances provides for improved quality and data integrity. This measure is calculated using spreadsheet functionalities focusing only on approved inspections and associated findings within approved inspections.

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 of Departure (LPD) airports identified and then discussed through stakeholder engagements and partnerships 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 vulnerabilities. The program also identifies vulnerabilities beyond the ICAO requirements through inspections, however TSA has limited authority to enforce mitigation activities. Through the identification of vulnerabilities, the sharing of findings and best practices, the program works to mitigate aviation security risks and to reduce vulnerabilities at foreign LPD airports.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
Scope of Data	The unit of analysis is a vulnerability identified by inspectors through assessments and inspections at a foreign LPD. 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 and recommended practices (SARPs). Inspections evaluate compliance of aircraft operators and foreign air carriers with TSA regulations beyond the international standards. The population is all vulnerabilities identified by inspectors through assessments and inspections at foreign LPDs within the reporting period. The attribute is whether the vulnerability was discussed through stakeholder engagements, trainings, partnerships, or other activities such as equipment procurement, and categorized as either closed or being addressed.
Data Source	The data source is the Global Risk Analysis and Decision Support (GRADS) Vulnerability Report. It contains data pertaining to all open and reported closed vulnerabilities at foreign LPD airports, and is maintained by TSA's Office of Compliance. GRADS is the repository for all LPD data, including past and present inspection and assessment results, a repository for governance information at each LPD, and root cause determinations.
Data Collection Methodology	Standards for assessments and inspections are based on International Civil Aviation Organization standards and TSA regulations. Inspectors conduct on-site assessments and inspections to identify vulnerabilities which are then entered

	into GRADs by the inspection team. Then, IO tracks status updates provided by a variety of program staff, including TSA Representatives, International Capacity Development Operations trainers and instructors, and inspectors who regularly engage with stakeholders. Twice a year, IO runs a report and validates that all identified vulnerabilities, both open and reported closed, have a clear description, root cause, and mitigation actions taken to address the specific vulnerability. The measure result calculated is the total number of closed and open vulnerabilities with a corrective action plan or other mitigation strategies divided by the total number of identified vulnerabilities at LPD airports within the reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	As part of the Foreign Airport Assessment Program Standard Operating Procedures process, International 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 review and approve all vulnerabilities submitted. If the data is incomplete, the Vulnerability Approver must reject the vulnerability and provide comments to justify the rejection in GRADS. In addition, Desk Officers and Program Analysts are responsible for conducting validation reports and quality control reports to track all identified vulnerabilities and their closure.

Performance Measure	Percent of inspected interchanges of rail cars containing Rail Security Sensitive Materials (RSSM) in compliance with security standards
Program	Other Operations and Enforcement
Description	This measure identifies the level of compliance for chain of custody activity and documentation required under 49 CFR Section 1580.205 involving loaded railcars containing RSSM. These interchanges occur between freight railroad carriers to other carriers and from freight rail carriers to certain chemical shippers and receivers. Interchanges are monitored and documentation is reviewed by TSA surface inspectors to ensure they are executed in accordance with regulations. Inspectors observe interchanges at established high-risk interchange points throughout their area of operations and complete an inspection based on guidelines and frequencies established at the beginning of each fiscal year in the Surface Operations Work Plan and Surface Program Manual. The secure transfer of custody of these rail cars strengthens transportation security

	and protects potentially impacted populations at these critical points in the freight rail supply chain.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
Scope of Data	The unit of analysis is a single transfer of custody of a loaded rail car carrying a RSSM at a high-risk freight rail interchange. The population is the total number of RSSM transfers inspected at high-risk freight rail interchanges under 49 CFR § 1580.205. Non-hazardous materials (i.e., materials not covered under 49 CFR § 1580.205) are not included. The attribute is whether the transfer at the attended high risk freight rail interchange was in compliance with security procedures and standards. A compliant transfer is a documented transfer of custody of a loaded rail car carrying RSSM from rail carrier to carrier, rail carrier to receiver, or shipper to carrier. Surface Operations Inspectors observe 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 by inspectors and maintained within PARIS. The system contains data on when an interchange was inspected, inspection results, and the location of interchange. Surface Operations HQ compiles the results from PARIS to provide the annual report on percentage of inspected RSSM interchanges.
Data Collection Methodology	Inspectors conduct 49 CFR § 1580.205 inspections of RSSM interchanges. Inspectors enter all details and results usually within 24 hours of completion. Data is retrieved from the system for metrics calculation by designated TSA Surface Operations staff every 2 weeks for internal reporting. Data is exported from the system as an Excel spreadsheet for review and metric calculation. Metric calculated by dividing the total of 'Compliant' inspections by total inspections and expressed as a percentage.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent errors and ensure data quality, PARIS employs analytical dashboards that compiles data, verifies accuracy (has a pre-text feature), and provides reports for review and approval. The system has select formatted fields, user-friendly dropdown menus, pre-defined selection and filtering features. 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–Inspectors, or other individuals exercising management authority. An additional quality control measure is the

	review/approval process by Surface Regional Security Inspectors. Once retrieved by designated staff at TSA HQ, data is reviewed again for errors and metrics are calculated.

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 (inspections) of shippers based on cargo regulations specified in Title 49 CFR 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.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
Scope of Data	The unit of analysis is an international cargo screening. The population is all international cargo screening inspections completed by the Transportation Security Specialists (TSS) conducting inspections at international locations. The attribute is if the result of the inspection is compliant.
Data Source	The data to support this measure is contained in PARIS, which serves as the data repository for TSA and international Compliance records. When an entity is inspected, the data and all findings are entered into PARIS by TSS conducting inspections at international locations.
Data Collection Methodology	International Cargo Screening Inspections are performed in accordance with an annual Master Work Plan (MWP). The CWP specifies frequencies of inspections along with ICAO Standards and Practices (SARPs). When inspections are completed, the results of each are entered into PARIS with an outcome of “In Compliance, Not in Compliance, or Not Applicable.” If the prompts are found to be “Not in Compliance” a finding is recorded. Findings are then addressed in an investigation record. This data collected for this measure pulls all inspections with or without investigations from PARIS. The total percentage reported represents the total number of international cargo

	screening inspections without investigations divided by the total number of cargo screening inspections.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data reliability is ensured through a series of actions. Entering a record into PARIS requires review and approval by a TSA official who has been delegated that authority (e.g., a first line supervisor or designee). No record can be approved by the same individual who created the record. All regulations required by ICAO SARPs are pre-populated in PARIS. Inspectors utilize a drop down menu to select if the regulation prompt was "In Compliance, Not in Compliance, or Not Applicable." The approval process requires the approver to review the record based on the prompt's methodology set forth by ICAO SARPs. PARIS inspection records are audited quarterly through the quality control reviews of the International Compliance Inspectors in Compliance HQ. This system of checks and balances provides for improved quality and data integrity. This measure is calculated using spreadsheet functionalities focusing only on approved inspections and associated findings within approved inspections.

Performance Measure	Percent of overall compliance of domestic airports with established aviation security indicators
Program	Other Operations and Enforcement
Description	Compliance Field Inspectors engage with Airport Security Coordinators to assess and mitigate risk at airports nationwide. To aide with identifying vulnerabilities, the TSA Industry Engagements Manager under Policy, Plans, and Engagement conducts monthly calls to discuss trends and analysis of findings. Continuous airport-centric testing is conducted to assess the compliance posture of airports nationwide. Human Error is a key factor in most violations. Compliance and Enrollment Services & Vetting Programs and the Security Threat Assessment Division engage regularly to vet aviation employee workers at U.S. commercial airports for links to terrorism, lawful presence, and disqualifying criminal offenses and U.S. commercial air carrier workers for disqualifying criminal offenses. By the end of Q4, 14,169 inspections were conducted. 13,158 of these inspections did not contain findings. Historically, TSA has not met this target.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats

Scope of Data	The unit of analysis for this measure includes all inspections conducted by Transportation Security Inspectors at U.S. airports that regularly serve operations of an aircraft operator as described in 49 CFR Part 1544.
Data Source	The data to support this measure is contained in PARIS, which serves as the official repository for TSA. The repository is owned by the office of Information Technology and managed by Security Operations - Compliance Directorate.
Data Collection Methodology	Domestic Airport Inspections are performed in accordance with an annual CWP and the NIS. The CWP specifies frequencies of inspections while the NIS specifies the specific methodology required to establish compliance for each set of regulation prompts which are derived from the requirements of 49 CFR Part 1542. When inspections are completed, the results of each are entered into PARIS with an outcome of "In Compliance, Not in Compliance, or Not Applicable." If the prompts are found to be "Not in Compliance" a finding is recorded. This data collected for this measure pulls all inspections with or without findings from PARIS. The total percentage reported represents the total number of airport inspections without findings divided by the total number of airport inspections.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data reliability is ensured through a series of actions. Entering a record into PARIS requires review and approval by a TSA official who has been delegated that authority (e.g., a first line supervisor or designee). No record can be approved by the same individual who created the record. All regulations required by the Airport NIS are pre-populated in PARIS. Inspectors utilize a drop down menu to select if the regulation prompt was "In Compliance, Not in Compliance, or Not Applicable." The approval process requires the approver to review the record based on the prompt's methodology set forth in the NIS. PARIS inspection records are audited quarterly by Compliance headquarters personnel through the National Quality Control Program. This system of checks and balances provides for improved quality and data integrity. This measure is calculated using spreadsheet functionalities focusing only on approved inspections and associated findings within approved inspections.

Performance Measure	Percent of overall level of implementation of industry agreed upon Security Action Items by Public Transportation Passenger Rail entities

Program	Other Operations and Enforcement
Description	This measure provides the rate of implementation by the largest Public Transportation Passenger Rail (PTPR) and other commuter transportation agencies on security standards and practices related to five critical Security Action Items (SAIs) reviewed during a Baseline Assessment for Security Enhancement (BASE). BASEs are completed jointly by a team of Transportation Security Inspectors (TSI) and participating systems. The entities provide information on key SAIs including: established written system security plans and emergency response plans; background investigations; security and emergency response training; exercises and drills; and public awareness. SAIs are key indicators of the overall security posture of a PTPR system. Measuring implementation of these SAIs assesses a transit system's vulnerabilities and is part of an overall risk reduction process.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
Scope of Data	The population for this measure includes the latest ratings for every participating PTPR system with an average daily ridership (DR) of 60,000 or more and evaluated on a BASE during the last 20 quarters. The unit of analysis is the score on a zero to four rating on each of the five relevant SAIs. The attribute is measured using results of achieving an 'Effectively Implementing' rating in each of these five SAIs.
Data Source	The source of data for this measure are BASEs 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 Salesforce database TSA application Surface Data Management System (SDMS) managed by Security Operations.
Data Collection Methodology	During a BASE, TSIs conduct interviews, review documents, and assign a score for each of the 17 SAIs based on the level of implementation. Only five SAIs are relevant to this measure. After TSIs post their BASE reports in SDMS, Security Operations (SO) TSS extract the past 20 quarters of data from BASEs conducted on agencies with over 60,000 DR. To obtain the numerator for this measure, TSSs 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 five SAIs. The denominator is the total number of agencies receiving a BASE inclusive of all ratings on the five SAIs. The result is the number of PTPR agencies achieving an 'Effectively Implementing' rating

	for the five SAIs divided by the total number of PTPR agencies rated for the past 20 quarters.
Reliability Index	Reliable
Explanation of Data Reliability Check	Quality reviews are performed on assessment data at multiple points in the process. Supervisory Transportation Security Inspectors (S-TSI) and Regional Security Inspectors (RSI) review the BASE reports conducted by TSI in their areas for accuracy, thoroughness, and quality. These reviews may result in inquiries to clarify information and inconsistencies in the 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.

Performance Measure	Percent of surface operations cybersecurity workforce personnel completing required cybersecurity training
Program	Other Operations and Enforcement
Description	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—IT Specialists, Transportation Security Specialists, Program Analysts, Surface TSIs in both supervisory and non-supervisory roles that perform cybersecurity-related assignments. These assignments may include program management/reviews, assessments, inspections, and supporting engagements with stakeholders. Completion of cybersecurity training creates a cybersecurity enriched surface operations workforce, improving staffing, education, and retention capabilities.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
Scope of Data	The unit of analysis is a single individual within Surface Operations that supports cybersecurity related program, projects, assignments, and engagements. Training requirements are determined on an annual basis by Surface Operations leadership based on operational needs and are assigned to employees via their Learning Plans. The population includes all surface operations personnel that support cybersecurity related programs, 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. Due to schedules, seasonal requirements, and training frequency, this measure will be reported on an annual basis.
Data Source	This measure gathers data from employee learning plans and completion rates which are tracked in TSA's OLC. All completed courses are available in an employee's OLC record. OLC is managed by Training and Development, with Surface Operations maintaining an OLC Training Point of Contact (TPOC) for record entry, data management, and reporting.
Data Collection Methodology	Surface Operations maintains written and electronic training records related to cybersecurity training completion and in OLC tracking. 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, which is approved 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. 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 TPOC inputs course completion information into the OLC.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent observation and assessment errors, the OLC is an automated learning system that tracks the assigning of annual training, the completion of training and mandatory certification requirements. Reports are generated for leadership's review to ensure employees' training requirements are being met promptly. For external trainings, the TPOC runs an OLC report, and the name rosters are then compared to staffing records to ensure accurate recording.

U.S. Coast Guard

Performance Measure	Availability of maritime navigation aids
Program	Marine Transportation System Management
Description	This measure indicates the hours that short-range federal Aids to Navigation (ATON) 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 ATON is counted as not being available from the initial time a discrepancy is reported until the time the discrepancy is corrected. Maintaining the availability of short-range federal ATON is an essential part of Coast Guard efforts with federal, state, local, tribal, and territorial partners, the marine industry, maritime associations, and the international community to safeguard our nation's waterway systems and the economic activity that flows through them.
Strategic Alignment	Objective 2.2: Expedite Lawful Trade and Travel
Scope of Data	The unit of analysis is the total number of hours of expected availability for a single short-range ATON. The population is the total number of hours of expected availability for all short-range ATONs. The attribute is the degree to which an ATON meets the target number of hours for availability. The measure is expressed as a percentage of the total number of hours of actual ATON availability as compared to the total number of planned or expected hours of availability for a given time period.
Data Source	The U.S. Aids to Navigation Information Management System (USAIMS) is the official system used by the U.S. Coast Guard to store information relating to short-range aids to navigation. USAIMS is managed by the Coast Guard Office of Navigation Systems (CG-NAV) and is used to report and store pertinent information relating to the condition and availability of short-range aids to navigation.
Data Collection Methodology	The total time short-range ATON 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, and then multiplying again 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 number of ATONs that are currently or have been discrepant during the measured period of time, and the total time these ATONs have been discrepant. Trained personnel in each Coast Guard District input discrepancy data in the USAIMS system. The Coast Guard

	Office of Navigation Systems queries USAIMS on a monthly basis and conducts several layers of review before reporting the results of its manual calculation to arrive at the measure result.
Reliability Index	Reliable
Explanation of Data Reliability Check	To ensure consistency and integrity, data entry in the USAIMS 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 for generating local Notices to Mariners, as well as by designated Coast Guard Unit and District personnel. Temporary changes to the short-range Aids to Navigation System are not considered because this is a point-in-time measure, and any discrepancies are due to the number of aids in the system on the day the report is run. The Coast Guard Office of Navigation Systems queries USAIMS on a monthly basis and conducts several layers of review before reporting the results of its manual calculation to arrive at the measure result. Quarterly, the availability rate is provided to Coast Guard Program Analysis and Evaluation which conducts additional review for accuracy.

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 (FFV), engaged in or prepared to illegally fish in the U.S. EEZ, that are interdicted by the Coast Guard. Illegal, unreported, and unregulated fishing (IUUF) is a national security threat with destabilizing effects on vulnerable coastal U.S. States and world markets. Protecting the integrity of the nation's maritime borders and ensuring the health of U.S. fisheries is a priority Coast Guard mission. Preventing foreign fishing vessels from illegally encroaching on the U.S. EEZ is a key outcome of the Coast Guard's broader efforts to combat IUUF, which include promoting targeted, effective, intelligence-driven enforcement operations; countering predatory and irresponsible behavior; promoting international rules-based order in the maritime domain; and expanding multilateral fisheries enforcement cooperation with international partners.
Strategic Alignment	Objective 2.2: Expedite Lawful Trade and Travel
Scope of Data	The unit of analysis a single detected illegal incursion made by a foreign fishing vessel into the U.S. EEZ. The population is all detected illegal incursions made by foreign fishing vessels inside the U.S. EEZ. A detection is evidence of an illegal

	incursion by a FFV into the U.S. EEZ. Detections may be made using electronic, manual, or other observation methods. Interdiction is defined as the stopping, boarding, and/or seizure of an FFV illegally fishing in the U.S. EEZ. Illegal incursions by FFVs are detected by the Coast Guard and through other sources such as partner agency reporting. The measure's attribute is whether the Coast Guard interdicts an FFV that was detected illegally entering the U.S. EEZ.
Data Source	Source data is collected monthly from Living Marine Resource (LMR) Enforcement Summary Reports and recorded in the Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) system. Data is entered into MISLE by field units after completion of foreign fishing vessel interdictions. MISLE is the primary operations business support system for capturing and reporting information supporting Coast Guard marine safety, security, environmental protection, and law enforcement programs. The MISLE database is managed by the Coast Guard Office of C5I Program Management (CG-68) and is used for recording and disseminating information about maritime resources including vessels, facilities, and waterways, in addition to managing information flow from triggering events to incident response and follow-on actions. The Coast Guard's Office of Maritime Law Enforcement receives LMR Enforcement Summary Reports from sub-units which are used for data validation and program management purposes.
Data Collection Methodology	Foreign vessels illegally fishing inside the U.S. EEZ are detected by the Coast Guard and other sources, and an interdiction occurs when the Coast Guard completes the interdiction process to include proper documentation of the incursion. Coast Guard personnel document the results of an interdiction using a law enforcement case package and record that information in the MISLE database following a completed interdiction. 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 total number of Coast Guard interdictions of foreign fishing vessels illegally fishing inside the U.S. EEZ, divided by the total number of foreign fishing vessels detected illegally fishing inside the U.S. EEZ, expressed as a percentage.
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 data entries, and limit choices to pre-determined options. The LMR Enforcement Summary Report purpose, format, and submission

	requirements, as well as guidance on the use of MISLE, are all provided in the Maritime Law Enforcement Manual. Comprehensive training and these user guides help ensure reliability, and the MISLE application itself contains embedded Help screens to further assist with data entry. Additionally, Coast Guard District summaries of EEZ cases are reviewed monthly by Areas and submitted to the Coast Guard Office of Maritime Law Enforcement, which are used to help 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. Detected migrants includes all migrants interdicted at sea plus the number of migrants that land in the U.S., its territories, or possessions. Through its enforcement of U.S. immigration laws and regulations in the maritime domain, the Coast Guard works with partners to detect, deter, and respond to migrants attempting to unlawfully enter the U.S. by sea. The Coast Guard is committed to preventing unsafe voyages at sea and encouraging migrants to use safe and orderly pathways to lawfully enter the United States. The fundamental challenge to Coast Guard migrant interdiction success is the difficulty in predicting the impact of interconnected push-pull political, economic, social, technological, and environmental factors that affect individuals' decisions to remain in place or migrate.
Strategic Alignment	Objective 2.1: Secure and Manage Air, Land, and Maritime Borders
Scope of Data	The unit of analysis is a detected attempt by an undocumented migrant of any nationality to unlawfully enter the U.S. by sea. The population is the total number of undocumented migrants of any nationality detected by the Coast Guard and its partners attempting to unlawfully enter the U.S. and excludes unknown or undetected migrant flow. The measure's attribute is whether the Coast Guard or its partners interdict a migrant detected attempting to unlawfully enter the U.S., its possessions, or territories through maritime routes.
Data Source	Data is stored in the U.S. Coast Guard MISLE database. The Coast Guard receives daily reports on known flow of migrants through its own intelligence and from international and federal partner agencies. Data on migrant flow is aggregated and reconciled monthly by the Coast Guard Office of Maritime Law

	Enforcement (CG-MLE) and then entered into the MISLE database. MISLE is the primary operations business support system for capturing and reporting the information required to support Coast Guard marine safety, security, environmental protection, and law enforcement programs. The MISLE database is managed by the Coast Guard Office of C5I Program Management (CG-68) and is used for recording and disseminating information about maritime resources including vessels, facilities, and waterways, in addition to managing information flow from triggering events to incident response and follow-on actions.
Data Collection Methodology	The Coast Guard Intelligence Coordination Center compiles and analyzes information from Coast Guard and partner intelligence on known migrant flow in the maritime domain. This information is then sent to CG-MLE for further aggregation and reconciliation before being entered into the MISLE database, which automatically calculates the measure results. The migrant interdiction effectiveness rate is expressed as a percentage that compares the number of migrants attempting to unlawfully enter the U.S. interdicted at sea by the Coast Guard and partner agencies, including deceased migrants recovered from smuggling events, to the total volume of known migrant flow, which includes those migrants that are interdicted, land and are apprehended, land and get away, deterred migrants (i.e., those who abort their venture and return to country of departure), and those found deceased and presumed lost at sea.
Reliability Index	Reliable
Explanation of Data Reliability Check	The Coast Guard Intelligence Coordination Center compiles and analyzes information from Coast Guard and partner intelligence on known migrant flow in the maritime domain. 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 unique pathways exist for Cubans to become lawful permanent residents. The Cuban Adjustment Act incentivizes Cubans to self-report as doing so is a requirement to apply for lawful permanent resident status. Migrant landing information is validated across multiple sources using Coast Guard intelligence guidelines that favor conservative estimates, and MISLE data entry and retrieval is compared with additional formal and informal reports and sources monthly to ensure data completeness, reliability, and validity.

Performance Measure	Observed fishing regulation compliance rate
Program	Maritime Law Enforcement
Description	This measure reports the percentage of all fishing vessels boarded and inspected by the U.S. Coast Guard, which had no documented significant violations of domestic fisheries regulations. The U.S. Coast Guard boards and inspects U.S. commercial, charter, and recreational fishing vessels subject to the jurisdiction of the United States. The commercial, charter, and recreational fishing industry generates hundreds of billions of dollars in sales annually and supports millions of jobs. Healthy fish stocks underpin the food security of coastal communities, and compliance with fishing regulations positively affects the sustainability of U.S. fisheries and the economic security of communities who rely on the sustainable harvest of these resources.
Strategic Alignment	Objective 2.2: Expedite Lawful Trade and Travel
Scope of Data	The unit of analysis is a single boarding and inspection of a U.S. commercial, charter, or recreational fishing vessel. The population includes all boardings and inspections of U.S. commercial, charter, and recreational fishing vessels conducted for domestic fisheries law enforcement purposes and excludes boardings of foreign vessels not permitted to fish within the U.S. EEZ. The measure's attribute is whether an individual U.S. commercial or recreational fishing vessel receives a compliant rating, which the Coast Guard assigns if the vessel is found to have no documented significant violations of domestic fisheries regulations during the boarding and inspection. Significant fisheries violations are violations deemed to be of critical importance by Coast Guard District Enforcement staff due to the value, economic importance, operational effect, and/or severity of the violation.
Data Source	Boardings, inspections, and significant violations of domestic fisheries regulations are documented by Coast Guard personnel on boarding forms and then entered in the MISLE database after completion of the boardings. MISLE is the primary operations business support system for capturing and reporting the information required to support Coast Guard marine safety, security, environmental protection, and law enforcement programs. MISLE is managed by the Coast Guard Office of C5I Program Management (CG-68) and is used for recording and disseminating information about maritime resources including vessels, facilities, and waterways, in addition to managing information flow from triggering events to incident response and follow-on actions. MISLE has an LMR Significant Violation Action

	data category that allows for identification, sorting, and filtering of information about vessels with significant violations.
Data Collection Methodology	U.S. Coast Guard personnel document violations of domestic fisheries regulations in Coast Guard boarding forms and enter them into the MISLE database after completion of fisheries enforcement boardings. The data is extracted by a manual query in MISLE conducted by Coast Guard headquarters staff CG-MLE. Once the data is extracted, MLE staff conduct manual calculations to determine the Observed Compliance Rate. To ensure data integrity, MLE staff compares monthly MISLE data to other formal and informal reporting sources, and then works with field units to resolve any discrepancies. The calculated results for a given year are the number of boarded fishing vessels with no documented significant violations of domestic fisheries regulations, divided by the total number of fishing vessels boarded and inspected by the Coast Guard, expressed as a percentage.
Reliability Index	Reliable
Explanation of Data Reliability Check	The consistency and integrity of MISLE data entry is controlled through program logic and pull-down menus that require users to provide key elements, prohibit inappropriate data entries, and limit choices to pre-determined options. Reliability is further ensured by comprehensive training and user guides, and MISLE itself has embedded Help screens. District, Area, and Headquarters staff review, validate, and assess the data on a quarterly basis as part of the 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 to ensure its completeness and reliability. When discrepancies are identified, Coast Guard headquarters staff in the Office of MLE coordinate with field personnel to rectify differences in data.

Performance Measure	Number of breaches at high-risk maritime facilities
Program	Maritime Prevention
Description	This measure reports the number of security breaches at facilities subject to the Maritime Transportation Security Act (MTSA) where no Transportation Security Incident has occurred, but established security measures have been circumvented, eluded, or violated. MTSA facilities are a high-risk subset of the national waterfront facility population given the nature of their activities and/or the products they handle. As such, they pose a greater risk for significant loss of life, environmental damage, or economic disruption if attacked. MTSA regulated facilities

	constitute more than 3,400 high-risk subset of all waterfront facilities. They are facilities that handle certain dangerous cargoes, liquid natural gas, transfer oil, hazardous materials in bulk; or receive foreign cargo vessels greater than 100 gross tons, U.S. cargo vessels greater than 100 gross tons carrying certain dangerous cargoes, or vessels carrying more than 150 passengers.
Strategic Alignment	Objective 1.2: Prevent and Disrupt Terrorist and Nation State Threats
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 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 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 $200,000; actual or constructive loss of certain vessels; discharge of oil of 10,000

	gallons or more; or a discharge of a reportable quantity of a hazardous substance. The Coast Guard works with partners to align prevention activities in the maritime domain associated with the safe operation of vessels and facilities and continually seeks to promote the safety of life and property at sea.
Strategic Alignment	Objective 5.1: Coordinate Federal Response to Incidents
Scope of Data	The unit of analysis is single Serious Marine Incident reported to or detected by the Coast Guard and partners, and the population is all serious marine incidents as defined in 46 CFR 4.03-2 that are reported to or detected by the Coast Guard and partners. The measure's attribute is whether the Coast guard determines the reported or detected event to meet the definitional requirement for a serious marine incident outlined in 46 CFR 4.03-1, 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.
Data Source	Data regarding serious marine incidents are recorded in the MISLE database, which includes dates, event types, property damage amounts, involved facilities, and several other data points for each incident. MISLE is the primary operations business support system for capturing and reporting the information required to support Coast Guard marine safety, security, environmental protection, and law enforcement programs. MISLE is managed by the Coast Guard Office of C5I Program Management (CG-68) and is used for recording and disseminating information about maritime resources including vessels, facilities, and waterways, in addition to managing information flow from triggering events to incident response and follow-on actions.
Data Collection Methodology	CG-INV receives, investigates, and verifies intelligence received from Coast Guard and partner reporting on serious marine incidents before recording that information in the MISLE database. To obtain the number of serious marine incidents for a given time period, investigations recorded in MISLE are manually extracted from the database and counted by CG-INV. 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 regarding serious marine incidents, published data is subject to revision with the greatest impact on recent quarters.
Reliability Index	Reliable

Explanation of Data Reliability Check	The consistency and integrity of MISLE data entry is controlled through program logic and pull-down menus that require users to provide key elements, prohibit inappropriate data entries, and limit choices to pre-determined options. Reliability is further ensured through comprehensive training and user guides, and MISLE itself contains embedded Help screens. Data verification and validation is also ensured through regular review of records by CG-INV and relevant Coast Guard program managers.

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. The search and rescue mission is one of the Coast Guard's oldest, and saving lives in peril at sea continues to be a priority for the service.
Strategic Alignment	Objective 5.1: Coordinate Federal Response to Incidents
Scope of Data	The unit of analysis is a single maritime distress incident reported to the U.S. Coast Guard, judged by Coast Guard operational commanders as requiring a response. The population is all such incidents to which the Coast Guard responds, and includes lives recorded as saved, lost after notification, or unaccounted, with the measure's attribute being whether a life or lives were saved. Single incidents with 11 or more people saved, lost, or unaccounted are excluded from the population so as not to skew results or impede trend analysis.
Data Source	All maritime distress incidents reported to the U.S. Coast Guard that are judged by U.S. Coast Guard operational commanders as requiring a response—and associated response data—are recorded in the U.S. Coast Guard's MISLE database. Data is extracted from MISLE using a Coast Guard Business Intelligence (CGBI) cube. MISLE is the primary operations business support system for capturing and reporting the information required to support Coast Guard marine safety, security, environmental protection, and law enforcement programs. MISLE is managed by the Coast Guard Office of C5I Program Management (CG-68) and is used for recording and disseminating information about maritime resources including vessels, facilities, and waterways,

	in addition to managing information flow from triggering events to incident response and follow-on actions.
Data Collection Methodology	Coast Guard operational response units record needed data in MISLE following response to an incident. The CGBI cube used to extract MISLE data is formulated to only look at cases with 0-10 lives impacted. The CGBI cube also automatically calculates the results for this measure and expresses them as a percentage, comparing the total number of lives recorded as saved to the total number of lives recorded as saved, lost after notification, or unaccounted in a given time period. Periodically, CGBI calculations are verified manually by the Office of Search and Rescue and the Office of Program Analysis and Evaluation.
Reliability Index	Reliable
Explanation of Data Reliability Check	The consistency and integrity of MISLE data entry is controlled through program logic and pull-down menus that require users to provide key elements, prohibit inappropriate data entries, 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, 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.
Strategic Alignment	Objective 2.2: Expedite Lawful Trade and Travel
Scope of Data	The population includes all MSRO associated with Tactical Activity plans for the 37 COTP zones. These MSRO occur at vessels, facilities, key assets, and other critical infrastructure at maritime ports. Tactical Activity Plans include only MSRO that

	impact addressable risk, which is risk the U.S. Coast Guard can address with its current capabilities and authorities. The scope of the results includes information about MSRO from the Tactical Activity Plans that were actually executed by the U.S. Coast Guard and/or federal, state, and local partners.
Data Source	MSRO data comes from the MISLE database what is managed by Office of C4 & Sensors Capability (CG-761). MSRO executed by federal, state, and local partners are collected in a formatted spreadsheet and entered into MISLE by the relevant COTP. The Maritime Security Risk Analysis Model (MSRAM) system managed by the Office of International and Domestic Port Security (CG-PSA) contains the data that is used to calculate the addressable risks to the 37 COTP zones using a variety of data such as port subject matter experts' judgements of vulnerabilities, actual port activity data, and intelligence. CGBI and associated data tools are used to pull data from MISLE and MSRAM to populate Risk-Based Maritime Security and Response Operations (RBMSRO) tools. These tools are used for both creating the 37 ports Tactical Activity Plans and for conducting the actual calculations for this measure.
Data Collection Methodology	The 37 COTPs gather a variety of data annually to update risk estimates for their zones. This information informs Ports' Tactical Activity Plans to optimize risk impact with the hours and assets available. Coast Guard units that perform MSRO enter that data directly into MISLE. MSRO performed solely by federal, state, and local partners are recorded on a formatted spreadsheet and collected by the relevant COTPs. Using CGBI, each COTP pulls their MISLE data for their respective zones to populate RBMSRO. The Coast Guard's Headquarters Maritime Security Operations Program Office sums these values for the risk reduction MSRO completed to determine the numerator for this measure. The same office calculates the addressable risk by summing the risk estimates for the 37 COTP Zones for the denominator. The result is calculated by dividing the sum of all MSRO completed by the addressable risk score across all 37 COTP Zones.
Reliability Index	Reliable
Explanation of Data Reliability Check	To ensure consistency and integrity, MISLE data entry is controlled through program logic and pull-down menus that require key elements, prohibit inappropriate entries, and limit choices to pre-determined options. Comprehensive training and user guides help ensure reliability and the MISLE application itself contains embedded Help Screens. MISLE records also get verification and validation through regular records review by District, Area, and Headquarters staffs. Annual risk exposure

	and risk reduction parameters are determined and annually validated in MSRAM by CG-PSA.

U.S. Citizenship and Immigration Services

Performance Measure	Percent of workers determined to be Employment Authorized after an initial mismatch
Program	Employment Status Verification
Description	This measure reports the number of cases in which adjudicating officials in the E-Verify program find a person employment authorized under U.S. law after the program issued the person under examination with a mismatch (Tentative Non-Confirmation) 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 Status Verification Analysts (Legal Instruments Examiners) make a final determination of the employee's eligibility for employment and transmits the determination both to the hiring employer and to the Verification Information System. Ensuring the accuracy of E-Verify program processing reflects the program's intent to minimize negative impacts imposed upon those entitled to undertake employment in the U.S. and those authorized to be employed while ensuring the integrity of immigration benefits by effectively detecting and preventing unauthorized employment.
Strategic Alignment	Objective 3.1: Administer the Immigration System
Scope of Data	The unit of analysis is the percentage of those in which a Tentative Non- Confirmation (i.e. 'initial mismatch') is identified and is then resolved as "Employment Authorized" after an employee has taken action to resolve the mismatch as a part of all E-Verify cases found to be "Employment Authorized". The population of this measure includes all E-Verify cases during the reporting period which are found to be "Employment Authorized". The attribute being counted is an evaluation of the accuracy of E-Verify program processing.
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 mismatch, whether the employee contested the mismatch, and the final eligibility determination. Each quarter, an analyst from the HQ section of Data Analytics and Performance (DAP) Branch in the Verification Division consolidates this data and evaluates the values for each portion

	of this measure. This measure is reported through the DAP Branch to the VER/IRIS Front Office.
Data Collection Methodology	E-Verify case information is entered into the E-Verify system, and cases are stored in the program's VIS. The VIS library is available to analysts in VER through SAS. An Operation Research Analyst in the Data Analytics and Performance Branch at VER queries the data from the VIS library using SAS on a quarterly basis. Validation is conducted with a one-quarter lag. The data is consolidated into an Excel file that tracks the summary of all E-Verify cases to account for those that were immediately verified, those verified without a mismatch, and those verified after a mismatch. Additionally, all cases that are not verified are also categorized. The measure is then calculated using the raw numbers from this analysis: All E-Verify cases that are verified after a mismatch are divided by the total number of cases found to be work authorized (the sum of those immediately verified, those verified without a mismatch, and those verified after a mismatch).
Reliability Index	Reliable
Explanation of Data Reliability Check	E-Verify transaction data from VIS is extracted daily into a SAS library for DAP analysis. Each quarter, analysts apply an algorithm to the extracted data, removing all duplicate and invalid queries. Analysts then query the data to consolidate performance results for program staff for review and clearance.

Performance Measure	Percent of completed social media checks found in compliance with applicable privacy policies
Program	Fraud Prevention and Detection
Description	Operational use of social media for security checks is a defined workload process conducted by the Fraud Detection and National Security Directorate's (FDNS) HQ Social Media Division (SMD) that requires checks for certain immigration requests, as a matter of policy, or based on an articulated justification or for detecting, pursuing, and deterring immigration request fraud. The measure will ensure social media checks comply with Privacy oversight requirements as demonstrated by results of privacy assessments on this process conducted monthly and reported quarterly by USCIS Office of Privacy.
Strategic Alignment	Objective 3.1: Administer the Immigration System
Scope of Data	The unit of analysis is a Social Media check record from the FDNS system of record that is in a completed status. The population is a sample of completed social media checks from the FDNS system of record. FDNS will randomly select a sample

	of completed social media records in the amount necessary to achieve or exceed a .05 margin of error with a 95% confidence interval, which will be a minimum of 32 cases each month, totaling 384 for the full fiscal year. The attribute being measured is if a completed Social Media check is in compliance. Cases in compliance are those that adhere to the Fair Information Practice Principles (FIPPS) and meet criteria including: 1) information collected and documented through social media is relevant to the case, 2) the use of social media is consistent with an approved Social Media Use Template (SMOUT) category, and 3) the use of social media research benefits the agency by producing results that allow USCIS to meets its mission and goals.
Data Source	The data is derived directly from the FDNS system of record, FDNS-DS NextGen. Social media check privacy compliance will be derived through review of monthly samples of completed social media cases. The USCIS Office of Privacy will assess privacy compliance of a completed case sample each month and report results quarterly.
Data Collection Methodology	USCIS will randomly select a sample of completed social media checks each month. The USCIS Office of Privacy will review the random sample of completed social media checks each month, assess compliance with privacy requirements for USCIS operational use of social media, and report results quarterly. Checks in compliance are those that adhere to FIPPS and meet criteria including: 1) information collected and documented through social media is relevant to the case, 2) the use of social media is consistent with an approved SMOUT category, and 3) the use of social media research benefits the agency by producing results that allow USCIS to meets its mission and goals. The result is calculated by dividing the checks found to be in compliance by the total number of completed social media checks assessed in the sample.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data for this measure are collected from the FDNS system of record, which has internal controls to ensure the accuracy of data, including the identification of stages and current status. To ensure that all social media checks are conducted in compliance with privacy requirements, FDNS conducts internal quality assurance reviews, which aligns to DHS and USCIS privacy policies, on all social media checks before completion. Any errors identified are returned to the case officer for resolution before the case is placed in completed status. To prevent analysis and calculation errors, standard and repeatable reporting templates are used. Quarterly assessment

	results are reviewed for anomalies or errors. Prior to delivery to OCFO, a FDNS manager will conduct a final quality check for accuracy of results.

Performance Measure	Average processing time for Application to Register Permanent Residence or Adjust Status (I-485) (in months)
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. 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.
Strategic Alignment	Objective 3.1: Administer the Immigration System
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 Applications for Naturalization (N-400) (in months)
Program	Immigration Services
Description	This measure assesses the ability of 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.
Strategic Alignment	Objective 3.1: Administer the Immigration System
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, 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 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

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. 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-129 (Petition for Nonimmigrant Worker) (in months)
Program	Immigration Services
Description	This measure assesses the ability of the Service Center Operations Directorate (SCOPS) to meet its published adjudication processing goals for the processing 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.
Strategic Alignment	Objective 3.1: Administer the Immigration System
Scope of Data	The unit of analysis is a single I-129 petition that was submitted for processing and has been fully adjudicated. The petition could have started adjudication before the reporting period, but a petition is only included if it finishes adjudication during the reporting period. The population is all I-129 petitions submitted for processing that were fully adjudicated during the reporting period. Eligible categories include E-1, E-2, E-3, H-1B, 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 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 ELIS. The eCISCOR system 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 C3/ELIS System from the time the petition starts until the petition is adjudicated and a decision has been made. The USCIS OPQ exports data from eCISCOR via SAS statistical 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. All quarterly results will be cumulative, with results reported inclusive across quarters for the fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent data entry and retrieval errors, the USA Staffing uses formatted fields and dropdown menus. Standardized reporting scripts 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. A SCOPS data analyst will be assigned to coordinate with OPQ to collect and provide reportable results on a quarterly basis, to include conducting 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. A SCOPS 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)
Program	Immigration Services
Description	This measure assesses the ability of 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 immigrant worker. This measure applies to E11, E12, E21 (non-national interest waiver (NIW)), E32, E31, and EW3 classifications.
Strategic Alignment	Objective 3.1: Administer the Immigration System

Scope of Data	The unit of analysis is a single I-140 petition that was submitted for processing and has been adjudicated. The petition could have started adjudication before the reporting period, but a petition is only included if it finishes adjudication during the reporting period. The population is all I-140 petitions submitted for processing that were fully adjudicated during the reporting period. For this measure, eligible categories include E11, E12, E21 (NIW), E32, E31, and EW3 classifications. 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, eCISCOR, for petitions adjudicated in ELIS. The eCISCOR system 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 C3/ELIS System from the time the petition starts until the petition is adjudicated and a decision has been made. The USCIS OPQ exports data from eCISCOR via SAS statistical 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. All quarterly results will be cumulative, with results reported inclusive across quarters for the fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	To prevent data entry and retrieval errors, the USA Staffing uses formatted fields and dropdown menus. Standardized reporting scripts 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 A SCOPS data analyst will be assigned to coordinate with OPQ to collect and provide reportable results on a quarterly basis, to include conducting 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. A SCOPS manager will conduct a final quality check of the performance measure data.

Performance Measure	Credible Fear average processing time (in days) for detainees
Program	Immigration Services
Description	This measure assesses how quickly the program processes the credible fear claims of individuals held in ICE or U.S. Border Patrol operated detention facilities. The purpose of credible fear screenings is to identify individuals who could establish eligibility for asylum, Statutory withholding of removal, or protection under the regulations implementing the Convention Against Torture and other Cruel, Unusual, or Degrading Treatment or Punishment. This measure reports the average number of days between when USCIS receives a credible fear referral from CBP or ICE and USCIS makes the credible fear determination and serves it upon the individual or administratively closes 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.
Strategic Alignment	Objective 3.1: Administer the Immigration System
Scope of Data	The unit of analysis is the processing time (in days) for a case of an individual who is placed in ICE or U.S. Border Patrol (BP) operated detention facilities who is referred to USCIS for a Credible Fear (CF) interview. The population includes all individuals who are placed in ICE and BP operated detention facilities who are referred to USCIS for Credible Fear processing. The attribute counted is the amount of time (in days) an individual who is in expedited removal, in BP or ICE detention, and expresses an intention to apply for asylum, a fear of persecution or torture, or a fear of returning to their country - from when USCIS receives and accepts the completed packet transferring jurisdiction for an individual and the case is entered into the Global case tracking system; a credible fear claim determination must be made and served upon the individual, or the case administratively closed, to count towards this measure.
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 accurately referred to USCIS and when the credible fear claim determination is made and served upon the individual or the case is administratively closed. Global is maintained by USCIS and data is extracted and consolidated into Excel and PDF formats. Tableau data visualization and business analysis tools

	is a web-based performance analysis tools used to create dashboards and reports on the data.
Data Collection Methodology	On a quarterly basis, analysts extract and analyze CF processing time data that is exported on an ongoing basis by Tableau. 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 and served upon the individual or the case is administratively closed. USCIS exports data from Global using Tableau to create dashboards and reports. Data collection using this tool 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, automated timestamps, 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	Number of asylum determination completions
Program	Immigration Services
Description	This measure assesses the productivity of the asylum officer workforce. The total number of asylum applications completed annually reflects the performance measure result based on capacity and capability of asylum operations. The performance measure is inclusive of non-interview adjudications, interview adjudications, and administrative closures, all of which result in cases being removed from the I-589 backlog. Adjudications may consist of grants, referrals, or denials. The processing of asylum application completions advances the objective to adjudicate

	protection, humanitarian, and other immigration benefits by making determinations on cases of individuals seeking protection from persecution or torture.
Strategic Alignment	Objective 3.1: Administer the Immigration System
Scope of Data	The unit of analysis is an individual I-589, Application for Asylum and for Withholding of Removal. The population is all I-589s. No sampling is used for this measure. The attribute counted is whether an I-589 was completed within the reporting period. An asylum application is considered complete if it receives a grant, denial, referral, an administrative action that completes the case, or transfers jurisdiction from USCIS.
Data Source	Data for this measure is stored in the Global case management system. The I-589, Application for Asylum and for Withholding of Removal, data is extracted from the system and consolidated daily into dashboards and reports using web-based reporting and data visualization tools. The data is managed by USCIS, Refugee, Asylum and International Operations Directorate and reported on by the Asylum Division.
Data Collection Methodology	The data is collected from the I-589 application and interviewing processes either online or by paper and stored in the Global case management system. The data is exported from Global and analyzed in Tableau and the Standard, Management, Analysis, and Reporting Tool (SMART) environments. Historical information and data are collected using data collection and gathering techniques, filters, and sorting for analysis. Numerical daily, monthly, quarterly, and year-to-date data is collected to measure the number of asylum determinations. The calculation for asylum completions is a cumulative aggregated sum of the total applications completed starting on the first day of the first quarter of the fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data reliability checks consist of a 100 percent (non-sampling) supervisory inspections and evaluations of all interviewed completed applications. Process controls and verification methods are used in accordance with Affirmative Policy Guidance, Standard Operating Procedures, and Quality Assurance reviews and analysis. Quality Assurance review checks are conducted randomly and systematically, and scheduled and unscheduled. Data reliability reviews are also integrated as controls within the process.
Performance Measure	Percent of approved applications for naturalization (N-400) that were appropriately decided
Program	Immigration Services

Description	This measure assesses the validity of final decisions of approved Form N-400, Application for Naturalization, by program adjudicators. A random N-400 sample receipts are pulled from ELIS in order to review and validate against the Government Performance and Results Act (GPRA) checklist questionnaire based on the final adjudication of each N-400 application. The results of the findings of these decisional quality reviews are performed by experienced SMEs. The program conducts quality reviews by drawing a statistically valid random sample of approved N-400s on a semi-annual basis. Ensuring 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.
Strategic Alignment	Objective 3.1: Administer the Immigration System
Scope of Data	The unit of analysis is an approved and oathed (sworn and signed) electronic N-400 Form received through ELIS. The population includes a statistically valid random sample of approved N-400s on a semi-annual basis. The confidence level is 90%, an accuracy rate of 85%, and a margin of error of 5%. Typical semi-annual volume is 171,600, resulting in a population sample of 139. The attribute counted are those N-400 files that fail the GPRA Review checklist and are deemed questionable. These files are returned to the original office after review for concurrence or non-concurrence with any error found during the GPRA review but may or may not affect the original approved decision.
Data Source	Data for this measure are stored in ELIS. Program headquarters staff in the OPQ, Office of the Chief Data Officer (OCDO), Advanced Analytics Branch, FOD Performance, Quality, and Data Integrity (PQDI), has access to this database, which is managed by OPQ. 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. The Excel file is stored on FOD's W:/ share drive with PQDI access only.
Data Collection Methodology	After creation of a quality review sample, teams of SMEs review records for each of the approved N-400s selected to complete the GPRA Review checklists, with data entered into an online database (GPRA database). The GPRA database contains the review checklists with formatted fields and dropdown menus for data entry and retrieval. Throughout the review process and data entry phase, the FOD PQDI review lead team monitors data entry to ensure its accuracy. Once the review activity is

	completed, the data from each review checklist is downloaded, manually imported, and tabulated in an Excel spreadsheet for analysis and reporting. FOD PQDI review lead team conducts a review of the data and its calculated results, which are obtained by using Excel functionalities. Results are 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	SMEs use original applicant requests to complete their quality reviews of the sample of approved N-400s, documenting their work using GPRA Review 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 an OPQ SharePoint site documented resolution of discrepancies within 10 business days.

Performance Measure	Percent of approved Applications to Register Permanent Residence or Adjust Status (I-485s) that were appropriately decided
Program	Immigration Services
Description	This measure assesses the validity of final decisions of approved Form I-485, Application to Register Permanent Residence or Adjust Status, by program adjudicators. A random I-485 sample receipts are pulled from ELIS in order to review and validate against the GPRA checklist questionnaire based on the final adjudication of each I-485 application. The results of the findings of these decisional quality reviews are performed by experienced SMEs. The program conducts quality reviews by drawing a statistically valid random sample of approved I-485s on a semi-annual basis. Ensuring 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.
Strategic Alignment	Objective 3.1: Administer the Immigration System
Scope of Data	The unit of analysis is an I-485 Form approved nationwide and received at the program's National Records Center, and electronically received through ELIS. The population is a

	statistically valid random sample of approved I-485s on a semi-annual basis. The confidence level is 90%, an accuracy rate of 85%, and a margin of error of 5%. Typical semi-annual volume is 171,600, resulting in a population sample of 139. The attribute counted are those I-485 files that fail the GPRA Review checklist and are deemed questionable. These files are returned to the original office after review for concurrence or non-concurrence with any error found during the GPRA review but may or may not affect the original approved decision.
Data Source	Data for this measure are stored in ELIS and at the program's National Records Center Program headquarters staff in the Office of Performance and Quality, Office of the Chief Data Officer, Advanced Analytics Branch, FOD PQDI, 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. The program conducts quality reviews of these cases, drawing a statistically valid random sample of approved I-485s on a semi-annual basis. FOD PQDI manages the data at the conclusion of the GPRA activities and prepares the final reports on a semi-annual basis.
Data Collection Methodology	After creation of a quality review sample, teams of SMEs review records for each of the approved I-485s selected to complete the GPRA Review checklists, with data entered into an online database (GPRA database). The GPRA database contains the review checklists with formatted fields and dropdown menus for data entry and retrieval. Throughout the review process and data entry phase, the FOD PQDI review lead team monitors data entry to ensure its accuracy. Once the review activity is completed, the data from each review checklist is downloaded, manually imported, and tabulated in an Excel spreadsheet for analysis and reporting. FOD PQDI review lead team conducts a review of the data and its calculated results, which are obtained by using Excel functionalities. Results are 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	SMEs use original applicant requests to complete their quality reviews of the sample of approved I-485s, documenting their work using GPRA Review 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 an OPQ SharePoint site documented resolution of discrepancies within 10 business days.

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.
Strategic Alignment	Objective 3.1: Administer the Immigration System
Scope of Data	The unit of analysis is an approved and oathed (sworn and signed) electronic N-400 Form that contained derogatory information that has been identified and resolved. The population includes all 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 ELIS with an indication of identified derogatory information. N-400 cases with no derogatory information are excluded from the calculation of this measure. The attribute counted is if an approved and oathed (sworn and signed) electronic N-400 Form that contained derogatory information that has been identified and resolved before the oathing ceremony. In the event issues identified are not resolved before the oathing ceremony, then the attribute is not counted in the numerator as part of the calculation.
Data Source	Data for this measure are stored in USCIS ELIS. ELIS is the system that contains all records of N-400 cases with derogatory information identified and resolved. The eCISCOR business intelligence tool is used to extract the data for N-400 cases oathed with a derogatory information flag identified in ELIS. The system is maintained by the Office of Information Technology (OIT). On an hourly basis, data from ELIS is consolidated into the eCISCOR system.

Data Collection Methodology	Derogatory information identified by adjudicators, or FDNS, is entered in ELIS by checking a flag. Adjudicators record the resolution by checking a resolved flag in the ELIS before scheduling an oath ceremony. Following the end of the quarters, FDNS data team sends a list of N-400 cases with TECS hits to USCIS OPQ. OPQ downloads this data to obtain a list with unique receipts numbers (cases). OPQ runs a query using a statistical program (SAS or Databricks) by selecting the latest resolution for each case that is before the oath date. The total number of cases is then recorded for the calculation. The calculation is the number of cases where derogatory information was resolved before the oath ceremony divided by the total number of cases where there was derogatory information. 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	Derogatory information is identified in ELIS by a Derogatory Information and Resolved flags. 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
Program	Immigration Services
Description	This measure assesses the proportion of pending forms considered as backlog. Backlog is defined as the number of cases pending within the government's control that exceed accepted goals for processing the case. For example, one goal is for USCIS to process all N-400 applications within five months of receipt; cases still pending after five months would be considered backlog. This measure will help senior leadership assess the effectiveness of the agency's multiple initiatives for reducing the existing backlog. These initiatives include strategic staffing, technology enhancements, regulatory and policy changes, and the use of overtime. External factors such as immigration policies, economic security, and issues like the COVID-19 pandemic could have a negative impact on the measure.

Strategic Alignment	Objective 3.1: Administer the Immigration System
Scope of Data	The unit of analysis is a pending case. The population is all active pending cases. The attribute for backlog are those that exceeded cycle time goals. Active pending cases are cases that are awaiting an initial adjudicative decision or reopened cases waiting a final decision that can be worked on by USCIS. Cases are considered backlogged if it is pending longer than the target cycle time for the benefit type. Cycle time is defined as the number of months of receipts that make up the current pending by form type. Due to data latency, each quarterly report includes three months of data but does not conform to the quarters within the federal fiscal year.
Data Source	Data for this measure are stored in the systems of record. From these systems, the USCIS National Performance Report (NPR) is produced by 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 is recognized as the official USCIS source for the number of monthly receipts, completions, and backlog.
Data Collection Methodology	The data for each form is entered into USCIS systems of record from the time the application starts until the application is fully adjudicated. The USCIS OPQ exports data 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.
Reliability Index	Reliable
Explanation of Data Reliability Check	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 applications that were appropriately decided
Program	Immigration Services
Description	This measure assesses the validity of final decisions by program adjudicators on Form I-589, Application for Asylum and for Withholding of Removal, and Form I-590, Registration for Classification as Refugee. A panel of SMEs is convened to

	review a sample of completed applications to determine whether the final decision was appropriately decided. The panel may sustain the decision, recommend a different decision or send the file back to the appropriate component for correction or additional information if it is determined that critical procedures were not correctly followed or the case is lacking sufficient interview evidence. Ensuring 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.
Strategic Alignment	Objective 3.1: Administer the Immigration System
Scope of Data	The scope of this measure includes all decision types on Forms I-589 and I-590 with final decisions which met appropriately decided and evidence criteria among all applications sampled by the program to determine the accuracy rate. The population for the review is determined through discussions with the Refugee, Asylum and International Operations Directorate (RAIO) Divisions and typically consists of adjudication decisions for standard cases that received supervisory review, were documented in case files, and recorded and stored in RAIO case management systems. Cases varying from standard asylum or refugee adjudications due to adherence to a different set of legal, procedural, or administrative guidelines, as well as cases requiring urgent travel or lacking supervisory review, are excluded. The confidence level for each review (90% to 95%) is set to accommodate the underlying purpose and resource requirements of each review at the given time. The sample size of total cases reviewed is the denominator for the calculation.
Data Source	Application and screening decision data are recorded and stored in RAIO case management system, Global. Decisional review check sheets completed by decision reviewers are consolidated in a custom database prepared for the review. The RAIO Strategic Planning and Performance Branch manages the final reporting within USCIS OCFO Performance Measure Management Tool.
Data Collection Methodology	A team of subject matter experts conducts reviews of a sample of the asylum and refugee decisions and documents these reviews using a checklist. The review team uses consensus panels or two-tiered review to analyze the appropriateness of decisions. Cases found to be inappropriately decided are returned to 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 appropriately decided cases in the sample that do not require correction in the form of changing the decision outcome by the total number of cases in the sample.
Reliability Index	Reliable
Explanation of Data Reliability Check	To ensure accuracy of the checklist and panel decisions, multiple layers of subject matter experts review and concur on correcting applications by changing decisions to approve. The results are double-checked by quality assurance experts before the results are submitted to Office of the Chief Financial Officer for submission. OCFO completes subsequent checks of the data during each reporting period, prior to an internal review meeting and before posting data to the DHS Annual Performance Report.

Performance Measure	Percent of respondents satisfied with the citizenship and immigration-related support received from the USCIS Contact Center
Program	Immigration Services
Description	This measure gauges the overall satisfaction of support received from the USCIS Contact Center based on accuracy of information, responsiveness to public inquiries, and accessibility to information. The Qualtrics Automated Omnichannel Survey Tool captures live feedback after customers complete their interaction with the contact center through the interactive voice response (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.
Strategic Alignment	Objective 3.1: Administer the Immigration System
Scope of Data	The population includes all email surveys completed by customers distributed through the Qualtrics Automated Omnichannel Survey Tool once a Service Item is closed after the customer interaction through IVR, telephony, virtual assistant, live chat agent, myUSCIS account experience, and/or website. The customer has the ability to accept or decline the survey. The unit of analysis is an individual survey completed by a customer. The attribute that determines whether a survey is included in the result is whether the customer rates the question as a 4 or a

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

Performance Measure	Percent of students 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 to successfully navigate the naturalization test and interview. Grant recipients are required to administer Comprehensive Adult Student Assessment Systems (CASAS) Citizenship Assessments for student placement and assessment of progress. This measure evaluates the percentage of students receiving civics-based ESL classes who demonstrate a four 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.
Strategic Alignment	Objective 3.1: Administer the Immigration System
Scope of Data	This measure is reported with a one quarter lag because the source data are found in grant recipient quarterly reports which 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 population is all students that received civics-based ESL services from a grant recipient that were pre-and post-tested. The attribute of whether a student is counted in the results is a student who demonstrates a four 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 System for Tracking Activities, Relationships and Services (STARS). The system contains quarterly reports on each permanent resident who receives civics-based ESL classes on the services provided, including dates of enrollment, and pre and post-test scores. The measure will be tracked using quarterly grant recipient performance reports submitted through Grant Book.
Data Collection Methodology	At the beginning and end of a class each participant takes a standardized CASAS Citizenship Assessment. Trained test administrators grade the assessments and record scores in their individualized data management systems. Grant recipients submit quarterly reports via Grant Book. 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 four points 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 access and use Grant Book and 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 monitoring visits to approximately one-third of all new grant recipients. During these visits, program staff members review records (e.g. student intake forms, classroom attendance sheets, student assessment scores, copies of filed Form N-400s, etc.) that were used to compile data for the quarterly reports.

Performance Measure	Percent of total USCIS benefits workload processed digitally in case management systems
Program	Immigration Services
Description	This measure identifies the percent of the agency workload received for processing within the ELIS and Global case management systems. This measure provides visibility into USCIS' efforts to increase the volume of digital processing resulting in improved efficiencies, enhanced accessibility, data security, and better user experience for applicants and USCIS personnel. All USCIS Directorates are stakeholders for this measure due to the large number of benefit forms (and subcategories) that are processed within ELIS and Global. This measure aligns to the agency's goal to "Strengthen the U.S. Legal Immigration System" by enhancing customer service and leveraging technology to transform business processes. It also aligns to the agency's goal to "Promote Effective and Efficient Management and Stewardship" by modernizing and safeguarding IT systems and solutions, improving data quality, and enhancing the experience of those we serve.

Strategic Alignment	Objective 3.1: Administer the Immigration System
Scope of Data	Unit of analysis is an individual form by category digitally processed in ELIS and Global case management systems. Population is total case workload of all applications, petitions, & other requests (forms, cases, filings, or receipts). The attribute counted is a form digitally processed in ELIS & Global to include a paper file that goes to a Lockbox location to be digitized and sent to ELIS, or an applicant uploads a file to ELIS via myUSCIS, or a file upload from a Manual Entry of Application (MEA) location.
Data Source	The data source for this metric is the NPR. The NPR draws data for the total case workload—receipts for applications, petitions, and other requests—from the Performance Analysis System (PASEXEC). The source of the PASEXEC is eCISCOR, the enterprise reporting and repository platform (e.g., USCIS data lake). eCISCOR receives its data from the Case Management systems (hourly from ELIS and Global). OPQ manages the NPR, and OIT manages eCISCOR. OIT Front Office will report the results on a one quarter lag. The data source containing the volume of forms used to calculate the measure is based on a point in time. The data changes daily due to forms that are in route. This impacts the ability to accurately report the cumulative average across quarters within a fiscal year.
Data Collection Methodology	OIT and OPQ analysts extract data from eCISCOR to gather the total number of applications, petitions, and other benefit requests using an automated query. OPQ analysts enter PASEXEC receipts data extracted from eCISCOR into NPR to calculate the total number of applications. The monthly NPR is received by the Transformation Data Scientist Services (TDSS) team and loaded into the Databricks integrated analytics platform environment. The ELIS data is pulled systematically, and manual adjustments are made to ensure data quality and accuracy. The Transformation data scientist also receives an Excel file each month via email consisting of Global cases by Form Type. This data is integrated with the TDSS ELIS report. The total number of forms that are digitally processed consists of all receipts within ELIS and Global (numerator) divided by all receipts received for processing at USCIS as reported in the National Performance Report (denominator).
Reliability Index	Reliable
Explanation of Data Reliability Check	The Transformation data scientist compares the ELIS data from the NPR with data from the ELIS Operational Dashboard, SMART, and TDSS ELIS database. TDSS compares the monthly ELIS receipts (per Form type) among all three sources to ensure

	that we have the most up to date data. The Global data is provided to TDSS by the Global team in an Excel format and manually compared against the corresponding data in the NPR. 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 ensures accuracy of the data.

Performance Measure	Total number of attendees at USCIS public engagements
Program	Immigration Services
Description	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. Public engagements will include scheduled engagements, both virtual and in-person, conducted for the public under the coordination of the Office of Citizenship, Partnership, and Engagement (OCPE). External factors such as immigration policies and issues like the COVID-19 pandemic could have a negative impact on the results for this measure.
Strategic Alignment	Objective 3.1: Administer the Immigration System
Scope of Data	The unit of analysis for this measure is a completed public engagement. 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. The population is all completed public engagements within the period being reported. The attribute to be measured are the number of attendees at USCIS public engagements. 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.

Data Source	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 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.
Data Collection Methodology	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 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.
Reliability Index	Reliable
Explanation of Data Reliability Check	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.

U.S. Secret Service

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.
Strategic Alignment	Objective 1.3: Protect Leaders and Designated Individuals, Facilities, and Events
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.
Strategic Alignment	Objective 1.3: Protect Leaders and Designated Individuals, Facilities, and Events
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%.
Strategic Alignment	Objective 1.3: Protect Leaders and Designated Individuals, Facilities, and Events
Scope of Data	The scope of this measure is the total number of protective stops. Protectees include the President and Vice President of the United States and their immediate families, former presidents, their spouses, and their minor children under the age of 16, major presidential and vice presidential candidates and their spouses, and foreign heads of state.
Data Source	Protective stops information is collected from the Agent Management & Protection Support System. This system is used

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

Performance Measure	Amount of Forfeited Assets Returned to Victims (in millions)
Program	Field Operations
Description	The measure assesses the effectiveness of efforts to return forfeited assets to victims who incurred economic loss as a direct result of the commission of an offense. Forfeited assets include money and other seized goods resulting from criminal/cyber investigations. Victims must file a petition or be eligible under a single petition for remission or mitigation in a civil or criminal forfeiture proceeding or a single ruling on the petition by the Secret Service. This measure corresponds to Secret Service authorities to seize for forfeiture assets derived from, or traceable to, any proceeds obtained directly or indirectly from an offense of a crime, as outlined in 18 U.S.C. § 981 and § 982. If there is no petition filed or assets are not available after the ruling, then victims cannot be compensated, or asset values are returned to the treasury.
Strategic Alignment	Objective 4.4: Combat Cybercrime
Scope of Data	The unit of analysis is a single petition for remission or mitigation in a civil or criminal forfeiture proceeding or a single ruling on the petition by the Secret Service. The population is the total petitions for remission or mitigation in a civil or criminal forfeiture proceeding and rulings on the petitions by the Secret Service. The attribute is total value of the assets returned to victims based on the petitions and rulings. The Secret Service

	initiates asset forfeitures in cases consistent with 18 U.S.C. § 981 and § 982. It is up to the Secret Service to identify which cases are consistent with these statutes, to identify and declare assets to be seized, to identify victims eligible for repayment, and to conduct legal notifications to those whose assets are being seized. This measure represents the final result of this process: the number of dollars that are successfully returned to victims.
Data Source	The data for the measure is recorded in the Field Investigative Reporting System (FIRS), a database that is the official source of record for all investigations conducted by the Secret Service. It is populated by personnel assigned to the Office of Investigations (INV), which encompasses domestic and foreign field offices and headquarters divisions. The data of FIRS is accessible at any time to analysts but is formally downloaded and validated twice a month to check for entry errors and maintain an official, reliable record of the system. These vetted biweekly downloads are what this measure is directly pulled from. The data itself is based upon receipt of petitions for remission or mitigation in a civil or criminal forfeiture proceeding, ruling on the petitions by the Secret Service, and payment to victims.
Data Collection Methodology	The calculation of this measure is based on the sum of remission payments to victims recorded by Secret Service personnel. INV employees manually enter data into FIRS on a daily basis to reflect what assets have been identified for seizure, the information of victims who were affected by pecuniary loss, as well as a series of legal documentation regarding notices and other legal steps required under 18 U.S.C. § 981 and § 982. This data is directly accessible by analysts but is also downloaded biweekly and checked for potential outliers or data entry errors that are flagged for INV to minimize error. A statistical program sums the values recorded as being paid to victims and returns that value to analysts for reporting. For example, if there were only two asset forfeiture payments returned to victims, and one was for $500 and the other was for $100, the total asset forfeiture payments returned to victims would be $600.
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. 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 data itself is downloaded biweekly and checked for potential outliers or data entry errors that are flagged for INV for confirmation. A statistical program sums the values recorded as being paid to victims and returns that value to analysts for reporting.

Performance Measure	Financial Crime Loss Recovered (in billions)
Program	Field Operations
Description	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.
Strategic Alignment	Objective 4.4: Combat Cybercrime
Scope of Data	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.
Data Source	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.
Data Collection Methodology	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 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. The Secret Service 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.
Strategic Alignment	Objective 4.4: Combat Cybercrime
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 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 federal arrests for crimes against children
Program	Field Operations
Description	This measure represents the number of federal arrests resulting from investigations conducted by the Secret Service in support

	of National Center for Missing and Exploited Children (NCMEC) and Internet Crimes Against Children (ICAC) Task Forces. This measure corresponds to Secret Service authority as outlined in 18 U.S.C. §3056(f), as well as other related violations under U.S.C. Title 18, Part I. This measure is an indirect way of measuring the Service's contribution to NCMEC'S efforts. However, since this measure was conceived and implemented, the Service's support of NCMEC has greatly expanded, to also include other evidentiary support. Because the number of federal arrests for crimes against children rely most heavily on the amount and quality of evidence against an offender, we are requesting the number of federal arrests for crimes against children serve as a proxy of the quality and quantity of the Secret Service's efforts in this area.
Strategic Alignment	Objective 6.3: Detect, Apprehend, and Disrupt Perpetrators
Scope of Data	The unit of analysis is a case where an arrest has been made of a potential crime against children. The attribute for this measure will be counted if a potential crime against children results in an arrest. The population is all cases where an arrest has been made of a potential crime against children. The calculation of this measure is the sum of federal arrests conducted by the Secret during the given fiscal year. To be included in the analysis, the Secret Service must be the arresting agency, and the crime of arrest must be consistent with 18 U.S.C. §3056(f) and/or U.S.C. Title 18, Part I. While investigations can last many months or even years, the arrest will report in the fiscal year that it occurred.
Data Source	The data for the measure is recorded in FIRS, a database that is the official source of record for all investigations conducted by the Secret Service. It is populated by personnel assigned to the Office of Investigations (INV), which encompasses domestic and foreign field offices and headquarters divisions. The data of FIRS is accessible at any time to analysts but is formally downloaded and validated twice a month to check for entry errors and maintain an official, reliable record of the system. These vetted biweekly downloads are what this measure is directly pulled from.
Data Collection Methodology	Data is recorded in the FIRS by personnel assigned to the INV, which encompasses domestic and foreign field offices and headquarters divisions. The data is based on NCMEC CyberTipline which result in investigations and lead to federal level arrests by Secret Service personnel. The number of federal arrests will be extracted from the system of record and summed by quarter.

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. This data is subject to supervisory reviews and approvals of the case records associated with this measure. The data itself is downloaded biweekly and checked for potential outliers or data entry errors that are flagged for INV for confirmation. A statistical program sums the number of federal arrests reported through FIRS to analysts for reporting.

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.
Strategic Alignment	Objective 4.4: Combat 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.
Strategic Alignment	Objective 4.4: Combat Cybercrime
Scope of Data	The scope of this measure includes the total U.S. dollars in circulation (reported from the U.S. 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 U.S. dollars in circulation (reported from the U.S 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 DHS.
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	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.
Strategic Alignment	Objective 4.4: Combat Cybercrime
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 NCFI.
Data Source	Both Secret Service and partner forensic data is collected from an application in 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 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.

Support Components

Performance Measure	Percent of Acquisition programs to counter chemical, biological, radiological, and nuclear (CBRN) threats that meet their Acquisition Program Baseline (APB) schedule, cost, and performance thresholds
Support Component	Countering Weapons of Mass Destruction Office
Description	This metric assesses 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 Full Operational Capability (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.
Strategic Alignment	Objective 1.4: Identify and Counter Emerging Chemical, Biological, Radiological, and Nuclear Threats
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, and DHS INVEST data (for Master Acquisition Oversight List 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 program manager presents a comprehensive brief of progress towards meeting the stated requirements. CAE provides annual certification to PARM.

Performance Measure	Number of students/participants who receive human trafficking awareness related training
Support Component	Federal Law Enforcement Training Centers
Description	This measure assesses the number of students/participants receiving human trafficking awareness-related training annually. FLETC currently accomplishes this in several ways. FLETC's human trafficking awareness-related training programs, which are available to federal, SLTT, and campus Law Enforcement Officers (LEOs) and direct law enforcement support personnel, provide instruction on how to recognize the indicators of and respond appropriately to suspected cases of human trafficking. Additionally, students/participants in certain FLETC basic training programs receive instruction that covers indicators of human trafficking and how to respond to suspected cases with a victim-centered approach. Further, FLETC periodically hosts virtual and in-person symposia and webinars that include human trafficking awareness-related training.
Strategic Alignment	Objective 6.1: Enhance Prevention through Public Education and Training
Scope of Data	The unit of analysis is a single student/participant. The attribute is the student receives instruction on human trafficking awareness. The population is all students who receive human trafficking awareness training. LEOs attending certain FLETC basic training programs receive instruction on the indicators of human trafficking and how to respond to suspected cases with a victim-centered approach. In addition to curriculum included in some basic training programs, FLETC also offers human trafficking awareness-related training programs (delivered both virtually and in-person), which explores this topic more in-depth. Further, FLETC periodically hosts virtual and in-person symposia and webinars that include human trafficking awareness-related training.
Data Source	Data on student/participant throughput is stored in FLETC's Student Administration and Scheduling System (SASS). SASS is an enterprise-wide IT solution that includes a scheduling system; a student registration and management system; a testing and evaluation function; a tuition component; and a student billing component.
Data Collection Methodology	To calculate the results, an End of Year Student Summary Report is extracted from SASS. The calculation is a count of students/participants who completed/graduated from a training

	program with human trafficking awareness-related curriculum during the specified timeframe.
Reliability Index	Reliable
Explanation of Data Reliability Check	Training records are generated and validated via FLETC's Student Services Division. The validated data populates the End of Year Student Summary Report. The number of students/participants who completed/graduated from a training program with human trafficking awareness-related curriculum during the reporting period are extracted from SASS via the End of Year Student Summary Report.

Performance Measure	Percent of Partner Organizations satisfied with Federal Law Enforcement Training Centers' training
Support Component	Federal Law Enforcement Training Centers
Description	This measure reflects the effectiveness of FLETC's training based on survey results documenting Partner Organizations' (PO's) satisfaction with the quality of instructional staff, whether FLETC's basic and advanced training addresses the right skills needed for officers and agents to perform their law enforcement duties, whether basic and advanced training prepare officers and agents to perform specific job-related tasks safely and effectively, and overall satisfaction with the training. Responses of "Strongly Agree" and "Agree" are considered satisfied. FLETC provides training to more than 100 POs, 12 of which are within DHS. The results provide on-going opportunities for improvements incorporated into FLETC training curricula, processes, and procedures.
Strategic Alignment	Objective E.2: Champion the Workforce
Scope of Data	This measure includes the results from all POs that respond to the PO Satisfaction Survey statements about satisfaction with the quality of instructional staff, whether FLETC's basic and advanced training addresses the right skills needed for officers and agents to perform their law enforcement duties, whether basic and advanced training prepare officers and agents to perform specific job-related tasks safely and effectively, and overall satisfaction with the training. Responses of "Strongly Agree" and "Agree" are considered satisfied. Responses of "Not Applicable" are excluded from the calculations.
Data Source	The source of the data is the FLETC PO Satisfaction Survey administered via a web-based survey program (Verint), which tabulates and calculates the survey results. The PO representative from each PO provides responses to the survey

	through Verint and saves the responses online when the survey is completed.
Data Collection Methodology	The FLETC POs are surveyed using the PO Satisfaction Survey. Data are collected annually from July to August. The survey uses a six-point Likert scale. Program personnel import the survey data as saved by survey respondents from Verint into Microsoft Excel to generate data charts and tables. The percent is calculated as the average of the number of POs that responded "Strongly Agree" or "Agree" to statements about satisfaction with the quality of instructional staff, whether FLETC's basic and advanced training addresses the right skills needed for officers and agents to perform their law enforcement duties, whether basic and advanced training prepare officers and agents to perform specific job-related tasks safely and effectively, and overall satisfaction with the training divided by the number of POs that responded to each of the respective statements. Responses of "Not Applicable" are excluded from the calculations.
Reliability Index	Reliable
Explanation of Data Reliability Check	The survey was developed using contemporary survey methods comparable to those used by the military services and other major training organizations. Following release of the survey summary report, FLETC leaders conduct verbal sessions with PO key representatives to confirm and discuss their responses. Throughout the year other formal and informal inputs are solicited from the PO representatives by FLETC staff and used to validate the survey results. No known data reliability problems exist.

Performance Measure	Percent of high-risk facilities that receive a facility security assessment in compliance with the Interagency Security Committee schedule
Line of Business	Federal Protective Service
Description	This measure reports the percentage of high risk (Facility Security Level 3, 4 and 5) facilities that receive a Facility Security Assessment (FSA) in compliance with the ISC schedule. An FSA is a standardized comprehensive risk assessment that examines credible threats to federal buildings and the vulnerabilities and consequences associated with those threats. Credible threats include crime activity or potential acts of terrorism. Each facility is assessed against a baseline level of protection and countermeasures are recommended to mitigate the gap identified to the baseline or other credible threats and vulnerabilities unique to a facility. Requirements for the

	frequency of federal building security assessments are driven by the ISC standards with high-risk facility assessments occurring on a three year cycle.
Strategic Alignment	Objective 1.3: Protect Leaders and Designated Individuals, Facilities, and Events
Scope of Data	The scope of this measure includes all high risk facilities with a security level of 3, 4, and 5. An FSA is considered completed when the assessment is presented to the FSC Chairperson or Designated Official and the package is signed in acknowledgement of receipt. This is documented in the FSA Manual, March 2014.
Data Source	Data is collected in the Modified Infrastructure Survey Tool (MIST) and is owned and maintained by FPS's Risk Management Division (RMD).
Data Collection Methodology	Results from each assessment are collected in MIST by inspectors. At the end of each reporting period, the percent of high risk facilities that receive an FSA is divided by the number of scheduled assessments for that period. The performance period for this measure is three years. The denominator for this measure is the total number of FSL 3, 4, and 5 facilities scheduled to be assessed within the three-year cycle. The numerator is the number of FSL 3, 4, and 5 facilities assessed within the three year cycle.
Reliability Index	Reliable
Explanation of Data Reliability Check	FSA results are consolidated and reviewed by FPS's RMD for quality assurance and performance measure reporting.

Performance Measure	Percent of women new hires in law enforcement positions
Line of Business	Office of the Chief Human Capital Officer
Description	This measure tracks the Department's ability to attract women into law enforcement and law enforcement related positions. The ability to recruit women into law enforcement positions help to create a workforce that is representative of the populace. The measure allows senior leadership to make policy decisions with regards to recruitment, incentives, targeted communication, as well as policy changes as needed to support this effort. Across the nation, both federal and state level law enforcement agencies are dealing with difficulties recruiting law enforcement candidates, especially women in law enforcement.
Strategic Alignment	Objective E.2: Champion the Workforce
Scope of Data	The unit of analysis is the number of women new hires into one of the law enforcement positions within the department. The

	population includes only those new hires into one of the defined law enforcement and law enforcement related positions. This attribute of the unit of analysis is the gender of the new hire.
Data Source	The data source is payroll and human resources (HR) data from the National Finance Center (NFC).
Data Collection Methodology	New hire data are entered into the NFC systems when an employee is hired into the department. This measure pulls all the new hire records for the measurement period and calculates the percentage between males and females.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data is based on HR and payroll records. Employees provide their information as part of the application, hiring and onboarding process. Additionally, HR Specialist ensure completeness of HR forms as part of the onboarding process.

Performance Measure	Percent of intelligence reports rated satisfactory and useful by customers
Support Component	Office of Intelligence and Analysis
Description	This measure gauges the extent to which intelligence products are satisfying customers' needs. 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.
Strategic Alignment	Objective 1.1: Collect, Analyze, and Share Actionable Intelligence and Information
Scope of Data	The unit of analysis is a single customer feedback survey that answered the degree of customer satisfaction question. The population of this measure is all customer feedback surveys (Physical or Web-based) that answered the degree of customer satisfaction question within the reporting period. The customer feedback surveys contain a standard question intended to elicit the degree of customer satisfaction with the usefulness of the intelligence product. 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). The attribute for a survey to be counted in the numerator is if a response of "very satisfied" or "somewhat satisfied" is provided for the degree of customer satisfaction question.

Data Source	The data sources for this performance measure are the I&A Performance Management system located on the unclassified and classified networks. The raw data consists of individual .xfdf files that are generated each time feedback is submitted from the feedback section of the intelligence product. Additionally, raw feedback is gathered from a web-based survey from the feedback that is provided from the Homeland Enterprise Library and Intelligence eXchange (HELIX).
Data Collection Methodology	Interactive customer feedback surveys are appended to each intelligence product. Customers enter their responses to the surveys and "submit feedback" via PDF in an email automatically generated 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 classified network. 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	I&A Performance Management 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 I&A Performance Management system. In the event of differences of opinion, an adjudication process exists to resolve discrepancies resulting in a final determination by I&A senior leadership.

Performance Measure	Percent of National Operations Center incident reports and situational awareness products produced and disseminated to the homeland security enterprise within targeted timeframes
Support Component	Office of Homeland Security Situational Awareness
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 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.
Strategic Alignment	Objective 1.1: Collect, Analyze, and Share Actionable Intelligence and Information
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 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 technology or knowledge products transitioned to customers for planned improvements
Support Component	Science and Technology Directorate
Description	This measure reflects the percent at which 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.
Strategic Alignment	Objective E.3: Harness Data and Technology to Advance Mission Delivery
Scope of Data	The unit of analysis is a technology or knowledge product. The population is all technology or knowledge products planned. The attribute is if the product is the successful transition to ownership and/or operation of a technology or knowledge product by a customer within the Homeland Security Enterprise. 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 (R&D) funded program/projects in the fiscal year of execution is compiled outside of STATS, in an Excel file that is then imported into STATS. S&T Offices are tasked through the S&T ExecSec process to submit the quarterly status of each R&D milestone planned, including planned transitions. S&T program/project managers report the quarterly status of each planned milestone.

	S&T leadership review and verify the quarterly status and explanation of each milestone prior to submitting to the S&T 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 R&D 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 S&T Performance Team, program/project managers report the status of each milestone planned for the fiscal year of execution, which are then verified by S&T leadership prior to review by the S&T 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 S&T leadership to the S&T Performance Team.
Reliability Index	Reliable
Explanation of Data Reliability Check	S&T leadership supervising program/project managers reviews the data submitted by program/project managers to ensure accuracy and consistency then verifies the status and explanation of milestones (specifically planned transitions) prior to submitting the data to the S&T Performance Team. The S&T Performance Team provides a third data reliability review before results are finalized and submitted to DHS.

WE ARE DHS

U.S. CUSTOMS AND BORDER PROTECTION
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
FEDERAL EMERGENCY MANAGEMENT AGENCY
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
TRANSPORTATION SECURITY ADMINISTRATION
U.S. COAST GUARD
U.S. CITIZENSHIP AND IMMIGRATION SERVICES
U.S. SECRET SERVICE
COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE
FEDERAL LAW ENFORCEMENT TRAINING CENTERS
SCIENCE AND TECHNOLOGY DIRECTORATE
OFFICE OF INTELLIGENCE AND ANALYSIS
OFFICE OF HOMELAND SECURITY SITUATIONAL AWARENESS
OFFICE OF HEALTH SECURITY
OFFICE OF INSPECTOR GENERAL
MANAGEMENT DIRECTORATE
OFFICE OF THE SECRETARY AND EXECUTIVE MANAGEMENT

WITH HONOR AND INTEGRITY, WE WILL SAFEGUARD THE AMERICAN PEOPLE, OUR HOMELAND, AND OUR VALUES.