Homeland Security

FY 2020 - 2022 Annual Performance Report

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

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

About this Report

The U.S. Department of Homeland Security Annual Performance Report (APR) for Fiscal Years (FY) 2020-2022 presents the Department's performance measure results and FY 2021 and FY 2022 targets. It also summarizes information on key initiatives in the DHS Performance Management Framework related to the Strategic Review, our FY 2020 results for the Department's Agency Priority Goals (APG), and also includes the Human Capital Operating Plan. The report is consolidated to incorporate our annual performance plan and annual performance report.

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

- DHS Agency Financial Report | Publication date: November 16, 2020
- DHS Annual Performance Report | Publication with the DHS Budget
- DHS Report to our Citizens (Summary of Performance and Financial Information) | Publication date: March 29, 2021

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

Contact Information

For more information, contact:

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

Table of Contents

Introduction

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

Performance Data Verification and Validation Process

The Department recognizes the importance of collecting complete, accurate, and reliable performance data that is shared with leadership and external stakeholders. Performance data are considered reliable if transactions and other data that support reported performance measures are properly recorded, processed, and summarized to permit the preparation of performance information in accordance with criteria stated by management. OMB Circular A-136, *Financial Reporting Requirements*, OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*, and the *Reports Consolidation Act of 2000* (P.L. No. 106-531) further delineate this responsibility by requiring agencies to ensure completeness and reliability of the performance data they report by putting management assurance procedures in place[1].

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

Performance Measure Definition Form (PMDF)

CFO/PA&E has used a continuous improvement process annually as a means to work to mature the breadth and scope of our publicly reported set of measures. This process employs a tool

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

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

Central Information Technology Repository for Performance Measure Information

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

Performance Measure Checklist for Completeness and Reliability

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

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

Independent Assessment of the Completeness and Reliability of Performance Measure Data

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

Management Assurance Process for GPRAMA Performance Measure Information

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

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

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

Countering Weapons of Mass Destruction Office

Performance Measure	Number of major metropolitan areas that have achieved Full Operational Capability to combat radiological/nuclear threats through the Securing the Cities Program (New Measure)
Program	Capability and Operational Support
Description	This measure assesses the number of major metropolitan areas that have achieved Full Operational Capability through the Securing the Cities (STC) program. The STC program seeks to give state and local agencies the ability to detect and deter nuclear terrorism. The program provides funding for equipment, such as radiation detectors, and training for up to five years. A major metropolitan area is deemed fully mission capable when 10 percent or more of its law enforcement is trained and equipped to conduct primary/secondary screening and alarm adjudication; has demonstrated a regionally coordinated radiological/nuclear detection; possesses operational and information exchange plans; and possesses protocols that facilitate mutual assistance and information sharing among regional partners and federal agencies.
Scope of Data	The population of this measure are all major metropolitan areas eligible for the STC program. Currently, there are 13 areas eligible for the STC program. Eligibility is determined by using the following criteria: population, risk, and presence of FBI Level 5 Stabilization Teams (key partners in radiological/nuclear detection mission).
Data Source	In accordance with the terms of the cooperative agreements between CWMD and the STC jurisdictions, the lead agency for each major metropolitan area submits Quarterly Performance Reports (QPRs). The QPRs are submitted via an inter-active PDF report form. The QPR data is then used to populate the STC authoritative data set stored in the DHS Geospatial Information Infrastructure (GII). The STC Program Office retains these reports and subsequent datasets on the CWMD Share Drive. Each QPR contains the number of personnel trained, the equipment issued, and results of exercises as evidence for the program office to use in assessing implementation status.
Data Collection Methodology	For the STC program to count a major metropolitan area as protected, the region must demonstrate it is fully mission capable. The criteria for a major metropolitan area being fully mission capable is 10 percent or more of its law enforcement is trained and equipped to conduct primary/secondary screening and alarm adjudication; has demonstrated a regionally coordinated radiological/nuclear detection; possesses operational and information exchange plans; and possesses protocols that facilitate mutual assistance and information sharing among regional partners and federal agencies. The datasets are queried to determine the number of major metropolitan areas that have met the criteria for being fully mission capable by the CWMD STC Program Manager (PM). The STC PM is the authority for declaring whether a jurisdiction is protected.
Reliability Index	Reliable
Explanation of Data Reliability Check	STC maintains a data verification process checked by action officers at various organizational levels, in accordance with the STC Standard Operating Procedure for Monitoring. This process ensures STC data is verified and approved by senior

	management. Reviews focus on equipment use and maintenance, as well as training and operational success.

Performance Measure	Percent of top 25 special events integrating biodetection monitoring
Program	Capability and Operational Support
Description	This measure is designed to identify how many Top 25 Special Events employ biological detection capability. To protect the Homeland from the threat of biological Weapons of Mass Destruction, the Department of Homeland Security Special Events Working Group determines annually the Top 25 special events that are integrating bio detection monitoring. This is done to increase National ability to counter attempts by terrorists and other threat actors to carry out an attack against the United States using a biological weapon of mass destruction.
Scope of Data	The data range is 0-25 based upon the number of the Special Events Working Group Top 25 designated events each year. This list is readily available from the DHS working group, and participation data is readily available through our BioWatch field operations tracking database. Based on all available data with high confidence.
Data Source	All biodetection capability special event data is entered into a sharepoint list called the Special Event Summary List, by the BioWatch jurisdictional coordinators. A subset of this data is exported by the Field Operations team to an excel spreadsheet titled Top 25 Special Event Tracking.
Data Collection Methodology	Simple count of deployments compared against the top 25 scheduled special events, and expressed as a percentage. Implementation Division of Field Support Operations Directorate will conduct an internal program review each quarter to gather the planning participation data, compare that against the DHS Top 25 list, and determine the cumulative percentage. This data will be reviewed and approved by the Deputy Assistant Secretary quarterly.
Reliability Index	Reliable
Explanation of Data Reliability Check	Reliable - there is no material inadequacy in the data to significantly impede the use of program performance data by agency managers and government decision makers. Results will be available quarterly. Annually, the final data will be reviewed once more for completion, and provided to the PDAS for confirmation prior to submission to DHS.

Customs and Border Protection

Performance Measure	Percent of cargo by value imported to the United States by participants in CBP trade partnership programs
Program	Trade Operations
Description	This measure reports all cargo imported to the United States through CBP trade partnership programs as a share of the total value of all cargo imported. Partnership programs include both the Customs Trade Partnership against Terrorism (CTPAT) and the Importer Self-Assessment (ISA) program. CBP works with the trade community through these voluntary public-private partnership programs to adopt tighter security measures throughout their international supply chain in exchange for benefits, such as a reduced number of inspections, shorter wait times at the border, and/or assignment of a Supply Chain Security Specialist to a partner firm. Trade partnership programs enhance the security of the supply chain by intercepting potential threats before the border while expediting legal trade.

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

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

	monthly basis. In calculating the incursion percentage, the total number of resolved incursions represents the numerator, while the total number of detected incursions represents the denominator.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data is routinely reconciled by a comparison of information in the systems manually by contractor and program staff on a monthly and/or quarterly basis.

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

Performance Measure	Percent of import revenue successfully collected
Program	Trade Operations
Description	This measure estimates amounts collected in duties, taxes, and fees expressed as a percent of all collectible revenue due from commercial imports to the U.S. directed by trade laws, regulations, and agreements. Specifically, this measure estimates the frequency of net under-collection of revenue during a given quarter and subtracts this estimated under-collection from all revenue formally owed from all import transaction types involving antidumping- or countervailing-duty (AD/CVD) payments—i.e. 100 percent--resulting in a percent of import revenue successfully collected. The proactive and strict enforcement of U.S. trade laws protects national economic security, facilitates fair trade, supports the

	health and safety of the American people, and ensures a level playing field for U.S. industry.
Scope of Data	This measure's scope includes data on all import transaction types involving antidumping- or countervailing-duty (AD/CVD) payments, maintained in CBP's Automated Targeting System (ATS). Each year, CBP's Trade Compliance Measurement (TCM) program creates a statistical sample of AD/CVD import-entry lines from a population of such imports, excluding non-electronic informal entries comprising about 15 percent of entries. Program staff stratify the sample lines by importers' assignment to one of CBP's operational Centers of Excellence and Expertise and the Importer Self-Assessment (ISA) program. A recent sample had a standard error of $528 million in collections at the 95-percent confidence interval, sampling from a total trade volume of many billions of dollars.
Data Source	Data resides in CBP's Automated Targeting System (ATS) with User Defined Rules (UDR) for processing. Program staff record findings from the Trade Compliance Measurement (TCM) review in CBP's Automated Commercial Environment (ACE) information technology system, using ACE's Validation Activity (VA) function.
Data Collection Methodology	At the start of each fiscal year, program staff define rules in ATS to construct a stratified random sample of import-entry lines from the previous year's data on imports, risk, volume, value, and compliance history. Data processing identifies import-entry records which may include an under-payment of some customs duty. Analysts determine the share of the sample comprised by records including under-payments and subtracts this estimated under-collection from all revenue formally owed, and multiplied by 100 to determine the percent of import revenue successfully collected.
Reliability Index	Reliable
Explanation of Data Reliability Check	ATS identifies user-defined summary lines of entry transactions, which opens a Validation Activity in ACE. Each CBP field office reviews the identified summary line transaction for compliance, and records findings with a Validation Activity Determination stored in ACE. CBP HQ analysts extract VAD data from ACE monthly, and a statistician resident in CBP's Trade Analysis and Measures Division compiles and reviews statistics monthly and at year-end. HQ staff hosts quarterly conference calls with field locations for open discussion of any issues and provides reports to field locations in the event requiring remediation. Analysts document this oversight, sharing this documentation annually with outside auditors as evidence of program control.

Performance Measure	Percent of imports compliant with U.S. trade laws
Program	Trade Operations
Description	This measure gauges the results of an annual CBP review of imports into the U.S., which assesses imports' compliance with U.S. trade laws, including laws related to customs revenue. CBP's Trade Compliance Measurement (TCM) program covers a population of all consumption and anti-dumping/countervailing duty (AD/CVD) transaction types, reporting the share of all transactions free from major discrepancies, excluding informal entries, excluding non-electronic informal entries comprising about 15 percent of entries. Reviewing transactions to ensure that imports remain legally compliant and free of major discrepancies facilitates lawful trade flows.
Scope of Data	This measure's scope includes data on all import transaction types involving antidumping- or countervailing-duty (AD/CVD) payments, maintained in CBP's Automated Targeting System (ATS). Each year, CBP's Trade Compliance Measurement (TCM) program creates a statistical sample of AD/CVD import-entry lines from a population of such imports. Program staff stratify the sample

	lines by importers' assignment to one of CBP's operational Centers of Excellence and Expertise and the Importer Self-Assessment (ISA) program.
Data Source	Data resides in CBP's Automated Targeting System (ATS) with User Defined Rules (UDR) for processing. Program staff record findings from the Trade Compliance Measurement (TCM) review in CBP's Automated Commercial Environment (ACE) information technology system, using ACE's Validation Activity (VA) function.
Data Collection Methodology	At the start of each fiscal year, program staff define rules in ATS to construct a stratified random sample of import-entry lines from the previous year's data on imports, risk, volume, value, and compliance history. Data processing identifies import-entry records containing a major discrepancy, defined by specified criteria reaching a specific threshold. Examples include a discrepancy in value or a clerical error producing a revenue loss exceeding $1,000.00; an intellectual property rights violation; or a country of origin discrepancy placing it in the top third of revenue losses or resulting in a revenue loss exceeding $1,000.00. Analysts determine the share of the sample which includes a major discrepancy under the criteria specified: This Major Transactional Discrepancy rate is subtracted from 1 and multiplied by 100 to determine the percent in compliance.
Reliability Index	Reliable
Explanation of Data Reliability Check	ATS identifies user-defined summary lines of entry transactions, which opens a Validation Activity in ACE. Each CBP field office reviews the identified summary line transaction for compliance, and records findings with a Validation Activity Determination stored in ACE. CBP HQ analysts extract VAD data from ACE monthly, and a statistician resident in CBP's Trade Analysis and Measures Division compiles and reviews statistics monthly and at year-end.

Performance Measure	Percent of inbound cargo identified as potentially high-risk that is assessed or scanned prior to departure or at arrival at a U.S. port of entry
Program	Trade Operations
Description	This measure reports the percent of international cargo coming to the U.S. via air, land, and sea, which CBP identified as potentially high-risk and then assessed or scanned prior to departure from a foreign port of origin or upon arrival at a U.S. port of entry to address security concerns. CBP assesses risk associated with a particular cargo shipment using information technology (IT) systems. Shipments include a wide range of cargo, from international mail to a palletized commercial shipment of packaged items. An automated system check flags a shipment as potentially high-risk when information meets specified criteria, which triggers actions in the field such as assessing or scanning of potentially high-risk shipments. Assessing, resolving, and scanning potentially high-risk cargo prior to departure from ports of origin or upon arrival at ports of entry ensures public safety and minimizes impacts on trade through effective use of risk-focused targeting.
Scope of Data	This measure's scope includes bill and entry data pertaining to all cargo from international mail to a palletized commercial shipment of packaged items in the land, sea, or air environments destined for a U.S. port of entry. The scope of reported results includes all shipments with final disposition status of assessed or scanned prior to departure.
Data Source	CBP collects and maintains this information on systems of record owned by CBP, including the Automated Commercial System (ACS), the Automated Export System (AES), the Automated Commercial Environment (ACE), TECS, and systems owned by partner governments and the private sector. All of these systems feed data in real time to the CBP's Automated Targeting System (ATS), which assesses the security risk associated with each shipment. ATS reviews bill and entry data pertaining to all destined for a U.S port of entry, identifying shipments as

	potentially high-risk using scenario-based modelling and algorithms. The ATS Exam Findings Module (EFM) contains the data used by the program to determine the disposition of cargo flagged as potentially high-risk.
Data Collection Methodology	Shippers and brokers provide manifest data for cargo through several systems feeding into ATS, which compiles the set of shipments scored as high-risk. CBP officers review information in ATS on high-risk shipments; resolve or mitigate security concerns; determine cases requiring more examination; and record findings from this review in ATS EFM. Program officers enter findings in the ACE for land shipments, a mandatory requirement for release of trucks and cargo at land ports of entry. Using data compiled in the ATS Exam Findings Module during a reporting period, program analysts calculate the results by counting all shipments scored as potentially high-risk and counting the subset of potentially high-risk shipments with final disposition status effectively determined. The number of status-determined potentially high-risk shipments is divided by the total number of potentially high-risk shipments, and multiplied by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	Supervisors periodically extract data on findings from examinations of potentially high-risk shipments from the Automated Targeting System's Exam Findings Module for review and validation of data entered by CBP officers in the field. Supervisors identify anomalies in findings data and ensure immediate corrective action(s) to ensure data integrity. Program HQ staff compiles this measure quarterly, provides it to program leadership and DHS. HQ staff investigates anomalies in quarterly results, tracing them back to field activities if necessary for clarification, explanation, and correction.

Performance Measure	Percent of international air passengers compliant with all federal, state, and local laws and regulations
Program	Travel Operations
Description	This measure reports the percent of international air passengers processed at ports of entry and assessed by CBP as compliant with all applicable federal, state, and local laws and regulations. Laws and regulations include those authorizing direct CBP jurisdiction, such as agriculture, immigration, and customs and those authorizing CBP enforcement responsibility, including pharmaceutical regulations from the Food and Drug Administration; state alcohol and cigarette laws; and warrants issued at the federal, state, and local levels. Inspecting air passengers for compliance with various agricultural, immigration, and customs laws and regulations enhances the security of trade and travel by intercepting potential threats before entry to the United States.
Scope of Data	This measure's scope includes all records of primary and secondary inspections of international air passengers completed by CBP at ports of entry. CBP conducts a random survey of cleared travelers. CBP selects travelers who have passed successfully through CBP's layered enforcement to undergo a comprehensive series of agriculture, admissibility, and customs checks to confirm these travelers' compliance. CBP's survey algorithm selects travelers to survey based on a time of a traveler's departure from the federal inspection area. The algorithm selects times proportionate to expected volumes of travelers, and CBP applies the rate of selection consistently across all airports.
Data Source	CBP collects and maintains this information on systems of record owned principally by CBP, including TECS, the Traveler Primary Arrival Client (TPAC), the Consolidated Secondary Inspection System (CSIS), the Seized Asset and Case Tracking System (SEACATS), and the Secure Integrated Government Mainframe Access System (SIGMA). TECS stores all primary inspection transactions processed through TPAC. CBP uses CSIS as the primary system to record all

	secondary inspections. CBP uses SEACATS as the primary system to record all arrests and seizures. CBP uses SIGMA as the primary system to record admissibility violations. CBP officers performing the survey inspections record the results in CSIS.
Data Collection Methodology	CBP processes all primary inspection transactions through TPAC and stores this data in TECS. CBP processes all secondary inspections using CSIS, SEACATS and SIGMA. For each reporting period, using survey data, CBP estimates a number of travelers missed by inspections by taking the fraction of surveyed travelers intercepted for violations, then multiplying this fraction by the number of all air travelers not referred for any secondary inspection. CBP then counts unsurveyed international air travelers intercepted for violations and adds the estimated number of missed violators produced from survey data. CBP then divides this sum into the total count of all air travelers. CBP then subtracts this estimated overall percentage of violators from all air travelers—i.e. 100 percent--resulting in a percent of international air passengers compliant with all federal, state, and local laws and regulations.
Reliability Index	Reliable
Explanation of Data Reliability Check	CBP OFO ensures measure reliability through four processes, focused respectively on reliability of (1) input data, (2) audit detection, (3) selection, and (4) sampling. To ensure reliability of audit data, both supervisors and management at the field level complete quality reviews of all survey and enforcement inspections to ensure reliability of input data. To ensure reliability of audit detection, field-level supervisors correct deficiencies observed in the inspections conducted by CBP officers, while field management and HQ staff conduct site visits for review and assessment of inspection quality. To ensure reliability of selection, analysts responsible for the survey algorithm follow formal schedules, policies, and procedures. To ensure reliability of sampling, CBP analysts conduct annual reviews using statistical best practices, adjusting the sampling rate accordingly.

Performance Measure	Percent of people apprehended or encountered multiple times along the Southwest Border between ports of entry
Program	Border Security Operations
Description	This measure examines the percent of deportable individuals who have entered the U.S. illegally and been apprehended or encountered multiple times by the Border Patrol along the Southwest Border. It serves as an indicator of the potential impact of the Border Patrol's consequence delivery system to deter future illegal crossing activity into the U.S. The consequence delivery system divides border crossers into categories, ranging from first-time offenders to people with criminal records, and delivers a consequence for illegal crossing based on this information. Effective and efficient application of consequences for illegal border crossers should, over time, reduce overall recidivism. The measure factors in border crossing activity just within a twelve-month rolling period.
Scope of Data	Deportable illegal entrants that have or receive a Fingerprint Identification Number (FIN), who are apprehended under Title 8 or encountered under Title 42 multiple times within a twelve-month rolling period, are included in calculating this measure. The scope includes only those apprehensions or encounters that occur within the nine sectors of the Southwest Border. Fingerprints are not taken and FINs are not generated for individuals under age 14, over age 86, and some humanitarian cases, and thus are not included in calculating the data for this measure.

Data Source	Apprehension and encounter data are captured by Border Patrol Agents at the station level and entered into the e3 Processing (e3) system. All data entered via e3 resides in the Enforcement Integrated Database (EID), the official system of record for this data, which is under the purview of the Border Patrol Headquarters Statistics and Data Integrity (SDI) Unit. The physical database is owned and maintained by U.S. Immigrations and Customs Enforcement (ICE).
Data Collection Methodology	Data relating to apprehensions and encounters are entered into e3 by Border Patrol Agents at the station level as part of the standardized processing procedure. Data input can be made by any agent who knows the details of the apprehension or encounter. This data is typically reviewed regularly at the station, sector or Headquarters level observing trends to provide feedback to the field on operational activity. Calculation of this measure completed by the SDI Unit at Border Patrol Headquarters and is the number of individuals that have been apprehended multiple times during the 12-month rolling period, divided by the total number of individuals apprehended or encountered during the same time period.
Reliability Index	Reliable
Explanation of Data Reliability Check	All apprehension and encounter data entered into e3 Processing is subject to review by supervisors at multiple levels. Data reliability tools are built into the system; for example, data input not conforming to appropriate expectations is reviewed for accuracy and flagged for re-entry. The EID continuously updates to compile all apprehension and encounter data. This data can then be extracted into summary reports, and these summaries are available for review and analysis at station, sector, and Headquarters levels. At the Headquarters level, the SDI conducts monthly data quality reports as well as weekly miscellaneous checks. When discrepancies are found, they are referred back to the apprehending Sector/Station for review and correction.

Performance Measure	Percent of privately owned vehicle passengers compliant with all federal, state, and local laws and regulations
Program	Travel Operations
Description	This measure reports the percent of passengers in privately owned vehicles (POVs) processed at land ports of entry and assessed by CBP as compliant with all applicable federal, state, and local laws and regulations. Laws and regulations include those authorizing direct CBP jurisdiction, such as agriculture, immigration, and customs, and those authorizing CBP enforcement responsibility, such as pharmaceutical regulations from the Food and Drug Administration; health and safety alerts from the Centers for Disease Control; and requirements to confiscate alcoholic beverages from minors on behalf of state authorities. Inspecting passengers in privately owned vehicles in for compliance with various agricultural, immigration, and customs laws and regulations enhances the security of trade and travel by intercepting potential threats before entry to the United States.
Scope of Data	This measure's scope includes all records of primary and secondary inspections of passengers in privately owned vehicles (POVs) completed by CBP at land ports of entry which process POVs. CBP selects POVs for the survey using a randomizing function in the Vehicle Primary Client (VPC), activated after POVs have completed primary inspection. CBP sets VPC's randomization function to produce a sample size with a 95 percent probability of producing at least one serious violation. Each quarter, CBP reports the average result for the preceding four quarters to address seasonality.
Data Source	CBP collects and maintains this information on systems of record owned principally by CBP, including TECS, the Vehicle Primary Client (VPC), the

	Consolidated Secondary Inspection System (CSIS), the Seized Asset and Case Tracking System (SEACATS), and the Secure Integrated Government Mainframe Access System (SIGMA). TECS stores all primary inspection transactions processed through VPC. CBP uses CSIS as the primary system to record all secondary inspections. CBP uses SEACATS as the primary system to record all arrests and seizures. CBP uses SIGMA as the primary system to record admissibility violations. CBP officers performing the survey inspections record results in CSIS.
Data Collection Methodology	CBP selects vehicles which successfully passed through layered enforcement to undergo a series of agriculture, admissibility, customs, and other checks. CBP processes all primary inspection transactions through VPC and stores this data in TECS. CBP processes all secondary inspections using CSIS, SEACATS and SIGMA. Using survey data, CBP estimates a number of POV passengers missed by inspections by taking the fraction of surveyed POV passengers intercepted for violations, then multiplying this fraction by the number of all POV passengers not referred for secondary inspection. CBP counts unsurveyed POV passengers intercepted for violations and adds the estimate of missed violators produced from survey data. CBP divides this sum into the number of all POV passengers. CBP subtracts this estimated overall percent of violators from all POV passengers—i.e. 100 percent—to get the result. The average result for the preceding four quarters is reported to address seasonality.
Reliability Index	Reliable
Explanation of Data Reliability Check	CBP OFO ensures measure reliability through three processes, focused respectively on reliability of (1) input data, (2) audit detection, and (3) sampling. To ensure reliability of audit data, both supervisors and management at the field level complete quality reviews of all survey and enforcement inspections to ensure reliability of input data. To ensure reliability of audit detection, field-level supervisors correct deficiencies observed in the inspections conducted by CBP officers, while field management and HQ staff conduct site visits for review and assessment of inspection quality. To ensure reliability of sampling, CBP analysts conduct annual reviews using statistical best practices, adjusting the sampling rate accordingly.

Performance Measure	Percent of recurring border surveillance implemented in remote, low-risk areas between ports of entry (Retired Measure)
Program	Border Security Operations
Description	This measure represents the percentage of remote low risk areas along the land border that are covered by recurring surveillance that can detect possible illicit activity. Low risk areas are geographically remote parts of the border that also have historically had low levels of illegal activity. Recurring surveillance is achieved through geospatial capabilities that monitor these areas for potential illicit activity and provide information to CBP Office of Intelligence (OI) analysts who review the information and determine if a response is needed. The measure demonstrates the U.S. Border Patrol's (USBP) ability to maintain awareness of illicit activity without needing to have agents directly located in these remote areas. Sector Chiefs report which miles of the border are low risk to CBP's OI, who then works to deploy Geospatial Intelligence (GEOINT) capabilities in those areas.
Scope of Data	This measure includes the entire Southwest and Northern land borders (excluding Alaska) that have been determined by CBP's USBP Sector Chiefs through trends and Intelligence gathering to be low flow/low risk areas. Each Sector Chief can change the designation for any mile within their area of responsibility. Sector Chiefs report which miles of the border are low risk to

	CBP's OI, who then works to deploy GEOINT capabilities in those areas. A "covered border mile" is defined as one mile of the border where CBP has the capability of deploying GEOINT capabilities if intelligence reports or risk analyses require GEOINT surveillance. This measure does not include the maritime domain.
Data Source	The data will be collected by CBP OI in the National Technical Collections Branch. The miles covered and required to be covered are currently stored in the CBP Shared Server in a Word document. That data is reported to U.S. Border Patrol enterprise Geospatial Information Services office for reporting. Sector Chiefs report which miles of the border are low risk to CBP's OI, who then works to deploy GEOINT capabilities in those areas.
Data Collection Methodology	As USBP coverage capability increases, USBP changes the designation of border miles from "proposed, to active, GEOINT collection areas." Sector Chiefs report which miles of the border are low risk to CBP's OI, who then work to deploy GEOINT capabilities. CBP OI maintains an excel spreadsheet in OI's National Technical Collections Branch (NTCB) by a Collections Manager, which is updated as OI adds designated miles of the border covered by GEOINT capabilities. The NTCB Branch Chief reviews the spreadsheet for accuracy. After approval, the spreadsheet is saved to the CBP Shared Server. The NTCB Collections Manager then emails the new miles to a Geospatial Information Services (GIS) analyst who updates the GIS map. The Branch Chief of the NTCB uses these maps in their monthly report to the Border Patrol Chief. The USBP liaison will report this information quarterly. The GEOINT covered border miles is the numerator and the total designated low flow/low risk miles are the denominator.
Reliability Index	Reliable
Explanation of Data Reliability Check	A CBP OI Collections Manager inputs the data, which is reviewed for accuracy by the Branch Chief quarterly.

Performance Measure	Percent of time the U.S. Border Patrol reaches a detection site in a timely manner to assess the nature of detected activity in remote, low-risk areas of the Southwest and Northern Borders
Program	Border Security Operations
Description	This measure gauges the percent of time agents reach remote low-risk areas to assess notifications of potential illegal activity and make a determination of the nature of this activity. The goal is for Border Patrol Agents to respond to these notifications in remote low risk areas within 24 hours. If not accomplished in a timely fashion, the evidence degrades and determinations cannot be made regarding the nature of the potentially illicit activity. Responding to notifications of activity provides valuable information in terms of both the nature of the detected activity, as well as with confirming whether or not the area continues to be low risk. This measure contributes to our situational awareness and ability to secure the border.
Scope of Data	This population for this measure encompasses all geospatial intelligence-informed reports of potential illicit activity in remote areas along the Southern and Northern land border (excluding Alaska) that Border Patrol sectors have determined to be low flow and low risk. This measure does not include the maritime domain. A response is defined as the time when a Border Patrol Agent arrives at the coordinates for the detection site that was communicated by the Office of Intelligence (OI).
Data Source	The data source is mined from e-mail notifications and individual Field Information Reports (FIR), which are stored in CBP's Intelligence Reporting System – Next Generation (IRS-NG) and maintained by CBP's Office of Information Technology.

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

Performance Measure	Rate of interdiction effectiveness along the Southwest Border between ports of entry
Program	Border Security Operations
Description	This measure reports the percent of detected illegal entrants who were apprehended under Title 8, encountered under Title 42, and those who were turned back after illegally entering the United States between ports of entry along the Southwest Border. The rate includes apprehensions, encounters, and turn backs to the total estimate of illegal entrants that includes these three groups and also those who got away without being apprehended. Border Patrol achieves desired results by maximizing the apprehension of detected illegal entrants, confirming that illegal entrants return to the country from which they entered, and by minimizing the number of persons who evade apprehension and can no longer be pursued (a Got-Away in border zones or a No Arrest in non-border zones). This measure is a key indicator of the Border Patrol's law enforcement and resolution impact, a key component of the Operational Control framework.
Scope of Data	The scope includes all Southwest Border areas that are south of the northernmost checkpoint within a given area of responsibility. In Border Zones, it includes all apprehensions, encounters, Turn-Backs (TB), and Got-Aways (GA). In non-Border Zones, it includes all apprehensions, encounters, and No Arrests (NA). An apprehension is a deportable illegal entrant who is taken into custody and receives a consequence. An encounter is an illegal entrant subject to 85 Fed Reg 17060. A GA is an illegal entrant who is not turned back, apprehended, or encountered and is no longer being actively pursued in a border zone. A NA is a subject identified as a result of a non-border-zone tracking action that does not result in an apprehension or encounter but is determined by agents to involve illicit cross-border activity. A TB is a subject who, after making an illegal entry into the United States, returns to the country from which he/she entered, not resulting in an apprehension, encounter, or GA.

Data Source	Apprehension, encounter, GA, NA, and TB data is captured by Border Patrol Agents at the station level into several systems. Apprehensions and encounters are entered into the e3 Processing (e3) system. All data entered via e3 resides in the Enforcement Integrated Database (EID), the official system of record for this data, which is under the purview of the Border Patrol Headquarters Statistics and Data Integrity (SDI) Unit. The physical database is owned and maintained by U.S. Immigrations and Customs Enforcement (ICE). GA's, TB's, and NA's are recorded in the Intelligent Computer Assisted Detection (ICAD) Tracking Sign-cutting and Modeling (TSM) application, which resides with the U.S. Border Patrol. TSM is under the purview of and is owned by the U.S. Border Patrol's Enforcement Systems Unit.
Data Collection Methodology	Data relating to apprehensions and encounters are entered into e3 by Border Patrol agents (BPAs) at the station level as part of the standardized processing procedure. BPAs use standard definitions for determining when to report a subject as a GA, NA, or TB in the TSM system. Some subjects can be observed directly as evading apprehension/encounter or turning back; others are acknowledged as GA's, NA's, or TB's after BPAs follow evidence that indicate entries have occurred, such as foot sign, sensor activations, interviews with subjects in custody, camera views, communication between and among stations and sectors, and other information. Calculation of the measure is done by the U.S. Border Patrol Headquarters Statistics and Data Integrity (SDI) Unit; the numerator is the sum of apprehensions and encounters and TBs, divided by the total entries, which is the sum of apprehensions, encounters, TBs, GAs, and NAs.
Reliability Index	Reliable
Explanation of Data Reliability Check	Patrol Agents in Charge ensure all agents at their respective stations are aware of and use proper definitions for apprehensions, encounters, GA's, NA's, and TB's. They also ensure the necessary communication takes place between and among sectors and stations to ensure accurate documentation of subjects who may have crossed more than one station's area of responsibility. In addition to station-level safeguards, SDI validates data integrity by using various data quality reports. The integrity of Turn-Back, Got-Away, and No Arrest data is monitored at the station and sector levels. Data issues are corrected at the headquarters level, or forwarded to the original inputting station for correction. All statistical information requests are routed through the centralized headquarters office within Border Patrol and SDI coordinates with these entities to ensure accurate data analysis and output is provided.

Cybersecurity and Infrastructure Security Agency

Performance Measure	Percent of all state and territory emergency communications interoperability components operating at the highest levels
Program	Emergency Communications
Description	The measure identifies the current level of emergency communications interoperability maturity across 56 states and territories as defined by the National Council of Statewide Interoperability Coordinators (NCSWIC) Interoperability Markers. The 24 markers cover a range of interoperability factors including governance, standard operating procedures, technology, training and exercises, usage, and others, allowing states and territories to benchmark their progress and enhance their capabilities for interoperable communications. Each state and territory self-evaluate their interoperability maturity annually against all 24 interoperability components. Markers operating as "defined" or

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

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

	usage during exercises, such as National Level Exercises (NLEs). Each quarter, OEC will also analyze and provide results for GETS usage during designated 'Code Red' events (defined in Data Source) , or other natural or human-made events that receive national-level press, thus potentially contributing to network congestion as people attempt to contact those within the affected area. When analyzing completion rates for a specified event, only GETS calls originating or terminating within a designated time period and geographic area for the event will be included.
Data Source	Data is obtained through Monthly Performance Reports (MPRs) from the carriers: AT&T, Sprint, and Verizon. The reports contain information on daily GETS call attempts: date of call attempt, time of call attempt, call duration, originating digit string & location, terminating digit string & location, disposition of the call attempt [answered, busy, ring no answer, invalid PIN], and network announcement. Daily reporting is requested by the NCCIC/NCC when an event appears to have a significant national impact (e.g., impact to an urban or large geographic area). This situation is known as a 'Code Red' event. To obtain daily data for a Code Red event, OEC will instruct each of the carriers to provide Emergency Performance Reports (EPRs). EPRs include the GETS call attempts for each day that OEC specifies, and must be provided the day after the specified date (i.e., GETS performance data is reported 24 hours later rather than waiting for the end-of-month distribution).
Data Collection Methodology	Each quarter, OEC analyzes all MPRs, and EPRs if applicable, from that time period to calculate the overall and event-specific call completion rates. Based on information from these reports, the program calculates call completion rate: defined as a percentage (%) = (Successful Valid Call Attempts * 100) / (Blocked Valid Call Attempts + Successful Valid Call Attempts), where a 'Valid Call Attempt' is a GETS attempt with a valid destination number and a valid GETS PIN. A valid call attempt is considered 'blocked' if it is unable to reach the intended endpoint due to network congestion. If one or more 'Code Red' events have been initiated during a quarter that would produce EPRs, or if there are any national-level events causing network congestion, then event-specific call completion rates will also be reported in the supporting narrative submitted along with the overall result.
Reliability Index	Reliable
Explanation of Data Reliability Check	Carrier data is recorded, processed, and summarized on a quarterly basis in accordance with criteria established by GETS program management. All data collected is also in accordance with best industry practices and is compared with previous collected data as a validity check by OEC analysts. The results are reviewed for clarity and consistency by CS&C before final submission.

Performance Measure	Percent of critical and high configuration-based vulnerabilities identified through high value asset assessments mitigated within 30 days
Program	Cybersecurity
Description	This measure reports the percent of critical and high configuration-based vulnerabilities identified in High Value Assets (HVA) assessments that have been mitigated within 30 days. HVA assessments are performed across the Federal Government to identify vulnerabilities associated with the most sensitive IT systems and data. Configuration-based vulnerabilities are those that can be more quickly be mitigated by agencies through such actions as changing security settings, software or configuration changes, patching software vulnerabilities, and adjusting user account privileges. Agencies report monthly to the program on the status of mitigating these configuration-based vulnerabilities. The results

	indicate if agencies are resolving less complex HVA vulnerabilities within the government-wide goal of 30 days.
Scope of Data	The population for this measure is all critical and high configuration-based vulnerabilities that are mitigated during the fiscal year. HVA vulnerabilities include both those identified in Risk and Vulnerability Assessments and Security Architecture Reviews. HVAs are those assets within federal agencies and departments they self-nominate as high value and do not include Department of Defense or the Intelligence Community assets. The value being assessed are those vulnerabilities mitigated within 30 days. The data included in this measure is based on Agency reports delivered to the program between September of the previous fiscal year to August of the current fiscal year.
Data Source	Each HVA vulnerability has a mitigation plan that the responsible agency serves as the data source for vulnerability status. These plans serve as the data source for determining configuration based vulnerabilities mitigation status. These plans are emailed to CISA by the agency and saved on the Homeland Security Information Network (HSIN). The program analysts record results of configuration-based vulnerability resolution in a spreadsheet that is stored HSIN. The CISA HVA program is responsible for oversight of these data sources.
Data Collection Methodology	After receiving a final HVA assessment report, agencies develop initial mitigation plans within 30 days and then report monthly on the status of mitigating their configuration based vulnerabilities. The submitted plan is reviewed by an analyst to determine if the milestones and objectives of the plan meet the objectives identified from the remediation recommendation of the assessment. Once the final plan has been submitted, an analyst will review the remiedation steps to verify that they meet the original plan objectives. These results are then recorded by the analyst on the tracking spreadsheet. The result is calculated by dividing the number of configuration-based vulnerabilities mitigated within 30 days of initial identification by all vulnerabilities mitigated during a fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	The results will be reviewed for accuracy by the Cybersecurity Division Capacity Building Office by comparing the master spreadsheet data with the individual agency submissions. The CISA Office of Strategy, Policy, and Plans will consolidate findings and transmit to DHS.

Performance Measure	Percent of critical and high vulnerabilities identified through cyber hygiene scanning mitigated within the designated timeframe
Program	Cybersecurity
Description	This measure calculates the percent of significant (critical and high) vulnerabilities, identified through cyber hygiene scanning, that have been mitigated within the specified timeline. For critical vulnerabilities, mitigation is required within 15 days from point of initial detection, and for high vulnerabilities mitigation is required within 30 days. Cyber hygiene scanning prioritizes vulnerabilities based on their severity as a means for agencies to make risk-based decisions regarding their network security. Identifying and mitigating vulnerabilities on a network in a timely manner is a critical component of an effective cybersecurity program, as it is critical to maintaining operational availability and integrity of IT systems.
Scope of Data	The scope of data for this measure is: 1) all significant (critical and high) vulnerabilities identified by cyber hygiene vulnerability scanning on internet-accessible devices; 2) all critical and high vulnerabilities detected in previous scanning that were mitigated during the measurement period; and 3) all critical and high vulnerabilities that were active greater than or equal to the designated timeline for mitigation (15 days for critical; 30 days for high) during the

	measurement period. The timeline for mitigation begins when a critical or high vulnerability is first detected on a scan and it ends when the critical or high vulnerability is no longer detected. When a vulnerability finding is 'closed' due to it being marked as a false positive (i.e. a reported finding that incorrectly indicates a specific vulnerability or setting is present on a stakeholder's internet-accessible devices), it is not included in the calculation for this measure.
Data Source	Cyber hygiene scans utilize two tools: Nmap for host discovery, and Nessus for scanning identified hosts for known vulnerabilities. Results from these scans are collected with a Client Access License (CAL) and stored on an internal DHS network that is operated and maintained by the Cyber Hygiene Scanning Team.
Data Collection Methodology	This measure gauges the total number of critical and high vulnerabilities compared to those mitigated within the designated timeframes. A vulnerability's age is calculated from when it is first detected on a scan to when it is no longer visible on the scan. Subsequent scanning tracks a vulnerability for 90 days after it appears closed to ensure the vulnerability isn't simply unresponsive to a scan. If a vulnerability is re-detected within 90 days, it is re-opened using the original date of detection, and included in subsequent cumulative calculations. Data analysis software will be used to run a report on the percent of criticals and highs that were mitigated within the designated timeframe. The result is calculated by adding the number of critical vulnerabilities mitigated within 15 days plus the number of high vulnerabilities mitigated within 30 days divided by total number of both open and closed critical and high vulnerabilities.
Reliability Index	Reliable
Explanation of Data Reliability Check	The Cyber Hygiene Scanning team within the CISA Cyber Assessments Team will coordinate with the CISA Insights Branch to review the algorithm to query the data and the quarterly result for this measure to ensure correct data collection and calculation procedures were used. CISA Program Analysis & Evaluation will also review the quarterly results and accompanying explanations prior to final submittal to DHS.

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

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

Performance Measure	Percent of potential malicious cyber activity notifications where impacted agencies were alerted within the specified timeframe
Program	Cybersecurity
Description	The measure tracks the percent of potential malicious cyber activity notifications identified as credible where the affected agency is alerted within the specified timeframe. Potential malicious cyber activity on federal networks is detected by automated tools through the National Cyber Protection System (NCPS) alert-based detection function. The system sends automated notifications to analysts within NCPS, who then manually review the notification(s), confirm if a potential credible threat exists, and if so, the affected agency is sent an email for their further exploration. The specified timeframe to notify affected agencies of potential malicious cyber activity is 18 hours for FY20 and 12 hours for FY21.
Scope of Data	The population of data includes cases of potential malicious cyber activity entered into the Remedy system. Notifcation times associated with these credible potential malicious cyber activity cases form the basis for this measure. The specified timeframe to notify affected agencies of potential malicious cyber activity is 18 hours for FY20 and 12 hours for FY21.
Data Source	NCPS sends alerts of potential malicious activity to program analysts. Computer Network Defense (CND) analysts create a case in the Remedy system if there appears to be credible malicious activity. Tableau, a graphical reporting tool, pulls data from Remedy to calculate this measure, Remedy tickets are maintained by the Integrated Operations Division (IOD) Helpdesk. Cybersecurity Division (CSD) manages both the NCPS and Remedy systems.
Data Collection Methodology	When the NCPS detects potential malicious cyber activity, it sends a notification to analysts, who review the notifications, and if credible, creates a case in the Remedy system which includes the initial NCPS alert time and an email is sent to the affected agency. The initial detection time is recorded in the NCPS system when it notifies the analyst team of the potential threat (the first notification time is used if multiple notifications occur for the same threat). The agency notification time is the date time stamp recorded when the email is sent from

	the Remedy system to the agency. The time to notify for each case is calculated by subtracting the initial detection time from the agency notification time. The Process, Metric and Reporting Analysts extract information from Remedy to Tableau to calculate the time to notify, and what percent of cases fall within the specified window.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data collection, review and vetting will be conducted by CSD Strategy and Resources Office (S&R) Process, Metrics and Reporting Analysts monthly and at each quarter in collaborations with CSD Branch Chiefs to assess validity, consistency and identify potential issues early on during the APG/GPRA reporting period.

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

	check for accuracy. The data and result for this measure will be submitted to analysts at the CISA HQ level for their review and concurrence. This provides a final check for any potential errors in data collection, calculation or scoping.

Federal Emergency Management Agency

Performance Measure	Average annual percentage of administrative costs for major disaster field operations, as compared to total program costs
Program	Regional Operations
Description	This measure gauges FEMA's efficiency in providing disaster assistance by indicating what share of its disaster expenditures are administrative costs compared to the share disseminated as grants to survivors as assistance. It helps FEMA know if the agency is being efficient in the way it provides disaster assistance. This measure is for FEMA's most common disasters of less than $50M (Level III).
Scope of Data	The results are based on all available data and not a sample of data for Major Disasters under $50M. The measure only applies to Major Disasters (DRs). It does not apply to Emergency Declarations (EMs), Fire Management Assistance Grants (FMAGs) or any other administrative costs in the disaster relief fund. Administrative Costs are those costs which are classified in IFMIS (Integrated Financial Management Information System) as 'Administrative' in FEMA's system of record, Enterprise Data Warehouse (EDW) reports and Financial Information Tool (FIT) reports. Examples include but are not limited to salaries and benefits, travel, facilities.
Data Source	The data is collected and stored in IFMIS. It is reported via FIT reports, in addition, the disaster administrative cost percentage for specific disasters is reported on in the Automated COP, which also pulls data from IFMIS. OCFO owns IFMIS and the FIT reports. ORR owns the Automated COP.
Data Collection Methodology	The data is collected via IFMIS and reported in FIT reports. The remaining steps are conducted by an analyst using data from a FIT report.The data is organized so that disasters are first separated by their size which is determined by the total actual federal dollars obligated. Small disasters have total actual federal obligations less than $50M. An administrative cost percentage is calculated for each disaster and is the (Total Administrative Costs for that disaster)/ (Total Obligations for that disaster) To create the score for each year, the analyst groups all disasters declared in that year of the same size and calculates the average administrative cost percentage across all those disasters (Sum of Admin Cost Percentages of Each Disaster)/Total Number of Disasters). This results in three scores per year, one each for small, medium, and large disasters. Note: Because the data is organized by declaration year, all of the previously reported numbers will need to be updated
Reliability Index	Reliable
Explanation of Data Reliability Check	The data is collected via IFMIS and reported in FIT reports. The remaining steps are conducted by an analyst using data from a FIT report. The data is organized so that disasters are first separated by their size which is determined by the total actual federal dollars obligated. An administrative cost percentage is calculated for each disaster and is the (Total Administrative Costs for that disaster)/ (Total Obligations for that disaster) To create the score for each year, the analyst groups all disasters declared in that year of the same size and calculates the average administrative cost percentage across all those disasters (Sum of Admin

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

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

Performance Measure	Average timeliness of the individual assistance awards of the Individuals and Households Program (in days)
Program	Response and Recovery
Description	This measure assesses how quickly the program provides disaster relief to qualified individuals and households. Specifically, for individuals or households receiving assistance from the Individuals and Households Program (IHP), this measure reports the average number of days between the submission of an application and the first receipt of an award. By evaluating how quickly disaster survivors receive financial assistance, the program can assess the effectiveness of a critical, customer-facing element of the agency's mission.

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

Performance Measure	Benefit to cost ratio of the Hazard Mitigation Grants
Program	Grants
Description	This measure reports the estimated annual benefit to cost ratio of grants provided by the FEMA Hazard Mitigation Assistance program to lessen the impact of disasters. A value greater than one indicates more benefit was reaped than cost expended. The program works with state, tribal, territorial, and local (STTL) governments engaged in hazard mitigation planning to identify natural hazards that impact them, identify strategies and activities to reduce any losses from those hazards, and establish a coordinated approach to implementing the plan. These plans are the basis for STTL grant requests. Once grants are provided, program staff evaluate the benefit to cost ratio of the implementation of the plan to ensure that taxpayer dollars are spent effectively.

Scope of Data	The scope of this measure includes all grants on an annual basis provided by the FEMA Hazard Mitigation Assistance program.
Data Source	The systems primarily used for the data collection includes FEMA's Enterprise Data Warehouse (EDW) which consolidates data from Hazard Mitigation Grant Program - National Emergency Management Information System (HMGP-NEMIS) and Mitigation Electronic Grants Management System (MT- eGrants) systems. Data is collected and consolidated into an Excel spreadsheet where the calculations for aggregate Benefit to cost ratio will be performed.
Data Collection Methodology	The total project cost and the benefits are calculated by the applicant for each of the projects. The estimated benefits are derived based on benefit-cost analysis methodologies developed by FEMA. These are proven methodologies and have been in use for the past 10 years. To determine the cost effectiveness of a Hazard Mitigation Assistance (HMA) project, FEMA utilizes a benefit-cost ratio, which is derived from the project's total net benefits divided by its total project cost. Each sub-grant obligation and total project cost is captured in the HMGP-NEMIS or MT-eGrants system by FEMA HMA staff. Quarterly reports will be generated utilizing FEMA's EDW which will be utilized for the data reporting.
Reliability Index	Reliable
Explanation of Data Reliability Check	Each sub-grant obligation and total project cost is captured in the HMGP-NEMIS or MT-eGrants system. This information is electronically consolidated in FEMA's EDW. FEMA HMA staff download relevant data from the EDW, and after making the calculations for an aggregate Benefit to cost ratio generate Quarterly excel based reports. These calculations go through a series of staff reviews before being reported on FEMA's performance system of record – the Performance Hub.

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

Reliability Index	Reliable
Explanation of Data Reliability Check	WYO's Financial Control Plan Requirements and Procedures provides data concerning reconciliation of policy and claim data submitted to TRRP with monthly financial reports and instructions for editing data. Because of the need for timely financial reconciliation, TRRP only rejects transactions with unreadable money fields or in case of any lack of clarity about how the system can process a transaction. Otherwise, information posts to the database, with potential errors flagged for correction at a later date. NAIS assures the reliability of data stored and reported through the Pivot system.

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

Performance Measure	Percent of adults that have set aside money for emergencies
Program	Preparedness and Protection
Description	This measure reports the share of all respondents to FEMA's annual National Household Survey who answered affirmatively to questions assessing whether they have set aside money for use in case of emergencies. FEMA has noted that access to financial resources has proven a strong predictor of how well someone can cope in the aftermath of a disaster.
Scope of Data	Annually, FEMA conducts a National Household Survey to understand and assess Americans' attitudes and behaviors regarding emergency preparedness. The scope of this measure includes all responses to questions in the survey which ask whether or not the respondent has set aside money for use in case of emergencies. Through a contractor, FEMA conducts the National Household Survey through telephone interviews.
Data Source	Interviewers capture responses and enter them into a Computer Assisted Telephone Interviewing (CATI) system, owned by the contractor and maintained at the contractor's facilities. The contractor conducting the survey establishes appropriate quality-control measures to ensure that data collection adheres to the outlined standards of the contract.
Data Collection Methodology	FEMA's survey contractor collects data using the CATI system, and completes analysis of responses using two statistical software packages: 1) the Statistical Package for the Social Sciences, and 2) the Statistical Analysis System. When processing the data from the surveys, analysts correct for respondents' unequal probabilities of selection. Analysts also post-stratify sample data according to respondents' geography, age, gender, and race, to account for potential biases such as over- and under-representation of certain population segments to match the distribution derived from the latest-available Current Population Survey estimates. To produce this measure, analysts divide the count of affirmative responses to the questions asking whether or not the respondent has set aside money for use in case of emergencies into the total number of responses.
Reliability Index	Reliable
Explanation of Data Reliability Check	The survey contractor certifies that each programmed survey instrument goes through a rigorous quality control process. Rigorous quality assurance extends from the design phase through data collection in the field. The overall process includes, but is not limited to, program testing, a pre-test and cognitive testing to determine the effectiveness of the survey and questions, monitoring of in-progress calls, recording of all interviews, and the production of tabulations of every question and variables to detect any missing data or errors. Additional quality measures include the checking of survey skip patterns and data accuracy and consistency checks. FEMA relies on the contractor's processes to ensure data reliability.

Performance Measure	Percent of adults that took multiple preparedness actions at their workplace, school, home, or other community location in the past year
Program	Preparedness and Protection
Description	This measure reports the share of all respondents to FEMA's annual National Household Survey who answered affirmatively to questions assessing whether they had taken more than one preparedness action in the past year, whether taking these actions at their workplace, school, home, or other community location. FEMA has noted that many Americans will experience a disaster or emergency at some point. FEMA emphasizes the importance of a national approach to preparedness, and will use results from this measure to assess the agency's effectiveness in this regard.

Scope of Data	Annually, FEMA conducts a National Household Survey to understand and assess Americans' attitudes and behaviors regarding emergency preparedness. The scope of this measure includes all responses to the questions on the survey which ask whether over the past year the respondent took multiple preparedness actions at their workplace, school, home, or other community location in the past year. Through a contractor, FEMA conducts the National Household Survey through telephone interviews.
Data Source	Interviewers capture responses and enter them into a Computer Assisted Telephone Interviewing (CATI) system, owned by the contractor and maintained at the contractor's facilities. The contractor conducting the survey establishes appropriate quality-control measures to ensure that data collection adheres to the outlined standards of the contract.
Data Collection Methodology	FEMA's survey contractor collects data using the CATI system, and completes analysis of responses using two statistical software packages: 1) the Statistical Package for the Social Sciences, and 2) the Statistical Analysis System. When processing the data from the surveys, analysts correct for respondents' unequal probabilities of selection. Analysts also post-stratify sample data according to respondents' geography, age, gender, and race, to account for potential biases such as over- and under-representation of certain population segments to match the distribution derived from the latest-available Current Population Survey estimates. To produce this measure, analysts divide the count of affirmative responses to the questions asking whether or not the respondent took multiple preparedness actions at their workplace, school, home, or other community location in the past year into the total number of responses.
Reliability Index	Reliable
Explanation of Data Reliability Check	The survey contractor certifies that each programmed survey instrument goes through a rigorous quality control process. Rigorous quality assurance extends from the design phase through data collection in the field. The overall process includes, but is not limited to, program testing, a pre-test and cognitive testing to determine the effectiveness of the survey and questions, monitoring of in-progress calls, recording of all interviews, and the production of tabulations of every question and variables to detect any missing data or errors. Additional quality measures include the checking of survey skip patterns and data accuracy and consistency checks. FEMA relies on the contractor's processes to ensure data reliability.

Performance Measure	Percent of applicants satisfied with simplicity of the Individuals and Households Program
Program	Response and Recovery
Description	This measure provides program managers with disaster survivors' impressions about the simplicity of the procedures required to receive disaster relief from the Individuals and Households Program (IHP). The program collects survivors' impressions of their interactions with IHP using standard surveys, administered by telephone, at three touchpoints of their experience with FEMA. The program sets a threshold for survivors' responses to survey questions to qualify for an overall rating of 'satisfied,' and the measure indicates the share of all questions answered and scored in the reporting period that meet the threshold, i.e. scores of four or five points on the five-point Likert-type scale. Managers will use insights derived from survey results to help drive improvements to IHP. Feedback from disaster survivors will ensure that the program provides clear information and high-quality service in critical, public-facing agency activities.
Scope of Data	This measure's scope includes valid responses to telephone surveys of disaster survivors in jurisdictions qualifying for the Individuals and Households Program

	(IHP). The Customer Survey and Analysis Section in the Recovery Reporting and Analytics Division conducts three surveys. The Office of Management and Budget (OMB) approved all of the surveys for dissemination. The surveys include a significant share of the registration population, enhancing results' validity. Analysts produce results using five (5) Likert-type-scale questions, each with a five (5)-point scale. Sampling includes all eligible applicants who contacted FEMA. The Initial survey begins about two weeks after registration, with a goal of 1,200 survivors per quarter. The Contact survey begins two weeks after a survivor's call or Internet contact, with a goal of 1,800 survivors per quarter. The Assessment survey begins 30 days after an IHP decision, with a goal of 400 survivors for each disaster declaration.
Data Source	The Customer Survey and Analysis Section (CSAS) in the Recovery Reporting and Analytics Division (RRAD) stores all survey responses in WinCATI (a Computer Assisted Telephone Interviewing system) for easy retrieval, statistical analyses, and reporting. CSAS staff export data from the survey system into a Microsoft Access database, where all survey data resides. RRAD operates and maintains systems used to store customer-survey data.
Data Collection Methodology	Using data stored in Microsoft Access, CSAS staff generate quarterly reports to the RRAD Performance Measurement and Analysis Team (PMAT) to calculate each question's comprehensive result. PMAT loads the results into PowerPivot for automatic calculation. For all surveys completed, PMAT analysts review respondents' answers to each of the five questions. RRAD has determined that answers to any question of 4 or 5 points on the five-point Likert-type scale satisfy the threshold for 'satisfaction with the simplicity of IHP.' Analysts then calculate the share of threshold-clearing answers for each question, and then calculate the average share of threshold-clearing responses across all five questions in the surveys submitted during a given reporting period, which yields the results for the performance measure.
Reliability Index	Reliable
Explanation of Data Reliability Check	A quality-control section monitors CSAS surveyors to ensure correct recording of data provided by applicants. The program engages in training, updating scripts, and coaching to mitigate reliability issues when recording applicant answers. CSAS program analysts and statisticians also review data after completion of surveys to ensure that recorded data accurately reflect what the surveys captured. After these accuracy checks, staff provide analysts with data in Excel format for performance measurement calculations. RRAD compares the raw data to the CSAS results summary. A peer review follows, followed by a supervisory review of the calculations. These multiple steps reinforce program confidence in the data's completeness, accuracy, and validity.

Performance Measure	Percent of applicants satisfied with simplicity of the Public Assistance process
Program	Response and Recovery
Description	This measure gauges the percent of applicants for Public Assistance (PA) grant programs that are satisfied with the simplicity of the process throughout the recovery lifecycle. Simplicity is measured through an initial customer survey and later assessment on the dimensions of Public Assistance (PA) Staff Interactions, Satisfaction with PA Program, Simplicity of the PA process; Simplicity of the PA System, and Simplicity of PA policy. Customer satisfaction data is collected from phone interviews as well as electronic submission of responses through the WinCATI survey system. Satisfied customers represent scores of three or greater on all dimensions of the 23 composite survey questions. Customer experience information is collected to better identify root causes for low satisfaction

	(primarily in simplicity) to guide future process changes and guidance to provide a more client-focused and user-friendly experience.
Scope of Data	The Customer Survey and Analysis Section (CSAS) within the Recovery Reporting and Analytics Division (RRAD) conducts two telephonic surveys for Public Assistance -- Initial and Assessment. The scope of the results includes all initial and assessment surveys that have an overall score of 3 or greater on a 5-point scale on all 23 questions that comprise the 5 assessed areas. The population includes all initial and assessment surveys conducted during the reporting period.
Data Source	The FEMA Recovery Reporting and Analytics Division's (RRAD) Customer Survey and Analysis Section (CSAS) conducts the surveys to collect the data for the measure. Collection techniques include phone interviews as well as electronic submission of responses through the WinCATI survey system. CSAS has a team of interviewers trained to conduct phone surveys of PA participants. All survey responses are stored in the WinCATI system for easy retrieval, statistical analyses, and reporting. Data are exported from the survey system into Access where all historical data are stored. CSAS generates quarterly reports to the RRAD Performance Measurement and Analysis Team (PMAT) to calculate metric results. PMAT loads the results into PowerPivot for automatic calculation. The Recovery Reporting and Analysis Division is the owner of the customer survey data.
Data Collection Methodology	All eligible applicants who had contact with FEMA (e.g. meetings, e-mails, or phone calls) are surveyed. The Initial survey is done around 60 days after the disaster/emergency declaration for two weeks with up to six contact attempts. The PA Assessment survey is conducted roughly 210 days after initial disaster declaration for two weeks with up to six contact attempts. CSAS generates reports and raw data and sends to RRAD PMAT for calculation. Each category's composite score includes the average scores of individual questions which are equally weighted within the category. Composite scores calculated as: PA Staff interactions has 6 survey questions weighed at 16.666667%; Satisfaction with the PA program has 5 questions at 20%; Simplicity of the PA process has 5 questions at 20%; Simplicity of PA System has 3 questions at 33.33%; Simplicity of policy has 4 questions at 25%. PMAT averages the score of all respondents for each of the 23 questions and converts the score into a percent.
Reliability Index	Reliable
Explanation of Data Reliability Check	CSAS surveyors are monitored by a quality control section to ensure data provided by applicants are recorded correctly. Training, updating scripts, and coaching take place to mitigate reliability issues when recording applicant answers. Data are also reviewed by CSAS program analysts and statisticians after the surveys are complete to ensure data accurately reflect what the surveys captured. Once accuracy is insured, data are provided in an Excel format for performance measurement. RRAD compares the raw data to the CSAS results summary. These results are then peer reviewed and followed up by a supervisory review of the calculations. Through these various steps we are confident that the data are complete, accurate, and thoroughly reviewed.

Performance Measure	Percent of communities in high earthquake, flood, and wind-prone areas adopting disaster-resistant building codes
Program	Mitigation
Description	This measure reports the percentage of high-risk communities in 50 states, the District of Columbia, and 5 territories (USVI, PR, Guam, American Samoa, CNMI) adopting building codes containing provisions that adequately address earthquake, flood, and wind hazards. FEMA tracks the number of high-risk communities that have adopted disaster resistant building codes by working with

	the Insurance Services Office (ISO) Building Code Effectiveness Grading Schedule (BCEGS). ISO collects data from the BCEGS survey daily and evaluates and assigns a grade of 1 (exemplary commitment to building code enforcement) to 10 to gauge adoption of building codes. Adopting disaster-resistant building codes helps strengthen mitigation nationwide to reduce the Nation's vulnerability to disasters.
Scope of Data	The population of this measure includes communities in 50 states, the District of Columbia, and 5 territories (USVI, PR, Guam, American Samoa, CNMI) in high earthquake, flood, and wind-prone areas as determined by the Insurance Services Office, Inc. (ISO) through their Building Code Effectiveness Grading Schedule (BCEGS) database and research. The two most recent building code editions, covering a time frame of six years of code development, are used to determine if a community has adopted disaster-resistant codes.
Data Source	The source of data for this measure is ISO's BCEGS database which tracks data on building codes adopted by participating jurisdictions from the BCEGS questionnaire. The BCEGS survey data is completed by communities electronically in the BCEGS database. BCEGS database is updated daily to include the latest surveys taken.
Data Collection Methodology	ISO collects data from the BCEGS survey daily and tracks building code adoption. ISO populates the BCEGS database with the survey results. The Mitigation program receives raw data from ISO through their BCEGS database.
Reliability Index	Reliable
Explanation of Data Reliability Check	FEMA relies on ISO to manage the completeness and reliability of the data provided thought their BCEGS database to the program; however, the data are reviewed by FEMA's Mitigation program to ensure results are consistent over time. If significant fluctuations in quarterly and annual results occur, the program will work with ISO to address issues with data reliability.

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

	agency's official property-management system. The Disaster Emergency Communications Division serves as the program of record for MEOV data stored in SAMS.
Data Collection Methodology	SAMS produces reports detailing the agency-wide inventory of MEOVs. The agency's Office of Response and Recovery maintains a tally of the types and numbers of Federal teams which have validated requirements for support by the program's Mobile Emergency Response Support Detachments, which include MEOVs. For any given fiscal year, dividing the total size of the MEOV inventory into the total number of federal response teams yields this performance measure.
Reliability Index	Reliable
Explanation of Data Reliability Check	Both the logistics section of the Disaster Emergency Communications Division and the agency's fleet-management staff in the agency's Office of the Chief Administrative Officer review reports of MEOV inventory produced by SAMS. These reviews ensure accurate counts of MEOV inventory. The agency's Office of Response and Recovery has responsibility for the types and numbers of Federal response teams which have validated requirements for support by the program's Mobile Emergency Response Support Detachments, which include MEOVs.

Performance Measure	Percent of funds provided to state, local, tribal, territorial, and other federal agencies for which data sets have been made publicly available and machine readable (Retired Measure)
Program	Grants
Description	This measure reports the fraction of the total amount of recorded agency spending in a given reporting period represented by the total funding of obligations with machine-readable amount and purpose data posted to a public-facing FEMA database during the same period.
Scope of Data	The scope of this measure includes all FEMA expenditures in the fiscal year-to-date assessed during a particular reporting period. For a subset of these expenditures, the program will have posted machine-readable amount and purpose data to a public-facing database.
Data Source	The Web Integrated Financial Management Integration System (WebIFMIS) serves as FEMA's financial system of record, with the exception of the National Flood Insurance Program (NFIP). Analysts supplement WebIFMIS data with reports on NFIP claim payments--provided by NFIP's Service Center and the Federal Insurance and Mitigation Administration's Management Directorate--to compile total expenditures. Program staff also group expenditures into several categories and sub-categories of machine readable data on the amount and purpose of expenditures, and post each of these data packages to the public-facing OpenFEMA website <http://www.fema.gov/openfema>. Package categories and sub-categories include Disaster Relief Fund (Individual Assistance & Public Assistance; Mission Assignments; Administrative Costs; and Mitigation); NFIP Claims; and Non-Disaster expenditures (Non-Disaster Grants; Administrative Costs; and Operations, Support, Procurement, Construction, and Improvements), respectively.
Data Collection Methodology	For each reporting period, using WebIFMIS and NHIP/FIMA data, analysts compile both total FEMA expenditures, and total expenditures contained in data packages posted to OpenFEMA. Dividing the latter amount into the former produces a percentage, which comprises the performance result for the reporting period in question.
Reliability Index	Reliable
Explanation of Data Reliability Check	Analysts will check data supporting this performance measure against data from other sources including WebIFMIS, FEMA's Enterprise Data Warehouse, and

	responses to previous data calls to agency program offices. In cases when data in these systems do not agree, analysts will consult relevant program, financial, and other analytic stakeholders to identify the causes of discrepancies and identify correct data for reporting purposes. In addition, the team supporting this performance measure plans to develop a dashboard incorporating inclusion and exclusion criteria for performance-measure reporting, with independent review from outside the program. This dashboard will include a consistent and reliable process for analyzing relevant data, with the aim of mitigating the risk of human error. Once the program begins to report on this measure, routine comparison to other systems will serve as a regular reliability check for the measure's underlying data.

Performance Measure	Percent of incident management and support actions taken that are necessary to stabilize an incident that are performed within 72 hours or by the agreed upon time (Retired Measure)
Program	Response and Recovery
Description	This measure reflects FEMA's role in effectively responding to any threat or hazard, with an emphasis on saving and sustaining lives within 72 hours, in support of state, local, tribal and territorial governments. 'Actions necessary to stabilize an incident' are defined as those functions that must be initiated immediately following an incident in order to ensure the best outcomes for survivors. These actions include establishing joint federal/state incident objectives and interoperable communications between FEMA-supported incident sites, deploying urban search and rescue resources, rapidly activating response coordination centers, and issuing timely alerts, warnings, operations orders, and situation reports.
Scope of Data	The scope of this measure includes all incidents—defined as all significant events, exercises, or activities—that require execution of the critical response functions. These functions must be performed within established timeframes and include: (1) Incident Management Assistance Teams (IMATs) establishing joint federal/state incident objectives; (2) disaster communication capabilities linking FEMA-supported incident sites; (3) national Urban Search and Rescue (US&R) resources arriving on-scene; (4) response coordination centers activating to directed levels; (5) watch centers transmitting operations orders and situation reports; and (6) the FEMA Operations Center issuing alerts, warnings, and notifications.
Data Source	National and Regional IMAT deployment data are submitted to the National Watch Center (NWC), which provides it to the Field Operations Support Branch for management and tracking. The Disaster Emergency Communications Division manages a database of Mobile Emergency Response Support-related deployment and response data. FEMA's US&R Branch manages deployment and response data associated with the National US&R Response System. National US&R statuses are updated every two hours during deployment, which is captured through National Response Coordination Center (NRCC) and NWC reporting and is tracked by the US&R Branch. Situation reports and operations orders are tracked by both the National and Regionals watch centers, electronically and on paper. NRCC and Regional Response Coordination Centers (RRCC) data are tracked through the manual comparison of operations orders and NRCC/RRCC activation logs. FEMA Operations Center data are managed and tracked through the Emergency Notification System.
Data Collection Methodology	For each quarter, FEMA tracks when an incident requires one or more of the six activities described above and whether or not the activity is accomplished in the time required. Each activity is scored quarterly based on percent of times

	completed within required timeframe (i.e. if the NRCC is activated 5 times in one quarter and activates to the directed level 4 of those times, the activity is scored as 80%). These six activity-level scores are then equally averaged for a total composite score each quarter.
Reliability Index	Reliable
Explanation of Data Reliability Check	The Field Operations Support Branch conducts an additional level of validation to ensure the reliability of the data and it has an established quality assurance process that is reviewed annually for relevance and accuracy. Each supporting activity mentioned above is responsible for reporting on the timeliness of the response for each incident requiring FEMA assistance.

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

	on and modified by multiple members of the RRAD reports staff, providing multiple levels of peer review. Prior to reporting of the data, it is then reviewed and summarized by the RRAD Performance Measurement and Analysis Team, shared with Subject Matter Experts (SMEs), supervisors, and the PA division for review and validation. During this time, any inconsistencies identified in the data analysis will be corrected.

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

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

Performance Measure	Percent of time the Integrated Public Alert and Warning System infrastructure is operating and available for use by federal, state, and local officials for the dissemination of emergency alerts
Program	Preparedness and Protection
Description	EO 13407 states 'It is the policy of the United States to have an effective, reliable, integrated, flexible, and comprehensive system to alert and warn the American people in situations of war, terrorist attack, natural disaster, or other hazards to public safety and well-being (public alert and warning system), taking appropriate account of the functions, capabilities, and needs of the private sector and of all levels of government in our Federal system, and to ensure that under all conditions the President can communicate with the American people.' The Integrated Public Alert and Warning System (IPAWS)infrastructure provides alert and warning message collection and dissemination so that United States residents will receive authenticated emergency alert messages over as many communications paths as possible.
Scope of Data	The data range covers the Continental United States (CONUS) as well as Alaska, Hawaii, and the 6 U.S. territories (OCONUS) Census population data and available audience reach measures.
Data Source	Data sources include: US Census bureau data for population; FCC radio station location and transmission data; Radio frequency propagation tools; OCIO server up time reports; test and exercise reports.

Data Collection Methodology	This is a composite of three metrics. The percent of time the Emergency Alert System (EAS) server is up and running: National Continuity Programs will receive reports from FEMA Office if the Chief Information Officer on server up time daily. This second metric is a result of a twice-weekly test of the IPAWS OPEN system: twice a week, IPAWS will send out a test message from the primary FEMA Operations Center (FOC) and the Alternate FEMA Operations Center (AFOC) systems to the FEMA Primary Entry Point (PEP) Stations. The final metric will be the results of a survey of PEP Station broadcasters as to whether the television and radio broadcasters received the weekly test and whether their systems operated as required.
Reliability Index	Reliable
Explanation of Data Reliability Check	FEMA can verify the availability and operability of the EAS server and PEP Stations. There are some vulnerabilities, such as the physical equipment at each PEP Station which is susceptible to local events. The remainder of the system is dependent upon numerous large and small national and local private sector partners who rebroadcast the EAS messages to the American people through a variety of communications technologies. NCP verifies the operability of the entire system with occasional tests.

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

	master All Regions Plan Approval Inventory. The Inventory is matched to Federal Information Processing Standard and Community Identification Database codes to jurisdictions and utilizes Census data to match populations for each jurisdiction. The information is sent back to the Regions for validation and updating each month.

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

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

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

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

Federal Law Enforcement Training Centers

Performance Measure	Percent of Participating Organizations satisfied with the training provided by the Federal Law Enforcement Training Centers (New Measure)
Program	Law Enforcement Training
Description	This measure reflects Participating Organizations' (POs) overall satisfaction with the Federal Law Enforcement Training Centers' (FLETC's) training and that training programs address the right skills needed for their officers/agents to safely and effectively perform their law enforcement duties. The POs are surveyed on their satisfaction with the quality of instructional staff, and whether FLETC's basic and advanced training addresses the right skills needed for officers and agents to perform their law enforcement duties safely and effectively. Responses of "Strongly Agree" and "Agree" are considered satisfied. FLETC provides training to more than 90 POs, both internal and external to the Department of Homeland Security. The results provide on-going opportunities for improvements incorporated into FLETC training curricula, processes and procedures.
Scope of Data	This measure includes the results from all POs that respond to the PO Satisfaction Survey statements about overall satisfaction with the training FLETC provides, satisfaction with the quality of instructional staff, and whether FLETC's

	basic and advanced training addresses the right skills needed for officers and agents to perform their law enforcement duties safely and effectively. The scope of results include POs that responded "Strongly Agree" or "Agree" to statements about overall satisfaction with the training, satisfaction with the quality of instructional staff, and that training addresses the right skills for officers/agents to perform their law enforcement duties safely and effectively. 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 overall satisfaction with the training, satisfaction with the quality of instructional staff, and that training addresses the right skills for officers/agents to perform their law enforcement duties safely and effectively 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 Participating Organizations that agree the Federal Law Enforcement Training Centers' training programs address the right skills (e.g., critical knowledge, key skills and techniques, attitudes/behaviors) needed for their officers/agents to perfo (Retired Measure)
Program	Law Enforcement Training
Description	This performance measure reflects the satisfaction of Partner Organizations (POs) that Federal Law Enforcement Training Centers' (FLETC) training programs address the right skills needed for their officers/agents to perform their law enforcement duties such as the prevention of the introduction of high-consequence weapons of mass destruction, terrorism and other criminal activity against the U.S. and our citizens. The results of the measure provide on-going opportunities for improvements that are incorporated into FLETC training curricula, processes and procedures.
Scope of Data	This measure includes the results from all PO that respond to the Partner Organization Satisfaction Survey Statements 1 and 2, respectively: 'The FLETC's basic training programs and courses of instruction address the right skills needed for my officers/agents to perform their law enforcement duties,' and 'The FLETC's advanced training programs and courses of instruction address the right skills needed for my officers/agents to perform their law enforcement duties.' FLETC collaborates with more than 85 Partner Organizations, both internal and external to the Department of Homeland Security.
Data Source	The source of the data is the FLETC Partner Organization Satisfaction Survey administered via a web-based survey program (Vovici), which tabulates and

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

Immigration and Customs Enforcement

Performance Measure	Average length of stay in detention of all convicted criminal noncitizens prior to removal from the United States (in days)
Program	Enforcement and Removal Operations
Description	This measure provides an indicator of efficiencies achieved in working to drive down the average length of stay (ALOS) for convicted criminals in ICE's detention facilities. Decreases in the average length of stay can significantly reduce the overall costs associated with maintaining a noncitizen population prior to removal.
Scope of Data	The scope of this measure includes all criminal noncitizens who were detained within ICE's detention facilities or while in ICE custody in federal, state, and local jails during the fiscal year awaiting due process. Noncitizens that are initially booked into the Department of Health and Human Services, Office of Refugee and Resettlement, Mexican Interior Repatriation Program, or transport facilities, and U.S. Marshals Service Prisoners are excluded from ICE's ALOS. All other detention facilities, including hold rooms, are included in the ALOS count.
Data Source	Data is maintained in the Removal Module of the ENFORCE database. This database is maintained at ICE headquarters and the data entry occurs at Enforcement and Removal Operations (ERO) field Offices throughout the country. Tools in the Integrated Decision Support System are used to query the Removal Module and produce reports to calculate the final results for this measure.
Data Collection Methodology	Enforcement and Removal Operations field offices are responsible for the entry and maintenance of data regarding the detention of noncitizens in ICE Custody. The length of stay for a noncitizens's detention stay is calculated by counting the

	number of days between the noncitizen's initial book-in date into ICE Custody and their final book-out date. If a noncitizen is booked in and out of ICE custody on the same day, the noncitizen's length of stay is 0 days. ALOS is the sum of the length of stay for all applicable detention stays divided by the number of detention stays using only detention stays that have concluded within a given fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	Headquarters staff validate the completeness and accuracy of the data entered by field offices into the Removal Module through trend analysis to look for aberrations and unusual patterns. Data is analyzed on a weekly basis and compared to statistics from prior months and the previous year. An additional reliability check occurs when data is cross-referenced between field office detention facility reports of the number of removals, and data entered into the database. The Statistical Tracking unit checks for consistency of the results or measuring instrument through validation, back-end testing or reproducibility of the data through alternative methodology. Depending upon the degree of consistency between two measures of the same measure allows the statistician to determine whether the data is considered reliable and or stable. Any inaccuracies will need to be sent to the Unit Chief, who will make the necessary corrections to the tasking query.

Performance Measure	Number of convicted criminal noncitizens who were returned or were removed from the United States
Program	Enforcement and Removal Operations
Description	This measure includes both the return and removal of noncitizens who have a prior criminal conviction from the United States by ICE Enforcement and Removal Operations (ERO). This measure reflects the program's efforts to ensure convicted criminal noncitizens do not remain in the United States.
Scope of Data	All returns and removals of illegal immigrants who have had a prior criminal conviction are included in this measure. All non-criminal immigration violators are excluded from the count. An immigration violator is only considered a convicted criminal if he or she has also been convicted of a crime.
Data Source	Data is maintained in the Removal Module of the ENFORCE database. This database is maintained at ICE headquarters and the data entry occurs at Enforcement and Removal Operations (ERO) Field Offices throughout the country. Tools in the Integrated Decision Support System (IIDS) are used to query the Removal Module and produce reports to calculate the final results for this measure. The IIDS data warehouse is maintained by ERO's Statistical Tracking Unit (STU).
Data Collection Methodology	Enforcement and Removals Operations field offices are responsible for the entry and maintenance of data regarding the removal and return of noncitizens. When a noncitizen is removed and/or returned from the United States, case officers in the field will indicate in the database the case disposition and date the removal/return occurred in the database. Officers track the status of administrative processes and/or court cases and indicate when actual removals occur in the Removal Module of the ENFORCE database. Reports generated from the Removal Module using IIDS determine the number of convicted illegal noncitizens returned/removed from the country during the specified time.
Reliability Index	Reliable
Explanation of Data Reliability Check	Headquarters staff validate the completeness and accuracy of the data entered by field offices into the Removal Module through trend analysis to look for aberrations and unusual patterns. Data is analyzed on a weekly basis and compared to statistics from prior months and the previous year. An additional

	reliability check occurs when data is cross - referenced between field office detention facility reports of the number of removals, and data entered into the database. The Statistical Tracking unit checks for consistency of the results or measuring instrument through validation, back-end testing or reproducibility of the data through alternative methodology. Depending upon the degree of consistency between two measures of the same measure allows the statistician to determine whether the data is considered reliable and or stable. Any inaccuracies will need to be sent to the Unit Chief, who will make the necessary corrections to the tasking query.

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

Performance Measure	Number of significant Homeland Security Investigation cases that resulted in a disruption or dismantlement (New Measure)
Program	Homeland Security Investigations
Description	This measure reports on the total cumulative number of significant transnational criminal investigations that resulted in a disruption or dismantlement. To be considered significant, the investigation must involve a high-threat transnational criminal organization engaged in criminal activity related to illicit trade, travel, or finance (both drug-related or non-drug-related); counter-terrorism; national security; worksite enforcement; gangs; or child exploitation. "Disruption" is defined as impeding the normal and effective operation of the targeted organization. "Dismantlement" is defined as destroying the organization's

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

Performance Measure	Percent of detention facilities found in compliance with the national detention standards by receiving a final acceptable inspection rating
Program	Enforcement and Removal Operations
Description	This measure gauges the percent of detention facilities, with an Average Daily Population (ADP) greater than 10, that have received an overall rating of acceptable or above within the Enforcement and Removal Operations (ERO)

	National Detention Standards Program as measured against the Performance Based National Detention Standards. Through a robust inspections program, the program ensures facilities utilized to detain noncitizens in immigration proceedings or awaiting removal to their countries do so in accordance with the Performance Based National Detention Standards.
Scope of Data	The scope of this measure includes all adult facilities on the Authorized Facility's List authorized to house ICE detainees through ERO Detention Management Control Program (DMCP). Per the DMCP, facilities that are used regularly by ICE (i.e., an APD greater than 10) to house adult detainees must be inspected. Once a facility has been inspected by ICE and determined to be appropriate to house adult detainees, the facility is scheduled for routine follow-up inspections and tracked on the Authorized Facility List. Authorized facilities include detention centers that have been inspected by ERO/Custody Operations law enforcement personnel, or their Subject Matter Experts (SME), to ensure the facility meets all requirements of the ICE/ERO National Detention Standards provisions. Family residential centers, or ERO juvenile facilities, staging facilities, or holding rooms that may temporarily hold ICE detainees are not included.
Data Source	The annual review rating is contained in formal inspection reports provided by the Detention Standards Compliance Unit (DSCU) contractor and is further reviewed by the DSCU. The information from these reports will be compiled to determine the agency-wide percentage of facilities receiving acceptable or above rating.
Data Collection Methodology	Data for this measure is collected by annual inspections, which are then evaluated by ERO inspectors. These inspections review the current National Detention Standards that apply to all facilities, and rate whether the facility is in compliance with each standard. Based on these ratings, the compliance for each facility is calculated. This information is communicated in formal reports to the program and the ERO Inspections and Audit Unit and the Detention Standards Compliance Unit at ERO Headquarters, which oversees and reviews all reports. The program reports semi-annually on agency-wide adherence with the Detention Standards based on calculating the number of facilities receiving an acceptable or better rating, compared to the total number of facilities inspected.
Reliability Index	Reliable
Explanation of Data Reliability Check	The program reviews all reports of detention facilities inspections. Inspections that receive a final rating of 'Acceptable' or above are reviewed by the Detention Standards Compliance Unit (DSCU) and the Inspections and Audit Unit. Inspections that receive deficient or at-risk rating are reviewed by DSCU SMEs.

Performance Measure	Percent of final administrative orders that result in orders of removal from the United States
Program	Office of Principal Legal Advisor
Description	This measure indicates the percent of total final administrative orders secured by Office of Principal Legal Advisor (OPLA) attorneys that result in removal of those found to be in the United States in violation of the Immigration and Nationality Act (INA). OPLA attorneys play an integral role in enforcing the nation's immigration laws by litigating cases in immigration court and securing orders of removal against those found to be in violation of the INA.
Scope of Data	The scope of data will consist of all immigration cases with a final administrative order date (Final Orders are orders where neither party has reserved appeal), including both Immigration Judge and Board of Immigration Appeals (BIA) decisions, occurring during the given reporting period.
Data Source	The data is collected from OPLA attorneys and support personnel and stored in the Principal Legal Advisor's Network (PLAnet) PLAnet is OPLA's case

	management system that documents and tracks litigation before the Executive Office for Immigration Review (EOIR), advice and guidance provided to ICE's clients, agency taskings, and administrative work performed by ICE's attorney and support personnel. Data stored in PLAnet is input manually and is not verified against the Dept. of Justice EOIR databases. PLAnet is not intended to be a statistical tool. The Office of the Chief Information Officer manages the PLAnet system located at Headquarters. The data retrieved for this measure is only based on what is collected within the PLAnet system, no external system or database are used.
Data Collection Methodology	OPLA Knowledge Management Division analysts export the data directly from PLAnet into Excel to calculate the percent of final administrative orders that result in removal. The following data collection methodology is used for this measure: 1) Obtain all final orders from PLAnet; 2) If the Immigration Judge (IJ) issues an order and there are no subsequent activity, it is included in the final order count; 3) If the IJ issues an order and the case is continuing (meaning that there are hearings, etc. that occur after the date of that order), then we do not count the case as a final order; 4) If the IJ issues an order that is appealed, and the BIA issues a different final order, then we count the BIA's order as final; and 5) If the IJ issues an order, and the BIA upholds the order, then we use the IJ order along with the date it was issued to determine if it should be included in that quarterly report. Based on this information the percent is calculated.
Reliability Index	Reliable
Explanation of Data Reliability Check	OPLA's Knowledge Management Division statisticians review and confirm the accuracy of the data presented on a quarterly basis. For quality control purposes, statisticians independently process and analyze the data using the defined criteria of the request. Upon completion, the statisticians compare results to ensure consistency. If the results differ, i.e. an error is found, the statisticians review the criteria used to derive the statistical results to confirm accuracy of the measure. Once the accuracy of the criteria has been confirmed, the statisticians individually re-run the analysis to determine whether the same results are obtained as a method of measuring the validity and reliability of the data output. If the results differ after re-running the analysis, the statisticians review the criteria and the data to determine the reason for the differing results and come to a consensus on the correct criteria to apply.

Performance Measure	Percent of significant Homeland Security Investigations cases that result in a disruption or dismantlement (Retired Measure)
Program	Homeland Security Investigations
Description	This measure reports on the percentage of significant transnational criminal investigations that resulted in a disruption or dismantlement. To be considered significant, the investigation must involve a high-threat transnational criminal organization engaged in criminal activity related to illicit trade, travel, or finance (both drug-related or non-drug-related); counter-terrorism; national security; worksite enforcement; gangs; or child exploitation. 'Disruption' is defined as impeding the normal and effective operation of the targeted organization. 'Dismantlement' is defined as destroying the organization's leadership, financial base and network to the degree that the organization is incapable of operating and/or reconstituting itself.
Scope of Data	The scope of this measure includes validated records of all transnational criminal investigations related to illicit trade, travel, and finance (both drug-related and non-drug-related); counter-terrorism; national security; worksite enforcement; gangs; and child exploitation that are entered in the Investigative Case Management (ICM) system and have been referred to and approved through

	HSI's Significant Case Review (SCR) process. HSI utilizes the SCR process to report its impact on the mission. Significant cases are nominated by the Special Agent conducting the investigation, based on predetermined criteria. SCRs consist of three types of submissions: an initial significant investigation, a disruption, and a dismantlement.
Data Source	Data are entered in the SCR module located in HSI's Investigative Case Management (ICM) system. ICM serves as the core law enforcement case management tool primarily used by HSI Special Agents and personnel supporting the HSI mission. ICM enables HSI 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 HSI's official system of record and is used to initiate cases, identify case categories, and record and report substantive case information during the investigative process, ultimately capturing arrest, indictment, conviction, and case closure. Management of the SCR program resides with the Domestic Operations Division located at ICE/HSI Headquarters (HQ).
Data Collection Methodology	Special Agents submit cases that are significant to the agency. These cases are then confirmed as significant by an HQ Program Manager, the field-based Group Supervisor, and the Special Agent in Charge. Following these confirmations, an independent team at HQ and an SCR panel reviews the case and verifies that it meets the criteria for a 'significant,' 'disruption,' or 'dismantlement' designation. The process and outcome is recorded in ICM. HSI analysts at HQ extract and aggregate data from ICM. The analysts count the total number of significant cases that are open at the beginning of the reporting period plus cases that are opened and approved, through the SCR process, during the reporting period. The analysts count the number of disruptions or dismantlements that were approved, through the SCR process, during the reporting period. The resulting percent is obtained by dividing the count of significant cases by the count of disruptions or dismantlements.
Reliability Index	Reliable
Explanation of Data Reliability Check	The SCR process begins with an HSI Special Agent (SA) identifying an investigation that meets the criteria to be designated as an initial significant investigation. The SA then completes and submits the Domestic Operations SCR worksheet. Once approved by a Domestic Operations Program Manager, the SA may enter the SCR in ICM. 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 SA submit enforcement actions that meet the definition of either a disruption or dismantlement of a significant investigation. ICE also conducts quality control verification on all data received through ICM to ensure performance data are accurate, complete, and unbiased.

Performance Measure	Total number of noncitizens who were returned or removed from the United States
Program	Enforcement and Removal Operations
Description	This measure describes the total number of noncitizens returned and/or removed from the United States by ICE Enforcement and Removal Operations (ERO). The measure includes both noncitizens who have entered the country illegally, but do not already have prior criminal conviction, along with those who have had a prior criminal conviction. This measure provides a complete picture of all the returns and removals accomplished by the program.

Scope of Data	The measure captures the sum of all noncitizens returned and/or removed by ICE ERO. Immigration violators can be classified into two groups: non-criminal and criminal. Non-criminal immigration violators include all those identified as illegally present with no previous criminal convictions. Criminal immigration violators would include all those identified who are illegally present with criminal convictions, such as a misdemeanor or felony.
Data Source	Data is maintained in the Removal Module of the ENFORCE database. This database is maintained at headquarters and the data entry occurs at Enforcement and Removal Operations (ERO) Field Offices throughout the country. Tools in the Integrated Decision Support System (IIDS) are used to query the Removal Module and produce reports to calculate the final results for this measure. The IIDS data warehouse is maintained by ERO's Statistical Tracking Unit (STU).
Data Collection Methodology	Enforcement and Removals Operations field offices are responsible for the entry and maintenance of data regarding the removal and return of noncitizens. When a noncitizen is removed and/or returned from the United States, case officers in the field will indicate in the database the case disposition and date the removal/return occurred in the database. Officers track the status of administrative processes and/or court cases and indicate when actual removals occur in the Removal Module of the ENFORCE database. Reports generated from the Removal Module using IIDS determine the number of convicted noncitizens returned/removed from the country during the specified time.
Reliability Index	Reliable
Explanation of Data Reliability Check	The IIDS, ERO's main data warehouse, is routinely maintained for accuracy. Law Enforcement Systems and Analysis' Statistical Tracking Unit (STU) has internal control measures in place to check data reliability. STU validates queries each week to benchmark against prior weeks' reported figures, which are archived internally. Data abnormalities are examined by the STU analyst to identify any technical issues and adjusted accordingly. The corrected data model is archived and used moving forward. If the data are determined to have potential data quality issues due to Field input, the STU analyst will work in conjunction with the STU officers to perform a case review in addition to a review of the noncitizen's criminal history in the front-end applications. Any major data quality issues and anomalies are shared with the Data Quality and Integrity Unit to potentially facilitate the Field fixing or addressing a larger-scale issue with the front-end applications.

Office of Intelligence and Analysis

Performance Measure	Number of intelligence reports shared with the intelligence community (Retired Measure)
Program	Analysis and Operations
Description	This measure reflects the DHS contribution of raw, unevaluated intelligence, to the intelligence community and the Federal Government so as to share the unique information obtained from intelligence officers in the field. This intelligence is only that which has been aligned to relevant Homeland Security Intelligence Priorities driven by the Homeland Security Intelligence Council. The measure counts the number of unique intelligence reports that the DHS Office of Intelligence and Analysis has disseminated.
Scope of Data	The measure reflects all Office of Intelligence and Analysis intelligence information reports that are tagged with the relevant Homeland Security priority

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

Performance Measure	Percent of finished intelligence products aligned to key intelligence questions (New Measure)
Program	Analysis and Operations
Description	This measure evaluates the extent to which finished intelligence products address Key Intelligence Questions aligned to customer requirements identified in the Program of Analysis. The Program of Analysis is organized around thematic responsibilities and ensures alignment of prioritized planned analytic efforts to customer requirements. Key Intelligence Questions are developed by the intelligence Mission Centers in partnership with the Intelligence Enterprise following a Homeland Security Intelligence Priorities Framework process that identifies the most pressing topics for the enterprise. All analytic products must include appropriate metadata tagging, including Homeland Security priority code and alignment against Program of Analysis Key Intelligence Questions. Prioritizing intelligence products around key analytic questions promotes transparency, reduces duplication of effort, and increases the value to customer.
Scope of Data	The population for this measure is based on all finished intelligence products. The numerator includes a subset of finished intelligence products that are aligned to Key Intelligence Questions. A finished intelligence product is a product of analytical judgement applied to address an intelligence question where the analytic conclusions have been drafted, reviewed, and disseminated outside of IA. Key Intelligence Questions are identified and periodically reviewed/ updated in the Program of Analysis.
Data Source	Analysts store their initial analysis in the System for Analytic Review and Approval (SARA) system, and then the finished analytical production and reports are stored in an internal system named HELIX. All analytic products must include appropriate metadata tagging, including Homeland Security priority code and alignment against Program of Analysis Key Intelligence Questions.

Data Collection Methodology	Analysts begin work by initiating a project, tracking its flow through the SARA system, which captures the necessary data and metadata to analyze alignment to identified Key Intelligence Questions. Once the analyst completes their analysis and produces a report of conclusions, it then moves through the work flow to leadership review for analytic tradecraft which validates judgements contained in the report of conclusions. If approved, the report then considered a finished intelligence product, and is disseminated outside the organization depending on classification level. The results for this measure are determined by dividing the number of finished intelligence products aligned to a Program of Analysis Key Intelligence Question by the total number of finished intelligence products.
Reliability Index	Reliable
Explanation of Data Reliability Check	The finished intelligence product information and the numbers themselves are validated monthly by the Performance Measurement and Evaluation and Production staff to ensure completeness and accuracy of the data and metadata in Helix. The information in this check may be cross-referenced with SARA to ensure its accuracy. The number of products aligned to Program of Analysis Key Intelligence Questions and the total number of products are consistently reviewed by senior leadership. If potential errors have been identified in this reliability check, corrections are made to the metadata element in the repository. In the event of differences of opinion, an adjudication process exists to resolve discrepancies over the determination of information that are determined by IA senior leadership.

Performance Measure	Percent of finished intelligence products shared with state, local, tribal, territorial, and private sector partners (New Measure)
Program	Analysis and Operations
Description	This measure reflects the percent of Office of Intelligence and Analysis (IA's) finished intelligence production that is considered compliant with Intelligence Community Directive (ICD) 203, and which is shared with its State, Local, Tribal, Territorial, and Private Sector partners. A finished intelligence product is a product of analytical judgement applied to address an intelligence question where the analytic conclusions have been drafted, reviewed, and disseminated outside of IA. This measure ensures that IA is leveraging its unique information sharing role by sharing finished intelligence products with State, Local, Tribal, Territorial, and Private Sector partners.
Scope of Data	The scope reflects finished intelligence products that are considered compliant with Intelligence Community Directive (ICD) 203, and which are shared with State, Local, Tribal, Territorial, and Private Sector partners (numerator) as a percent of the total number of ICD 203-compliant finished intelligence products. IA finished intelligence products that are ICD 203-compliant constitute a smaller subset of IA's finished intelligence production, including products, Homeland Intelligence Todays, Intelligence Assessments, and Field Analysis Reports. IA employs a formal review process to verify compliance; reporting restricted to this compliance is predicated by the Office of the Director of National Intelligence's role as IA's funding source.
Data Source	Finished intelligence products are stored in an internal system named HELIX, and entered into various dissemination systems, including the Homeland Security Information Network (HSIN). HSIN is the trusted DHS Information Sharing Environment, and allows trusted partners access to information via controlled community of interest portals (e.g., intelligence, critical infrastructure, and etc).
Data Collection Methodology	Analysts initiate a project and track its flow through the System for Analytic Review and Approval (SARA) system. Once the analyst produces a report of conclusions, it then moves through the work flow to leadership review for

	analytic tradecraft, validating judgements contained in the product. If approved, the report is then considered a finished intelligence product compliant with Intelligence Directive 203. Finished intelligence products are disseminated outside the organization depending on classification level, and available to properly cleared State, Local, Tribal, Territorial, and Private Sector (SLTT) partners. The results for this measure are determined by dividing the number of finished intelligence products that are compliant with ICD 203 and shared with SLTTP partners by the total number of finished intelligence production, which includes products, Homeland Intelligence Todays, Intelligence Assessments, and Field Analysis Reports.
Reliability Index	Reliable
Explanation of Data Reliability Check	IA employs a formal review process to verify the data for this measure. Data in the SARA and HELIX systems are reviewed at least monthly for completeness and accuracy by the Office of Intelligence and Analysis Enterprise Performance and Evaluation Branch, as well as operational analysts. In the event that inaccurate data is reported, processes are in place to adjudicate any issues and correct the record to ensure accuracy.

Performance Measure	Percent of finished intelligence products shared with the Intelligence Community (New Measure)
Program	Analysis and Operations
Description	This measure reflects the percent of Office of Intelligence and Analysis (IA's) finished intelligence products that are considered compliant with Intelligence Community Directive (ICD) 203, and which are shared with the Intelligence Community. A finished intelligence product is a product of analytical judgement applied to address an intelligence question where the analytic conclusions have been drafted, reviewed, and disseminated. ICD 203-compliant products constitute a smaller subset of finished intelligence production that includes Homeland Intelligence Todays, Intelligence Assessments, and Field Analysis Reports. Providing finished intelligence products equips the Homeland Security Enterprise with the timely intelligence and information it needs to keep the homeland safe, secure, and resilient.
Scope of Data	The scope is finished intelligence production that is considered compliant with Intelligence Community Directive (ICD) 203, and which is shared with the Intelligence Community (numerator) as a percent of the total number of IA's ICD 203-compliant finished intelligence production (denominator). IA finished intelligence products that are ICD 203-compliant constitute a smaller subset of IA's finished intelligence production that includes products, Homeland Intelligence Todays, Intelligence Assessments, and Field Analysis Reports.
Data Source	Finished intelligence products are stored in an internal system named HELIX, and entered into various dissemination systems, including the official federal intelligence repository, the Library of National Intelligence. This is the same system used by the rest of the Intelligence Community to access all intelligence reporting.
Data Collection Methodology	Analysts initiate and track projects through the System for Analytic Review and Approval (SARA) system. Once the analyst produces a report of conclusions, it then moves through the work flow to leadership review for analytic tradecraft which validates judgements contained in the product. If approved, the report is then considered a finished intelligence product compliant with Intelligence Directive 203. Finished intelligence products are disseminated outside the organization depending on classification level. The results for this measure are determined by dividing the number of finished intelligence products that are compliant with ICD 203 and shared with the Intelligence Community divided by

	the total number of finished intelligence production, which includes products, Homeland Intelligence Todays, Intelligence Assessments, and Field Analysis Reports.
Reliability Index	Reliable
Explanation of Data Reliability Check	IA employs a formal review process to verify the data for this measure. Data in the SARA and HELIX systems are reviewed at least monthly for completeness and accuracy by the Office of Intelligence and Analysis Enterprise Performance and Evaluation Branch, as well as operational analysts. In the event that inaccurate data is reported, processes are in place to adjudicate any issues and correct the record to ensure accuracy.

Performance Measure	Percent of intelligence reports rated satisfactory and useful by customers (New Measure)
Program	Analysis and Operations
Description	This measure gauges the extent to which finished intelligence products are satisfying customers' needs. An intelligence report is a product of analytical judgement applied to address an intelligence question produced by DHS or through partnerships with other agencies where the analytic conclusions have been drafted, reviewed, and disseminated to customers. Responses of "very satisfied" and "somewhat satisfied" are considered to have met the criteria for "satisfactory and useful." Providing intelligence on topics of concern equips the Homeland Security Enterprise with the timely intelligence and information it needs to keep the homeland safe, secure, and resilient.
Scope of Data	The population of this measure is all customer feedback received from surveys appended to each IA intelligence report. The customer feedback surveys contain a standard question intended to elicit the degree of customer satisfaction with the usefulness of the intelligence report. The question asks customers to rate satisfaction on a five-point rating scale (very satisfied, somewhat satisfied, neither satisfied nor dissatisfied, somewhat dissatisfied, very dissatisfied). Responses of "very satisfied" and "somewhat satisfied" will be considered to have met the criteria for "satisfactory and useful" and are included in the scope of this measure.
Data Source	The data sources for this performance measure will be the Enterprise Performance and Evaluation Branch (EPE) Dashboards located on the unclassified and high-side networks, as well as the unclassified EPE SharePoint site. Note that analysts initiate and track projects in the System for Analytic Review and Approval (SARA) system, and then the finished analytical production and reports are stored in an internal system named HELIX.
Data Collection Methodology	Once the analyst produces a report, it moves to leadership review, which validates judgements contained in the report. Approved reports are disseminated outside the organization depending on classification level. Interactive customer feedback surveys are appended to each intelligence report. Customers enter their responses to the surveys and click a "Submit Feedback" button that automatically generates an email on the appropriate network. The feedback is automatically ingested from the email responses and fed into the dashboards on SharePoint, to include an automated file transfer and consolidation to the high-side. The results for this measure are determined by dividing the total number of those responding they are "very satisfied" or "somewhat satisfied" by the total number of survey responses received.
Reliability Index	Reliable
Explanation of Data Reliability Check	EPE verifies the successful ingest of feedback at least weekly and ensures the removal of any redundant entries through rigorous data cleansing and direct customer follow-up, where necessary. Satisfaction and usefulness metrics are

	consistently reviewed by senior leadership. If potential errors have been identified in this reliability check, corrections are made to the dashboards and SharePoint site. In the event of differences of opinion, an adjudication process exists to resolve discrepancies over the determination of information that are determined by IA senior leadership.

Performance Measure	Percent of intelligence reports rated satisfactory or higher in customer feedback that enable customers to manage risks to cyberspace (Retired Measure)
Program	Analysis and Operations
Description	This measure gauges the extent to which the DHS Intelligence Enterprise (DHS IE) is satisfying their customers' needs related to managing risks to cyberspace. This measure encompasses reports produced by all DHS component intelligence programs and provided to federal, state, and local customers.
Scope of Data	The scope of this measure is all feedback received from customer satisfaction surveys returned to the DHS IE member that originated the intelligence report. For this performance measure 'intelligence report' is defined per Component.
Data Source	The data source for this performance measure will be customer feedback surveys fielded by the DHS IE.
Data Collection Methodology	Members of the DHS IE will attach an electronic survey instrument to each intelligence product disseminated to customers. The recipient of the intelligence completes and then returns the survey to the issuer. The DHS Intelligence Enterprise will provide Intelligence and Analysis (I&A) with the survey results on the second Friday following the end of each quarter. Upon receipt of the data, I&A will average the data across the Intelligence Enterprise for each of the DHS mission areas and report the total. For this measure, customer satisfaction is defined as responsiveness of the product and its value in helping the customer manage risks to cyberspace. Customers rate their satisfaction on a five point Likert scale with 'very satisfied' and 'somewhat satisfied' meeting the criteria for 'satisfactory.' The result is calculated by dividing the number of 'satisfactory' ratings by the number of total responses.
Reliability Index	Reliable
Explanation of Data Reliability Check	Individuals within the DHS IE are responsible for collecting, storing, and reporting data generated by the source above. I&A Performance Management & Evaluation (PME) personnel are responsible for aggregating the data from the DHS IE and reporting the results quarterly. Once the survey responses are received and aggregated, I&A PME staff review the results for consistency and look for any anomalous trends that would signal a data integrity problem. Any issues are researched and if any erroneous data is found, it is corrected or removed from the overall calculation.

Performance Measure	Percent of intelligence reports rated satisfactory or higher in customer feedback that enable customers to understand the threat (Retired Measure)
Program	Analysis and Operations
Description	This measure gauges the extent to which the DHS Intelligence Enterprise (DHS IE) is satisfying their customers' needs related to anticipating emerging threats. This measure encompasses reports produced by all DHS component intelligence programs and provided to federal, state, and local customers.
Scope of Data	The scope of this measure is all feedback received from customer satisfaction surveys returned to the DHS IE member (U.S. Coast Guard, Transportation Security Administration, etc.) that originated the intelligence report. For this performance measure 'intelligence report' is defined per Component.
Data Source	The data source for this performance measure will be customer feedback surveys fielded by the DHS IE.

Data Collection Methodology	Members of the DHS IE will attach an electronic survey instrument to each intelligence product disseminated to customers. The recipient of the intelligence completes and then returns the survey to the issuer. The DHS IE will provide Intelligence and Analysis (I&A) with the survey results on the second Friday following the end of each quarter. Upon receipt of the data, I&A will average the data across the Intelligence Enterprise for each of DHS mission area and report the total. For this measure, customer satisfaction is defined as responsiveness of the product and its value in helping the customer anticipate emerging threats. Customers rate their satisfaction on a five point Likert scale with 'very satisfied' and 'somewhat satisfied' meeting the criteria for 'satisfactory.' The result is calculated by dividing the number of 'satisfactory' ratings by the number of total responses.
Reliability Index	Reliable
Explanation of Data Reliability Check	Individuals within the DHS IE are responsible for collecting, storing, and reporting data generated by the source above. I&A Performance Management & Evaluation (PME) personnel are responsible for aggregating the data from the DHS IE and reporting the results quarterly. Once the survey responses are received and aggregated, I&A PME staff review the results for consistency and look for any anomalous trends that would signal a data integrity problem. Any issues are researched and if any erroneous data is found, it is corrected or removed from the overall calculation.

Office of Operations Coordination

Performance Measure	Percent of National Operations Center incident reports and situational awareness products produced and disseminated to the homeland security enterprise within targeted timeframes
Program	Analysis and Operations
Description	This measure evaluates percent of Situational Awareness (SA) Products disseminated within targeted timeframes. These products serve as the basis for senior leader decision-making and SA across the Homeland Security Enterprise. To augment SA, facilitate coordination, and provide decision support, the National Operations Center (NOC) utilizes a web-based DHS Common Operating Picture (COP). The COP can be accessed through various Briefing Display Systems within the NOC, or through any computer using the Homeland Security Information Network (HSIN). HSIN allows only authorized users to manipulate information on the COP. The NOC Watch Team creates a geographically located icon on the COP and an overall written situation summary to provide SA on the event to decision makers and the Homeland Security Enterprise. The targeted timeframe to create and display information on the COP is within 30 minutes of the Senior Watch Officer determining that an incident requires posting to the COP.
Scope of Data	This measure includes all Incident Reports and situational awareness products at the 'monitor' or higher incident level as determined by the Senior Watch Officer. The NOC Standard and Operating Procedures (SOP) promulgate the type of report and timeline requirements for incident reporting. Type of reportable events can include initial breaking, pre-planned, weather, and current reports updates. Incident reports are at the Monitored, Awareness, Guarded (Phase 1), Concern (Phase 2), or Urgent (Phase 3) level.
Data Source	Primary source for the required data is the Phase Notification Log which is an electronic database with controlled access on the DHS shared network drive.

	During an event, a designated desk position on the NOC Watch Team captures and manually enters the data into the database which provides the detailed report timing information.
Data Collection Methodology	The data for this measure will include the creation of an icon and summary on the DHS Common Operating Picture (COP) for all 'monitored' and higher level Homeland Security situations. The targeted timeframe for this measure starts when the Senior Watch Officer announces designation of an incident at the 'monitored' or higher level. The time stops when the incident has been added to the COP, thus informing the Homeland Security Enterprise. The Notification Log (monitored and higher) will be used to provide the times for this measure as it maintains a detailed incident timeline summary. The manually captured data is entered into the notification log for management review.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data is entered into the program as the incident/event is being reported. Data in the system is reviewed by the Knowledge Management Officer desk supervisor and Operations Officer to ensure standardization is maintained.

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

Science and Technology Directorate

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

	submitted by program/project managers with the approval of ST leadership to the ST Performance Team.
Reliability Index	Reliable
Explanation of Data Reliability Check	ST leadership supervising program/project managers reviews the data submitted by program/project managers to ensure accuracy and consistency then verifies the status and explanation of milestones (specifically planned transitions) prior to submitting the data to the ST Performance Team. The ST Performance Team provides a third data reliability review before results are finalized and submitted to DHS.

Transportation Security Administration

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

Explanation of Data Reliability Check	Data is auto generated from the Redress Management System. For the quarterly submission, Redress program specialists review the data to ensure the report is pulling from the correct fields, that the date range is correct for the reporting quarter, and that the formula is properly formatted to calculate the average. The redress process itself include data quality assurance steps at multiple points to ensure data is input properly, that cases are assigned to components properly, and that cases are closed out properly. The Director and Operations Manager review daily reports to ensure the data is complete and accurate. These reports include the given measure along with other measures/indicators that assist with corroboration.

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

Performance Measure	Percent of attended interchanges of rail cars containing rail security sensitive materials transiting into or through high-threat urban areas

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

Performance Measure	Percent of canine teams that pass Operational Training Assessments within 90 days of completing basic course at the Canine Training Center
Program	Aviation Screening Operations
Description	This measure gauges the percent of canine teams that pass the Operational Training Assessment (OTA) within 90 days of graduating from the Canine Training Center's (CTC) basic course. The CTC trains canine 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 program trains two types of teams: passenger screening canines (PSC) and explosive detection canines (EDC). Basic training for both occurs at the CTC followed by additional transition training at their respective duty locations. An OTA takes place approximately 30 to 40 days after canine teams complete transition training. Once a team passes the OTA, they are allowed to begin working in operational areas. The overall pass rate on OTAs for PSC and EDC teams serves as an indicator of the CTC's training program success.
Scope of Data	The scope of this measure includes both PSC and EDC teams that have completed both the basic training at the CTC and the transition training at their duty locations. Completion of the basic training at CTC is a pre-requisite to additional training conducted at duty locations. PSC teams serve as an added layer of security at passenger checkpoints while EDC teams provide explosive detection

	capabilities at all modes of transportation in partnership with federal, state, and local law enforcement. A canine team is considered operational once it passes the OTA. Data used for this measure include all OTA results available within the fiscal year. PSC and EDC teams are weighted equally.
Data Source	This measure gathers data from OTAs conducted by Regional Canine Training Instructors (RCTI) and CTC Canine Training Instructors approximately 30-40 days after the team returns to their duty location. Data is stored in an asset management system and Canine Web Site that are owned by Security Operations' (SO) Threat Assessment Division (TAD).
Data Collection Methodology	RCTIs and CTC Canine Training Instructors conduct OTAs approximately 30-40 days after the canine team completes transition training at their duty locations. Once the OTA is complete, instructors upload the results (pass/fail) to the Canine Web Site and run a national report on canine team performance. The measure result calculated is the number of assessed teams that pass OTA divided by the total number of assessed canine teams within 90 days of graduating the basic course at the CTC.
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 Operational Evaluations scheduled resulting from OTA failures. The CTC and Training Center Division leadership team will assess the report and performance on semi-annual basis to gage success.

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

	operation, and periodic reports on hourly expedited throughput are generated to gage efficiency of the operation. This information will be is calculated each quarter, with results being reported cumulatively.
Reliability Index	Reliable
Explanation of Data Reliability Check	PMIS data is required to be collected and entered each day for every screening lane in operation. Missing information is immediately flagged for follow-up with the specific airport. Data on individuals eligible for expedited screening from Secure Flight and the number of individuals who actually received expedited screening at the airport allows for daily reliability and accuracy checks. Data anomalies are quickly identified and reported back to the airport for resolution.

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

Performance Measure	Percent of identified vulnerabilities at last point of departure airports addressed through stakeholder engagement and partnerships
Program	Other Operations and Enforcement
Description	This measure gauges the percent of vulnerabilities at last point departure airports (LPD) identified and then discussed through stakeholder engagements and partnerships so as to encourage resolution. An LPD country is a country with at least one port providing direct traffic to a specific destination - usually a foreign airport with direct passenger and/or cargo flights to a U.S. destination airport. Inspectors conduct the security assessments at LPDs based on International Civil Aviation Organization (ICAO) standards and identify vulnerability gaps. The program also identifies vulnerabilities beyond the ICAO requirements through inspections but has limited authority to enforce mitigation activities. Through the identification of vulnerabilities, the sharing of findings

	and best practices, the program works to mitigate aviation security risks and have them addressed so as to reduce vulnerabilities at foreign LPD airports.
Scope of Data	The population is any vulnerabilities identified by TSA inspectors through assessments and inspections at foreign last point departure airports (LPD) within the reporting period. An assessment is an on-site review that determines whether aeronautical authorities effectively maintain and carry out security measures to support International Civil Aviation Organization standards. Inspections evaluate compliance of aircraft operators and foreign air carriers with TSA regulations beyond the international standards. The value are those vulnerabilities discussed through stakeholder engagements and partnerships and categorized as either closed or being addressed.
Data Source	The data source is the Global Risk Analysis and Decision Support (GRADS) Vulnerability Report. It contains data pertaining to all open and reported closed vulnerabilities at foreign LPD airports, and is maintained by International Operations (IO) within Security Operations (SO).
Data Collection Methodology	The program establishes the standards for assessments and inspections based on International Civil Aviation Organization standards and TSA regulations. Inspectors then conduct on-site assessments and inspections to identify vulnerabilities which are then entered into GRADs. Once a vulnerability is identified and added into GRADS, IO tracks status updates provided by a variety of program staff who regularly engage with stakeholders. Twice a year, IO runs a report and validates that all identified vulnerabilities, both open and reported closed, have a clear description, root cause, and mitigation actions taken to address the specific vulnerability. The measure result calculated is the total number of closed and open vulnerabilities with a corrective action plan or other mitigation strategies divided by the total number of identified vulnerabilities at LPD airports within the reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	As part of the Foreign Airport Assessment Program Standard Operating Procedures process, Global Operations personnel are required to enter and review every identified vulnerability in the GRADS system. Once the vulnerability has been added into the GRADS system, the Vulnerability Approver in GRADS must approve all vulnerabilities submitted. If the data is incomplete, the Vulnerability Approver must reject the vulnerability and provide comments to justify the rejection in GRADS. In addition, Desk Officers and Program Analysts are responsible for conducting validation reports and quality control reports for Global Operations senior leadership to track all identified vulnerabilities and their closure.

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

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

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

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

	ongoing training sessions to improve the quality and consistency of the data and data collection process. Final results for this measure are reviewed by headquarters staff prior to submission.

Performance Measure	Percent of passenger data submissions that successfully undergo Secure Flight watch list matching
Program	Aviation Screening Operations
Description	This measure will report the percent of qualified message submissions received from the airlines that are successfully matched by the Secure Flight automated vetting system against the existing high risk watch lists. A qualified message submission from the airlines contains passenger data sufficient to allow successful processing in the Secure Flight automated vetting system. Vetting individuals against high risk watch lists strengthens the security of the transportation system.
Scope of Data	This measure relates to all covered flights operated by U.S. aircraft operators that are required to have a full program under 49 CFR 1544.101(a), 4. These aircraft operators generally are the passenger airlines that offer scheduled and public charter flights from commercial airports.
Data Source	The data source is SLA_RAW_DATA table from the Service Level Agreement (SLA) database.
Data Collection Methodology	Ad-hoc reports will be created in the Reports Management System to pull both the number of Boarding Pass Printed Results and the number of unique qualified data submissions received from U.S. and foreign aircraft operators out of the SLA database for a specified date range. These numbers will be compared to ensure 100% of the qualified data submissions are vetted using the Secure Flight automated vetting system.
Reliability Index	Reliable
Explanation of Data Reliability Check	Vetting analysts review a report (produced daily) by the Secure Flight Reports Management System. An analyst then forwards the data to Secure Flight leadership for review. Once reviewed, reports are forwarded to the TSA Office of Intelligence and Analysis management, TSA senior leadership team (SLT), as well as the DHS SLT. It is also distributed to the TSA Office of Security Policy and Industry Engagement, and the TSA Office of Global Strategies.

Performance Measure	Percent of Transportation Security Officers that achieve a first-time pass rate on the Image Interpretation Test
Program	Aviation Screening Operations
Description	This measure gauges the ability of Transportation Security Officers (TSO) to identify prohibited items such as guns, knives, and improvised explosive devices through X-ray screening. The Image Interpretation Test is a pass/fail test conducted in a simulated classroom environment that mimics X-ray screening of carry-on baggage at passenger checkpoints. Image interpretation is a key learning objective of TSO-Basic Training Program and a skill required for TSOs to successful. The measure serves as an indicator of the degree to which the training transfers to individual students, preparing TSOs to safeguard the aviation transportation system.
Scope of Data	The population for this measure reflects all students that undergo TSO-Basic Training Program (TSO-BTP) and take the Image Interpretation Test (IIT) within the designated timeframe. The value are those who passed on the first test experience at the required detection level.
Data Source	This measure gathers data from the Online Learning Center (OLC), which serves as the system of record for TSO-BTP test results.

Data Collection Methodology	After completing the TSO-BTP training at the TSA academy, a training simulator is used to deliver the IIT and results are recorded in the OLC automatically. It is a pass/fail test and serves as an indicator that the student is ready to move to the on-the-job training phase. A passing score consists of two elements: 70% detection rate and no more than a 50% false alarm rate. A member of the OLC team generates ad hoc Item Status Reports using qualifiers to identify which students passed the IIT. In the case of an OLC to IIT data load failure for a student, a Tier 2 OLC Administrator attempts to reload the test for a student. If this fails, the staff may take the IIT on a stand-alone device and the Administrator will record the score into OLC manually. The measure result calculated is total number of students that passed the IIT on their first attempt divided by the total number of students who took the IIT within the measurement period.
Reliability Index	Reliable
Explanation of Data Reliability Check	Once the Item Status Report is generated by a member of the OLC team the IIT data is validated by staff at the TSA Academy and also by program staff at headquarters. The TSA Academy Operations Team checks the IIT data to identify and correct any recording errors in OLC. The TSA Academy Registrar verifies the student scores recorded against a course 'Completion Report' for TSO-BTP to verify that a score was collected for each student on the first attempt. The confirmation of the Pass/Fail status by the TSA Academy staff provides the data integrity to conduct reporting of IIT First time pass rates. The headquarters staff also validate the data by comparing the numbers against training plans.

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

U.S. Citizenship and Immigration Services

Performance Measure	Percent of appealed decisions that are dismissed by the Administrative Appeals Office (Retired Measure)
Program	Immigration Services
Description	This measure gauges the percent of Form I-290B, Notice of Appeal or Motion appeals dismissed by the Administrative Appeals Office (AAO) for all immigration forms. The Administrative Appeals Office has jurisdiction to review all immigration cases regarding law and regulation interpretations, except the I-130 and I-129 cases which fall under the jurisdiction of the Board of Immigration Appeals. Decisions not overturned by the AAO validate the accuracy of the adjudicative decisions.
Scope of Data	The scope of this measure includes adjudicative decisions dismissed by the AAO, among all final appeal decisions from I-290B cases recorded in CLAIMS3, CLAIMS4, and ELIS. The population includes all Form I-290B appeal cases with a final appeal decision by the AAO during the reporting period. Motions are excluded from the calculation, as well as appeals filed in different adjudicative forums. Forms appealable under the AAO by filing Form I-290B include: I-129CW; I-129F; I-129 H-1B, H-2, H-3, L, O, P, Q, R; I-131 Re-entry Permit and Refugee Travel Document; I-140; I-212; I-360 (excluding Widow(ers)); I-485 Indochinese, U & T Visas, Section 13, Life Act; I-526; I-601; I-612; I-821; I-914; I-914A; I-918; I-918A; I-929; N-565; N-600; N-600K. Notice of Appeal or Motion decisions may occur in a different quarter or fiscal year than the appeal's date of receipt, but are only counted for the purposes of this measure at the time of the decision.
Data Source	Data will be drawn from the Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR) warehouse that can access applications and petitions adjudicated in Computer Linked Adjudication Information Management System (CLAIMS 3), Computer Linked Adjudication Information Management System (CLAIMS 4), Electronic Immigration System (ELIS).
Data Collection Methodology	The Adjudicative Appeals Office populates the appeal decision in CLAIMS 3, CLAIMS 4 or ELIS by checking an indicator flag in the relevant system. The USCIS Office of Performance and Quality (OPQ) exports data from eCISCOR via SAS statistical analysis software program a week following the end of the quarter to ensure all decisions/actions taken place have been updated. The measure is calculated as the Number of Form I-290B - Notice of Appeal or Motion appeals that are dismissed by an AAO divided by the Total Number of Form I-290B Appeals (approvals + denials) for all form types and classifications that occurred during the reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data will be provided a 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 and outcome measure to ensure completeness, reliability and accuracy. Before submitting results to the program's Office of the Chief Financial Officer (OCFO), an OPQ manager will conduct a final quality check of the performance measure data. OCFO completes subsequent checks of the data during each reporting period, prior to an internal review meeting and before posting data to the Future Years Homeland Security Program System (FYHSP).

Performance Measure	Percent of approved applications for naturalization that were appropriately decided
Program	Immigration Services
Description	This measure assesses the validity of final decisions by program adjudicators to approve all electronic N-400 Naturalization Forms received through USCIS Electronic Immigration System (ELIS) by reporting the findings of regular quality reviews of these decisions by experienced subject matter experts (SMEs). The program conducts quality reviews by drawing a statistically valid random sample of approved N-400s on a quarterly basis. Insuring that the program provides immigration services accurately and with full documentary support through quality reviews identifies opportunities to improve training and business processes and enhances confidence in the legal immigration system.
Scope of Data	The scope of this measure includes all approved and oathed (sworn and signed) electronic N-400 Forms received through USCIS Electronic Immigration System (ELIS). The program conducts quality reviews of these cases, drawing a statistically valid random sample of approved N-400s on a quarterly basis. For a typical quarterly total of roughly 171,600 N-400s, the program constructs a sample of roughly 139 files, which provides accuracy with a ±5% margin of error. Quarterly reviews draw on approvals completed in the preceding quarter. Year-end results from a stratified sample, with each quarterly review providing one stratum of data.
Data Source	After creation of a quality review sample, teams of SMEs review records for each of the approved N-400s selected to complete Decisional Quality Review (DQR) checklists, with data entered into an online database. Program headquarters staff in the Office of Performance and Quality, Office of the Chief Data Officer, Data Quality Branch has access to this database. These HQ staff members maintain the information from each review and integrate it into a consolidated spreadsheet, which serves as the data source for this measure.
Data Collection Methodology	SMEs use original applicant requests to complete their quality reviews of the sample of approved N-400s, documenting their work using DQR checklists. A SME sets aside cases when the SME determines that documentation does not support the original adjudication. After the SME has reviewed all files, at least two other SMEs review flagged applications. If any of the additional reviewers question a decision, that file goes back to the original adjudicating office to resolve discrepancies. The original office must submit to a SharePoint site documented resolution of discrepancies within 10 business days. The result is calculated by dividing the number of files returned to original offices by the review's sample size, subtracting this quantity from 1 and multiplying by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	Layers of subject matter experts review and concur on correct or questionable decisions to ensure data reliability. The program obtains a valid random sample to conduct this audit, compile results, and develop corrective action plans to address any deficiencies noted.

Performance Measure	Percent of approved applications for permanent residence that were appropriately decided
Program	Immigration Services
Description	This measure assesses the validity of final decisions by program adjudicators to approve Form I-485 applications to register for permanent residence or to adjust status by reporting the findings of regular quality reviews of these decisions by experienced subject matter experts (SMEs). The program conducts quality reviews of these cases, drawing a statistically valid random sample of approved I-485s on a quarterly basis. Insuring that the program provides immigration

	services accurately and with full documentary support through quality reviews identifies opportunities to improve training and business processes and enhances confidence in the legal immigration system.
Scope of Data	The scope of this measure includes all I-485 Forms approved nationwide and received at the program's National Records Center. To validate the I-485, the program conducts quality reviews of such cases, drawing a statistically valid random sample of approved I-485s on a quarterly basis. For a typical quarterly total of roughly 103,600 I-485s, the program constructs a sample of roughly 139 files, which provides accuracy with a ±5% margin of error. Quarterly reviews draw on approvals completed in the preceding quarter. Year-end performance results from a stratified sample, with each quarterly review providing one stratum of data.
Data Source	After creation of a quality review sample, teams of SMEs review records for each of the approved I-485s selected to complete Decisional Quality Review (DQR) checklists, with data entered into an online database. Program headquarters staff in the Office of Performance and Quality, Office of the Chief Data Officer, Data Quality Branch has access to this database. These HQ staff members maintain the information from each review and integrate it into a consolidated spreadsheet, which serves as the data source for this measure.
Data Collection Methodology	SMEs use original applicant requests to complete their quality reviews of the sample of approved I-485s, documenting their work using DQR checklists. A SME sets aside cases when the SME determines that documentation does not support the original adjudication. After the SME has reviewed all files, at least two other SMEs review flagged applications. If any of the additional reviewers question a decision, that file goes back to the original adjudicating office to resolve discrepancies. The original office must submit to a SharePoint site documented resolution of discrepancies within 10 business days. The result is calculated by dividing the number of files returned to original offices by the review's sample size, subtracting this quantity from 1 and multiplying by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	Layers of subject matter experts review and concur on correct or questionable decisions to ensure data reliability. USCIS is able to obtain a valid random sample to conduct this audit, compile results, and develop corrective action plans to address noted deficiencies.

Performance Measure	Percent of approved refugee and asylum applications that were appropriately decided
Program	Immigration Services
Description	This measure assesses the ability of officers to process Form I-589 and Form I-590 refugee and asylum applications in a fully supportable and accurate manner. A panel of subject matter experts are convened to review a sample of approved applications to determine whether the final decision was appropriately supported and legally sufficient. The panel may sustain the decision to grant asylum, recommend denial, or send the file back to the appropriate field office for correction or more information if it is determined that procedures were not correctly followed, or the case is lacking sufficient interview evidence. This measure helps ascertain the accuracy of decisions and to improve the training and processes used in conducting asylum and refugee adjudications.
Scope of Data	The scope of this measure includes those Forms I-589 and I-590 which met legal sufficiency and evidence criteria among all Forms I-589 and I-590 sampled by the program to determine the accuracy rate. Cases varying from standard asylum or refugee adjudications due to adherence to a different set of legal, procedural, or administrative guidelines, as well as cases requiring urgent travel or lacking

	supervisory review are excluded. The confidence level for each review (90% to 95%) is set to accommodate the underlying purpose and resource requirements of each review at the given time. The sample size of total cases reviewed is the denominator for the calculation.
Data Source	Application and screening decision data are recorded and stored in RAIO case management systems, e.g. Global and CAMINO. Decisional review check sheets completed by decision reviewers are consolidated in a database. The RAIO Performance Management and Planning Program owns the final reporting database.
Data Collection Methodology	A team of subject matter experts conducts reviews of a sample of the asylum and refugee decisions, and documents these reviews using a checklist. The review team uses consensus panels, two-tiered review, or limited two-tiered review with discussion groups to analyze the appropriateness of decisions. Cases found to be inappropriately decided are returned the responsible field office for correction. Reviews are made periodically throughout the year using a sample size to reach a confidence level of 90% to 95% and the annual result is determined by aggregating these samples as the final annual sample for that year. The percentage is calculated by dividing the number of approved cases in the sample that do not require correction by changing the decision outcome by the total number of approved cases in the sample.
Reliability Index	Reliable
Explanation of Data Reliability Check	To ensure accuracy of the checklist and panel decision, multiple layers of subject matter experts review and concur on correcting applications by changing decisions to approve. The results are double-checked by supervisors before the results are submitted to Office of the Chief Financial Officer for submission. OCFO completes subsequent checks of the data during each reporting period, prior to an internal review meeting and before posting data to the Future Years Homeland Security Program System (FYHSP).

Performance Measure	Percent of fraud referrals from adjudicative directorates that are closed or converted into fraud cases within 90 calendar days
Program	Fraud Prevention and Detection
Description	This measure gauges the percent of referrals received from adjudicative officers to the Fraud Detection and National Security (FDNS) Directorate that are resolved within 90 days. Adjudication Officers may contact FDNS if they suspect fraudulent activity related to the adjudication of immigration benefits. Fraud referrals that are either declined or administratively returned to adjudications, closed as leads, converted into cases, or linked to existing cases within the time limit of the referral are included in this measure. Performance is measured as the percentage of. Referrals pending with FDNS greater than the time limit will be counted as not meeting the measurement. Ensuring prompt resolution of fraud concerns helps to safeguard the integrity of the nation's lawful immigration system while fostering timely and accurate adjudication of applications.
Scope of Data	This measure's scope includes all fraud referrals closed or converted from adjudication offices from Field Operations (FOD), Service Center Operations (SCOPS), and Refugee, Asylum, and International Operations (RAIO) Directorates, respectively, entered into the Fraud Detection and National Security Data System (FDNS-DS) or CLAIMS 3. Those referrals declined and returned to the adjudication office; determined to have no basis for continuing the investigation; or determined to involve a reasonable suspicion of fraud exists and converted into an active fraud case are included in the numerator. All active referrals from the above offices. make up the denominator A case record with a "Resolved" flag in the FDNS-DS database or a "Resolved" HAC code in CLAIMS 3 identifies cases

	closed or converted. This measure does not include system generated fraud referrals or "hits" from law enforcement databases.
Data Source	Adjudicative referral dates, referral declination and administrative return dates, lead closure dates, and case linkage and conversion dates for referrals from FOD and RAIO are derived from the Fraud Detection and National Security Directorate's system of record, FDNS-DS. Adjudicative referral dates, referral rejection dates, lead closure dates, and case linkage and conversion dates for referrals from SCOPS are derived from CLAIMS 3.
Data Collection Methodology	All fraud referrals "resolved" in the current fiscal year are included. The adjudicative referral date is subtracted from the date of the resolution to derive the total number of days. Adjudication Officers (AOs) vet potential fraud issues with their Supervisors. When supervisors concur with AOs with regard to creating a referral to FDNS, AOs enter a referral in FDNS-DS or CLAIMS3. Subsequently, FDNS officers enter the status of resolved cases in FDNS-DS or update the CLAIMS3 HAC code corresponding to resolution in CLAIMS3. FDNS Statisticians conduct a query from FDNS-DS and CLAIMS3 using SAS a statistical analysis software package, to extract data on all referrals closed or converted during the reporting period. SAS is also used to calculate the duration in working days of the time to close or convert referrals. The number of all referrals resolved within 90 days is the numerator and the total number of all referrals resolved for the reporting period is the denominator.
Reliability Index	Reliable
Explanation of Data Reliability Check	FDNS-DS supervisors review the SAS query results to ensure that records to ensure that they contained correct information at the time of closure. Analysts in The Office of the Chief Financial Officer checks performance results for internal leadership reviews and before posting data to the DHS Performance System.

Performance Measure	Percent of Immigration Officers who are trained to perform their duties within six months of entry on duty (New Measure)
Program	Immigration Services
Description	This measure includes Immigration Services Officers who complete BASIC training. BASIC training is typically held at residential training facility. At the completion of their required BASIC training, officers are then considered certified to performance their duties. Ensuring officers are adequately trained and certified before performing their job duties protects the integrity of the immigration system.
Scope of Data	The population included in this measure are all newly hired Immigration Officers in the fiscal year. The value for this measure is those officers who have completed the required BASIC training. Officers who are deferred attendance due to deferments allowed under published USCIS policy, as well as students that fail to achieve a passing grade, or withdraw will be excluded from the results.
Data Source	The data sources for training attendance records include the Basic Training Dashboard Summary spreadsheet. The Table of Organization Position System (TOPS) managed by the Human Capital Directorate will provide the data to the Entry on Duty (EOD) date and the current date.
Data Collection Methodology	The registrar will begin the data collection process by downloading appropriate quarters data from the BASIC Dashboard. The dashboard houses an automated excel formula that computes the individual EOD to basic times and number of attendees. Then all EOD to BASIC completion times equal to or less than six months are counted, which make up the numerator. The total numerator is then divided by the number of officers scheduled to attend BASIC. The results are added each quarter for a cumulative result.
Reliability Index	Reliable

Explanation of Data Reliability Check	USCIS HCT is responsible for validating the accuracy of the completed training reports, and the calculations made regarding how many Officers met their training requirements within six months. They also confirm that the list of Officers is accurate and those who are on deferred attendance, or failed the course, have not been included in the numbers. The Office of the Chief Financial Officer checks performance results for internal leadership review meetings and before posting data to the DHS Performance System.

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

	Training Report. The consolidated PALMS and Directorate training is the numerator and the TOPS query provides the denominator for this measure.
Reliability Index	Reliable
Explanation of Data Reliability Check	Supervisory HR Analysts validate exclusion of data for basic fraud and interviewing courses prior to submitting the Report to the Office of the Chief Financial Officer (OCFO). OCFO completes subsequent checks of the data during each reporting period, prior to an internal review meeting and before posting data to the Future Years Homeland Security Program System (FYHSP).

Performance Measure	Percent of Immigration, Fraud, and Asylum and Refugee Officers who are trained to perform their duties within six months of entry on duty (Retired Measure)
Program	Immigration Services
Description	This measure reports the percent of officers from three critical functions who have completed the training they need to perform their job duties. This measure includes Immigration Services Officers who complete BASIC training or the equivalent, Immigration Officers who complete Fraud Detection Officer Basic Training, and Refuge Asylum Officers and Refugee Officers who complete Refugee, Asylum, and International Operations (RAIO) combined training or the equivalent. Each directorate has separate requirements for certifying their respective officers' eligibility to perform their job duties. At the completion of their required training(s), officers are then considered certified to performance their duties. Ensuring officers are adequately trained and certified before performing their job duties protects the integrity of the immigration system.
Scope of Data	The population included in this measure are all newly hired Officers in the fiscal year who will perform immigration, fraud, or refuge and asylum duties. The value for this measure are those officers who have completed the required training for their function. Officers who are deferred attendance due to deferments allowed under published USCIS policy, as well as students that fail to achieve a passing grade, or withdraw will be excluded from the results.
Data Source	The data sources for training attendance records include the Basic Training Dashboard Summary spreadsheet, Performance and Learning Management System (PALMS) Fraud training spreadsheet, and RAIO Training Database for RAIO Combined Training (or equivalent). The Table of Organization Position System (TOPS) managed by the Human Capital Directorate will provide the data to the Entry on Duty (EOD) date and the current date.
Data Collection Methodology	Directorates provide data on total number of eligible Officers needing training whose six-month window expires by the end of the quarter and number completing all required training in six months minus deferrals and failures from both. The first calculation is the time between EOD and when Officers completed all required training(s). The second calculation is the number completing their training requirements in six months divided by the total number of eligible individuals needing training. The Registrar downloads a Basic Dashboard report that computes the individual EOD to basic times and number of attendees. Fraud Training data is from a PALMS Excel extract compared to the EOD from TOPS. Asylum/Refugee training data is from the Human Resource report on number and EOD of Asylum/Refugee Officers compared to training completion records. HCT consolidates data from BASIC, FDNS, RAIO, then divides the total numerator of three courses by the denominator of three courses for overall percent.
Reliability Index	Reliable
Explanation of Data Reliability Check	Supervisors within each Directorate are responsible for validating the accuracy of the completed training reports, and the calculations made regarding how many Officers met their training requirements within six months. They also confirm that the list of Officers is accurate and those who are on deferred attendance, or

	failed the course, have not been included in the numbers. These checks will occur before Directorates submits the total number of Officers to be trained, and the number who completed all required training within six months, to the Human Capital division for the roll-up calculation. The Human Capital division will double-check the data received from each of the three Directorates, based on trends from previous reports, to ensure the numbers are valid. The Office of the Chief Financial Officer checks performance results for internal leadership review meetings and before posting data to the Future Years Homeland Security Program System (FYHSP).

Performance Measure	Percent of naturalization cases where derogatory information was identified and resolved prior to taking the oath of allegiance
Program	Immigration Services
Description	This measure gauges the rate at which derogatory information is identified and resolved before N-400 Form naturalization applicants take the final the Oath of Allegiance at a naturalization ceremony. Taking the oath at a ceremony completes the process of becoming a U.S. citizen for approved applicants. USCIS employs continual vetting of applicants and a final check for derogatory information close to the oathing ceremony to ensure that ineligible applicants are not naturalized due to criminal activity, national security, or public safety concerns. Continuous vetting ensures the integrity of the immigration system and protects our national security.
Scope of Data	The scope of the measure includes cases that have been 'oathed' (sworn and signed) with derogatory information identified and resolved out of the population of all N-400 Forms/cases received through USCIS' Electronic Immigration System (ELIS) with an indication of identified derogatory information. N-400 cases with no derogatory information are excluded from the calculation of this measure.
Data Source	ELIS is the system that contains all records of N-400 cases with derogatory information identified and resolved. Derogatory information is identified in ELIS by a Derogatory Information and Resolved flags. The Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR) business intelligence tool is used to extract the data for N-400 cases oathed with a derogatory information flag identified in ELIS.
Data Collection Methodology	Derogatory information identified by adjudicators or the Fraud Detection and National Security Directorate is entered in ELIS by checking a flag. Adjudicators record the resolution of this information checking a resolved flag in the ELIS system before scheduling an oathing ceremony. The USCIS Office of Performance and Quality (OPQ) will export data from eCISCOR via SAS statistical analysis software program a week following the end of the quarter to ensure all N-400 cases oathed during the reporting period with a derogatory information flag are included in the calculation. The calculation is the number of cases where derogatory information was resolved before the oathing ceremony divided by the total number of cases where there was derogatory information identified before or after oathing. Data is calculated from the beginning of the fiscal year until the end of the reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	After the results have been generated, a second OPQ data analyst will conduct a peer-review of the data to ensure completeness, reliability and accuracy. Prior to submission of the final results to OCFO, an Office of Performance and Quality manager will conduct a final quality check of the data. The Report is subsequently checked by the Office of the Chief Financial Officer during each

	reporting period prior to an internal review meeting and before posting data to the Future Years Homeland Security Program System (FYHSP).

Performance Measure	Percent of system generated notifications related to national security, public safety, or fraud triaged within 60 calendar days
Program	Fraud Prevention and Detection
Description	This measure gauges the timely resolution of notifications sent regarding system generated notifications related to national security, public safety, or fraud for immigration benefits before a final decision to approve or deny is rendered. System generated notifications provide continuous vetting capabilities to alert Fraud analysts to investigate potential issues of concern. Analysts may resolve the notification by determining that there is no basis for continuing the investigation or that a reasonable suspicion exists which warrants the opening of a fraud case in the Fraud Detection and National Security Data System (FDNS-DS). Continuous vetting of information helps safeguard the integrity of the nation's lawful immigration system.
Scope of Data	This measure's scope includes system generated notifications (SGNs) in cases pending a decision to approve or deny immigration benefits that are triaged within 60 calendar days during the fiscal year. Scope excludes cases linked to applications approved, denied, or withdrawn before creation of an SGN , and includes all benefit forms except SGNs that pertain to a form type of I-589 (Application for Asylum and for Withholding of Removal) or I-590 (Registration for Classification as Refugee) or forms received in a Refugee, Asylum, and International Operations (RAIO) location.
Data Source	Fraud Detection and National Security (FDNS) Reports and Analysis Branch (RAB) uses the SAS system to extract data from FDNS-DS, FDNS' system of record, to report the data. The system generated notices (SGNs) originate from ATLAS, a screening functionality incorporated into FDNS-DS. Records of SGNs reside in a different segment of FDNS-DS. Analysts may identify resolved SGNs in FDNS-DS by searching for records with active identifier flags. Information available in FDNS-DS includes each SGN; the status--pending or complete--of all benefits decisions linked to each SGN; and time stamps for the receipt and disposition of each SGN.
Data Collection Methodology	System generated biometric notifications (SGNs) issued from law enforcement databases require Immigration Officers to record their actions in FDNS-DS. FDNS Statisticians use SAS to conduct a query from FDNS-DS on the date of all SGNs during the reporting period and the date of their resolution. Staff compile reports using SAS--a statistical analysis software package--to extract data from FDNS-DS for all SGNs resolved during the reporting period. Staff use SAS to calculate duration, in working days, of the period from receipt of each SGN to its disposition by FDNS. The number of all in-scope SGNs triaged within 60 or fewer calendar days for disposition in a given reporting period provides the numerator. The total number of all relevant SGNs in a given reporting period is the denominator. The percentage of these two quantities is the result for the reporting period and is cumulative throughout the fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	The programs used to calculate the measures are quality checked before implementation by an independent FDNS RAB staff member or contractor. Additionally, as end users also monitor the data, they are likely to identify any potential data issues that can be corrected as they arise, if necessary. Additionally, supervisors in FDNS review the data to ensure exclusion of post-adjudicative forms from this measure's data. The Office of the Chief Financial

	Officer checks results per reporting period for internal leadership review meetings and before posting data to the DHS Performance System.

Performance Measure	Percent of time U.S. Citizenship and Immigration Services responds within four calendar days to U.S. Customs and Border Protection screening requests under the Migrant Protection Protocols (Retired Measure)
Program	Immigration Services
Description	This measure gauges the timeliness of processing of U.S. Customs and Border Protection (CBP) requests for screening under the Migrant Protection Protocols (MPP). The MPP apply when certain foreign individuals entering or seeking admission to the U.S. from Mexico illegally or without proper documentation may be returned to Mexico and wait outside of the U.S. for the duration of their immigration proceedings, where Mexico provides all appropriate humanitarian protections for their stay. CBP requests assistance from USCIS to assess noncitizens who claim a fear of return to Mexico at any point during apprehension, processing, or related proceedings. Unaccompanied noncitizen children, those in expedited removal proceedings, and individuals from vulnerable populations on a case-by-case basis are not subject to MPP. Determining valid claims on a timely basis helps restore a safe and orderly immigration process while ensuring that vulnerable populations receive the protections they need.
Scope of Data	This measure includes all Migrant Protection Protocol Screening Requests received from CBP that are entered into the Global case management system as identified with a unique identifier (MPP flag). Requests in the case management system are 'closed' either by an administrative close or negative or affirmative decision of fear of return to Mexico. MPP requests processed within four days are the numerator for this measure and the total number of MPP requests are the denominator. Unaccompanied noncitizen children, thiose in expedited removal proceedings, and individuals from vulnerable populations on a case-by-case basis are not subject to MPP and are excluded from the calculation.
Data Source	The program uses the Global case management system to record and store the data, and uses the Electronic Immigration System's Standard Measurement and Analysis Reporting Tool (SMART) environment to report the data for this measure. The data is queried from SMART using the MPP identifier and saved in the Migrant Protocol Protection report. The Refugee Asylum and International Operations (RAIO) Division owns the final reporting database for this measure.
Data Collection Methodology	Asylum Division personnel enter a request received from CBP for MPP screening into the Global system. An Asylum officer interviews the noncitizen onsite at a processing center or remotely and makes a decision that is reflected as a 'completed' case in the Global system. The Asylum Division calculates the measure using data collected from Global by dividing the cumulative total number of MPP completions reached within 4 calendar days by the cumulative total number of MPP referrals from CBP to USCIS for each reporting period.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data reliability checks consist of the use of standard operating procedures, supervisory controls, and quality reviews and analysis. Supervisors in RAIO conduct a check of the data for accuracy before reporting to the program's Office of the Chief of Financial Officer (OCFO). OCFO completes subsequent checks of the data during each reporting period, prior to an internal review meeting and before posting data to the Future Years Homeland Security Program System (FYHSP).

Performance Measure	Percent of workers determined to be Employment Authorized after an initial mismatch
Program	Employment Status Verification
Description	This measure reports the number of cases in which adjudicating officials in the E-Verify program find a person employment authorized under U.S. law after the program issued the person under examination with a Tentative Non-Confirmation (TNC) of eligibility for employment, and the person in question contested this initial mismatch. In cases when an employee contests an eligibility determination, the program's Legal Instrument Examiners (LIEs) make a final determination of the employee's eligibility for employment and transmits the determination both to the hiring employer and to VIS. Ensuring the accuracy of E-Verify program processing reflects the program's intent to minimize negative impacts imposed upon those entitled to employment in the U.S. while ensuring the integrity of immigration benefits by effectively detecting and preventing cases of unauthorized employment.
Scope of Data	The population of this measure includes all E-Verify cases during the reporting period in which a Tentative Non- Confirmation (i.e. 'initial mismatch') is identified. The scope of the results includes E-Verify cases in which actions following a Tentative Non-Confirmation (i.e. 'initial mismatch') result in a finding of 'Employment Authorized' for the person in question. Tentative Non-Confirmations that result in a finding of 'Not Employment Authorized' are excluded from the calculation.
Data Source	Data for this measure come from records stored in the program's Verification Information System (VIS). This system contains detailed, searchable information regarding all steps taken in resolving E-Verify cases, including whether the program issued a TNC, whether the employee contested the TNC, and the final eligibility determination.
Data Collection Methodology	In cases when an employee contests an eligibility determination, the program's Legal Instrument Examiners (LIEs) make final determination of the employee's eligibility for employment. Upon completing a final determination of eligibility, an LIE transmits the determination both to the hiring employer and to VIS. The program has configured VIS to produce a standard quarterly summary of case outcomes, which includes both the number of Tentative Non-Confirmations, and the subset of contested Tentative Non-Confirmations which produce a final finding of 'Employment Authorized.' The result is calculated by dividing the number of all Tentative Non-Confirmations which produce a final finding of 'Employment Authorized' by the all total number of all E-Verify cases for the reporting period as the denominator, and multiplying by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	Each quarter, the contractor managing VIS for the program extracts E-Verify transaction data from VIS. Analysts apply an algorithm to the extracted data, removing all duplicate and invalid queries. The contractor then refers data and performance results to program staff for review and clearance.

U.S. Coast Guard

Performance Measure	Availability of maritime navigation aids
Program	Maritime Transportation System Management
Description	This measure indicates the hours that short-range federal Aids to Navigation are available. The aid availability rate is based on an international measurement standard established by the International Association of Marine Aids to

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

Performance Measure	Fishing regulation compliance rate
Program	Maritime Law Enforcement
Description	This measure gauges the percent of all fishing vessels boarded and inspected at sea by the U.S. Coast Guard, which had no documented violations of domestic fisheries regulations. The U.S. Coast Guard boards and inspects U.S. commercial and recreational fishing vessels in the waters of the United States; U.S. commercial and recreational fishing vessels in the U.S. Exclusive Economic Zone (EEZ); and U.S. commercial and recreational fishing vessels outside the U.S. EEZ. Compliance to fishing regulations impact the health and well-being of U.S. fisheries and marine protected species.
Scope of Data	The population includes all boardings and inspections of U.S. commercial and recreational fishing vessels in the waters of the United States; U.S. commercial and recreational fishing vessels in the U.S. Exclusive Economic Zone (EEZ); and U.S. commercial and recreational fishing vessels outside the U.S. EEZ. The U.S. does not permit foreign vessels to fish within the U.S. EEZ. Vessels without any documented violations are reported for this measure.
Data Source	Boardings and violations of domestic fisheries regulations are documented by U.S. Coast Guard Boarding Forms and entered into the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database. The MISLE database has a specific LMR Violation Action box to facilitate identifying, sorting, and filtering vessels with violations.
Data Collection Methodology	U.S. Coast Guard units document violations of domestic fisheries regulations in U.S. Coast Guard Boarding Forms and enter them into the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database after completion of fisheries enforcement boardings. The data is extracted by a manual query in MISLE conducted by Coast Guard headquarters staff in the Office of Maritime Law Enforcement. The calculated results for a given year are

	the number of boarded fishing vessels with no documented violations of domestic fisheries regulations divided by the number of fishing vessels boarded and inspected at sea by the U.S. Coast Guard, multiplied by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	MISLE data consistency and integrity is controlled through program logic and pull-down menus that require key elements, prohibit the inappropriate, and limit choices to pre-determined options. Reliability is further ensured by comprehensive training and user guides, and the application itself has embedded Help screens. District, Area and Headquarters staffs review, validate and assess the data on a quarterly basis as part of the U.S. Coast Guard's Standard Operational Planning Process; and Program managers review and compare MISLE data to after-action reports, message traffic and other sources of information.

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

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

Performance Measure	Number of breaches at high-risk maritime facilities
Program	Maritime Prevention
Description	This measure reports the number of security breaches at facilities subject to the Maritime Transportation Security Act (MTSA) where no Transportation Security Incident has occurred, but established security measures have been circumvented, eluded or violated. MTSA facilities are a high-risk subset of the national waterfront facility population given the nature of their activities and/or the products they handle. As such, they pose a greater risk for significant loss of life, environmental damage, or economic disruption if attacked. MTSA regulated facilities constitute more than 3,400 high-risk subset of all waterfront facilities. They are facilities that handle certain dangerous cargoes, liquid natural gas, transfer oil, hazardous materials in bulk; or receive foreign cargo vessels greater than 100 gross tons, U.S. cargo vessels greater than 100 gross tons carrying certain dangerous cargoes, or vessels carrying more than 150 passengers.
Scope of Data	The scope of this measure includes incidents that occur at any of the more than 3,400 maritime facilities subject to Maritime Transportation Security Act regulation, which are investigated and confirmed incidents where no Transportation Security Incident has occurred, but established security measures have been circumvented, eluded or violated.

Data Source	The data source for this measure is the Coast Guard Marine Information for Safety and Law Enforcement (MISLE) database as a Breach of Security Investigation.
Data Collection Methodology	Qualified Coast Guard Inspectors investigate incidents reported to the National Response Center by MTSA regulated facilities where security measures have been circumvented, eluded or violated. Verified incidents are documented in the Coast Guard Marine Information for Safety and Law Enforcement (MISLE) database as a Breach of Security Investigation. Results for a given year are the total number of confirmed breaches of security that occurred over the past 12-months at any of the more than 3,400 MTSA regulated facilities.
Reliability Index	Reliable
Explanation of Data Reliability Check	To ensure consistency and integrity, MISLE data entry is controlled through program logic and pull-down menus that require key elements, prohibit the inappropriate, and limit choices to pre-determined options. Comprehensive training and user guides help ensure reliability and the MISLE application itself contains embedded Help screens. Data verification and validation is also affected through regular records review by the Office of Investigations and Casualty Analysis (CG-INV) and Coast Guard Program managers.

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

Performance Measure	Percent risk reduction of coordinated anti-terrorism activities throughout the maritime transportation system
Program	Maritime Security Operations
Description	This measure gauges risk reduction impact of maritime security and response operations (MSRO) conducted in and around ports in the 37 Captain of the Port (COTP) zones by the U.S. Coast Guard or federal, state, and local partners. MSRO include conducting vessel security boardings, providing vessel escorts, enforcing fixed security zones, and conducting surface and land patrols around ports based on available hours and assets. Security risks in the maritime environment include waterborne explosive device attacks, hijacked large vessel attacks, hostage taking, and terrorist assault teams. Executing planned MSRO helps detect, deter, prevent, disrupt, and recover from terrorist attacks and other criminal acts in the maritime domain.
Scope of Data	The population includes all MSRO associated with Tactical Activity plans for the 37 COTP zones. These MSRO occur at vessels, facilities, key assets, and other critical infrastructure at maritime ports. Tactical Activity Plans include only MSRO that impact addressable risk, which is risk the U.S. Coast Guard can address with its current capabilities and authorities. The scope of the results includes information about MSRO from the Tactical Activity Plans that were actually executed by the U.S. Coast Guard and/or federal, state, and local partners.
Data Source	MSRO data comes from the Marine Information for Safety and Law Enforcement (MISLE) database what is managed by Office of C4 & Sensors Capability (CG-761). MSRO executed by federal, state, and local partners are collected in a formatted spreadsheet and entered into MISLE by the relevant COTP. The Maritime Security Risk Analysis Model (MSRAM) system managed by the Office of International and Domestic Port Security (CG-PSA) contains the data that is used to calculate the addressable risks to the 37 COTP zones using a variety of data such as port subject matter experts' judgements of vulnerabilities, actual port activity data, and intelligence. The U.S. Coast Guard Business Intelligence (CGBI) and associated data tools are used to pull data from MISLE and MSRAM to populate Risk-Based Maritime Security and Response Operations (RBMSRO) tools. These tools are used for both creating the 37 ports Tactical Activity Plans and for conducting the actual calculations for this measure.
Data Collection Methodology	The 37 COTPs gather a variety of data annually to update risk estimates for their zones. This information informs Ports' Tactical Activity Plans to optimize risk impact with the hours and assets available. Coast Guard units that perform MSRO enter that data directly into MISLE. MSRO performed solely by federal, state, and local partners are recorded on a formatted spreadsheet and collected by the relevant COTPs. Using CGBI, each COTP pulls their MISLE data for their respective zones to populate RBMSRO. The Coast Guard's Headquarters Maritime Security Operations Program Office sums these values for the risk reduction MSRO completed to determine the numerator for this measure. The same office calculates the addressable risk by summing the risk estimates for the 37 COTP Zones for the denominator. The result is calculated by dividing the sum of all MSRO completed by the addressable risk score across all 37 COTP Zones.
Reliability Index	Reliable
Explanation of Data Reliability Check	To ensure consistency and integrity, MISLE data entry is controlled through program logic and pull-down menus that require key elements, prohibit inappropriate entries, and limit choices to pre-determined options. Comprehensive training and user guides help ensure reliability and the MISLE application itself contains embedded Help Screens. MISLE records also get verification and validation through regular records review by District, Area, and

	Headquarters staffs. Annual risk exposure and risk reduction parameters are determined and annually validated in MSRAM by CG-PSA.

Performance Measure	Three-year average number of serious marine incidents
Program	Maritime Response
Description	This measure reports the three-year average number of Serious Marine Incidents as defined by 46 CFR 4.03-2, which include: death or injury requiring professional treatment beyond first aid, reportable property damage greater than $100,000, actual or constructive loss of certain vessels, discharge of oil of 10,000 gallons or more; or a discharge of a reportable quantity of a hazardous substance.
Scope of Data	This measure reports the three-year average number of serious marine incidents as defined in 46 CFR 4.03-2. Serious Marine Incidents include any marine casualty or accident defined by 46 CFR 4.03-1 which meets defined thresholds. These include: death or injury requiring professional treatment beyond first aid, reportable property damage greater than $100,000, actual or constructive loss of certain vessels, discharge of oil of 10,000 gallons or more; or a discharge of a reportable quantity of a hazardous substance.
Data Source	Serious Marine Incidents are recorded in the Marine Information for Safety and Law Enforcement (MISLE) database
Data Collection Methodology	To obtain serious marine incidents, investigations recorded in the MISLE database are counted. Commercial mariner deaths and injuries include casualties of crewmembers or employees aboard U.S. commercial vessels in U.S. waters. Passenger deaths and injuries include casualties from passenger vessels operating in U.S. waters (disappearances or injuries associated with diving activities are excluded). Oil discharges of 10,000 gallons or more into navigable waterways of the U.S. and reportable quantities of hazardous substances, whether or not resulting from a marine casualty, are included. The three-year average for a given year is calculated by taking the average of the number of serious marine incidents for the most recent three years. Due to delayed receipt of some reports, published data is subject to revision with the greatest impact on recent quarters.
Reliability Index	Reliable
Explanation of Data Reliability Check	To ensure consistency and integrity, MISLE data entry is controlled through program logic and pull-down menus that require key elements, prohibit the inappropriate, and limit choices to pre-determined options. Comprehensive training and user guides help ensure reliability and the application itself contains embedded Help screens. MISLE system quality control, and data verification and validation, is affected through regular review of records by the U.S. Coast Guard Office of Investigations and Analysis. MISLE system quality control, and data verification and validation, is affected through regular review of records by the Coast Guard Office of Investigations and Casualty Analysis.

U.S. Secret Service

Performance Measure	Amount of cyber-financial crime loss prevented (in billions)
Program	Field Operations
Description	This measure is an estimate of the direct dollar loss to the public prevented due to cyber-financial investigations by the U.S. Secret Service. The dollar loss prevented is based on the estimated amount of financial loss that would have occurred had the offender not been identified nor the criminal enterprise

	interrupted. The measure reflects the U.S. Secret Service's efforts to reduce financial losses to the public attributable to cyber financial crimes.
Scope of Data	This measure reports an estimate of the direct dollar loss prevented due to Secret Service intervention/interruption of a cyber-financial crime. It includes all investigations by the Secret Service (authorized under 18 USC 3056) which were closed in the fiscal year being reported. Potential error is due to lag time in data entry or corrections to historical data.
Data Source	The Cyber Financial Crimes Loss Prevented measure is collected from the Field Investigative Reporting System (FIRS). This system is used by all Secret Service investigative field offices, and provides a means of record keeping for all case and subject information. This system is owned and maintained internally by the U.S. Secret Service.
Data Collection Methodology	Data is input to FIRS via Secret Service personnel located in field offices throughout the United States and overseas. Field personnel entering the data have already estimated the loss prevented using standards from the Federal Sentencing Guidelines. These values are extracted from FIRS by cyber financial crime codes (case codes) and the dates these cases were closed. The data is then aggregated up to the highest levels by month, year, office, and Service-wide. This information is then reported through various management and statistical reports to Secret Service headquarters program managers, field offices, and the Department of Homeland Security.
Reliability Index	Reliable
Explanation of Data Reliability Check	FIRS has many features built into it in order to provide the most accurate data possible. Along with the mainframe security features, there are many edit checks built into the applications to ensure the accuracy and validity of the data. Only authorized headquarters and field personnel have access to the applications, and they are governed by specific procedures to input case and arrest data. An annual audit is conducted and recurring verification reports are generated and reviewed to reduce errors and ensure data accuracy.

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

Reliability Index	Reliable
Explanation of Data Reliability Check	Only authorized USSS personnel have access to the applications. Once the data has been aggregated, it is double checked for verification and to ensure data accuracy.

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

Performance Measure	Number of law enforcement individuals trained in cybercrime and cyberforensics both domestically and overseas
Program	Field Operations
Description	This measure represents the number of individuals trained in cybercrime and cyber forensics by the Secret Service. This specialized technical training occurs both domestically and overseas in an effort to strengthen our ability to fight cyber crime.
Scope of Data	The scope of this measure is the number of individuals trained by the Secret Service in cybercrime and cyber forensics. This includes both internal agents and external law enforcement partners.
Data Source	Data on individuals trained by the USSS is currently collected through internal tracking devices. An enterprise solution is contemplated to allow for easier dataset extraction and analysis.
Data Collection Methodology	Data is entered through internal tracking devices by authorized Secret Service personnel. Quarterly data is then extracted and aggregated up to the highest levels by month and year. Training data is collected and aggregated by the number of individuals who attend each training class. Because of this, the

	potential exists for counting unique individuals multiple times if they attend more than one training per fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	Only authorized Secret Service personnel have access to the information and systems. Once the data has been aggregated, it is double checked for verification and to ensure data accuracy.

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

Performance Measure	Percent of days with incident-free protection at the White House Complex and Vice President's Residence
Program	Protective Operations
Description	This measure gauges the percent of instances where the Secret Service provides incident free protection to the White House Complex and the Vice President's

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

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

Performance Measure	Percent of National Special Security Events that were successfully completed
Program	Protective Operations
Description	This measure is a percentage of the total number of National Special Security Events (NSSEs) completed in a Fiscal Year that were successful. A successfully completed NSSE is one where once the event has commenced, a security incident(s) inside the Secret Service - protected venue did not preclude the event's agenda from proceeding to its scheduled conclusion.
Scope of Data	The scope of this measure is every NSSE where the Secret Service has a role in the protection or planning of the NSSE.
Data Source	This program measure originates from the protective event or visit and all data is available through After-Action Reports.
Data Collection Methodology	The Secret Service completes an After-Action Report following every National Special Security Event. This comprehensive report depicts all aspects of the event to include any and all incidents that occurred during the event. Subsequently, the After-Action reports are reviewed to determine the number of National Special Security Events that were successfully completed. This information is then calculated as a percentage and reported through various management and statistical reports to Secret Service headquarters program managers.
Reliability Index	Reliable
Explanation of Data Reliability Check	Any breach of Protective Operations would be immediately known and subject to a thorough investigation.

FY 2020-2021 Agency Priority Goal (APG) Measures

APG: Enhance Southern Border Security

Performance Measure	Number of known illegal entries between the ports of entry on the Southwest Border
Program	Border Security Operations
Description	This measure reports the known number of detected people who crossed illegally into the United States between the ports of entry on the Southwest Border. The number includes those who have crossed the border illegally who were apprehended, those who got away without being apprehended, and those who were turned back to Mexico. This measure is an important indicator of the volume of activity occurring along the Southwest Border that consumes Border Patrol Agent time and resources.
Scope of Data	The population of total entries is all apprehensions (voluntary surrenders and those who seek to evade), Got Aways (GA) and Turn Backs (TB) in areas of the Southwest Border that are generally at or below the northernmost checkpoint within a given area of responsibility. In Border Zones, it includes all apprehensions, GA and TB. In non-border zones, it includes apprehensions who have been in the United States illegally for 30 days or less. An apprehension is someone who enters the United States illegally who is taken into custody and receives a consequence. A GA is someone who enters the United States illegally and is no longer being actively pursued by Border Patrol agents. A TB is someone who enters the United States illegally and returns to the country from which he or she entered, not resulting in an apprehension or GA.
Data Source	Apprehension, GA, and TB data is captured by Border Patrol agents at the station level in several different systems. Apprehension data is entered into the e3 processing system which resides in the Enforcement Integrated Database (EID). The EID is under the purview of the Border Patrol Headquarters Statistics and Data Integrity (SDI) Unit, but the database is owned and maintained by U.S. Immigrations and Customs Enforcement. Data concerning GAs and TBs are entered into the Intelligent Computer Assisted Detection (ICAD) Tracking Sign-cutting and Modeling (TSM) application, which is under the purview and owned by the Border Patrol's Enforcement Systems Unit.
Data Collection Methodology	As part of the standardized processing procedure, Border Patrol agents at the station level enter apprehension, TB, and GA data in the appropriate systems. Agents use standard definitions for determining when to report a subject as a GA or TB. Some subjects can be observed directly as evading apprehension or turning back; others are acknowledged as GAs or TBs after agents follow evidence that indicate entries have occurred, such as foot signs, sensor activations, interviews with apprehended subjects, camera views, or communication between and among other stations and sectors. At the Headquarters level, the SDI Unit extracts data from the e3, ICAD, and TSM systems into a spreadsheet, sums information as appropriate, and then calculates the result by adding together the number of apprehensions, TBs, and GAs.
Reliability Index	Reliable

Explanation of Data Reliability Check	Border Patrol Agents in Charge ensure all agents are aware of and use proper definitions for apprehensions, GAs and TBs at their respective stations. They also ensure the necessary communication takes place between and among sectors and stations to ensure accurate documentation of subjects who may have crossed more than one station's area of responsibility. In addition to station-level safeguards, SDI validates data integrity by using various data quality reports. The integrity of TB and GA 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.

Performance Measure	Percent of illegal entrants apprehended by the U.S. Border Patrol in the Containment Zone along the Southwest Border between ports of entry
Program	Border Security Operations
Description	This measure reports the percent of the known illegal entrants who have crossed into the U.S. along the Southwest Border who are then immediately apprehended within the containment zone. The containment zone is the geographic area at the U.S. border where ideally 100% of apprehensions would occur. Station Border Patrol agents and leadership, led by experts from Border Patrol's Strategic Planning and Analysis Directorate (SPAD), use a number of factors such the physical terrain, slope, features, accessibility, and technological capabilities to determine the containment zone depth for each kilometer of the border. This measure reflects the ability of the Border Patrol to minimize the distance an illegal entrant travels into the U.S. before apprehension, thus demonstrating the effectiveness of impedance and denial and law enforcement response and resolution for those entrants who have been successful at evading border physical structures/barriers.
Scope of Data	This measure includes only those illegal entrants apprehended "at entry," defined as those being observed in the act of illegally crossing the Southwest Border. An entrant includes both immigrants seeking to remain in the U.S., along with others such as drug smugglers and human traffickers who may be apprehended in the border area but are not seeking to remain in the U.S. An "at entry apprehension" does not include those who may be apprehended when observed in movement in the area around the border but are not in the immediate act of crossing the border, such as moving between housing structures or building where they have been seeking temporary shelter. The numerator includes those at entry apprehensions that occur within the containment zone. The containment zone is the area where ideally 100% of all apprehensions would occur. Containment zone areas have been defined and are not expected to change unless extensive unplanned development and/or new infrastructure is built.
Data Source	Station Border Patrol Agents enter apprehension data through a portal into the e3 system which is uploaded to the U.S. Immigration and Customs Enforcement's Enforcement Integrated Database (EID). Data stored in e3 includes the geographic location of each apprehension collected using global positioning system equipment, along with other biographical information. E3 data is extracted and entered into the Border Patrol's Enterprise Geospatial Information Services (eGIS) system, which is used to both render apprehensions physically on a map and provide information to be able to calculate if apprehensions are either in or out of the containment zone. The Border Patrol's Statistics and Data Integrity (SDI) unit manages this data transformation and calculation process for the Border Patrol.

Data Collection Methodology	SPAD Border Patrol experts meet with station level agents and leadership to determine through a consensus process the geographic coordinates that defines the containment zone. These coordinates are validated and approved by Sector Chiefs, provided to SPAD for final approval, and entered into the EGIS System. Apprehension data is entered daily by station Border Patrol Agents into the portal that uploads to e3. Periodically SDI analysts extract data into excel to conduct data cleaning activities, such as resolving missing data or citizenship status. Data is loaded from excel to EGIS to calculate, within a 1-kilometer square, apprehensions in or outside the containment zone. SDI extracts these calculations back into excel, where station, sector, and roll-up containment zone calculations are made. This measure reflects the roll-up of data from all 47 stations and reports the number of apprehensions within the containment zone divided by the total number of at entry apprehensions.
Reliability Index	Reliable
Explanation of Data Reliability Check	Border Patrol Agents in Charge ensure agents at their stations use proper procedures for reporting the geographical information for apprehensions in e3. Station-level leaders also ensure the necessary communication occurs among sectors and stations to ensure accurate documentation of subjects who may have crossed more than one station's area of responsibility. Watch commanders at Stations daily review the arrest records for completeness of data reporting. Enforcement System Liaisons at the sector level review information in e3 for anomalies, such as the lack of citizenship status or latitude and longitude information, and request corrections from the relevant stations. The SDI Office conducts reviews of the data using data quality reports so as to prepare it for leadership or external reporting. Lastly, SPAD analysts review the data over time and across stations to look at trends or inconsistencies with known activity in geographical areas along the Southwest Border.

Performance Measure	Percent improvement in the surveillance capability score on the Southwest Border
Program	Border Security Operations
Description	The measure gauges the improvements being made along Southwest Border sectors regarding their capability to surveil the border. The Surveillance Capability (SC) score quantitatively measures the maximum ability to actively monitor and detect activity at or near the border, representing the combined contributions of technology assets and agents on patrol. The SC score examines each surveillance asset in terms of area coverage, performance, and persistence. The ability to surveil the border environment is critical to situational awareness, a key element of operational control of the border. This measure will allow tracking of progress in surveillance capability over time, and across the nine sectors on the Southwest Border, based on assets assigned.
Scope of Data	This measure represents the sum of the surveillance capability contributions from all surveillance assets in each station of the Southwest border, assuming they are located in the land area within 20 miles of the border. A calculation for the surveillance capability contribution of each asset is performed as a function of area coverage (the land area viewshed that is under surveillance, excluding areas where visibility is limited by line-of-sight blockages); performance (the ability of the surveillance asset to detect and monitor that area); and persistence (the amount of time the asset is available to conduct surveillance).

Data Source	The source of the counts of asset types within each station are provided by Program Managers within the Program Management Office Directorate (PMOD) and Enterprise Services Division (ESD) in Border Patrol Headquarters. The source of data used for calculation of the SC contributions of each asset type are derived from asset specifications, sector input as to persistence, and modeling of terrain features that impact viewsheds. The SC scores are maintained in an excel document maintained by the Planning Division at Headquarters.
Data Collection Methodology	Each Southwest Border station's surveillance baseline capability is based on FY18 assets and their capability to provide area of coverage, performance, and persistence. The baseline SC score is determined by manual expert review of each asset and its capability, and this information is recorded in the SC model. The model uses defined mathematical procedures to calculate a SC score for entire Southwest Border. During the year, when new assets are delivered, or assets become inoperable or redeployed, PMOD communicates that to the Planning Division, who ensures that the information is updated in the model. At the end of the fiscal year, a manual expert review is again done for the current assets and their capability, stored in the model, and a new SC score calculated. The percent improvement is calculated based on changes from the FY18 SC score to the current score.
Reliability Index	Reliable
Explanation of Data Reliability Check	The SC model was developed by a third-party expert outside of the Border Patrol and has undergone peer review regarding its methodology and calculation procedures. Changes in scores are reviewed by the Director of the Planning Division and shared with PMOD Director for review. Station review of more detailed results provides a validation of the surveillance capability score and results not consistent with field experience are evaluated and resolved.

Performance Measure	Percent of milestones met for establishing Northern Border measures that will integrate the Operational Control framework
Program	Border Security Operations
Description	This measure tracks the ability of Border Patrol Headquarters and the eight Northern Border sectors to complete important steps and milestones needed each year over the two-year process of integrating the Operational Control (OPCON) framework with Northern Border sector operations. This measure is valuable for demonstrating an expansion of efforts to make pursuit of OPCON viable beyond the Southwest border, by tailoring operational measures that apply to the Northern Border to each of the three elements in the OPCON framework: Situational Awareness, Impedance and Denial, and Law Enforcement Response and Resolution.
Scope of Data	This measure will include milestones for completion each fiscal year within all eight Northern Border (NB) sectors, which includes Blaine, Spokane, Havre, Grand Forks, Detroit, Buffalo, Swanton, and Houlton sectors. Milestones to be monitored for completion in FY20 include initial consultation with representatives from all NB sectors on measures needed for the OPCON framework; Pilot the identified NB OPCON measures at Blaine Station to determine feasibility and relevance; Gather data and analyze feedback/results from pilot station and socialize with representative from all Northern Border sectors to determine feasibility and viability of Northern Border framework; If the Northern Border framework is viable, travel to 4 of the 8 sectors to gather data to populate the framework.

Data Source	Milestones that need to be completed during each Fiscal Year are documented on the Northern Border OPCON Integration Milestone Checklist, an excel spreadsheet maintained by the Planning Division at Border Patrol Headquarters. The spreadsheet is stored on a share drive for easy access and updating by Planning staff.
Data Collection Methodology	At the end of each fiscal year quarter, an analyst from the Planning Division, USBP Headquarters, tabulates the number of annual milestones that were completed for that quarter, and divides the completed milestones by the total number of annual milestones, to arrive at the percent completed for that fiscal year. As the fiscal year progresses, milestones in each preceding quarter are added to the cumulative count of completed milestones, allowing each quarter to build on the progress of the previous quarters.
Reliability Index	Reliable
Explanation of Data Reliability Check	Each fiscal year quarter, Planning Division analysts finalize the results reported on the Northern Border OPCON Integration Milestone Checklist, which is reviewed for accuracy and completeness by the Head of the Planning Division or designee. Milestones are pre-defined at the beginning of the fiscal year, and this allows for no opportunities for adding or subtracting new milestones, which would alter the completed milestones result. The spreadsheet results are transmitted, along with the sectors' quarterly reports, to the Law Enforcement Operations Division (LEOD) for review and concurrence.

Performance Measure	Percent of Southwest Border sector planned strategies associated with the Operational Control framework that are completed
Program	Border Security Operations
Description	This measure gauges the percent of planned strategies that were executed by the nine Southwest Border sectors of the Border Patrol, as part of the sector Concepts of Operation Plans (CONOPs) associated with the Operational Control (OPCON) framework. A planned strategy is defined in the OPCON Planning Guidance as the ways and means by which each sector plans to mitigate or address their highest priority capability gaps using operations, technology deployments, and partnerships. Sectors submit their CONOPS at the start of the fiscal year to describe how each will work to improve elements of operational control through specific strategies. Quarterly reports provide progress updates regarding execution of sector strategies, along with initial sector data on measures associated with the OPCON framework. This measure is valuable in demonstrating sectors early efforts to operationally use the OPCON framework to improve security along the Southwest Border.
Scope of Data	This measure will include data for the nine Southwest Border sectors, which includes San Diego, El Centro, Yuma, Tucson, El Paso, Big Bend, Del Rio, Laredo, and Rio Grande Valley sectors. Concepts of Operation (CONOPs) establish the overall sector strategies to improve security for the entire Area of Operation, and thus cover all the stations in a sector. Sectors consider the existing resources available to the sector for each fiscal year when formulating the CONOPs. Resources include elements such as personnel, surveillance technology, mobility assets, physical infrastructure, roads, and other support assets such as those provided by the Department of Defense.
Data Source	CONOPS, along with sector quarterly reports, are transmitted by email to Headquarters Border Patrol, Planning Division. The reports are then downloaded and saved on a share drive within the Planning Division for easy access.
Data Collection Methodology	Each sector annually develops its CONOPS, where leadership considers how to advance operational control in their sector and balances the use of existing resources to address the greatest threats. The CONOPs list by quarter the

	strategies that have been developed to improve each element in operational control. Sectors deliver quarterly reports detailing progress on execution of the strategies associated with the CONOPs to the Border Patrol Headquarters Planning Division. The quarterly information is then manually compared by analysts in the Planning Division to determine if planned strategies were executed. This information is then recorded on the Master CONOPs Quarterly Report spreadsheet excel spreadsheet. The result for this measure is calculated by totaling the number of planned strategies for all nine Southwest Border sectors against those executed.
Reliability Index	Reliable
Explanation of Data Reliability Check	Planning Division analysts finalize the results reported on the Master CONOPs Quarterly Report spreadsheet, which are reviewed by an Assistant Chief and the Head of Planning Division. The spreadsheet results are transmitted, along with the sectors' quarterly reports, to the Law Enforcement Operations Division (LEOD) for review and concurrence. Analysts in LEOD for each sector examine the findings to confirm whether the report provided and results concluded match evidence in the Border Patrol Enforcement Tracking System (BPETS) and other sources. If differences occur, LEOD and Planning analysts meet to review and adjudicate the results.

Performance Measure	Percent of time the U.S. Border Patrol reaches a detection site in a timely manner to assess the nature of detected activity in remote, low-risk areas of the Southwest and Northern Borders
Program	Border Security Operations
Description	This measure gauges the percent of time agents reach remote low-risk areas to assess notifications of potential illegal activity and make a determination of the nature of this activity. The goal is for Border Patrol Agents to respond to these notifications in remote low risk areas within 24 hours. If not accomplished in a timely fashion, the evidence degrades, and determinations cannot be made regarding the nature of the potentially illicit activity. Responding to notifications of activity provides valuable information in terms of both the nature of the detected activity, as well as with confirming whether or not the area continues to be low risk. This measure contributes to our situational awareness and ability to secure the border.
Scope of Data	This population for this measure encompasses all geospatial intelligence-informed reports of potential illicit activity in remote areas along the Southern and Northern land border (excluding Alaska) that Border Patrol sectors have determined to be low flow and low risk. This measure does not include the maritime domain. A response is defined as the time when a Border Patrol Agent arrives at the coordinates for the detection site that was communicated by the Office of Intelligence (OI).
Data Source	The data source is mined from e-mail notifications and individual Field Information Reports (FIR), which are stored in CBP's Intelligence Reporting System – Next Generation (IRS-NG) and maintained by CBP's Office of Information Technology.

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

Performance Measure	Percent of U.S. Border Patrol agents who are trained and certified to perform enforcement actions
Program	Border Security Operations
Description	The measure assesses training readiness of U.S. Border Patrol agents. Agents complete extensive Academy Basic Training and are required throughout their career to maintain time-limited certifications in areas such as Firearms Proficiency, Intermediate Use of Force, and Use of Force Policy. In addition, because each sector has a unique climate, terrain, and operational environment, each sector has differing region-specific training requirements. These specialties include handling canines, counter-tunnel operations, horse patrol, All-Terrain-Vehicle (ATV), radiation detection, and snowmobile training. As agent numbers fluctuate, fully trained, deployable agents can mitigate agent-hiring shortfalls. Increasing agents' levels of basic and advanced training enhances the capability to perform mission-essential, law enforcement tasks.
Scope of Data	This measure encompasses every person categorized and assigned as a Border Patrol agent (GS-1896 classification). To be considered fully trained, Border Patrol agents must meet minimum requirements, including the successful completion of Academy Basic Training and post-Academy Field Training Unit instruction and testing, as well as maintaining time-limited certifications in Firearms Proficiency, and a sequence of trainings in Use of Force Policy and techniques for Intermediate Use of Force. In addition, each sector determines required region-specific training based on operating environment and threat. Each sector's Chief Patrol Agent determines region-specific, specialty training requirements based on mission requirements and capability assessments related to the local operating environment and terrain.

Data Source	Multiple systems provide the data for this measure, including: a quarterly Resource Readiness Report, fed data from program training-record databases—the Performance and Learning Management System (PALMS); Training, Records, and Enrollment Network (TRAEN) system; the Firearms, Armor and Credentials Tracking System (FACTS); and individual sector training-personnel analysis. As agents complete training courses and certifications, supervisory personnel ensure documentation of those accomplishments in systems that include PALMS, TRAEN, FACTS, and the Border Patrol Enforcement Tracking System (BPETS).
Data Collection Methodology	As agents complete training courses, training personnel enter each agent's progress into one of the above-listed data sources. The Chief Patrol Agent's (CPA) designee collects data from the systems of record to populate the sector's quarterly Resource Readiness Report (RRR), an Excel spreadsheet listing the required training based on the sector's Table of Organization (TO) and the CPA's mission-needs determination. Agents occupy a position on a sector's TO from the moment they enter on duty, making it possible for a sector to have untrained agents on its TO. The CPA's designee compiles the data into the RRR and submits data to headquarters, where the overall percentage is computed by dividing the number of agents who have completed the required training by the total number of assigned agents; or in the region-specific-training categories, by dividing the number of agents trained in a specialty by the number required by the CPA.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data being reported will be sourced by U.S. Border Patrol sector and station leadership directly from the systems of record (i.e., PALMS, TRAEN, FACTS, BPETS), as well as official sector-specific mechanisms. The data is aggregated by the Logistics Division in the Mission Readiness Operations Directorate at U.S. Border Patrol Headquarters. For audit purposes when needed, the data in the Resource Readiness Report can be traced directly back to those systems of record.

Performance Measure	Rate of interdiction effectiveness along the southwest border between ports of entry
Program	Border Security Operations
Description	This measure reports the percent of detected illegal entrants who were apprehended or were turned back after illegally entering the United States between ports of entry along the Southwest border. The rate includes those who have crossed the border illegally who were apprehended and those who were turned back to Mexico, as compared to the total that includes both of these groups and also those who got away without being apprehended. Border Patrol achieves desired results by maximizing the apprehension of detected illegal entrants, confirming that illegal entrants return to the country from which they entered, and by minimizing the number of persons who evade apprehension and can no longer be pursued. This measure is a key indicator of the Border Patrol's law enforcement and resolution impact, a key component of the Operational Control framework.
Scope of Data	The population of total entries is all apprehensions (voluntary surrenders and those who seek to evade the Border Patrol), Got Aways (GA) and Turn Backs (TB) in areas of the Southwest Border that are generally at or below the northernmost checkpoint within a given area of responsibility. In Border Zones, it includes all apprehensions, GA and TB. In non-border zones, it includes apprehensions who have been in the United States illegally for 30 days or less. An apprehension is someone who enters the United States illegally who is taken into custody and receives a consequence. A GA is someone who enters the United States illegally and is no longer being actively pursued by Border Patrol agents. A

	TB is someone who enters the United States illegally and returns to the country from which he or she entered, not resulting in an apprehension or GA.
Data Source	Apprehension, GA, and TB data is captured by Border Patrol agents at the station level in several different systems. Apprehension data is entered into the e3 processing system which resides in the Enforcement Integrated Database (EID). The EID is under the purview of the Border Patrol Headquarters Statistics and Data Integrity (SDI) Unit, but the database is owned and maintained by U.S. Immigrations and Customs Enforcement. Data concerning GAs and TBs are entered into the Intelligent Computer Assisted Detection (ICAD) Tracking Sign-cutting and Modeling (TSM) application, which is under the purview and owned by the Border Patrol's Enforcement Systems Unit.
Data Collection Methodology	As part of the standardized processing procedure, Border Patrol agents at the station level enter apprehension, TB, and GA data in the appropriate systems. Agents use standard definitions for determining when to report a subject as a GA or TB. Some subjects can be observed directly as evading apprehension or turning back; others are acknowledged as GAs or TBs after agents follow evidence that indicate entries have occurred, such as foot signs, sensor activations, interviews with apprehended subjects, camera views, or communication between and among other stations and sectors. At the Headquarters level, the SDI Unit extracts data from the e3, ICAD, and TSM systems into a spreadsheet, sums information as appropriate, and then calculates the result by dividing the number of apprehensions and TBs by the total number of entries (apprehensions, TBs, and GAs).
Reliability Index	Reliable
Explanation of Data Reliability Check	Border Patrol Agents in Charge ensure all agents are aware of and use proper definitions for apprehensions, GAs and TBs at their respective stations. They also ensure the necessary communication takes place between and among sectors and stations to ensure accurate documentation of subjects who may have crossed more than one station's area of responsibility. In addition to station-level safeguards, SDI validates data integrity by using various data quality reports. The integrity of TB and GA 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.

APG: Strengthen Federal Cybersecurity

Performance Measure	Percent of agencies for which a reliable Agency-Wide Adaptive Risk Enumeration score can be calculated for assets reporting to the federal dashboard
Program	Cybersecurity
Description	This measure reports the percent of participating federal agencies that have established a reliable active Continuous Diagnostics and Mitigation (CDM) connection with the Federal Dashboard allowing the calculation of an Agency-Wide Adaptive Risk Enumeration (AWARE) score. Reliable AWARE scores use numerical scales to quantify the severity of identified vulnerabilities of IT systems (assets), how long they have been present, and the impact to these systems. This measure is an indicator of agencies' cybersecurity posture, and their ability to provide information to the Federal Dashboard to identify system vulnerabilities. AWARE scores serve as a mechanism to prioritize and remediate system vulnerabilities.
Scope of Data	The population for this measure defines participating federal agencies as the 23 Federal civilian CFO Act agencies, excluding the Department of Defense, and the 24th agency being a roll-up of the mid- to small-sized agencies that receive CDM

	shared services. The mid- to small-sized agencies who elect to receive the CDM shared service platform will be counted as the equivalent of a single CFO Act agency. The value being counted is whether any one of the agencies' organizations is providing valid data to the Federal Dashboard that then allows for the calculate of the automated AWARE score.
Data Source	The CDM Project Management Office is responsible for maintaining data used for this measure. Data is captured via the CDM Federal Dashboard and entered into the FY20-21 APG Data Collection Instrument spreadsheet, which is stored on the CDM IPT SharePoint site.
Data Collection Methodology	The CDM Program Office in coordination with Federal Network Resilience (FNR) Office tracks progress of agencies' ability to provide valid data to the Federal Dashboard, and the calculation of an AWARE score for that organization. Program Analysts do a manual review to ensure the data is considered valid based on tests of the data consistency protocol. This review focuses on ensuring that an agency's CDM tools and sensors have been properly configured, that missing or duplicative data issues have been resolved, and that data transfer between CDM layers is functioning properly, thus allowing for the calculation of an AWARE score. The results of organizations providing valid data are saved in the CDM FY20-21 APG Data Collection Instrument spreadsheet. This measure is calculated by dividing the number of agencies where any organization in that agency has a reliable AWARE score by the 23 CFO Act agencies and the 24th being the roll-up of the mid- to small-sized federal agencies.
Reliability Index	Reliable
Explanation of Data Reliability Check	The CDM Program Manager, CDM Deputy Program Managers, CDM Portfolio Management Section Chief, the FNR Director, and the FNR Deputy Director will review the data to verify its validity as compared to other authoritative sources (e.g., agency FISMA reporting), along with a trend analysis from previous quarters. The Strategy, Policy, and Plans Office will also review the results and accompanying explanations to ensure accuracy.

Performance Measure	Percent of agencies where IT hardware devices reported in the Federal Dashboard is within ten percent of agency self-reported numbers for Federal Information Security Management Act devices
Program	Cybersecurity
Description	This measure reports the percent of participating federal agencies with an active Continuous Diagnostics and Mitigation (CDM) connection with the Federal Dashboard whose automated collection of the number of hardware devices is within ten percent of the agency's self-report Federal Information Security Management Act (FISMA) device numbers. Currently due to complexities with automated detection along with the status of CDM implementation, device data can vary significantly for federal agencies. This measure provides an indicator of the extent of this deviation and is intended to drive attention to addressing and resolving these differences and improve data integrity.
Scope of Data	The population for this measure defines participating federal agencies as the 23 federal civilian CFO Act agencies, excluding the Department of Defense, and the 24th agency being a roll-up of the mid- to small-sized agencies. The mid- to small-sized agencies who elect to receive the CDM shared service platform will be counted as the equivalent of a single CFO Act agency. The value being counted is the agencies where their deviation score is within 10%.
Data Source	The CDM Project Management Office is responsible for maintaining all the data used for this measure. Data is captured via the CDM Federal Dashboard and entered into the FY20-21 APG Data Collection Instrument spreadsheet, which is stored on the CDM Integrated Project Team SharePoint site. FISMA self-report

	data from agencies' CIO staff is collected via CyberScope, a web-based application designed to streamline IT security reporting for federal agencies that gathers and standardizes data from federal agencies to support FISMA compliance.
Data Collection Methodology	Analysts in the CDM Program Office extract automated information on the last day of the quarter from the Federal Dashboard regarding the number of hardware devices on agency networks to the APG Data Collection Instrument. Analysts also enter agency FISMA device data into the Instrument from this same timeframe. The first step to calculating the result is determining for each agency the difference in the device numbers by dividing the hardware number by the FISMA device number. A summary calculation is then made for mid-to-small sized agencies by dividing the number of mid-to-small sized agencies where the difference is ten percent or less by the total mid-to-small number, so as to determine if that value is 80% or higher. If so, the mid-to-small agencies are included as one agency in the numerator. The final result is calculated by dividing the number of agencies where the difference is ten percent or less by the 24 participating agencies.
Reliability Index	Reliable
Explanation of Data Reliability Check	Upon collection and calculation of the quarterly data, the CDM Program Manager, CDM Deputy Program Managers, CDM Portfolio Management Section Chief, the FNR Director, and the FNR Deputy Director will review the data to verify its validity as compared to other authoritative sources. This review will examine the quality of the data provided and how the current data compares to previous quarters as a means to ensure accuracy of reporting. The Strategy, Policy, and Plans Office will also review the results and accompanying explanations to ensure accuracy.

Performance Measure	Percent of agencies where the number of active users in the Federal Dashboard is within ten percent of agency self-reported numbers for Federal Information Security Management Act users
Program	Cybersecurity
Description	This measure reports the percent of participating federal agencies with an active Continuous Diagnostics and Mitigation (CDM) connection with the Federal Dashboard whose automated collection of the number of active users is within ten percent of the agency's self-report Federal Information Security Management Act (FISMA) users. Currently due to complexities with automated detection along with the status of CDM implementation, user data can vary significantly for federal agencies. This measure provides an indicator of the extent of this deviation and is intended to drive attention to addressing and resolving these differences and improve data integrity.
Scope of Data	The population for this measure defines participating federal agencies as the 23 Federal civilian CFO Act agencies, excluding the Department of Defense, and the 24th agency being a roll-up of the mid- to small-sized agencies. The mid- to small-sized agencies who elect to receive the CDM shared service platform will be counted as the equivalent of a single CFO Act agency. The value being counted is the agencies where their deviation score is within 10%.
Data Source	The CDM Project Management Office is responsible for maintain all the data used for this measure. Data is captured via the CDM Federal Dashboard and entered into the FY20-21 APG Data Collection Instrument spreadsheet, which is stored on the CDM Integrated Project Team SharePoint site. FISMA self-report data reported from agencies' CIO staff is collected via CyberScope, a web-based application designed to streamline IT security reporting for federal agencies that

	gathers and standardizes data from federal agencies to support FISMA compliance.
Data Collection Methodology	Analysts in the CDM Program Office extract on the last day of the Federal Dashboard regarding the number of active users on agency networks to the APG Data Collection Instrument. Analysts also enter agency FISMA users from the same timeframe into the Instrument. The first step to calculating the result is determining for each agency the difference in the users by dividing the active users by the FISMA users. A summary calculation is then made for mid-to-small sized agencies by dividing the number of mid-to-small sized agencies where the difference is ten percent or less by the total mid-to-small number and determining if that value is 80% or higher. If so, the mid-to-small agencies are included as one agency in the numerator. The final result is calculated by dividing the number of agencies where the difference is ten percent or less by the 24 participating agencies.
Reliability Index	Reliable
Explanation of Data Reliability Check	Upon collection and calculation of the quarterly data, the CDM Program Manager, CDM Deputy Program Managers, CDM Portfolio Management Section Chief, the FNR Director, and the FNR Deputy Director will review the data to verify its validity as compared to other authoritative sources. This review will examine the quality of the data provided and how the current data compares to previous quarters as a means to ensure accuracy of reporting. The Strategy, Policy, and Plans Office will also review the results and accompanying explanations to ensure accuracy.

Performance Measure	Percent of agencies who have established a data connection and begun providing user access data to the federal dashboard
Program	Cybersecurity
Description	This measure reports the percent of participating federal civilian executive branch agencies where they have established an active Continuous Diagnostics and Mitigation (CDM) connection with the Federal Dashboard and begun providing user access and privilege information. The value being counted is whether any one of the agencies' organizations is providing user access and privilege information to the Federal Dashboard. The user access and privileged information being gauged relates to Identity and Access Management (formerly Phase Two) of the CDM tools reflecting "who is on the network" and demonstrates the successful deployment, integration, display and exchange of data. The measure gauges implementation progress for restricting network privileges and access to only those individuals who need it to perform their duties on federal networks.
Scope of Data	The population of this measure defines participating federal agencies as the 23 federal civilian CFO Act agencies and the 24th agency being a roll-up of the mid-to small-sized agencies that receive CDM shared services. The mid- to small-sized agencies receiving the CDM shared service platform will be counted as the equivalent of a single CFO Act agency. The value being counted is whether any one of the agencies' organizations is providing user access and privilege data to the Federal Dashboard.
Data Source	The CDM Project Management Office (PMO) is responsible for maintaining all the data used for this measure. The CDM PMO will verify Agency Identity and Access Management summary-level data exchanges via the Federal Dashboard. Verification results are recorded in the CDM Capability Roadmap spreadsheet, maintained on the CDM Integrated Project Team SharePoint site.
Data Collection Methodology	The CDM Program Office in coordination with the Federal Network Resilience Office tracks progress of agencies' ability to provide user access and privilege

	information to the Federal Dashboard. Program analysts review Federal Dashboard data to manually verify the scope and veracity of the summary-level user access management information being shared. The data are then used to calculate the result by dividing the number of agencies where any organization in that agency is providing user access management information on the Federal Dashboard by the 24 total participating agencies (23 CFO Act agencies and a combination of non-CFO Act agencies as the 24th).
Reliability Index	Reliable
Explanation of Data Reliability Check	Upon collection and calculation of the quarterly data, the Test Manager, Federal Dashboard Project Manager, CDM Portfolio Management Section Chief, the System Engineer, and the CDM Program Manager will review the list of agencies exchanging Identity and Access Management data with the Federal Dashboard to verify its accuracy. The Strategy, Policy, and Plans Office will also review the results and accompanying explanations to ensure accuracy.

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

	remediation steps to verify that they mediate the vulnerability and did so within 30 days. These results are then recorded by NCATS analysts on the tracking spreadsheet. The result is calculated by dividing the number of configuration-based vulnerabilities mitigated within 30 days of initial identification by all vulnerabilities mitigated during a fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	The results are reviewed by the NCATS Program Manager looking for trends and inconsistencies, and exploring in more detail those vulnerabilities not closed within the 30 days. The CISA Office of Strategy, Policy, and Plans will consolidate findings and transmit to DHS.

Performance Measure	Percent of critical and high vulnerabilities identified through cyber hygiene scanning mitigated within the designated timeframe
Program	Cybersecurity
Description	This measure calculates the percent of critical and high vulnerabilities, identified through cyber hygiene scanning, that have been mitigated within the specified timeline. Cyber scanning occurs in federal agencies and departments but does not include the Department of Defense or the Intelligence Community. For critical vulnerabilities, mitigation is required within 15 days from point of initial detection, and for high vulnerabilities mitigation is required within 30 days. Cyber hygiene scanning prioritizes vulnerabilities based on their severity as a means for agencies to make risk-based decisions regarding their network security. Identifying and mitigating vulnerabilities on a network in a timely manner is a critical component of an effective cybersecurity program, as it is critical to maintaining operational availability and integrity of IT systems.
Scope of Data	Cyber hygiene scanning occurs in the 23 federal civilian CFO Act agencies (excluding the Department of Defense) and nearly 100 mid- to small-agencies who participate in the cyber hygiene scanning. The measure includes: 1) all critical/high vulnerabilities identified by cyber hygiene vulnerability scanning on internet-accessible devices; 2) all critical/high vulnerabilities detected in previous scanning that were mitigated during the measurement period; and 3) all critical/high vulnerabilities that were active greater than or equal to the designated timeline for mitigation (15 days for critical; 30 days for high) during the measurement period. The timeline for mitigation begins when a critical or high vulnerability is first detected on a scan and it ends when the critical or high vulnerability is no longer detected. When a vulnerability finding is “closed” due to it being marked as a false positive, it is not included in the calculation for this measure.
Data Source	Cyber hygiene scans utilize two tools maintained by the Cyber Hygiene Scanning Team: Nmap for host discovery, and Nessus for scanning identified hosts for known vulnerabilities. Results from these scans are collected with a Client Access License (CAL) and stored on an internal CISA network. The Cyber Hygiene Report collates data from the scans by the is generated by CISA’s National Cybersecurity Assessments and Technical Services Office on a weekly basis, and is distributed to Departments and Agencies responsible for remediating the vulnerabilities.
Data Collection Methodology	This measure gauges the total number of critical and high vulnerabilities compared to those mitigated within the designated timeframes. A vulnerability’s age is calculated from when it is first detected on a scan to when the vulnerability is no longer visible on the scan. Subsequent scanning tracks a vulnerability for 90 days after it appears closed to ensure the vulnerability isn’t simply unresponsive to a scan; it is a better indication that a vulnerability has been remediated when it remains undetected for a substantive period of time. If

	a vulnerability is re-detected within 90 days, it is re-opened using the original date of detection, and included in subsequent cumulative calculations. Data analysis software will be used to run a report on the percent of criticals and highs that were mitigated within the designated timeframe. The result is calculated by adding the number of critical vulnerabilities mitigated within 15 days plus the number of high vulnerabilities mitigated within 30 days divided by total number of both open and closed critical and high vulnerabilities.
Reliability Index	Reliable
Explanation of Data Reliability Check	The Cyber Hygiene Scanning team within the CISA Cyber Assessments Team will coordinate with the CISA Insights Branch to review the algorithm to query the data and the quarterly result for this measure to ensure correct data collection and calculation procedures were used. CISA Program Analysis & Evaluation will also review the quarterly results and accompanying explanations prior to final submittal to DHS.

Performance Measure	Percent of mitigation activities for critical and high structural-based vulnerabilities identified through high value asset (HVA) assessments that are on schedule
Program	Cybersecurity
Description	This measure reports the percent of mitigation activities federal agencies and departments have established to resolve critical and high structural vulnerabilities identified in High Value Assets (HVA) asset assessments that are on schedule. HVA assessments are performed across the Federal Government to identify vulnerabilities associated with the most sensitive IT systems and data. Structural-based vulnerabilities are those that have adverse impact across multiple business units and require long-term and detailed planning, procurement, integration, and testing to be mitigated (such as network segmentation, data loss prevention, and data encryption). Ensuring mitigation activities stay on schedule ensure agencies and departments are on track and dedicating resources to mitigate structural-based vulnerabilities so as to protect the Federal Government's most sensitive IT systems and data.
Scope of Data	The population of data for this measure is all open mitigation activities associated with critical and high structural-based vulnerabilities that were identified during HVA assessments. HVA vulnerabilities include both those identified in Risk and Vulnerability Assessments and Security Architecture Reviews. HVAs are those assets within federal agencies and departments and departments they self-nominate as high value and do not include Department of Defense or the Intelligence Community assets. The value is all open mitigation activities that are on schedule. The data included in this measure is based on Agency and department reports delivered to the program between September of the previous fiscal year to August of the current fiscal year. All closed vulnerabilities that have been mitigated are not included in this measure.
Data Source	The data source for determining structural-based vulnerabilities is the HVA Risk Vulnerability Assessment/Security Assessment Report (RVA/SAR) produced by the CISA National Cybersecurity Assessment and Technical Services (NCATS) team. Each HVA vulnerability has an agency or department produced mitigation plan that the responsible agency and department serves as the data source for mitigation status. These plans are emailed to the NCATS team by the agency or department and it is saved on the Homeland Security Information Network (HSIN). The program analysts record results in a spreadsheet that is stored on the HSIN. The CISA HVA program is responsible for oversight of these data sources.

Data Collection Methodology	After receiving a final HVA assessment report, agencies and departments develop initial mitigation plans within 30 days that are reviewed and agreed upon by NCATS analysts to ensure the steps proposed are designed to remediate the identified vulnerabilities. Agencies and departments submit monthly reports on the status their activities to mitigate these structural-based vulnerabilities. NCATS analysts use judgement to determine if sufficient progress is in regards to the plan. These results are then recorded by the NCATS analyst on the structural remediation tracking spreadsheet. The result is calculated by dividing the number of structural-based mitigation activities on schedule by the total number of open structural-based mitigation activities.
Reliability Index	Reliable
Explanation of Data Reliability Check	The results will be reviewed for accuracy by the NCATS Program Manager by comparing the agencies and departments' proposed mitigations activities status and timeline against NCAT analysts progress assessments and investing any instance where progress is indicated as unsatisfactory. The CISA Office of Strategy, Policy, and Plans will consolidate findings and transmit to DHS.

Performance Measure	Percent of potential malicious cyber activity notifications confirmed by agencies as not malicious
Program	Cybersecurity
Description	This measure tracks all the potential malicious cyber activity notifications that were sent to agencies where the notified agency confirmed the activity as not malicious. Potential malicious cyber activity on federal networks is detected by automated tools through the National Cyber Protection System (NCPS) alert-based detection function. The system sends automated notifications to analysts within NCPS, who then manually review the notification(s), confirm if a potential credible threat exists, and if so, the affected agency is sent an email notification for their further exploration. Upon receipt of the notification, agencies investigate the potential malicious activity and communicate back to the program if the notification pertained to non-malicious activity. This measure provides an indicator of the precision of the diagnosis process.
Scope of Data	The population for this measure is the total number of cases where agencies were notified of potential malicious cyber activity on their networks during a fiscal year. The value being measured are those notifications where the notified agency responded the activity was not malicious; those that are still be investigated and are inconclusive in terms of being non-malicious are not included.
Data Source	The Einstein set of tools is the data source for the initial identification of malicious activity. The ticket of potential credible malicious activity is entered in the Remedy system, along with the responses. Tableau, a graphical reporting tool, pulls data from Remedy to calculate this measure. Remedy tickets are maintained by the Integrated Operations Division (IOD) Helpdesk. Cybersecurity Division (CSD) manages both the NCPS and Remedy systems.
Data Collection Methodology	Computer Network Defense (CND) analysts create a case in the Remedy system for each potential malicious activity after receiving notification from the National Cyber Protection System (NCPS). The system then generates an email that is sent to the affected agency and the agency investigates to determine the nature of the activity. They then record their determination of investigation by selecting the which category best reflects the results of their investigation in the Remedy system (choices include non-malicious/authorized activity, unsuccessful, confirmed, inconclusive). No response from the agency is categorized as unresponsive by the Remedy system. Often these determinations are complex, and agencies may not be able to provide conclusive confirmation of non-

	malicious activity. The calculation for this measure is based on the number of notifications that were determined to be non-malicious divided by the total number of notifications that were sent to agencies.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data collection, review and vetting will be conducted by CSD Strategy and Resources Office's Process, Metrics and Reporting Analysts monthly and at each quarter in collaborations with CSD Branch Chiefs to assess validity, consistency and identify potential issues.

Performance Measure	Percent of potential malicious cyber activity notifications where the notified agency acknowledges receipt
Program	Cybersecurity
Description	This measure tracks all the potential malicious cyber activity notifications that were sent to agencies where the notified agency acknowledges receipt. Potential malicious cyber activity on federal networks is detected by automated tools through the National Cyber Protection System (NCPS) alert-based detection function. The system sends automated notifications to Computer Network Defense (CND) analysts within NCPS, who then manually review the notification(s), confirm if a potential credible threat exists, and if so, the affected agency is sent an email for their further exploration. This measure provides confirmation to the program that the notification has been received.
Scope of Data	The population of data includes cases of potential malicious cyber activity entered into the Remedy system where the agency has been provided a notification by email. The value being measured are those notifications where the notified agency responded that they received the notification.
Data Source	The Einstein set of tools is the data source for the initial identification of malicious activity. The ticket of potential credible malicious activity is entered in the Remedy system, along with the responses. Tableau, a graphical reporting tool, pulls data from Remedy to calculate this measure. Remedy tickets are maintained by the Integrated Operations Division (IOD) Helpdesk. Cybersecurity Division (CSD) manages both the NCPS and Remedy systems.
Data Collection Methodology	When the NCPS detects potential malicious cyber activity, the system both records the initial detection time and sends a notification to Computer Network Defense (CND) analysts for review to determine if the potential malicious activity appears credible. If so, analysts then create a case in the Remedy system for each potential malicious activity that includes the initial NCPS alert time (the first notification time is used if multiple notifications occur for the same threat. The system then generates an email that is sent to the affected agency, and the is the date time stamp recorded in Remedy. The Remedy system also had a field where agencies record the nature of the activity, and whether a response was received. NCPS case data is pulled from Remedy by the analysts using Tableau to calculate the agency response rate. The calculation for this measure is the number of responses indicating receipt of notifications divided by the total number of notifications that have been sent.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data collection, review and vetting will be conducted by CSD Strategy and Resources Office Process, Metrics and Reporting Analysts monthly and at each quarter in collaborations with CSD Branch Chiefs to assess validity, consistency and identify potential issues.

Performance Measure	Percent of potential malicious cyber activity notifications where impacted agencies were alerted within the specified timeframe
Program	Cybersecurity

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

This Page Intentionally Left Blank

Homeland
Security

Homeland
Security