U.S. Department of Homeland Security Annual Performance Report

Fiscal Years 2014 – 2016

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

Homeland Security

About this Report

The *U.S. Department of Homeland Security Annual Performance Report for Fiscal Years (FY) 2014 – 2016* presents the Department's performance measures and applicable results aligned to our missions, provides the planned performance targets for FY 2015 and FY 2016, and includes information on the Department's Agency Priority Goals. In addition, this report presents several FY 2014 Department-wide management initiatives followed by a summary of major management and performance challenges and high-risk areas identified by the DHS Office of Inspector General and the Government Accountability Office. The report is consolidated to incorporate our annual performance plan and annual performance report.

The *FY 2014 – 2016 Annual Performance Report* is one in a series of three reports which comprise the Department's performance and accountability reports:

- ***DHS Agency Financial Report***: Delivery date – November 17, 2014.
- ***DHS Annual Performance Report***: Delivery date – February 2, 2015.
- ***DHS Summary of Performance and Financial Information:*** Delivery date – February 16, 2015.

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

For more information, contact:

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

Information may also be requested by sending an email to par@hq.dhs.gov or calling (202) 447-0333.

Homeland Security

Visit Our Website
www.dhs.gov

Table of Contents

Introduction

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

Verification and Validation Process

The Department recognizes the importance of collecting complete, accurate, and reliable performance data since this helps determine progress toward achieving program and Department goals and objectives. Performance data are considered reliable if transactions and other data that support reported performance measures are properly recorded, processed, and summarized to permit the preparation of performance information in accordance with criteria stated by management. OMB Circular A-136, Financial Reporting Requirements, OMB Circular A-11, and the Reports Consolidation Act of 2000 (P.L. No. 106-531) further delineate this responsibility by requiring Agency heads to attest to the completeness and reliability of the performance data they report. DHS implemented a two-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) the Government Performance and Results Act (GPRA) Performance Measure Checklist for Completeness and Reliability; and 2) independent assessments of the completeness and reliability of GPRA performance measures.

GPRA Performance Measure Checklist for Completeness and Reliability

The GPRA Performance Measure Checklist for Completeness and Reliability is used by Components to self-evaluate key controls over GPRA performance measure planning and reporting actions. For each key control, Components are required to describe their control activities and provide their assessment regarding their level of achievement at the end of each fiscal year. Components also factor the results of any internal or independent measure assessments into their rating. The GPRA Performance Measures Checklist for Completeness and Reliability supports the Component Head assurance statements attesting to the completeness and reliability of the performance data. Individual Component Head assurance statements serve as the primary basis for the Secretary's assertion whether or not the Department has effective controls over financial and performance reporting as well as efficiencies of our operations.

Independent Assessment of the Completeness and Reliability of GPRA Performance Measures

The Office of Program Analysis and Evaluation conducts an assessment of performance measure data for completeness and reliability on a sample of its performance measures annually using an independent review team. An independent review team assesses selected measures using the methodology prescribed in the DHS Performance Measure Verification and Validation Handbook, documents their findings, makes recommendations for improvement, and performs a subsequent follow-up review within a year after the initial assessment to observe the Component's implementation of their recommendations. Corrective actions are required for performance measures determined to be unreliable. The Handbook is distributed and made available to all

Components to encourage the development and maturation of internal data verification and validation capabilities, increase transparency, and facilitate the review process. The results obtained from the independent assessments are also used to support the Component's assertions over the reliability of its performance information reported in the GPRA Checklist and Component Head Assurance Statement. DHS has shared our process with other Agencies in support of their verification and validation improvement efforts.

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

Analysis and Operations

Performance Measure	Percent of initial breaking homeland security blast calls initiated between the National Operations Center and designated homeland security partners within targeted timeframes
Program	Analysis and Operations
Description	This measure assesses the rate at which DHS completes inter- and intra-agency blast calls to provide executive decision makers inside and outside DHS immediate verbal situational reports on breaking homeland security situations of national importance. All of the National Operations Center (NOC) duties following an incident are designed to prepare the Secretary to brief the American public within 60 minutes of a significant event. If the blast call does not happen in a timely manner, the NOC will not have the information and situational awareness necessary to prepare DHS senior leadership for this essential requirement. The targeted timeframe to initiate the blast call is within 10 minutes of the Senior Watch Officer (SWO) determining that the breaking homeland security situation is at least a Phase-1 event.
Scope of Data	The data for this measure will include all initial blast calls (conference calls) made for breaking situations that are at least Phase-1 incidents. The scope does not include blast calls made about ongoing situations or updates to breaking situations. The recorded time for the start of the 10 minute period is the moment the SWO announces that the breaking incident requires at least a Phase-1 designation. The recorded time of the blast call is the moment that the SWO starts to speak on the blast call. There will be no sampling required, as the program has access to and maintains records on all blast calls conducted.
Data Source	The data source for this measure is contained within the program's tracking logs. The data logs are entered into an automated database known as the Phase Notification Report in real time and are maintained by the program office.
Data Collection Methodology	Each blast call is logged into the program's tracking log by the NOC desk officer. Data is extracted to calculate the percent of time blast calls are initiated within the targeted timeframe.
Reliability Index	Reliable
Explanation of Data Reliability Check	Desk officers receive training and guidance on tracking and logging procedures, and supervisors perform regular "spot checks" to ensure that procedures are being followed appropriately. Additionally, the NOC Director coordinates random and systematic verification and validation of the data.

Performance Measure	Percent of intelligence reports rated "satisfactory" or higher in customer feedback that enable customers to manage risks to cyberspace
Program	Analysis and Operations
Description	This measure gauges the extent to which the DHS Intelligence Enterprise (DHS IE) is satisfying their customers' needs related to understanding the threat. This measure encompasses reports produced by all DHS component intelligence programs and provided to federal, state, and local customers.
Scope of Data	The scope of this measure is all feedback received from customer satisfaction surveys returned to the DHS IE member (USCG, TSA, etc.) that originated the intelligence report. For this performance measure "intelligence report" is defined

	per Component.
Data Source	The data source for this performance measure will be customer feedback surveys fielded by the DHS IE.
Data Collection Methodology	Members of the DHS IE will attach an electronic survey instrument to each intelligence product disseminated to customers. The recipient of the intelligence completes and then returns the survey to the issuer. The DHS Intelligence Enterprise will provide Intelligence and Analysis (I&A) with the survey results on the second Friday following the end of each quarter. Upon receipt of the data, I&A will average the data across the Intelligence Enterprise for each of DHS mission area and report the total. For this measure, customer satisfaction is defined as responsiveness of the product and its value in helping the customer manage risks to cyberspace. Customers rate their satisfaction on a five point scale from: very satisfied, somewhat satisfied, neither satisfied nor dissatisfied, somewhat dissatisfied, or very dissatisfied. Responses "very satisfied" and "somewhat satisfied" will be considered to have met the criteria for "satisfactory."
Reliability Index	Reliable
Explanation of Data Reliability Check	Individuals within the DHS IE are responsible for collecting, storing, and reporting data generated by the source above. I&A Performance Management & Evaluation personnel are responsible for aggregating the data from the DHS IE and reporting the results quarterly. Once the survey responses are received and aggregated, I&A PME staff review the results for consistency and look for any anomalous trends that would signal a data integrity problem. Any issues are researched and if any erroneous data is found, it is corrected or removed from the overall calculation.

Performance Measure	Percent of intelligence reports rated "satisfactory" or higher in customer feedback that enable customers to understand the threat
Program	Analysis and Operations
Description	This measure gauges the extent to which the DHS Intelligence Enterprise (DHS IE) is satisfying their customers' needs related to anticipating emerging threats. This measure encompasses reports produced by all DHS component intelligence programs and provided to federal, state, and local customers.
Scope of Data	The scope of this measure is all feedback received from customer satisfaction surveys returned to the DHS IE member (USCG, TSA, etc.) that originated the intelligence report. For this performance measure "intelligence report" is defined per Component.
Data Source	The data source for this performance measure will be customer feedback surveys fielded by the DHS IE.
Data Collection Methodology	Members of the DHS IE will attach an electronic survey instrument to each intelligence product disseminated to customers. The recipient of the intelligence completes and then returns the survey to the issuer. The DHS IE will provide Intelligence and Analysis (I&A) with the survey results on the second Friday following the end of each quarter. Upon receipt of the data, I&A will average the data across the Intelligence Enterprise for each of DHS mission area and report the total. For this measure, customer satisfaction is defined as responsiveness of the product and its value in helping the customer anticipate emerging threats. Customers rate their satisfaction on a five point scale from: very satisfied, somewhat satisfied, neither satisfied nor dissatisfied, somewhat dissatisfied, or very dissatisfied. Responses "very satisfied" and "somewhat satisfied" will be considered to have met the criteria for "satisfactory."
Reliability Index	Reliable
Explanation of Data	Individuals within the DHS IE are responsible for collecting, storing, and

Reliability Check	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.

Domestic Nuclear Detection Office

Performance Measure	Number of people covered by Securing the Cities program preventive radiological and nuclear (rad/nuc) detection capabilities (in millions)
Program	Domestic Rad/Nuc Detection, Forensics and Prevention Capability
Description	The Securing The Cities (STC) program provides financial assistance to state, local, and tribal organizations to develop a robust regional radiological/nuclear detection program. For the STC program to count the population as covered by a robust radiological/nuclear detection capability, the region must demonstrate that 10% or more of its standing law enforcement are trained and equipped to conduct primary screening and patrolling as part of their daily routine duties and there are equipped and trained personnel to conduct secondary screening and alarm adjudication. In addition, the region must conduct at least one multi-jurisdictional exercise a year, and allow the exchange of information among regional partners and with federal agencies, and mutually assist each other in performing the radiological/nuclear detection mission. If the measure is met, the entire population from the statistical area is counted as covered.
Scope of Data	The measure includes data for the rad/nuc detection capability coverage within STC regions and the population data for the applicable regions. The population data range is calculated using the U.S. Census Bureau Population of Combined Statistical Areas in the United States and Puerto Rico 2010 (as defined in February 2013). Census numbers are rounded to the nearest 500,000. The rad/nuc detection capability coverage within STC regions will calculate the percentage of standing law enforcement trained and equipped to conduct primary screening and patrolling as part of their daily routine duties and personnel trained and equipped to conduct secondary screening and alarm adjudication.
Data Source	Data for this measure are collected from the STC program and population data will be sourced from the U.S. Census Bureau information from the 2010 census which provides the Population of Combined Statistical Areas. The measure includes all communities and capabilities within the supported UASI-eligible region that exist to protect the population of the United States against the possession, transportation, or use of rad/nuc material outside of regulatory control.
Data Collection Methodology	Quarterly reports required of the STC grant recipients provide the operational, deployed capabilities, indicating the coverage of rad/nuc detection capabilities. Additionally, regional Multi-Year Training and Exercise Programs validate the status of readiness to include information exchange and regional coordination between State, local, county, tribal, and Federal agencies. Data indicate whether or not the region has achieved the necessary robust capability for implementing rad/nuc detection operations, as defined in the measure description. Population data are based on the U.S. Census Bureau 2010 census data.
Reliability Index	Reliable

Explanation of Data Reliability Check	Programmatic completion with the quarterly reporting mechanisms; major training and exercise performance outlined within the program to validate the overall capability readiness; and long-term sustainment plans to maintain the program's capabilities are the key indicators of the population's security against illicit rad/nuc material outside of regulatory control.

Performance Measure	Percent of cargo conveyances that pass through radiation portal monitors upon entering the nation via land border and international rail ports of entry
Program	Domestic Rad/Nuc Detection, Forensics and Prevention Capability
Description	This measure gauges the proportion of cargo scanned by radiation detection equipment deployed to the Nation's land border crossing ports of entry and international rail ports of entry. It is expressed in terms of the percent that is scanned by radiation portal monitors of the total number of cargo conveyances entering the Nation through land ports of entry and by international rail. The Domestic Nuclear Detection Office (DNDO) procures and/or installs radiation portal monitors (RPMs) at ports of entry and the U.S. Customs and Border Patrol (CBP) conducts the cargo scanning using the RPMs to prevent nuclear and other radioactive materials that are out of regulatory control from being brought into the country via cargo conveyances.
Scope of Data	The measure is based on the total number of cargo conveyances entering the Nation through U.S. Customs and Border Protection (CBP) land ports of entry and railroad cars entering through international rail ports of entry. It identifies the portion that is scanned using radiation detection equipment.
Data Source	This data is jointly managed, reviewed, and provided by the CBP and DNDO Radiation Detection Equipment (RDE) Integrated Product Team (IPT). Weekly reports of new detection portal installations are provided by the installation agent, the Pacific Northwest National Laboratory (PNNL). Data are provided in tabular form, based on new installations completed in a given week. Baseline land border cargo data are maintained by CBP, and baseline rail cargo data are maintained by the Department of Transportation, Bureau of Transportation Statistics, and is published in their on-line database. They maintain monthly and annual data on the amount of rail cargo arriving at U.S. rail crossing sites. Current detector coverage is tabulated by the DNDO Product Acquisition and Deployment Directorate (PADD) on the Land Border Cargo Analysis spreadsheet.
Data Collection Methodology	Weekly progress reports are provided by Pacific Northwest National Laboratory and sent to both DNDO and CBP which summarize installation progress for the last week and any changes to the overall number of conveyances being scanned. The percent of conveyances passing through portal monitors is calculated by the DNDO Mission Management Directorate, based on the number of deployed portals, to determine the percent of scanned cargo containers and railroad cars out of the total entering through U.S. land and rail ports of entry.
Reliability Index	Reliable
Explanation of Data Reliability Check	Portal monitor installation and system availability information is monitored and verified by DNDO and CBP headquarters, and validated by annual system recalibrations in the field. Data generated by the Department of Transportation is integrated and reviewed by the DNDO Mission Area Manager.

Performance Measure	Percent of containerized cargo conveyances that pass through radiation portal monitors at sea ports of entry
Program	Domestic Rad/Nuc Detection, Forensics and Prevention Capability
Description	This measure gauges the amount of containerized cargo scanned by the radiation detection equipment deployed to the Nation's sea ports of entry. It is expressed in

	terms of the percent that is scanned by fixed radiation portal monitors of the total number of containerized cargo conveyances entering the nation through sea ports of entry.
Scope of Data	The measure is based on the total number of cargo conveyances entering the Nation through U.S. Customs and Border Protection (CBP) sea ports of entry. It identifies the portion that is scanned using fixed radiation detection equipment. This measure does not include roll-on/ roll-off (for example, vehicles) and bulk cargo.
Data Source	Port cargo data for conveyances entering the U.S. are provided by CBP field offices. Additionally, weekly reports of new portal installations are provided by the installation agent, the Pacific Northwest National Laboratory. This data is provided to CBP and the Domestic Nuclear Detection Office (DNDO) in tabular form, based on new installations completed in a given week. The DNDO Mission Management Directorate calculates the final percent coverage from that data using the Sea Port Cargo Analysis spreadsheet.
Data Collection Methodology	Weekly progress reports are provided by Pacific Northwest National Laboratory and sent to both the DNDO and CBP which summarize installation progress for the last week and any changes to the overall number of conveyances being scanned. The percent of cargo containers passing through portal monitors is calculated based on the number of such conveyances through seaports, where portals are deployed, compared to the total entering through U.S. sea ports of entry.
Reliability Index	Reliable
Explanation of Data Reliability Check	Portal monitor installation and system availability information is monitored and verified by DNDO and CBP headquarters, and validated by annual system recalibrations in the field. Data generated by the Department of Transportation is integrated and reviewed by the DNDO Mission Area Manager.

Federal Emergency Management Agency

Performance Measure	Number of states and territories that have demonstrated improvement towards achieving their core capability targets established through their Threat and Hazard Identification and Risk Assessment (THIRA) (New Measure)
Program	Preparedness
Description	This measure assesses the number of states that have demonstrated an improvement in their assessment of their capabilities to prepare for, protect against, respond to, recover from, and mitigate against disasters. States and territories assess themselves annually on the 31 core capabilities identified in the National Preparedness Goal and this captures the number of states and territories that demonstrated improvement from the base year of 2012 on at least one core capability.
Scope of Data	The scope of this measure includes all 50 states and six territories.
Data Source	States and territories assess their current core capability levels relative to their own capability targets annually through the State Preparedness Report (SPR). This annual self-assessment provides detailed data on the number of states and territories whose capability levels increase or decrease each year. SPR data used in this measure are a self-assessed rating for each POETE solution area and a priority (high, medium, or low) for each core capability.
Data Collection	For each core capability, states and territories assess their preparedness levels in

Methodology	each of the five solution areas—planning, organization, equipment, training, and exercises (POETE). They use a five-point scale for each assessment, where level one indicates little-to-no capability, and level five indicates that they have all or nearly all of the capability required to meet their target. Since self-assessments are conducted at the solution area POETE level, a state and territory could make 155 assessment in the SPR (31 core capabilities times 5 solution areas = 155 assessments per jurisdiction). As a result, the average capability level for each state and territory is calculated across a possible 155 assessments. Since states and territories chose different solution areas to rate and rated different capabilities as high priority, the number of values used to calculate the average capability level was less than 155 and varied for each state and territory.
Reliability Index	Reliable
Explanation of Data Reliability Check	States and territories receive substantial technical assistance (TA) on conducting the THIRA and submitting their capability levels estimates through the SPR. TA takes the form of published guidance (Comprehensive Preparedness Guide (CPG) 201: THIRA Guide, Second Edition), workshop sessions in the FEMA Regions, and just-in-time instruction during the assessment period. SPR submissions are routed through the Homeland Security Grant Program State Administrative Agency to ensure it represents all preparedness stakeholders in the jurisdiction. The Regional Federal Preparedness Coordinator and/or his or her staff review all state, territorial, and other eligible grantee THIRA submissions in their area of responsibility. The review ensures that the submitted THIRAs are developed in alignment with CPG 201.

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

	and combined perils and those communities that have adopted disaster-resistant building codes. This data is used to calculate the percent of communities in high earthquake, flood, and wind-prone areas adopting disaster-resistant building codes.
Reliability Index	Reliable
Explanation of Data Reliability Check	FEMA relies on ISO to manage the completeness and reliability of the data provided thought their BCEGS database to the program; however, the data are reviewed by FEMA's Mitigation program to ensure results are consistent over time. If significant fluctuations in quarterly and annual results occur, the program will work with ISO to address issues with data reliability.

Performance Measure	Percent of corrective actions that have been completed on time to improve performance following Capstone national level exercises (Retired Measure)
Program	Preparedness
Description	This measure indicates the percent of corrective actions assigned to DHS components following national level exercises that were completed by the deadline. A national level exercise helps the Federal Government to prepare and coordinate a multiple-jurisdictional integrated response to a national catastrophic event. Corrective actions are identified during the exercise and tracked to completion to improve the national response to an event.
Scope of Data	National level exercises involve participation from various agencies and organizations from across the whole community; the degree of involvement for each is typically determined by the individual scenario. This measure will focus on the unclassified corrective actions (CAs) assigned to DHS components. CAs completed by the deadline include those designated as "completed" or "validated" in the Corrective Action Program (CAP) system. A status of "completed" indicates a solution has been identified, but the solution has not yet been validated through training or an exercise. An action must be completed before it can be validated, so an action status of "completed" or "validated" by the due date would count as being completed on time.
Data Source	Corrective Actions are detailed in the National Level Exercise Improvement Plan, which is finalized and agreed upon by the interagency at the After Action Meeting and approved by the DHS Secretary. Then, the unclassified CAs are uploaded to the CAP system, an unclassified IT system owned and operated by FEMA.
Data Collection Methodology	Following a national level exercise, FEMA's National Preparedness Assessment Division (NPAD) enters the list of Corrective Actions into the CAP system. Each DHS component's Action Officer updates the status of the CA on a quarterly basis to say whether it is open, complete, validated, or canceled. The percent is calculated with the numerator as the total number of CAs assigned to DHS that have been marked as completed or validated by their due date in the CAP system and the denominator is the total number of CAs assigned to DHS. This will be measured cumulatively, where the sum of the numerators for all quarters that have been completed in the fiscal year are divided by the sum of the denominators for all quarters that have been completed in the fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	NPAD will verify the Action Officers for each DHS component and send reminders to update the status of their assigned corrective action in the CAP system. Each DHS component is responsible for reporting data on their corrective actions. NPAD personnel are responsible for aggregating the data from all DHS components and reporting the results quarterly. NPAD accepts other DHS agencies' categorization of CA status and does not independently verify, but

	the calculation is verified by an analyst and then a supervisor in NPAD.

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

Performance Measure	Percent of high-priority core planning capabilities rated as proficient by states and territories
Program	Preparedness
Description	This measure reports the percent of high-priority core capabilities related to planning that states and territories rate as proficient. Planning is a key indicator of their overall level of preparedness. This information is gathered from the State Preparedness Report (SPR), which is an annual self-assessment by states and territories of their levels of preparedness in nationally established capabilities to prevent, protect against, mitigate the effects of, respond to, and recover from those threats and hazards that pose the greatest risk to the security of the Nation.
Scope of Data	The National Preparedness Goal establishes 31 core capabilities to prevent, protect against, mitigate the effects of, respond to, and recover from those threats and hazards that pose the greatest risk to the security of the Nation. The SPR tool allows states and territories to assess each core capability in terms of the planning, organization, equipment, training, and exercises (POETE framework) elements on

	a nominal 1-5 scale. Proficient, for the purposes of this measure, is defined by a rating of a 4 or 5 on the nominal scale for the planning element of the POETE framework. This measure considers only the planning element in the core capabilities rated as a high priority by states and territories.
Data Source	The data are collected from the official states' and territories' responses to the annual SPR capability assessment that is submitted to the National Preparedness Assessment Division (FEMA\NPD\NPAD).
Data Collection Methodology	This measure is the fraction of high-priority capabilities for which states and territories are proficient for planning. For this metric, the numerator is calculated by finding the total number of high-priority core capability planning elements rated as proficient (4 or 5). The denominator is calculated by determining the total number of high-priority core capability planning elements rated as 1, 2, 3, 4, or 5 for all states and territories.
Reliability Index	Reliable
Explanation of Data Reliability Check	FEMA NPAD reviews the states' and territories' self-assessments. Final SPR responses represent an informed estimate by states and territories. NPAD reviews all SPR data for inconsistencies, missing/invalid data, and outliers that do not pass the logic test. Any inconsistencies, outliers, or missing/invalid data are flagged and then reviewed with the state, in coordination with the FEMA regions, for accuracy. The data is contained on a spreadsheet that automatically calculates the percentages; this data is then verified by NPAD staff for accuracy.

Performance Measure	Percent of households surveyed reporting they have taken steps to mitigate damage to property and protect themselves in the event of a disaster (Retired Measure)
Program	Mitigation
Description	This measure tracks the percent of surveyed households that indicate they have taken steps to mitigate damage to their home in the event of a flood, hurricane, tornado, or other wind hazard. Mitigation helps to reduce the loss of life and property by lessening the impact of natural disasters.
Scope of Data	As part of the RiskMAP Survey Instrument, a total of 1,000 telephone interviews are conducted during June each year on the steps being taken to mitigate damage to property and protect individuals. The survey covers 100 interviews from each of FEMA's 10 regions, which cover the United States and the six territories.
Data Source	The 2011 FEMA National Survey Instrument was used to collect all the data for 2011. For 2012 and the following years, data collection will occur through the RiskMAP Survey Instrument.
Data Collection Methodology	In the RiskMAP Survey Instrument, FEMA requires at least two mitigation activities to better measure those households that are proactively taking mitigation steps. A threshold of two also takes into account that the survey items were associated with either flood or wind hazards and individuals may not be susceptible to both. The methodology for this measure is calculated by the percent of households surveyed who responded they have taken two or more of the following mitigation actions: (1) purchased flood insurance, (2) sealed the walls in your basement with waterproofing compounds, (3) installed storm shutters, (4) installed roof straps or clips to protect your roof from strong winds, (5) built a space in your home specifically to provide shelter in an emergency and (6) raised the furnace or water heater above the floor.
Reliability Index	Unreliable
Explanation of Data Reliability Check	Interviews for the survey are monitored throughout the process and the tracking software is tested to ensure proper programming. Survey responses are analyzed and checked for completeness and reliability through four layers of reviews by the

	contractor, reviewed by Federal Insurance and Mitigation Administration personnel, and vetted by FEMA Senior Leaders.

Performance Measure	Percent of households that participated in a preparedness exercise or drill at their workplace, school, home or other community location in the past year
Program	Preparedness
Description	This measure calculates the percent of households responding to a survey who indicate that they have participated in a preparedness exercise or drill in their workplace, school, home, or community in the past year. The survey collects individual disaster preparedness data from a random sample of households across the nation. Improving the public's knowledge and ability to take effective protective actions for hazards is a key objective of preparing the public to act quickly and effectively in emergency situations.
Scope of Data	As part of the Nationwide Household Survey, a total of about 3,000 or more telephone interviews are conducted during the summer each year on individual and household preparedness. The survey contacts individuals throughout the United States and the six territories.
Data Source	As part of the FEMA National Survey, a total of about 3,000 or more telephone interviews are conducted yearly on individual and household preparedness. The survey, which is conducted by National Preparedness Directorate (NPD) contractors, collects the data in the statistical analysis program SPSS and then provides a report to NPD on the survey responses.
Data Collection Methodology	The measure calculates the percent of households surveyed via landline or cellular phone who responded affirmatively to the question that asked whether they have participated in a disaster preparedness exercise or drill in their workplace, school, home, or another community location in the past year. Survey data is collected using a Computer Assisted Telephone Interviewing (CATI) system and results from the survey are analyzed in SPSS and SAS. When processing the data from the random digit dialing surveys, results are weighted to correct for unequal probabilities of selection. The sample data are also post-stratified according to geography, age, gender, and race to account for potential biases such as over- and under-representation of certain population segments. This will adjust the sample's demographic distributions to match the distribution derived from the latest available Current Population Survey estimates.
Reliability Index	Reliable
Explanation of Data Reliability Check	There is currently no way to independently verify the accuracy of participants' responses or the responses recorded by the survey administrator. But, each programmed survey instrument goes through a rigorous quality control process. When the instrument is in the field, this rigorous quality assurance process continues. The overall process includes, but is not limited to, program testing, a pre-test and cognitive testing to determine the effectiveness of the survey and questions, monitoring of in-progress calls, recording of all interviews, and the production of tabulations of every question and variables to detect any missing data or errors. Additional quality measures include the checking of survey skip patterns and data accuracy and consistency checks.

Performance Measure	Percent of incident management and support actions taken that are necessary to stabilize an incident that are performed within 72 hours or by the agreed upon time
Program	Response
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 described above. These functions must be performed within established timeframes and include: (1) Incident Management Assistance Teams (IMATs) establishing joint federal/state incident objectives; (2) disaster communication capabilities linking FEMA-supported incident sites; (3) national Urban Search and Rescue (US&R) resources arriving on-scene; (4) response coordination centers activating to directed levels; (5) watch centers transmitting operations orders and situation reports; and (6) the FEMA Operations Center issuing alerts, warnings, and notifications.
Data Source	National and Regional IMAT deployment data are submitted to the National Watch Center (NWC), which provides it to the Field Operations Support Branch for management and tracking. The Disaster Emergency Communications Division manages a database of Mobile Emergency Response Support-related deployment and response data. FEMA's US&R Branch manages deployment and response data associated with the National US&R Response System. National US&R statuses are updated every two hours during deployment, which is captured through National Response Coordination Center (NRCC) and NWC reporting and is tracked by the US&R Branch. Situation reports and operations orders are tracked by both the National and Regionals watch centers, electronically and on paper. NRCC and Regional Response Coordination Centers (RRCC) data are tracked through the manual comparison of operations orders and NRCC/RRCC activation logs. FEMA Operations Center data are managed and tracked through the Emergency Notification System.
Data Collection Methodology	For each quarter, FEMA tracks when an incident requires one or more of the six activities described above and whether or not the activity is accomplished in the time required. Each activity is scored quarterly based on percent of times completed within required timeframe (i.e. if the NRCC is activated 5 times in one quarter and activates to the directed level 4 of those times, the activity is scored as 80%). These six activity-level scores are then equally averaged for a total composite score each quarter.
Reliability Index	Reliable
Explanation of Data Reliability Check	Each supporting activity mentioned above is responsible for reporting on the timeliness of the response for each incident requiring FEMA assistance. For each incident a score is determined based on the data collection methodology. Each quarter the sum of these scores is additive and divided by the number of incidents occurring during the quarter, resulting in an equally weighted average.

Performance Measure	Percent of Incident Management Assistance Teams establishing joint federal and state response objectives within 18 hours
Program	Response
Description	This measure gauges the percent of time that Incident Management Assistance Teams (IMATs) have deployed and have established initial joint federal and state response objectives within 18 hours of a request from a state or jurisdiction.

	IMATs rapidly deploy to an incident, provide leadership for federal assistance, and coordinate and integrate inter-jurisdictional response in support of an affected state or territory.
Scope of Data	FEMA is responsible for three National and thirteen Regional Incident Management Assistance Teams (IMATs). The scope of this measure includes all significant activities or events that require the deployment of one or more IMATs. This measure is restricted to IMATs that are deployed within the continental United States.
Data Source	IMAT notification and arrival times are tracked by the National Watch Center (NWC) and the NRCC. The NWC maintains this information on a shared drive.
Data Collection Methodology	The teams are notified of deployment and FEMA's NWC documents the notification. Once the team arrives on scene, the team chief contacts the NRCC to update their status in the NWC shared drive. This tool is used during declared disasters and for other emergency incidents or exercises. FEMAs Response staff at HQ extract data from the database related to on-scene arrival times of any (or all) teams deployed to one or more incidents and compares to when teams were notified of deployment for corresponding incidents. This data is analyzed by comparing team arrival times to the times teams were initially notified of deployment. The data is based on the total number of actual real-world or exercise deployments, rather than a specific number of deployments throughout the year.
Reliability Index	Reliable
Explanation of Data Reliability Check	FEMA's National Watch Center (NWC) database is used as the system of record to report and archive data for historical reference. Program personnel review the data after each deployment to ensure accuracy of data entered. Any anomalies are researched against other data records to confirm time of notification.

Performance Measure	Percent of orders 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
Description	This measurement evaluates the percentage of orders from FEMA Distribution Centers or logistics partners that arrive at the specified location by the validated and agreed upon delivery date. Orders include but are not limited to: meals, water, tarps, plastic sheeting cots, blankets, and generators. The measure is derived by dividing the number of orders that are received by the total number requested.
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 orders resulting in a valid order and 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	Orders for disaster assets are entered into LSCMS by supply chain managers at FEMA HQ or regional staff. When shipments are received at designated locations (either FEMA or state sites), the receipt is recorded in LSCMS by FEMA staff (state representatives report data to FEMA). FEMA analysts extract Tier I (life-saving/life-sustaining resources) and Tier II (key operational resources) data from LSCMS: (1) the number of orders arriving by the required delivery date (RDD) and (2) the number of shipments in an order meeting the RDD. Since an order may be comprised of multiple shipments, an order is not considered "complete" until the arrival of all shipments at agreed upon destination by the RDD. For each tier, FEMA staff tabulates the percent of orders arriving by the RDD using both the total number of orders arriving by the RDD and the total number of shipments in an order meeting the RDD.
Reliability Index	Reliable
Explanation of Data Reliability Check	Orders for disaster assets are entered into LSCMS by supply chain managers at FEMA HQ or regional staff at Joint Field Offices or Regional Response Coordination Center. Each Order in LSCMS includes a Destination and Required Delivery Date (RDD) for the material based on the information in the original Request. When initial Required Delivery Date is unattainable because of time, distance or operational conditions, a revised date is negotiated. When Shipments are received at the designated locations the receipt is recorded in the LSCMS system by FEMA staff at the receiving location. If there is a problem with a shipment when received (e.g., wrong material, shortage) the receipt record is "locked" in the LSCMS system until the issue can be researched and resolved by FEMA. The data is verified and validated by federal supply chain managers and State representatives at the receiving location who determine that what in fact was ordered is received accurately and by the agreed upon date.

Performance Measure	Percent of recovery services through Individual Assistance delivered to disaster survivors gauging the quality of program services, supporting infrastructure, and customer satisfaction following a disaster
Program	Recovery
Description	This is a weighted percent that reflects FEMA's role in delivering quality services to disaster survivors. This measure is based upon three categories: program services, supporting infrastructure, and customer satisfaction. Sub-elements within these three categories include providing temporary housing assistance and case management; having available grant management and internet and telephone registration systems; ensuring call centers respond quickly and business staff are in place; and, delivering these services to enhance customer satisfaction of those receiving individual assistance from FEMA following a disaster. Recovery assistance helps individuals affected by disasters and emergencies return to normal quickly and efficiently.
Scope of Data	The scope of this measure is for all federally-declared disasters within the year. Data collected as part of the customer satisfaction sub-element uses a random sample of registered disaster assistance applicants who received assistance within the previous fiscal quarter of all individual disaster applicants who registered with FEMA and received assistance within the previous quarter.
Data Source	Several FEMA-owned data systems and sources are used to provide data for this measure. Data on the eligible applicants provided temporary housing assistance within 60 day of a disaster and the State grant award of Disaster Case

	Management come from the Individual Assistance (IA) Grants Management System. The availability of the IA Grants Management System and Internet and Telephone Registration System availability comes from the Office of the Chief Information Officer Operational Report. Call Center Average Answer Time comes from the Call Center Database. The Recovery Human Capital Report provides data on IA, National Processing Service Center, and the Business Management Division Organizational Fill. Data on the IA Customer Service Satisfaction Survey comes from the National Processing Service Center Survey Team report.
Data Collection Methodology	The Recovery Performance Management Team collects, conducts a peer review, and analyzes all data. Once validated, data are grouped into three categories and weighted for the composite score. Weighting is as follows: program services are 40 percent, supporting infrastructure 35 percent and customer satisfaction 25 percent. Program services are the percent of eligible applicants provided temporary housing assistance within 60 days of a disaster and the awarding of a Disaster Case Management State Grant Award within 120 days of the receipt of a complete application. Supporting infrastructure is the percent of time the Individual Assistance (IA) grants management system is available, the percent of time the internet and phone registration systems are available, the percent of time calls are answered within two minutes for the Call Center, and IA's organizational fill. Customer satisfaction is the percent of people who express satisfaction after receiving an IA grant in the previous quarter.
Reliability Index	Reliable
Explanation of Data Reliability Check	Recovery Business Management Division manually checks the completeness and validity for Output factor data against status reports from the Chief Human Capital, Chief Financial, and Chief Procurement Officers. HQ Recovery Individual Assistance Division checks Preparedness, Awareness, Access, and Action factor data using its IT systems and associated reporting tools, and its Executive Communications Unit (ECU).

Performance Measure	Percent of recovery services through Public Assistance delivered to communities gauging the quality of program services, supporting infrastructure, and customer satisfaction following a disaster
Program	Recovery
Description	This is a weighted percent of how FEMA delivers quality services to communities following a disaster based upon three categories: program services, supporting infrastructure, and customer satisfaction. Sub-elements within these three categories include ensuring timely kickoff meetings following requests for public assistance; having available grant management systems; assuring that business staff are in place; and, delivering these services to enhance customer satisfaction of those receiving public assistance. Supporting and ensuring our citizens have quality support after a disaster is critical to facilitating a community's recovery.
Scope of Data	The scope of this measure is for all federally-declared disasters within United States and territories.
Data Source	Several data sources are used to provide data for this measure. Data for the number of days for the Request for Public Assistance to the kickoff meeting comes from the Emergency Management Mission Integrated Environment (EMMIE). Information on EMMIE availability comes from the Office of the Chief Information Officer Operational Report. Organizational fill information comes from the Recovery Human Capital Report and the Customer Service Satisfaction Survey data comes from the National Processing Service Center Survey Team report.

Data Collection Methodology	All data are collected, recorded, collated, and analyzed by the Recovery Performance Management Team. All data are checked for quality including completeness, potential errors, and by conducting a peer review. Once data are validated, the data is grouped into three categories, and weighted to determine the composite score for the measure. Weighting is as follows: program services are 50 percent, supporting infrastructure is 25 percent, and customer satisfaction is 25 percent. Program services encompass the percent of time that kickoff meetings occur within 60 days of a request for public assistance. Supporting infrastructure encompasses the percent of time that the Public Assistance grants management system (EMMIE) is available and the organizational fill of FEMA's Public Assistance organization. Customer satisfaction information expresses the percent of grantees and sub-grantees who expressed satisfaction after receiving a Public Assistance grant in the previous quarter.
Reliability Index	Reliable
Explanation of Data Reliability Check	The Recovery Performance Management Team manually checks the completeness and validity for Output factor data against status reports from the Chief Human Capital, Chief Financial, and Chief Procurement Officers. HQ Recovery Public Assistance Division checks Preparedness, Awareness, Access, and Action factor data using EMMIE and its associated reporting tools.

Performance Measure	Percent of states and territories with a Threat and Hazard Identification and Risk Assessment (THIRA) that meets current DHS guidance
Program	Preparedness
Description	This measure quantifies the percentage of states and territories that develop a THIRA in accordance with the DHS guidance. The FY 2012 Homeland Security Grant Program (HSGP)/Urban Areas Security Initiative (UASI) grant guidance requires the development and maintenance of a THIRA. Developing and maintaining an understanding of risks faced by communities and the Nation is an essential component of the National Preparedness System. THIRA guidance provides a common and consistent approach for identifying and assessing risks and their associated impacts. This common approach will enable the whole community to maintain a baseline understanding of the risks that they face, facilitating efforts to identify capability and resource gaps, focus capability improvements, and inform the community of actions they can take to manage their risks.
Scope of Data	The scope of this measure includes all 50 states and six territories.
Data Source	Grantees will be required to develop and submit a THIRA to PrepCAST no later than December 31 annually. The regions will review the THIRAs received and submit to headquarters via e-mail verification that the THIRAs meet current guidance; NPAD will be reviewing the results to use in the annual National Preparedness Report (NPR).
Data Collection Methodology	Grantees will be required to develop and submit a THIRA to their FEMA region no later than December 31 annually as part of the FY 2012 Homeland Security Grant Program (HSGP)/Urban Areas Security Initiative (UASI) grant guidance. The regions will review the THIRAs received and submit to headquarters verification that the THIRAs meet current guidance. Headquarters then calculates the percent of states and territories that completed all steps of the THIRA guidance and obtained regional review and verification. As THIRAs are submitted to FEMA at the end of the calendar year, there is a data lag for this measure - the activities occurring during calendar year 2012 will be analyzed during 2013 and will be reported as end of year results at the close of fiscal year 2013.

Reliability Index	Reliable
Explanation of Data Reliability Check	The FEMA Regional Federal Preparedness Coordinators (FPCs) will review all state and territorial THIRA submissions to ensure that the submitted THIRAs meet current DHS guidance.

Performance Measure	Percent of the U.S. population directly covered by FEMA connected radio transmission stations
Program	Protection
Description	This measure tracks the percentage of U.S. residents that will be capable of receiving an emergency alert message from a broadcast station that is connected and enhanced by FEMA to provide resilient, last resort capability for the President to address the American people. Executive Order 13407 requires the Integrated Public Alert Warning System (IPAWS) to implement a capability to alert and warn the American people in all hazards and "to ensure that under all conditions the President can communicate with the American people."
Scope of Data	The population in the Continental United States as well as Alaska, Hawaii, and the 6 U.S. territories.
Data Source	For population data, the source of data in the most recent U.S. Census bureau data. The source of data for radio locations, transmission data, contour maps, frequency propagation tools, and population coverage is provided by the Federal Communications Commission (FCC).
Data Collection Methodology	An accounting of the Continental United States, Hawaii, Alaska, and the 6 U.S. territories population that can receive alert and warning messages directly from an initial delivery system is developed as follows: Service contours for stations participating in the Primary Entry Point (PEP) program are calculated using standard FCC methodology. Reference signal levels follow recommendations of Primary Entry Point Administrative Council (PEPAC): AM signal level: 0.5 mV/m, FCC M3 ground conductivity data; FM signal level 50 dBu, USGS 3 second terrain data. Station power and antenna specifications used were extracted from the FCC's online data resource. Served population is based on the most current US Census data aggregated into one kilometer tiles. The calculation of the population that can receive alert and warning messages is then divided by the total population to determine the percent of the U.S. population directly covered by FEMA connected radio transmission stations.
Reliability Index	Reliable
Explanation of Data Reliability Check	The program office uses standard Federal Communications Commission accepted means and methods to calculate the amount of the population reached. Calculations are verified by a broadcast engineer within the program office.

Performance Measure	Percent of 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 an 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 MS 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	Reduction in the potential cost of natural disasters to communities and their citizens (in billions)
Program	Mitigation
Description	This measure reports the estimated dollar value of losses to the American public which are avoided or averted through a strategic approach of natural hazard risk management.
Scope of Data	This measure includes community information from FEMA's Mitigation Grant Programs and the National Flood Insurance Program (NFIP) that track local initiatives that result in safer communities by reducing the loss of life and property. Data is maintained in real-time and entered by FEMA staff and State partners. Data is current and updated nearly daily. Data is collected and maintained nationwide.
Data Source	The National Emergency Management Information System (NEMIS) and the eGrants system are used to track project grant data. NEMIS is an integrated system that provides FEMA, the states, Native American tribes, and certain other federal agencies with automation to perform disaster response and recovery operations. NEMIS provides users at all regional, headquarters, state, and Disaster Field Office locations with standard processes to support emergency management wherever a disaster occurs. eGrants is a web-based electronic grants system that currently processes applications for FEMA's mitigation grant programs. The Community Information System is used to track NFIP and Community Rating System (CRS) data. The Community Information System is the official record of the NFIP and is a database system that provides information about floodplain management, mapping, and insurance for NFIP participating communities.

Data Collection Methodology	The methodology used to estimate the annual flood losses that are avoided resulting from the National Flood Insurance Programs mitigation requirements are based on estimates of the number of Post-Flood Insurance Rate Map structures in Special Floodplain Hazard Areas, the estimated level of compliance with those requirements, and an estimate of average annual damages that are avoided. Through FEMA grant programs, losses avoided are determined by adding all Federal Share obligations and multiplying by 2 (based on estimated historical average benefit to cost ratio of 2 for projects). All mitigation activities, except for Management Costs/Technical Assistance, are included.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data totals and projections are validated against previously reported data and funding by comparing our current projections against previously reported milestones and FEMA's Integrated Financial Management Information System funding reports.

Federal Law Enforcement Training Centers

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

Performance Measure	Percent of Partner Organizations that agree the Federal Law Enforcement Training Centers training programs address the right skills (e.g., critical

	knowledge, key skills and techniques, attitudes/behaviors) needed for their officers/agents to perform their law enforcement duties
Program	Law Enforcement Training
Description	This performance measure reflects the satisfaction of Partner Organizations that Federal Law Enforcement Training Centers' (FLETC) training programs address the right skills needed for their officers/agents to perform their law enforcement duties such as the prevention of the introduction of high-consequence weapons of mass destruction, terrorism, and other criminal activity against the U.S. and our citizens. The results of the measure provide on-going opportunities for improvements that are incorporated into FLETC training curricula, processes and procedures.
Scope of Data	This measure includes the results from all Partner Organizations (POs) that respond to the Partner Organization Satisfaction Survey Statements 1 and 2, respectively: "The FLETC's basic training programs and courses of instruction address the right skills needed for my officers/agents to perform their law enforcement duties," and "The FLETC's advanced training programs and courses of instruction address the right skills needed for my officers/agents to perform their law enforcement duties." FLETC collaborates with more than 85 Partner Organizations, both internal and external to the Department of Homeland Security.
Data Source	The source of the data is the FLETC Partner Organization Satisfaction Survey administered via a web-based survey program (Vovici), which tabulates and calculates the survey results. The PO representative from each Partner Organization provides responses to the survey through Vovici and saves the responses online when the survey is completed.
Data Collection Methodology	The FLETC POs are surveyed using the PO Satisfaction Survey. Data are collected from mid-May through June. The measure uses an average of survey Statements 1 and 2. Statement 1 begins "The FLETC's basic" and Statement 2 begins "FLETC's advanced." Each statement ends with "training programs and courses of instruction address the right skills needed for my officers/agents to perform their law enforcement duties." The survey uses a modified six-point Likert scale. Program personnel import the survey data as saved by survey respondents from Vovici into the Statistical Package for the Social Sciences to generate descriptive statistics and then into Excel to generate data charts and tables. The percent is calculated as the average of the number of POs that responded "Strongly Agree" or "Agree" to Statements 1 and 2 divided by the number of POs that responded to each of the respective statements. POs that responded "Not Applicable" to either Statement were excluded from the calculations.
Reliability Index	Reliable
Explanation of Data Reliability Check	The survey was developed using contemporary survey methods comparable to those used by the military services and other major training organizations. Following release of the survey summary report, FLETC leaders conduct verbal sessions with Partner Organization key representatives to confirm and discuss their responses. Throughout the year other formal and informal inputs are solicited from the Partner Organization representatives by FLETC staff and used to validate the survey results. No known integrity problems exist.

National Protection and Programs Directorate

Performance Measure	Number of cybersecurity vulnerability and resiliency assessments and self-assessments facilitated by DHS (Retired Measure)
Program	Cybersecurity and Communications
Description	This measure assesses the extent to which DHS is providing onsite cybersecurity vulnerability and resiliency assessments (either onsite or self-assessment) to owners and operators of critical infrastructure across the private sector and State and local government stakeholder communities. This measure is based upon the number of site assessments conducted and the number of tools disseminated for use in self-assessments. Conducting these assessments is critical because critical infrastructure owners and operators have primary responsibility for the security of their information technology systems.
Scope of Data	Results are based on all data collected by the Control Systems Security Program and the Cyber Security Evaluations Program. This data consists of a record of each onsite assessment conducted by these programs and a record of each Cyber Security Evaluation Tool delivered to a requesting party via CD format or downloaded from the US-CERT.gov public-facing website. Onsite assessments include Cyber Resilience Reviews and control systems assessments. Results are based on all data collected by the Control Systems Security Program and the Cyber Security Evaluations Program. This data consists of a record of each onsite assessment conducted by these programs and a record of each Cyber Security Evaluation Tool delivered to a requesting party via CD format or downloaded from the US-CERT.gov public-facing website.
Data Source	A list of the Cyber Resilience Reviews (CRR) conducted is stored in the NPPD/Cyber Security Evaluations SharePoint page on our "CSEP Assessment Tracker." CSEP owns this list and maintains the integrity of the data collected. Control systems site assessments data are maintained in the Control Systems Security Program's event planner (and a separate spreadsheet is maintained at the program's Idaho National Laboratories facility). For CSET tools, the Control Systems Security Program maintains a list of the number of CDs created and the number distributed to critical infrastructure owners, which are stored on the ICS-CERT Assessment Tracker Excel spreadsheet. It also maintains data based on the number of tools downloaded from its public-facing website.
Data Collection Methodology	For CRRs, the CSEP lead facilitator for each individual CRR is responsible for collecting and inputting individual site data into the "CSEP Assessment Tracker." Data for the number of CSETs are recorded based on the number of CDs created and left with or mailed to critical infrastructure owners and the number of tools downloaded from the control systems public-facing website. The number of CSEP and CSETs are then added together to determine the number of cybersecurity site assessments conducted and the number of tools disseminated for use in self-assessments.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data are collected and reviewed by analysts in both the CSSP and CSEP. The total results of the assessments are checked by program leadership and reviewed by the Office of Cybersecurity and Communications.

Performance Measure	Percent of calls made by National Security/Emergency Preparedness users during emergency situations that DHS ensured were connected
Program	Cybersecurity and Communications

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

Performance Measure	Percent of facilities that are likely to integrate vulnerability assessment or survey information into security and resilience enhancements
Program	Infrastructure Protection
Description	This measure demonstrates the percent of facilities that are likely to enhance their security and resilience by integrating Infrastructure Protection vulnerability assessment or survey information. Providing facilities with vulnerability information allows them to understand and reduce risk of the Nation's critical infrastructure.
Scope of Data	The results are based on all available data collected during the fiscal year through vulnerability assessments and Enhanced Critical Infrastructure Protection (ECIP) security surveys. "Security and resilience enhancements" can include changes to physical security, security force, security management, information sharing, protective measures, dependencies, robustness, resourcefulness, recovery, or the implementation of options for consideration.
Data Source	Data from interviews with facilities following vulnerability assessments and surveys are stored in the Infrastructure Survey Tool (IST), which is input into a central Link Encrypted Network System residing on IP Gateway. The Office of Infrastructure Protection owns the final reporting database.
Data Collection Methodology	Infrastructure Protection personnel conduct voluntary vulnerability assessments and ECIP security surveys 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 high risk facilities that receive a facility security assessment in compliance with the Interagency Security Committee (ISC) schedule
Program	Federal Protective Service
Description	This measure reports the percentage of high risk (Facility Security Level 3 & 4) facilities that receive a facility security assessment (FSA) in compliance with the ISC schedule. An FSA is a standardized comprehensive risk assessment that examines credible threats to Federal buildings and the vulnerabilities and consequences associated with those threats. Credible threats include crime activity or potential acts of terrorism. Each facility is assessed against a baseline level of protection and countermeasures are recommended to mitigate the gap identified to the baseline or other credible threats and vulnerabilities unique to a facility. Requirements for the frequency of Federal building security assessments are driven by the ISC standards with high risk facility assessments occurring on a three year cycle.
Scope of Data	The scope of this measure includes all high risk facilities with a security level of 3 or 4.
Data Source	Data is collected in the Modified Infrastructure Survey Tool (MIST) and is owned and maintained by the Federal Protective Service's (FPS's) Risk Management Division (RMD).
Data Collection Methodology	Results from each assessment are collected in MIST by inspectors. At the end of each reporting period, the percent of high risk facilities that receive an FSA is divided by the number of scheduled assessments for that period.
Reliability Index	Reliable
Explanation of Data Reliability Check	FSA results are consolidated and reviewed by FPS's RMD for quality assurance and performance measure reporting.

Performance Measure	Percent of incidents detected by the U.S. Computer Emergency Readiness Team for which targeted agencies are notified within 30 minutes
Program	Cybersecurity and Communications
Description	The United States Computer Emergency Readiness Team (US-CERT) detects malicious cyber activity targeting Federal agencies. This measure assesses the percent of incidents directed at Federal agencies and detected by the US-CERT for which agencies are informed of this malicious activity within 30 minutes. This measure demonstrates the US-CERT's ability to share situational awareness

	of malicious activity with its Federal agency stakeholders through the EINSTEIN intrusion detection systems and other tools.
Scope of Data	The scope of the data includes all federal agency incidents derived by EINSTEIN (1 or 2) recorded in the Incident Management System, Remedy.
Data Source	As incident data are collected from EINSTEIN, they are stored in a HPD Help Desk Remedy Table, a file that is owned by the Office of Cybersecurity and Communications.
Data Collection Methodology	A python script is used to run a MySQL query against the Remedy Table HPD HelpDesk to pull the pertinent data. This data is exported into a .csv file. Then the data are added to the historical data (previously collected) in the .csv file. The results are calculated by taking the difference from the Submit Date and the Report Date for the respective date range (e.g., Q1 of FY12), which is the notification time. Once all the notifications times have been calculated, then the number of all EINSTEIN incidents that US-CERT notified a federal agency in less than or equal to 30 minutes are divided by the total number of EINSTEIN incidents for the respective date range, multiplied by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	The date time stamps stored in the fields Report Date and Submit date are computer generated. The formula is entered into Excel and checked by US-CERT leadership and performance management personnel to ensure quality.

Performance Measure	Percent of known malicious cyber traffic prevented from causing harm at federal agencies
Program	Cybersecurity and Communications
Description	This performance measure assesses the percent of known malicious activity that is mitigated on federal agencies' networks through an active defense capability known as EINSTEIN 3 Accelerated (E3A). This is achieved by actively defending against malicious activity through detection and prevention, and applying countermeasures if needed for protection. This measure assesses the ability of the Department of Homeland Security to defend federal civilian agency networks from cyber threats.
Scope of Data	The scope of the data includes all federal agencies covered by E3A and all incidents derived by E3A recorded in the SourceFire Defense Center Database. This measure covers countermeasures applied through automated mitigation that is performed as designed. This measure excludes discovery signature activity, which is designed to identify potential malicious activity.
Data Source	Detection and countermeasure data are collected and stored in the SourceFire Defense Center database that is owned by United States Computer Emergency Readiness Team Network Analysis.
Data Collection Methodology	On a quarterly basis, data are pulled from the SourceFire Defense Center database and exported into a .csv file. The data from the most recent quarter are added to the previously collected data. The results are calculated with the numerator being the number of indicators that have an associated countermeasure that were applied divided by the denominator of the number of all indicators that alerted. The result is then multiplied by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data is contained in an empirical data source that cannot be manipulated across scale. US-CERT leadership performs quality management to ensure reliability of data entry.

Performance Measure	Percent of organizations that have implemented at least one cybersecurity enhancement after receiving a cybersecurity vulnerability assessment or survey
Program	Cybersecurity and Communications
Description	This measure addresses the extent to which critical infrastructure owners and operators use the results of cybersecurity vulnerability and resiliency assessments to improve their cybersecurity posture. This measure demonstrates the percent of assessed asset owners and operators that are not only developing a better understanding of their cybersecurity posture, but also implementing at least one cybersecurity enhancement to improve that posture.
Scope of Data	Data consists of the results of reviews and assessments of the Cyber Security Evaluation Program (CSEP) and the Control Systems Security Program (CSSP) as well as responses to a feedback form regarding whether the asset owner is planning to, has scheduled, or has implemented any of the options or areas for consideration. Both the CSEP Cyber Resilience Reviews (CRRs) and CSSP assessments using the Cyber Security Evaluation Tool (CSET) are voluntary, as are the feedback forms.
Data Source	Data for CSEP are collected and stored on the CSEP Assessment Tracker, and completed forms are stored on CSEP's SharePoint site. CSET information is kept in an Excel spreadsheet, called the "ICS-CERT Assessment Tracker."
Data Collection Methodology	The Control Systems Security Program and the Cyber Security Evaluation Program reach out to each assessed asset owner and operator 180 days after completing the CSET assessment or CRR to ask whether any cybersecurity enhancements were implemented since the date of the assessment. Analysts from the CSSP and CSEP programs store the associated data in the ICS-CERT Assessment Tracker and the CSEP Assessment Tracker, respectively. The measure result will be calculated by dividing the number of those asset owners and operators who indicate the implementation of at least one enhancement by the total number of onsite assessments conducted and for which a feedback form was received.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data is collected in the ordinary course of operations for both the Control Systems Security Program and the Cyber Security Evaluation Program. Results are reported to the Office of Cybersecurity and Communications, which will also review the data sources.

Performance Measure	Percent of performance standards implemented by the highest risk chemical facilities and verified by DHS
Program	Infrastructure Protection
Description	This measure reports the percent of applicable risk based performance standards (RBPS) that are approved and implemented within site security plans (SSPs) or alternative security programs (ASPs) for Tier 1 and Tier 2 facilities that are compliant with the Chemical Facility Anti-terrorism Standards (CFATS) regulation. Following submission of a proposed SSP/ASP by a covered facility, the CFATS regulatory authority will conduct an "authorization inspection" of the covered facility to verify that the SSP/ASP is compliant with the CFATS regulation. For this measure, SSPs/ASPs determined to meet the RBPS requirements with current and planned measures will be approved. Upon approval of its SSP/ASP, the covered facility is required to fully implement the existing measures that are described in the SSP/ASP.
Scope of Data	The scope of this data includes all of the chemical facilities that have been given a risk based classification of Tier 1 or 2. The number of facilities identified as Tier 1 or 2 changes over time.

Data Source	Reported data are the resulting summaries from queries against internal systems and are stored in the Chemical Security Assessment Tools Suite (CSATs). CSATs is used to provide facility identification and registration, to identify facilities that meet the Department's criteria for high risk chemical facilities, and store the methodologies to record and initially evaluate security vulnerability assessments (SVAs) and to create and store respective site security plans (SSPs) and alternate security programs (ASPs). CSATs is a secure web-based system.
Data Collection Methodology	High-risk chemical facilities provide originating source data via the CSATs system. Infrastructure Security Compliance Division (ISCD) HQ staff and inspection cadre posts added information and status to the CSATs system that includes Chemical Security Evaluation and Compliance System (CHEMSEC) applications as a course of normal operations. The success percentage for this measure will be based upon: the number of approved RBPS measures of Tier 1 and Tier 2 regulated facilities that have been implemented (existing and planned with past completion dates). This number does not include those planned RBPS with future completion dates. This number is then divided by the total number of applicable RBPS measures for facilities receiving a final tiering letter (tiers 1-2 inclusive) (TRBPSFTL). Formula: Approved and Implemented RBPS (Tiers 1 and 2) ÷ TRBPSFTL (Tier 1 + Tier 2) = %. Additional details on the calculation methodology are available in ISCD's GPRA Measure Guidance.
Reliability Index	Reliable
Explanation of Data Reliability Check	The accuracy of data captured and reported via the CSATs system is validated during the Systems Engineering Life Cycle (SELC) phases (deployment readiness and testing). Information is reviewed by Infrastructure Security Compliance Division Director/Deputy Director, leadership at the Office of Infrastructure Protection, and NPPD leadership.

Performance Measure	Percent of respondents indicating that operational cybersecurity information products provided by DHS are timely and actionable
Program	Cybersecurity and Communications
Description	This measure assesses whether the products that the DHS National Cybersecurity and Communications Integration Center (NCCIC) provides are timely and actionable for its customers. The NCCIC will follow up with cyber customers, to whom information products were provided, in order to determine the timeliness and effectiveness of those products. A customer survey will be used to acquire data on areas such as usefulness, timeliness, actionable nature, and relevance.
Scope of Data	This measure is limited to customer feedback from a stakeholder survey covering the Office of Cybersecurity and Communications' National Cybersecurity and Communications Integration Center (NCCIC) operational information products.
Data Source	The data source for this performance measure is a stakeholder survey disseminated and completed in connection with NCCIC information products. The surveys contain the standard Departmental question intended to elicit the degree of customer satisfaction with the usefulness of the product as well as its timeliness, actionable nature and relevance. The questions asks customers to rate satisfaction on a five-point rating scale (very satisfied, somewhat satisfied, neither satisfied nor dissatisfied, somewhat dissatisfied, very dissatisfied). Responses "very satisfied" and "somewhat satisfied" will be considered to have met the criteria for "satisfactory." NPPD will aggregate the results obtained based on the survey metadata, and maintain the results in the CS&C Enterprise Performance Management Office. The spreadsheet will contain several elements, including the unique product identifier, date disseminated, date survey results received, and score for each question.

Data Collection Methodology	CS&C Enterprise Performance Management Office (EPMO) will make available a customer satisfaction survey in connection with its information products. Two questions are used to collect data for this measure: "Was this product timely?" and "Was this product actionable?" Responses are weighted and the answers to the question will be divided by the total number of points possible based on responses received. A third question will be included in the survey to identify respondents for whom the product's information is not applicable (i.e. the product addresses a vulnerability in an application or operating system that a given respondent does not use). The denominator will be adjusted to account for stakeholders who self-identify with the population for whom the product is not applicable. In addition to collecting feedback through disseminated surveys, a sample of NCCIC stakeholders will be interviewed each quarter during customer feedback sessions, which will include the use of the survey.
Reliability Index	Reliable
Explanation of Data Reliability Check	Survey responses will be collected and maintained by CS&C Enterprise Performance Management Office (EPMO) and shared with relevant CS&C divisions and programs, including the NCCIC, in the ordinary course of business. Data will be validated by program manager reviews in relevant divisions and programs and by the EPMO Performance Management branch.

Performance Measure	Percent of tenants satisfied with the level of security provided at federal facilities
Program	Federal Protective Service
Description	This measure assesses the effectiveness of security services provided by the Federal Protective Service (FPS) to the Government Services Agency (GSA) tenants through the use of a formal customer satisfaction survey. FPS uses the feedback from this survey to identify opportunities for improvement in the security services provided to its customers.
Scope of Data	GSA distributes the Public Building Service (PBS) tenant satisfaction survey on an annual basis. This web-based survey is distributed throughout the 11 GSA regions to gauge the level of effectiveness of FPS and contract guard security services.
Data Source	The source of the data for this measure is GSA's PBS web based survey.
Data Collection Methodology	Using the data from the PBS survey, FPS records the level of satisfaction regarding security services provided in an Excel spreadsheet. These data are averaged to derive the results of this measure These results are analyzed at the Headquarters level and then submitted to FPS leadership.
Reliability Index	Reliable
Explanation of Data Reliability Check	FPS uses the Public Building Survey (PBS) data provided by GSA. In this case this is third party information. The program has reviewed GSA's process and has determined there is sufficient oversight of data quality by GSA.

Performance Measure	Percent of traffic monitored for cyber intrusions at civilian Federal Executive Branch agencies
Program	Cybersecurity and Communications
Description	This measure assesses DHS's scope of coverage for malicious activity across those non-DOD Chief Financial Officers (CFO) Act and Trusted Internet Connection Access Provider (TICAP) Federal Executive Branch civilian agency networks. Federal Executive branch network monitoring uses EINSTEIN 2 intrusion detection system sensors, which are deployed to Trusted Internet Connections locations at agencies or Internet Service Providers. These sensors capture network flow information and provide alerts when signatures, indicative of malicious activity, are triggered by inbound or outbound traffic. The federal

	government's situational awareness of malicious activity across its systems will increase as more networks are monitored and the methodology will require data normalization to account for the addition of large numbers of networks.
Scope of Data	The measure includes the non-DOD CFO Act agencies and the TICAP Federal Executive Branch civilian agencies. Percentage is determined by compiling and averaging estimates provided by the Departments and Agencies (D/As) of percent of total traffic monitored on their respective networks. The individual percentages are currently reported to OMB.
Data Source	From data reported to NCSD from the agencies.
Data Collection Methodology	For TICAP locations with operational sensors: Once EINSTEIN installations are successfully tested (including a formal Installation Test & Checkout Review) notification is provided to the respective program managers. The number of installations is tracked and published by NCPS program managers. For D/As percentage of traffic monitored (consolidated): Each TICAP Agency currently tracks and reports the estimated percent of traffic consolidated (monitored) to DHS on a yearly basis. DHS also tracks each CFO Act Agency that obtains EINSTEIN 2 coverage through an Internet Service Provider. EINSTEIN is already fully deployed and operational at each Internet Service Provider. Tracking for these agencies is binary--the information provided to DHS indicates either 100% consolidation through the ISP or 0% consolidation. DHS reports TICAP and non-TICAP CFO Act agency information to OMB on an individual D/A basis.
Reliability Index	Reliable
Explanation of Data Reliability Check	The completion of EINSTEIN installations are validated by the respective program managers during the review process. The percentage of traffic consolidated (monitored) is a best-effort estimate provided by the respective D/As to DHS and OMB.

Performance Measure	Percent of urban area interoperable communications capabilities that are rated at the most advanced levels (Retired Measure)
Program	Cybersecurity and Communications
Description	This measure reports the percent of four capabilities targeted by the Office of Emergency Communications (OEC) in the 60 urban area security initiative (UASI) regions as of 2008 that are rated as "established" or "advanced." The ratings are based on the SAFECOM Interoperability Continuum, which provides a maturity model for jurisdictions to track progress in strengthening interoperable communications. Per the National Emergency Communications Plan, OEC has prioritized four capabilities that are necessary to ensure interoperable communications in an area: governance, standard operating procedures, usage, and training and exercises. Through statewide interoperability coordinators, urban areas assess their capabilities based on clearly defined criteria from the continuum.
Scope of Data	The 60 urban area security initiative (UASI) regions as of 2008.
Data Source	Through statewide interoperability coordinators, urban areas assess their capabilities based on clearly defined criteria from the continuum. Information is captured on a standard form and provided to OEC.
Data Collection Methodology	Once data is received, it is compiled by OEC and provided to the Office of Cybersecurity and Communications' (CS&C) Enterprise Performance Management Office to evaluate the results. The percent of urban area interoperable communications capabilities that are rated at the most advanced levels is calculated by dividing the number of UASIs that are rated as

	"established" or "advanced" by the number of UASIs.
Reliability Index	Unreliable
Explanation of Data Reliability Check	The personnel in OEC who compile the performance results are independent of the OEC personnel who collect the data. CS&C Enterprise Performance Management Office receives the performance results on an annual basis and maintains a standard operating procedure to check performance results against underlying data sources.

Science and Technology Directorate

Performance Measure	Percent of Apex technologies or knowledge products transitioned to customers for planned improvements in the Homeland Security Enterprise (New Measure)
Program	Research, Development, and Innovation
Description	This measure gauges the transition of high priority, and high value research and development projects known as Apex projects. Apex technologies and knowledge products are quickly delivered to improve homeland security operations. Apex products consist of cross-cutting, multi-disciplinary efforts which employ 3 to 5 year innovation cycles from project inception through operational testing.
Scope of Data	This measure encompasses the Apex technology or knowledge products determined prior to the beginning of the fiscal year. A successful transition is considered to be the ownership and operation of a technology or knowledge product by a customer within the Homeland Security Enterprise.
Data Source	The system of record is the quarterly data call spreadsheet submitted to the Homeland Security Advanced Research Projects Agency (HSAPRA) front office by the S&T Performance Team through the ExecSec Process. This spreadsheet is completed by the HSARPA front office and provided back to the S&T Performance Team for maintenance.
Data Collection Methodology	The status of each Apex technology or knowledge product is gathered from the individual divisions within HSARPA from a variety of sources including final reports, test or pilot results collected during trials, and various reviews (technology reviews and portfolio reviews) where senior leadership is briefed on end results, metrics, current status, go/no go decisions, as well as milestone success. This information is captured in a quarterly data call spreadsheet (as defined above) and the exact percent of Apex projects transitioned is divided by the total number of planned Apex technologies transitions within the Fiscal Year and multiplied by 100.
Reliability Index	Reliable
Explanation of Data Reliability Check	Following the collection and analysis of data by program managers, the Director of HSARPA reviews the data to ensure accuracy and consistency. The Science and Technology Finance and Budget Division provides a third data reliability review before results are finalized.

Performance Measure	Percent of planned cyber security products and services transitioned to government, commercial and open sources
Program	Research, Development, and Innovation
Description	This measure reflects the percent of identified and completed planned transitions of cybersecurity products and/or services (e.g. technologies, tools, capabilities, standards, knowledge products) within Science & Technology Directorate's

	Cyber Security Division projects to government, commercial or open sources. The percent reported is reviewed using the number of planned transition milestones stated in the Cyber Security Division's budget execution plan for the fiscal year, and the explanation that is provided in each quarterly performance data call. The Program identifies funds and coordinates cyber security research and development resulting in deployable security solutions. These solutions include user identity and data privacy technologies, end system security, research infrastructure, law enforcement forensic capabilities, secure protocols, software assurance, and cybersecurity education.
Scope of Data	This measure includes identified project transition milestones for each Fiscal Year as reported as part of the Future Year Homeland Security Program (FYHSP) Milestones and Performance Measures. A "transition" includes a variety of items including completion/delivery of a developed tool or capability, release of a knowledge product, publication of standards, demonstration of a capability and so forth. During Q4 of each Fiscal Year, the Cyber Security Division (CSD) works with the S&T Performance Team to identify expected transition milestones for the upcoming Fiscal Year. Once defined, that number serves as the baseline denominator for the measure for the given Fiscal Year.
Data Source	The source of the data is the individual project schedules and planning documents maintained by each Program Manager and their Systems Engineering and Technical Assistance Support Contractor. Program Reviews (such as the S&T Portfolio Review and Homeland Security Advanced Research Projects Agency (HSARPA) Tech Reviews) also identify planned completion dates for project milestones, including transitions, and are maintained on the CSD SharePoint site.
Data Collection Methodology	The status of planned transition milestones are reviewed following the completion of each Fiscal Year quarter per request of the S&T Performance Team who send out quarterly performance data calls for the FYHSP Milestones. The CSD Front Office requests feedback from the applicable Program Managers during these data calls, and the Program Managers indicate whether the milestone has been met or is still on-going. If on-going and the milestone is still likely to be met, Program Managers provide the expected quarter of completion within the subject fiscal year. If a milestone will not be met during the given fiscal year, the Program Manager provides details as to why not (such as development delays, budget delays, and so forth).
Reliability Index	Reliable
Explanation of Data Reliability Check	The results for this measure are checked against program project records, and HSARPA/S&T review of the analysis behind the measure results.

Performance Measure	Percent of projects that involve outside collaboration with DHS components, other government agencies, the private sector, universities and international offices to advance cybersecurity research efforts (Retired Measure)
Program	Research, Development, and Innovation
Description	This measure reflects the amount of collaboration between DHS Science and Technology (S&T) and external partners on cybersecurity projects. This measure includes outside collaboration with DHS components, other government agencies, private sector, universities, and international offices, for both user coordination and strengthening the performance and quality of research efforts (examples: Working Groups, shared policy documents, teaming exercises, etc.). Collaboration for these purposes is defined as entering into an agreement between an individual or group within S&T CSD and an external collaborator; both parties must have approval by an individual that has designated authority to execute a

	contract or obligate resources on behalf of the party. This may include, but is not limited to: a signed artifact (MOU, MOA, IA, email, etc.); leveraging shared resources such as personnel, facilities, and funding; or a combination of these items.
Scope of Data	All Phase II and III research projects and programs efforts will be included in developing this measure (CSD groups its research into Phase I/II/III, with Phase II and then III research addressing the most advanced technology readiness levels and associated with intended users). The data will be both quantitative and qualitative, i.e. absolute numbers of projects/programs and user/collaboration organizations, the existence of collaboration documentation, and several judgments of the quality of the collaboration, where multiple individuals will provide input as to quality through a limited Delphi approach.
Data Source	The source of the data is a project-level planning and programming records repository housed on the S&T Directorates share drive. The repository reflects the most recent status of information gathered from the program managers on a quarterly basis. Its purpose is to provide ready access to individual and aggregate project data for reporting, planning, status reviews and analysis. The program will use project and program/project review documentation as the reference material to develop an annual "collaboration analysis paper," where the numbers and nature of projects are listed and discussed, collaboration efforts are similarly listed and discussed, and analytical explanation and justification for the determination of the final qualitative measure of collaboration will be provided.
Data Collection Methodology	The percent reported is reviewed using the number of projects stated in the program's budget plan for the fiscal year, and the explanation that is provided in each quarterly performance data call. Project managers update the planning/programming data on at least a quarterly basis from project status reports provided by performers that can be objectively corroborated by artifacts such as signed documents, financial responsibility shared, resources provided in the form of personnel or facilities, and joint ownership of intended outcomes for projects (agreements between S&T and the intended partner, customer, end-user, etc.)
Reliability Index	Reliable
Explanation of Data Reliability Check	The results for this measure is checked against Cyber Security Division (CSD) program and project records, and Homeland Security Advanced Research Projects Agency (HSARPA)/S&T and collaborator organization review of the analysis behind the measure results.

Transportation Security Administration

Performance Measure	Average number of days for DHS Traveler Redress Inquiry Program (TRIP) redress requests to be closed
Program	Intermodal Screening Operations
Description	This measure describes the average number of days for the processing of traveler redress requests, excluding the time DHS waits for the traveler to submit all required documents. DHS TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs or crossing U.S. borders. DHS TRIP is part of an effort by the Departments of State and Homeland Security to welcome legitimate travelers while securing our country from those who want to do us harm.

Scope of Data	Results are based on a sampling of 15% of closed cases for each month. The sampling does not include requests pending because of insufficient data received from the complainant.
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.
Data Collection Methodology	Redress program specialists pull data weekly from RMS and convert the data to MS Excel using an automated program. Data is then sorted by month. Specialists pull a 15% sampling of current month closed cases and then subtract days the case was pending because of incomplete traveler data to arrive at the average processing time. Reports are sent monthly to TSA and DHS senior management.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data is auto generated from the Redress Management System and a second redress program specialist double checks the work of the first specialist. Testing requirements are reported to TSA senior leadership quarterly via the Management Control Objective Plan.

Performance Measure	Number of daily travelers eligible to receive expedited physical screening based on assessed low risk
Program	Intermodal Screening Operations
Description	This measure describes the average number of daily travelers eligible to receive expedited physical screening based on assessed low risk. This low risk is established by focusing on risk-based, intelligence-driven security procedures and enhancing use of technology. Increases in this measure will strengthen aviation security while enhancing the passenger experience.
Scope of Data	Quarterly reporting is based on the daily average of passengers eligible to receive expedited screening based on assessed low risk either through TSA Pre?™, Known crewmember (KCM), Managed Inclusion or some other form of expedited screening process.
Data Source	TSA's Performance Management Information System (PMIS) and Secure Flight
Data Collection Methodology	Data on eligible for expedited screening is generated within Secure Flight. 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 individual 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.
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 air cargo screened on commercial passenger flights originating from the United States and territories
Program	Intermodal Screening Operations
Description	This measure captures the percent of air cargo screened on commercial passenger flights originating from the United States and territories. Screening methods approved in the Certified Cargo Screening Program include: physical search (includes opening boxes, removing and opening all inner cartons), X-ray, explosives trace detection, explosives detection system, canine teams, and the use of other approved detection equipment. The air cargo screening strategy uses a multi-layered, risk-based approach to securing air cargo by permitting indirect air carriers, shippers, and other entities further up the supply chain to screen cargo closer to its point of origin through the Certified Cargo Screening Program and allow air carriers to accept pre-screened certified cargo.
Scope of Data	The scope of this data includes all cargo shipped on commercial passenger flights originating from all U.S. airports. Excluded from this measure are all general aviation passenger flights. Screening reporting is a compilation of master air waybills (MAWB) and pounds of cargo by air carriers at each airport. Data collected on total weight and MAWB numbers include cargo subject to alternative security measures.
Data Source	The data to support this measure is submitted via email or through a website from regulated air carriers and Certified Cargo Screening Facilities in the Certified Cargo Screening Program, to include indirect air carriers, shippers, and other entities further up the supply chain screening cargo for uplift on domestic passenger flights. The Air Cargo Security Division collects, reviews, verifies, and compiles this data in a Cargo Reporting Database.
Data Collection Methodology	Air carriers operating domestically report data electronically each month pursuant to their security programs on the amount of cargo screened at each airport for the total number of Master Air Waybills (MAWBs) and pounds screened to include sensitive cargo subject to alternative security measures. Indirect air carriers, shippers, and other entities screening cargo for uplift on domestic originating passenger flights as Certified Cargo Screening Facilities in the Certified Cargo Screening Program also report cargo screening data pursuant to their program requirements. Total weight and MAWB numbers include cargo subject to alternative security measures. This data is collected from regulated entities and analyzed each month to determine the amount of cargo screened at each screening facility.
Reliability Index	Reliable
Explanation of Data Reliability Check	The Office of Security Operations randomly evaluates the regulated entities submissions to determine the extent of cargo compliance with the current program requirements and regulations issues. Data is routinely analyzed, and issues are addressed through communication and outreach to the carriers, compliance monitoring, and issuing revised guidance to clarify the accounting for cargo screened and transported on passenger aircraft. The program is considering utilizing an automated cargo reporting tool to enhance data quality.

Performance Measure	Percent of air carriers operating from domestic airports in compliance with leading security indicators
Program	Intermodal Assessments and Enforcement
Description	This measure identifies air carrier compliance for U.S. flagged aircraft operating domestically with leading security indicators. These critical indicators are derived from security laws, rules, regulations, and standards. A leading security indicator is a key indicator that may be predictive of the overall security posture

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

Performance Measure	Percent of domestic air enplanements vetted against the terrorist watch list through Secure Flight
Program	Intermodal Screening Operations
Description	The Secure Flight program compares domestic passenger information to the No Fly and Selectee List components of the Terrorist Screening Database (TSDB), which contains the Government's consolidated terrorist watch list, maintained by the Terrorist Screening Center. The No Fly and Selectee Lists are based on all the records in the TSDB, and represent the subset of names who meet the criteria of the No Fly and Selectee designations. Secure Flight will also match data against additional subsets of the TSDB as determined by Department and Agency leadership. This is a unified approach to watch list matching for covered passenger flights, to avoid unnecessary duplication of watch list matching efforts and resources and reduce the burden on aircraft operators.
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	Data source is the Secure Flight Reports Management System (RMS). This system provides daily statistics including the number of enplanements vetted against the terrorist watch lists.
Data Collection Methodology	TSA requires covered aircraft operators to collect information from passengers, transmit passenger information to TSA for watch list matching purposes, and process passengers in accordance with TSA boarding pass printing results regarding watch list matching results. Covered aircraft operators must transmit to TSA the information provided by the passenger in response to the request described above.
Reliability Index	Reliable
Explanation of Data Reliability Check	Vetting analysts review a report (produced daily) by the Secure Flight Reports Management System (RMS). RMS provides the number of enplanements by U.S. aircraft operator and the estimated number of U.S. aircraft operator enplanements covered by the Secure Flight Final Rule for that year. A Secure Flight vetting analyst forwards the data to Secure Flight leadership for review. Secure Flight

	forwards the data to Transportation Threat Assessment and Credentialing management, TSA senior leadership team (SLT), as well as the DHS SLT. It is also distributed to the TSA Office of Intelligence, Transportation Sector Network Management, and the Office of Global Strategies.

Performance Measure	Percent of foreign airports that serve as last points of departure and air carriers involved in international operations to the United States advised of necessary actions to mitigate identified vulnerabilities in order to ensure compliance with critical security measures
Program	Intermodal Assessments and Enforcement
Description	This index combines: (1) percent of foreign airports serving as Last Point of Departure (LPD) to the U.S. notified of critical vulnerabilities and accompanying recommendations, and (2) percent of foreign air carriers operating flights from these foreign airports and U.S. air carriers operating from any foreign airport regardless of destination notified of violations of critical regulations and accompanying recommendations/follow-up action. TSA evaluates/documents security at foreign airports with service to U.S., airports from which U.S. air carriers operate, and other sites on a 5-point scale against critical International Civil Aviation Organization (ICAO) aviation and airport security standards. TSA assess compliance with these standards and provides feedback to the host governments for awareness and recommended follow-up action. Identifying and notifying air carriers of non-compliance with critical regulations mitigates air carrier vulnerabilities and reduces risk.
Scope of Data	Airport assessments reflect information collected by Transportation Security Specialists during evaluation of implementation of ICAO aviation security standards at LPD foreign airports with direct service to the U.S. and those airports from which U.S. air carriers operate, regardless of destination. Attention focuses on critical standards across 5 categories: Aircraft & Inflight Security, Passenger & Cabin Bag Screening, Hold Baggage Security, Cargo/Catering Security, and Access Control. Assessement is done using a risk informed approach that includes threat, vulnerability, and consequence ratings: low-risk airports every 3 years; medium-risk airports every 2 years; high-risk airports yearly.
Data Source	The data to support foreign airport assessments is contained in Foreign Airport Assessment Program (FAAP) reports prepared by Transportation Security Specialists (TSSs) following each airport assessment. Completed reports are submitted by the TSSs in Regional Operation Centers (ROCs) to the ROC Managers and stored in a database maintained by the Office of Global Strategies (OGS). Each FAAP report contains data and observations collected during the assessment and highlights any shortfalls in security. Air carrier inspection results are maintained in TSA's Performance and Results Information System (PARIS), which serves as the official data repository for TSA's regulatory activities. The OGS and PARIS databases also store accompanying information indicating that notification of shortfalls was provided to the host government and air carriers following airports assessments and air carrier inspections.
Data Collection Methodology	A standard template is used for collecting/reporting data on airport assessments. Vulnerability ratings are assigned by Global Compliance leadership to ensure consistent application of the ratings from 1 (no shortfalls) through 5 (instances of egregious non-compliance). Results are entered into the OGS database at TSA headquarters. The measure is calculated by OGS headquarters staff who identify airports receiving notification of vulnerability scores of 4 or 5 in any of the critical ICAO standards. Compliance inspections for air carriers are performed according to an annual work plan specifying frequencies/targets for inspection

	based on criteria established by OGS including risk methodology. Inspection results are entered into PARIS and are used to calculate the data. OGS headquarters staff identify notification/follow-up action with air carriers in question. The index averages the percentage of airports and air carriers notified of non-compliance with leading security indicators.
Reliability Index	Reliable
Explanation of Data Reliability Check	TSSs submit a comprehensive airport assessment report to ROC Managers. Reports are reviewed for quality and consistency and forwarded through senior leadership in Global Compliance to the Assistant Administrator, OGS, for final approval. This process may result in inquiries to a TSA Representative or the TSS for clarifying information. Analysis for strengths and weaknesses, consistency or divergence from other airports, trends, and smart practices also occurs from these reviews. Results are maintained for each assessed airport as well as consolidated into a report of overall security posture of the airports relative to the ICAO standards. Results are also shared with the foreign airport and host government to determine next steps and proposed areas of cooperation and assistance. Data reliability for air carrier assessments is ensured through system record tracking audit trails and spot audit checks followed by a management review and validation process at the headquarters level.

Performance Measure	Percent of inbound air cargo screened on international passenger flights originating from outside the United States and Territories
Program	Intermodal Screening Operations
Description	This measure captures the amount of inbound air cargo screened from last point of departure countries on commercial passenger flights originating from outside the United States and Territories. Screening is defined as a physical examination or non-intrusive methods of assessing whether cargo poses a threat to transportation security. Methods of screening include x-ray systems, explosives detection systems, explosives trace detection, explosives detection canine teams certified by the Transportation Security Administration, or a physical search together with manifest verification, or additional methods approved by the TSA Administrator, pursuant to Section 1602 of Public Law 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007.
Scope of Data	The scope of this data includes all inbound air cargo on commercial passenger flights originating outside the United States and Territories. Screening data is a compilation of the cargo volume screened and transported by air carriers from each international Last Point of Departure (LPD) airport.
Data Source	The data to support this measure is submitted via email or through a website from regulated air carriers screening cargo for uplift from international departure points into the United States. The Air Cargo Security Division collects, reviews, verifies, and compiles this data in a Cargo Reporting Database.
Data Collection Methodology	Passenger air carriers operating inbound flights to the U.S. report data electronically each month pursuant to their security programs on the amount of cargo screened at each last point of departure (LPD) airport. This data is collected from regulated entities and analyzed each month to determine the amount of cargo screened based on current security requirements. Transportation Sector Network Management Air Cargo then generates quarterly reports on passenger air cargo screening performance.
Reliability Index	Reliable
Explanation of Data Reliability Check	TSA evaluates the regulated entities submissions to determine the extent of cargo compliance with the current program requirements and regulations issued. Data is routinely analyzed, and issues are addressed through communication and

	outreach to the carriers, compliance monitoring, and guidance to clarify the accounting for cargo screened and transported on passenger aircraft.

Performance Measure	Percent of international air enplanements vetted against the terrorist watch list through Secure Flight
Program	Intermodal Screening Operations
Description	The Secure Flight program compares international passenger information to the No Fly and Selectee List components of the Terrorist Screening Database (TSDB), which contains the Government's consolidated terrorist watch list, maintained by the Terrorist Screening Center. The No Fly and Selectee Lists are based on all the records in the TSDB, and represent the subset of names who meet the criteria of the No Fly and Selectee designations. Secure Flight will also match data against additional subsets of the TSDB as determined by Department and Agency leadership This is a unified approach to watch list matching for covered passenger flights, to avoid unnecessary duplication of watch list matching efforts and resources and reduce the burden on aircraft operators.
Scope of Data	This measure relates to all flights conducted by a covered foreign air carrier arriving in or departing from the United States, or overflying the continental United States, defined as the lower contiguous 48 states, that are required to have a security program under 49 CFR 1546.101(a) or (b). These aircraft operators generally are the passenger airlines that offer scheduled and public charter flights from commercial airports.
Data Source	Data source is the Secure Flight Reports Management System (RMS). This system provides daily statistics including the number of enplanements vetted against the terrorist watch lists.
Data Collection Methodology	TSA requires covered aircraft operators to collect information from passengers, transmit passenger information to TSA for watch list matching purposes, and process passengers in accordance with TSA boarding pass printing results regarding watch list matching results. Covered aircraft operators must transmit to TSA the information provided by the passenger in response to the request described above.
Reliability Index	Reliable
Explanation of Data Reliability Check	Vetting analysts review a report (produced daily) by the Secure Flight Reports Management System (RMS). RMS provides the number of enplanements by foreign air carrier, as well as the estimated number of foreign air carrier enplanements covered by the Secure Flight Final Rule for that year. A Secure Flight vetting analyst forwards the data to Secure Flight leadership for review. Secure Flight forwards the data to Transportation Threat Assessment and Credentialing management, TSA senior leadership team (SLT), as well as the DHS SLT. It is also distributed to Office of Intelligence, Transportation Sector Network Management, and the Office of Global Strategies.

Performance Measure	Percent of overall compliance of domestic airports with established aviation security indicators
Program	Intermodal Assessments 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	Intermodal Assessments and Enforcement
Description	This measure provides the rate of implementation by mass transit, light and passenger rail, bus, and other commuter transportation agencies with established security standards and practices related to six critical Security Action Items (SAIs). These six SAIs are key indicators of the overall security posture of a mass transit and passenger rail transportation system. Measuring implementation of these six SAIs assesses transit vulnerabilities and is part of an overall risk reduction process.
Scope of Data	The scope of the data is limited to the largest mass transit and passenger rail systems based on passenger volume (average weekday ridership > 60,000) that have agreed to participate in the Baseline Assessment for Security Enhancement (BASE) program. BASE assessments are completed jointly by a team of Transportation Security Inspectors and participating mass transit and passenger rail systems. The BASE program assesses whether comprehensive Security and Emergency Management Action Items that are critical to an effective security program, including security plans, training, exercises, public awareness, and other security areas, are in place.
Data Source	The source of the data is the assessments completed by a team of Transportation Security Inspectors and transit agencies. Transportation Security Inspectors document assessment results by placing the information in a central database on the TSA computer system, which is analyzed by staff members at Headquarters.

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

U.S. Citizenship and Immigration Services

Performance Measure	Average of processing cycle time (in months) for adjustment of status to permanent resident applications (I-485)
Program	Adjudication Services
Description	An I-485, Application to Register for Permanent Residence or Adjust Status, is filed by an individual to apply for permanent residence in the United States or to adjust their current status. This measure assesses the program's ability to meet its published processing time goals by reporting on the volume of pending applications and petitions by Center or Field Office. The Cycle Time, reflected in months (e.g. 4.0 months), measures only the pending volume in Active Pending status, deducting from Gross Pending the total volume of cases subject to customer-induced delays and Department of State visa availability, categorized as Active Suspense.
Scope of Data	This measure represents the volume in Active Pending status of I-485 applications. Applications are classified in an Active Suspense category if a visa number is not available or if the case is awaiting additional evidence from the customer. Active Suspense cases are not included in this measure. Active Suspense categories include: Pending Request for Evidence or Intent to Deny/Revoke; Visa Unavailable. Additionally, the measure only includes the aggregate of I-485 Adjustment based on eligibility from Employment, Family, certain Cuban nationals and All Other. It excludes I-485 Adjustment based on Refugee, Asylee, or Indochinese Status, which are categories that have discrete

	cycle times.
Data Source	Offices self-report performance metrics (e.g. case counts) to the Office of Performance & Quality (OPQ) through the Performance Reporting Tool (PRT).
Data Collection Methodology	On a monthly basis, USCIS collects performance data on I-485 applications received, completed, and pending through the PRT. Field Offices and Services Centers report receipt volumes, case completion totals, and labor hours to the PRT, which calculates the end-of-month pending totals. This data is then used to calculate the average cycle time, expressed in months relative to the volume of applications/petitions in Active Pending status.
Reliability Index	Reliable
Explanation of Data Reliability Check	OPQ conducts monthly quality control reviews of the data reported to ensure data integrity. Data and performance reports are published in both preliminary and final stages, allowing OPQ/PMB an opportunity to vet data anomalies with the reporting entities.

Performance Measure	Average of processing cycle time (in months) for naturalization applications (N-400)
Program	Adjudication Services
Description	An N-400, Application for Naturalization, is filed by an individual applying to become a United States citizen. This measure assesses the program's ability to meet its published processing time goals by reporting on the volume of pending applications by Center or Field Office. The Cycle Time, reflected in months (e.g. 5.0 months), measures only the pending volume in Active Pending status, deducting from Gross Pending the total volume of cases subject to customer-induced delays, categorized as Active Suspense.
Scope of Data	This measure represents the volume in Active Pending status of N-400 applications. Applications are classified in an Active Suspense category if the applicant has failed the English/Civics requirement and is waiting the statutory period between testing attempts, if the applicant has requested rescheduling of the required interview, or if the case is awaiting additional evidence from the customer. Active Suspense cases are not included in this measure. Active Suspense categories include: Pending Request for Evidence or Intent to Deny/Revoke and Pending Re-exam as requested by the customer. The measure excludes naturalization applications based on eligibility from service in the Armed Forces of the United States, which has a discrete cycle time.
Data Source	Offices self-report performance metrics (e.g. case counts) to the Office of Performance & Quality (OPQ) through the Performance Reporting Tool (PRT).
Data Collection Methodology	On a monthly basis, USCIS collects performance data on N-400 applications received, completed, and pending through the Performance Reporting Tool (PRT). Field Offices and Services Centers report receipt volumes, case completion totals, and labor hours to the PRT, which calculates the end-of-month pending totals. This data is then used to calculate the average cycle time, expressed in months relative to the volume of applications in Active Pending status.
Reliability Index	Reliable
Explanation of Data Reliability Check	The USCIS Office of Performance & Quality, Performance Management Branch (PMB), conducts monthly quality control reviews of the data reported to ensure data integrity. Data and performance reports are published in both preliminary and final stages, allowing OPQ/PMB an opportunity to vet data anomalies with the reporting entities.

Performance Measure	Overall customer service rating of the immigration process
Program	Information and Customer Service
Description	This measure gauges the overall rating of the immigration process and is based on the results from the following areas: 1) Accuracy of information; 2) Responsiveness to customer inquiries; 3) Accessibility to information; and 4) Customer satisfaction.
Scope of Data	Using the telephone number, the National Customer Service Center (NCSC) captures the telephone numbers of incoming calls and the level of service reached by each call. The data is then downloaded into a master file, resulting in a database with approximately 120,000 phone numbers. Duplicate phone numbers and calls with duration of less than one minute are eliminated. The data is then randomized using a query which randomly assigns different values to each record and sorts the records by value. The first 5,000 records are selected. The telephone number data is retrieved for the week preceding the execution of the phone survey so that the target population is contacted for the survey within approximately one week of having called the NCSC 800-Line to capture the customers' most recent experience.
Data Source	U.S. Citizenship and Immigration Services (USCIS) uses four sources to determine the results of this measure. First, USCIS controlled anonymous call approach to determine the accuracy of information provided by the call centers. Second, responsiveness to customer inquiries is determined from an analysis of abandoned calls to the call center (calls that have been put on hold and then abandoned by the customer). Third, USCIS conducts an analysis of web portal activity to determine accessibility to information. Last, customer satisfaction is determined by conducting surveys of those seeking information about the immigration process to determine their satisfaction with the information provided by USCIS.
Data Collection Methodology	On a quarterly basis, the results of these four sources of information are combined on an equal basis to determine the overall service rating.
Reliability Index	Reliable
Explanation of Data Reliability Check	The Independent Contractor submits the survey results to Program Manager for review, comment, and approval.

Performance Measure	Percent of initial mismatches for authorized workers that are later determined to be "Employment Authorized"
Program	Immigration Status Verification
Description	This measure assesses the accuracy of the E-verify process by assessing the percent of employment verification requests that are not positively resolved at time of initial review.
Scope of Data	The percentage of all E-Verify queries that are issued Tentative Non-Confirmations and are successfully contested as work authorized.
Data Source	Verification Information System (VIS) transaction data.
Data Collection Methodology	The data are recorded by the Verification Division's VIS system and collected through standard quarterly reports. When an inquiry is made, if a prospective employee disagrees with the information, USCIS begins the process of checking the reliability of the information. If the initial information obtained is incorrect, and it is determined that the employee is designated employment authorized, this result is recorded in the VIS. Quarterly, USCIS runs a report to determine the number of mismatches that were corrected and is then used to calculate the percent of mismatches that were later determined to be employment authorized.
Reliability Index	Reliable
Explanation of Data	E-Verify transaction data are extracted quarterly from the VIS by the contractor

Reliability Check	that manages VIS. An algorithm is then applied to the data to remove all duplicate and invalid queries. The data are referred to the USCIS Verification Division for review and clearance.

Performance Measure	Percent of non-immigrant worker (H1-B) site visits where potential fraud or other technical noncompliance concerns were identified
Program	Immigration Security and Integrity
Description	This measure reflects how many H1-B fraud incidents have been discovered by the Administrative Site Visit Verification Program (ASVVP). This information begins the process to identify and counter systematic vulnerabilities that exist in our immigration system.
Scope of Data	Data will reflect all Fraud Detection and National Security Data System (FDNS-DS) ASVVP records that relate to H1-B worker site visits performed and completed (with a site inspection report and a Statement of Findings attached) during the fiscal year.
Data Source	Data will be drawn from the FDNS-DS by FDNS Headquarters. Calculations (to determine the percentage of fraud findings among all records) will be performed by FDNS Headquarters analysts.
Data Collection Methodology	Result will reflect the number of FDNS-DS H1-B cases identifiable as ASVVP cases where a Statement of Findings indicates Fraud, as a percentage of all ASVVP H1-B cases where a Statement of Findings exists.
Reliability Index	Reliable
Explanation of Data Reliability Check	Primarily, the data will be validated by contract and government analysts familiar with FDNS-DS and methodologies employed to extract data from that system. Data will be further validated by FDNS Fraud Detection Branch personnel who are familiar with the ASVVP operation and can verify that results reflect operational expectations.

Performance Measure	Percent of religious worker site visits where potential fraud or other technical noncompliance concerns were identified
Program	Immigration Security and Integrity
Description	This measure reflects how many religious worker fraud incidents have been discovered as part of the Administrative Site Visit Verification Program (ASVVP). This information begins the process to identify and counter systematic vulnerabilities exist in our immigration system.
Scope of Data	Data will reflect all Fraud Detection and National Security Data System (FDNS-DS) ASVVP records that relate to religious worker site visits performed and completed (with a site inspection report and a Statement of Findings attached) during the fiscal year.
Data Source	Data will be drawn from the FDNS-DS by FDNS Headquarters. Calculations (to determine the percentage of fraud findings among all records) will be performed by FDNS Headquarters analysts.
Data Collection Methodology	Result will reflect the number of FDNS-DS religious worker cases identifiable as ASVVP cases where a Statement of Findings indicates Fraud, as a percentage of all ASVVP religious worker cases where a Statement of Findings exists.
Reliability Index	Reliable
Explanation of Data Reliability Check	Primarily, the data will be validated by contract and government analysts familiar with FDNS-DS and methodologies employed to extract data from that system. Data will be further validated by FDNS Fraud Detection Branch personnel who are familiar with the ASVVP operation and can verify that results reflect operational expectations.

Performance Measure	Percent of students enrolled in classes under the Citizenship and Integration Grant Program that show educational gains (New Measure)
Program	Citizenship
Description	This measure reports on the success of grant recipients to increase knowledge of English necessary for students receiving services under the program to pass the naturalization test. Under the Citizenship and Integration Grant Program, grant recipients are required to use a nationally normed standardized test of English language proficiency for student placement and assessment of progress. This measure evaluates the percentage of students receiving these services who demonstrate an increase in score
Scope of Data	This measure will draw on cumulative English language proficiency test results for Q1-Q3 of the fiscal year. The measure will only include results from students who receive services from a grant recipient and were pre- and post-tested.
Data Source	The data source is the OoC Database Management Tool owned by the Office of Citizenship and is located on the USCIS Enterprise Collaboration Network (ECN). The measure will be tracked using quarterly grant recipient performance reports submitted in MS Excel format. For each permanent resident who receives citizenship instruction and/or naturalization application services under the grant program, each grant recipient must provide information on the services actually provided, including dates of enrollment in citizenship class and pre and post-test scores. These reports are submitted quarterly within 30 days of the conclusion of each quarter. The data contained in each quarterly report is then reviewed, uploaded into the data source, and analyzed by Office of Citizenship program officers.
Data Collection Methodology	Grant recipients complete and submit quarterly reports via email within 30 days of the end of each quarter. The calculation is the total number of students who were pre and post-tested and who scored higher on the post-test divided by the total number of students who were pre and post-tested through Q3.
Reliability Index	Reliable
Explanation of Data Reliability Check	The reliability of this measure will be established through uniform data collection and reporting procedures, ongoing follow-up with grant recipients on information included in the quarterly reports, and through onsite monitoring visits, as necessary. All grant recipients will receive training at the beginning of the performance period on how to complete the quarterly report forms. The Office of Citizenship will provide written feedback on each quarterly report, and will ask grant recipients for clarification if there are questions about information in the reports. The Office of Citizenship will annually conduct onsite monitoring visits to approximately one-third of all new grant recipients. During these visits, program staff members review records (e.g. student intake forms, classroom attendance sheets, student assessment scores, copies of filed Form N-400s, etc.) that were used to compile data for the quarterly reports.

U.S. Coast Guard

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

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

Performance Measure	Fishing regulation compliance rate
Program	Maritime Law Enforcement
Description	The U.S. Coast Guard uses the percentage of fishing vessels observed at sea complying with domestic regulations as a measure of the Coast Guard's activities and their impact on the health and well-being of U.S. fisheries and marine protected species. This specific measure reflects the percent of boardings at sea by the U.S. Coast Guard during which no significant violations of domestic fisheries regulations are detected.
Scope of Data	This measure addresses compliance in and around domestic fisheries. Most inspections take place on U.S. commercial fishing vessels inside the U.S. Exclusive Economic Zone (EEZ), but the measure also includes inspections of (a) U.S. commercial and recreational fishing vessels outside the U.S. EEZ, (b) foreign fishing vessels permitted inside the U.S. EEZ, (c) recreational fishing vessels in the U.S. EEZ, and (d) U.S. commercial and recreational fishing vessels inside the portion of state waters that extends from three to nine nautical miles seaward of the boundary line.
Data Source	Boardings and violations are documented by U.S. Coast Guard Report of Boarding Forms and entered into the Marine Information for Safety and Law Enforcement (MISLE) database.
Data Collection Methodology	U.S. Coast Guard units enter their enforcement data directly into the MISLE database after completion of fisheries enforcement boardings. Each year a compliance rate is calculated for the data quality. This is determined by dividing the total number of Living Marine Resources boardings without a significant number of violations by the total number of Living Marine Resources boardings
Reliability Index	Reliable
Explanation of Data	The program manager reviews entries into MISLE database monthly and

Reliability Check	compares to other sources of information (i.e., after-action reports, message traffic, etc.) to assess reliability of the database. District, Area, and Headquarters law enforcement staffs review, validate, and assess the data on a quarterly basis as part of the Law Enforcement Planning and Assessment System.

Performance Measure	Five-year average number of commercial and recreational boating deaths and injuries (Retired Measure)
Program	Maritime Prevention
Description	This measure reports the sum of the five-year average numbers of reportable commercial mariner, commercial passenger, and recreational boating deaths and injuries. It is an indicator of the long-term trend of the Maritime Prevention Program's impact on marine safety. 45 CFR 4.05-1 requires the owner, agent, master, operator, or person in charge to notify the U.S. Coast Guard of any loss of life or injury that requires professional medical treatment beyond first aid. 33 CFR 173.55 requires the operator of a vessel that is used for recreational purposes or is required to be numbered, to file a Boating Accident Report when a person dies; or is injured and requires medical treatment beyond first aid; or disappears from the vessel under circumstances that indicate death or injury as a result of an occurrence that involves the vessel or its equipment.
Scope of Data	This measure reports the sum of the five-year average numbers of reportable commercial mariner, commercial passenger, and recreational boating deaths and injuries. Passenger deaths and injuries include casualties from passenger vessels operating in U.S. waters; deaths, disappearances, or injuries associated with diving activities are excluded. Commercial mariner deaths and injuries include casualties of crewmembers or employees aboard U.S. commercial vessels in U.S. waters. For recreational boating deaths and injuries, only casualties recorded in the BARD database are counted. Boating fatalities include deaths and disappearances caused or contributed to by a vessel, its equipment, or its appendages.
Data Source	Mariner and passenger casualties are recorded in the Marine Information for Safety and Law Enforcement (MISLE) database and recreational boating casualties are recorded in the Boating Accident Report Database (BARD) database.
Data Collection Methodology	This measure is a roll up measure of three data sets. To obtain commercial mariner and passenger deaths and injuries, 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). To obtain recreational boating deaths and injuries, only casualties recorded in the BARD database are counted. Boating fatalities include deaths and disappearances caused or contributed to by a vessel, its equipment, or its appendages. The five-year average for a given year is calculated by taking the average of the deaths and injuries for the most recent five 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 effected 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 effected through regular review of records by the Coast Guard Office of Investigations and Analysis. To ensure all fatal boating accidents are captured, the U.S. Coast Guard crosschecks BARD data with incidents reported in MISLE and with boating casualty media announcements or articles provided by a news clipping service. A one-percent under-reporting factor is added to boating casualty statistics.

Performance Measure	Migrant Interdiction Effectiveness in the Maritime Environment (New Measure)
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 detected incursions of foreign fishing vessels violating U.S. waters
Program	Maritime Law Enforcement
Description	This measure is the number of detected illegal fishing incursions into the U.S. Exclusive Economic Zone (EEZ). Incursions detected by both the U.S. Coast Guard and other sources are included when the reports are judged by operational commanders as being of sufficient validity to order resources to respond.
Scope of Data	This measure includes incursions of foreign fishing vessels detected by the U.S. Coast Guard or other sources that results in either: 1) significant damage or

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

Performance Measure	Percent of people in imminent danger saved in the maritime environment
Program	Maritime Response
Description	This is a measure of the percent of people who were in imminent danger on the oceans and other waterways and whose lives were saved by U.S Coast Guard. The number of lives lost before and after the U.S Coast Guard is notified and the number of persons missing at the end of search operations are factored into this percentage. Several factors hinder successful response including untimely distress notification to the U.S Coast Guard, incorrect distress site location reporting, severe weather conditions at the distress site, and distance to the scene.
Scope of Data	One hundred percent of the maritime distress incidents reported to the U.S. Coast Guard are collected in the Marine Information for Safety and Law Enforcement (MISLE) database. The scope is narrowed to include only cases where there was a positive data element in the field lives saved, lives lost before notification, lives lost after notification, or lives unaccounted for. The scope of this data is further narrowed by excluding any case reports with eleven or more lives saved and/or lost in a single incident. Data accuracy is limited by two the rescuer's subjective interpretation of the policy criteria for the data point lives saved (for instance, was the life saved or simply assisted).
Data Source	The data source is the U.S. Coast Guard's MISLE database.
Data Collection Methodology	Operational units input Search and Rescue data directly into the MISLE database. Program review and analysis occurs at the Districts, Area, and Headquarters levels. First, one hundred percent of the maritime distress incidents reported to the U.S. Coast Guard are collected in the MISLE database. Then, these reports are narrowed to include only cases where there was a positive data element in the fields lives saved, lives lost before notification, lives lost after notification, or

	lives unaccounted for. The scope of this data is further narrowed by excluding any case reports with eleven or more lives saved and/or lost in a single incident, which would overweight and mask other trends. After the data is properly scoped, the percentage of people in imminent danger saved in the maritime environment is calculated by dividing the number of people saved by the total number of people in imminent danger.
Reliability Index	Reliable
Explanation of Data Reliability Check	Checks on data input are made by individual case owners during the case documentation processes. Data is reviewed by the SAR Mission Coordinator either at the District or Sector level. This review occurs when cases are validated during a Search and Rescue case and after a case is concluded when the case is reviewed by individuals formally charged with that review. Data is also verified quarterly by the Headquarters program manager via data extraction and checks for anomalies within the data. The database includes built-in prompts to check questionable data.

Performance Measure	Security compliance rate for high risk maritime facilities
Program	Maritime Prevention
Description	This measure is a leading indicator of maritime facility security and resiliency in our nation's ports. Compliance of high risk (Maritime Transportation Security Act (MTSA)) facilities is determined based upon finding a major problem during an inspection, requiring a notice of violation or civil penalty. MTSA facilities are a high risk subset of the national waterfront facility population given the nature of their activities and/or the products they handle; which pose a greater risk for significant loss of life, environmental damage, or economic disruption if attacked. This subset is approximately 3,100 facilities. The Coast Guard completes one scheduled and one unscheduled inspection on each facility annually. This measure provides insight into resiliency by verifying MTSA facilities maintain proper access safeguards and exercise approved plans/procedures to prevent and react to security emergencies; making them better suited to resist, adapt, and recover to adversity or disruption.
Scope of Data	MTSA facilities are a high risk subset of the entire national waterfront facility population given the nature of their activities and/or the products they handle; which pose a greater risk for significant loss of life, environmental damage, or economic disruption if attacked. MTSA regulation applies to facilities that: handle dangerous cargoes, liquid natural gas, or transfer oil or hazardous materials in bulk; or receive vessels that: carry more than 150 passengers, are foreign cargo vessels greater than 100 gross tons, or are U.S. cargo vessels greater than 100 gross tons carrying dangerous cargoes as prescribed by Federal Regulations. This does not apply to facilities that have a waiver or exemption including facilities that: are U.S. military, do not store minimum established amounts of dangerous cargoes, are shipyards, or are deemed public access facilities. This measure includes the results from annual Coast Guard security inspections conducted on all MTSA-regulated facilities
Data Source	The data source is Marine Information for Safety and Law Enforcement database (MISLE).
Data Collection Methodology	Results of MTSA compliance examinations and security spot checks are entered into the Marine Information for Safety and Law Enforcement database. Data is collected centrally by a HQ-level office responsible for compliance. The percent is calculated by dividing the number of MTSA facilities who did not receive a notice of violation and/or civil penalty by the total number of MTSA facilities inspected.

Reliability Index	Reliable
Explanation of Data Reliability Check	There is no material inadequacy in the data, i.e., those that significantly impede the use of program performance data by agency managers and government decision makers.

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

U.S. Customs and Border Protection

Performance Measure	Amount of smuggled outbound currency seized at the ports of entry (in millions)
Program	Securing and Expediting Travel
Description	This measure provides the total dollar amount of all currency in millions seized during outbound inspection of exiting passengers and vehicles, both privately-

	owned and commercial. The scope of this measure covers both the southwest and northern borders and includes all modes of transportation, (land, air, and sea).
Scope of Data	All outbound-related currency seizures are included in this measure. This covers both the southwest and northern borders and includes all modes (land, air, and sea).
Data Source	All currency seizures are entered into the Seized Assets and Case Tracking System (SEACATS) which is a subsystem of TECS, the principal system of record used by CBP. Currency seizures information is accessed in report format through the BorderStat reporting tool.
Data Collection Methodology	All CBP officers effecting outbound currency seizures enter seizure data into TECS via the Seized Assets and Case Tracking System (SEACATS) subsystem, using the proper codes to denote the seizure was made at exit during outbound operations. The SEACATS subsystem analyzes all seizure data and extracts currency seized data for the different categories of currency violations.
Reliability Index	Reliable
Explanation of Data Reliability Check	CBP Officers enter information into TECS for each currency seizure performed. A first line supervisor must review the information and approve it before it can be extracted and included in daily, monthly, and annual reporting. A validation check is also conducted when the data is extracted from TECS and reported via BorderStat.

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

Performance Measure	Percent of cargo by value imported to the U.S. by participants in CBP trade partnership programs
Program	Securing and Expediting Trade

Description	This measure describes the percent of all cargo that is imported from CBP trade partnership programs based on the value compared to total value of all imports. Partnership programs include both Customs-Trade Partnership Against Terrorism (C-TPAT) and Importer Self-Assessment (ISA). CBP works with the trade community through these voluntary public-private partnership programs, wherein some members of the trade community adopt tighter security measures throughout their international supply chain and in return are afforded benefits. A variety of trade actors are included in these partnership programs, such as importers, carriers, brokers, consolidators/third party logistic providers, Marine Port Authority and Terminal Operators, and foreign manufacturers.
Scope of Data	This measure includes all cargo and is a comparison of the value of cargo that is imported from trade partnership programs to the total value of all imports
Data Source	Data is extracted from the Automated Targeting System (ATS) and the Automated Commercial Environment (ACE).
Data Collection Methodology	Importers, or brokers acting on their behalf, submit data electronically, which is captured by the Automated Commercial System (ACS). The Office of International Trade (OT) pulls this data from their systems of record (ACS and the Automated Commercial Environment (ACE)) once a month. After the line value data is extracted, the measure is calculated by dividing the import value associated with ISA or C-TPAT importers by the total value of all imports.
Reliability Index	Reliable
Explanation of Data Reliability Check	Monthly internal monitoring of process and data quality issues is conducted at both the field level and HQ level. As part of our analytical process, the data used for this measure is compared to other known reliable data sets and measures.

Performance Measure	Percent of detected conventional aircraft incursions resolved along all borders of the United States
Program	Securing America's Borders
Description	The measure represents the percent of conventional aircraft, once detected visually or by radar that are suspected of illegal cross border activity and are brought to a successful law enforcement resolution. In some cases, Office of Air and Marine (OAM) assets are launched to interdict the aircraft. In most cases, resolution of the aircraft identity is made by the Air and Marine Operations Center (AMOC) working with interagency partners such as the Federal Aviation Administration (FAA). If the incursion is deemed legal, OAM considers the incursion resolved. If not resolved, AMOC working with our partners including OAM assets - could not identify the target and is thus considered illegal.
Scope of Data	The scope of this measure includes all potential identified air space incursions by conventional aircraft along all borders of the United States.
Data Source	The data source for this measure is TECS, maintained by Customs and Border Protection and Immigration and Customs Enforcement.
Data Collection Methodology	Airspace incursions are identified by the Air and Marine Operations Center. Once identified, this information is transmitted to the closest air branch for air support. The results are then entered into the TECS and the Air and Marine Operations Report systems, and tallies of all incursions are summarized on a monthly basis.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data is routinely reconciled by a comparison of information in the systems manually by contractor and program staff on a monthly and/or quarterly basis.

Performance Measure	Percent of import revenue successfully collected
Program	Securing and Expediting Trade
Description	This measure estimates the collected duties, taxes, and fees (called net undercollection of revenue) expressed as a percent of all collectable revenue due from commercial imports to the United States directed by trade laws, regulations, and agreements. The total collectable revenue is total collected revenue plus the estimated net undercollected revenue based on trade violations. The revenue gap is a calculation of uncollected duties (the difference between estimated undercollection and overpayment) based on statistical sampling.
Scope of Data	This measure is part of the annual Trade Compliance Measurement (TCM) program. The program involves taking a statistical sample (about 65,000 import entry lines) from a given population of imports. This population covers consumption and Anti-Dumping/Countervailing Duty (AD/CVD) entry types, excluding informal entries. This data will be produced monthly, aggregated year-to-date, and then presented as an annual figure.
Data Source	The Automated Commercial System (ACS) is the source until 2/14/2010. After 2/14/2010, the targeting feature of the program resides in the Automated Targeting System (ATS) with User Defined Rules (UDR) and the review findings are recorded in the Automated Commercial Environment (ACE) using the Validation Activity (VA) functionality.
Data Collection Methodology	At the start of each fiscal year, an analysis of import data is conducted to help design a statistical survey program, which is implemented with User Defined Rules (UDR) in the Automated Targeting System (ATS). Entry Summary line transactions are identified by ATS which opens a Validation Activity in ACE. Each Field Office must review the identified entry summary line transaction for compliance and record the findings with a Validation Activity Determination (VAD). VAD data is extracted monthly by HQ analysts and statistics are compiled monthly and annually by the resident statistician within the Trade Analysis and Measures Division.
Reliability Index	Reliable
Explanation of Data Reliability Check	Monthly internal monitoring of process and data quality issues are conducted at both the field level and HQ level. This is treated as a shared responsibility of both HQ and field locations, where multiple levels of checks are conducted, and any found problems are quickly addressed. HQ also hosts quarterly conference calls with field locations to openly discuss these issues, and provides reports to field locations when remediation action is needed. This oversight is documented and provided as evidence of program control to outside independent auditors each year.

Performance Measure	Percent of imports compliant with U.S. trade laws
Program	Securing and Expediting Trade
Description	This measure reports the percent of imports that are compliant with U.S. trade laws including customs revenue laws. Ensuring that all imports are compliant and free of major discrepancies allows for lawful trade into the U.S.
Scope of Data	The measure is part of the annual Trade Compliance Measurement (TCM) program. The program involves taking a statistical sample (about 65,000 import entry lines) from a given population of imports. This MTD measure covers the population consumption and Anti-dumping and Countervailing Duty entry types, excluding informal entries. Recorded discrepancies are considered to be significant or major as they have additional conditions on the value of imports, amount of revenue loss, etc. For example, a discrepancy in value with a revenue loss greater than $1,000, a clerical error that results a revenue loss greater than

	$1,000, an IPR violation, and a country of origin discrepancy with value greater than 33rd percentile or revenue loss greater than $1,000.
Data Source	Data resides in the Automated Targeting System (ATS) with User Defined Rules (UDR) and the review findings are recorded in the Automated Commercial Environment (ACE) using the Validation Activity (VA) functionality. Data from before 2/14/2010 resided in the Automated Commercial System (ACS).
Data Collection Methodology	At the start of each fiscal year, based on previous year imports risk, volume, value, and compliance history a stratified random sampling methodology is used to select import entries summary lines, which is implemented with User Defined Rules (UDR) in the Automated Targeting System (ATS). Entry Summary line transactions are identified by ATS which opens a Validation Activity in ACE. Each Field Office must review the identified entry summary line transaction for compliance and record the findings with a Validation Activity Determination (VAD). VAD data is extracted monthly by HQ analysts and statistics are compiled monthly and annually by the resident statistician within the Trade Analysis and Measures Division.
Reliability Index	Reliable
Explanation of Data Reliability Check	Monthly internal monitoring of process and data quality issues are conducted at both the field level and HQ level. This is treated as a shared responsibility of both HQ and field locations, where multiple levels of checks are conducted, and any found problems are quickly addressed. HQ also hosts quarterly conference calls with field locations to openly discuss these issues, and provides reports to field locations when remediation action is needed. This oversight is documented and provided as evidence of program control to outside independent auditors each year.

Performance Measure	Percent of inbound cargo identified by CBP as potentially high-risk that is assessed or scanned prior to departure or at arrival at a U.S. port of entry
Program	Intelligence and Targeting
Description	This measure gauges the percent of international cargo coming to the United States via air, land, and sea identified as potentially high-risk using the Automated Targeting System (ATS) that is assessed or scanned prior to lading or at arrival at a U.S. port of entry. Assessing, resolving, and when necessary scanning potentially high-risk cargo prior to lading or at arrival at the ports of entry ensures the safety of the U.S. public and minimizes the impact to the trade through the effective use of risk-focused targeting.
Scope of Data	For FY 2012 Q3 and Q4 reporting, this measure includes cargo in the sea and air environment destined for a U.S. port of entry. Land cargo will be included in this measure beginning in FY 2013. Cargo is identified as potentially high-risk by CBP's Automated Targeting System (ATS) using a risk-focused security index scoring algorithm. Shipments are flagged as potentially high-risk if they have an ATS security index score of 190 or above on either bill or entry. The National Targeting Center - Cargo works with the Targeting and Analysis Systems Program Office (TASPO), Office of Information Technology to determine the final status of all identified potentially high-risk cargo.
Data Source	CBP's Automated Targeting System (ATS) contains the requisite data to determine the total amount of cargo that was scored 190 or above by either bill or entry. The ATS 4 module (CERTS) contains the data used to determine the disposition of the cargo that was flagged as potentially high-risk by ATS.
Data Collection Methodology	Electronic manifest data is provided to CBP by shippers and brokers and loaded into CBP's Automated Targeting System (ATS) database. The ATS screening algorithms are applied to this data and the results are provided electronically to

	the Cargo Enforcement Reporting and Tracking System (CERTS), including entry status data for all modes of cargo identified as high-risk. Based on this information, the percent of cargo reviewed, scanned, and resolved is calculated by taking all cargo shipments with a score of 190 or above that have been reviewed/examined/mitigated (determined from CERTS) and dividing this by the total number of cargo shipments with a score of 190 or above.
Reliability Index	Reliable
Explanation of Data Reliability Check	CBP Officers review and examine the Automated Targeting System (ATS) information on potentially high-risk cargo, resolve or mitigate security concerns, determine those cases where further examination is required, and record the findings of this review/examination process in the ATS 4 (CERTS) module, annotating all methods and tools they required to complete the examination. For land border ports of entry, they also enter findings into the Automated Commercial Environment (ACE) system, which is mandatory for land ports to allow the truck and cargo to be released from CBP. Supervisors periodically extract high threat examination findings data from the CERTS module for review and validation of the data entered by CBP Officers. Anomalies in the findings data are identified and immediate corrective actions are taken to ensure data integrity.

Performance Measure	Percent of people apprehended multiple times along the Southwest border
Program	Securing America's Borders
Description	This measure examines the percent of deportable individuals who have been apprehended multiple times by the U.S. Border Patrol. This measure calculates the number of people apprehended multiple times divided by the total number of apprehensions of people during a fiscal year. Effective and efficient application of consequences for illegal border crossers will, over time, reduce overall recidivism.
Scope of Data	All apprehensions of deportable illegal aliens apprehended that have or receive a Fingerprint Identification Number (FIN) within the nine sectors of the Southwest Border within the defined time period of the reporting year are used in calculating the denominator of this measure. The numerator of the calculation includes a count of the number of apprehensions of the same person (with FIN) more than one time that occurred in the same defined time period. Fingerprints are not taken and FINs are not generated for individuals under age 14, over age 86, and for some humanitarian cases; but, these individuals compose the approximately 2% of the population which is not included in the scope of this measure.
Data Source	This data is captured by Border Patrol agents at the station level, where apprehension data is entered into the e3 Processing system. All data entered via e3 Processing 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 unit. The physical database is owned and maintained by Immigrations and Customs Enforcement's (ICE) Office of Chief Information Officer (OCIO).
Data Collection Methodology	Apprehension data is entered into the e3 Processing application by Border Patrol Agents at the Station level. Data input can be made by the apprehending agent, or by another agent who obtains details concerning the apprehension from the apprehending agent. The e3 Processing application continuously updates the Enforcement Integrated Database with the apprehension data. This data can be reviewed at the station, sector, or Headquarters level in a variety of reporting formats. Calculation of this measure is as follows: The number of Unique Subjects (with FIN) that have been apprehended multiple times within a specified

	time period and geographic parameter, divided by the total number of Unique subjects (with FIN) apprehended during the same time period and geographic parameter.
Reliability Index	Reliable
Explanation of Data Reliability Check	All apprehension data entered into e3 Processing is subject to review by supervisors at multiple levels. Data reliability tools are built into the system; for example, data input not conforming to appropriate expectations for each cell is flagged for re-entry. The Enforcement Integrated Database continuously updates to compile all apprehension data. This data can then be extracted into summary reports, and these summaries are available for review and analysis at station, sector, and Headquarters levels. At the Headquarters level, the Statistics and Data Integrity Unit conducts monthly Data Quality reports as well as weekly miscellaneous checks. When discrepancies are found, they are referred back to the apprehending Sector/Station for review and correction.

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

	have occurred, such as foot sign, sensor activations, interviews with apprehended subjects, camera views, communication between and among stations and sectors, and other information. Data input into the BPETS1 system occurs at the station level. The e3 Processing application and BPETS1 are used continuously to document apprehension, GA, and TB data. Calculation of the measure is done by the HQ SDI Unit and is: (Apprehensions + TB)/Total Entries. Total entries are the sum of Apprehensions, TBs, and GAs.
Reliability Index	Reliable
Explanation of Data Reliability Check	Patrol Agents in Charge ensure all agents are aware of and utilize proper definitions for apprehensions, GAs and TBs at their respective stations. They also ensure the necessary communication takes place between and among sectors and stations to ensure accurate documentation of subjects who may have crossed more than one station's area of responsibility. In addition to station level safeguards, the HQ Statistics and Data Integrity (SDI) Unit validates data integrity by utilizing various data quality reports. Data issues are corrected at the headquarters level, or forwarded to the original inputting station for correction. All statistical information requested from within DHS, USBP, or external sources are routed through the centralized HQ office within USBP. The SDI Unit coordinates with these entities to ensure accurate data analysis and output.

U.S. Immigration and Customs Enforcement

Performance Measure	Average length of stay in detention of all convicted criminal aliens prior to removal from the United States (in days)
Program	Enforcement and Removal Operations (ERO)
Description	This measure provides an indicator of efficiencies achieved in working to drive down the average length of stay for convicted criminals in ICE's detention facilities. Decreases in the average length of stay can significantly reduce the overall costs associated with maintaining an alien population prior to removal.
Scope of Data	The scope of this measure includes all criminal aliens who were detained within ICE's detention facilities or while in ICE custody in federal, state, and local jails during the fiscal year awaiting due process.
Data Source	Data is maintained in the Alien Removal Module of the ENFORCE database. This database is maintained at headquarters and the data entry occurs at Enforcement and Removal Operations (ERO) Field Offices throughout the country. Tools in the Integrated Decision Support System are used to query the Alien Removal Module and produce reports to calculate the final results for this measure.
Data Collection Methodology	ERO field offices are responsible for the entry and maintenance of data regarding the removal/return of illegal aliens. Officers track the status of administrative processes and/or court cases and indicate when actual removals occur in the Alien Removal Module of the ENFORCE database. When an alien is removed/returned from the United States, case officers in the field will indicate the case disposition and date the removal/return occurred in the database. Reports generated from the Alien Removal Module are used to determine the total number of illegal aliens removed/returned from the country during the specified time.
Reliability Index	Reliable
Explanation of Data Reliability Check	Headquarters staff validate the completeness and accuracy of the data entered by field offices into the Alien Removal Module through trend analysis to look for aberrations and unusual patterns. Data is analyzed on a weekly basis and

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

Performance Measure	Number of convicted criminal aliens removed per fiscal year
Program	Enforcement and Removal Operations (ERO)
Description	This measure includes removals from the U.S. under any types of removal order as well as voluntary returns of immigration violators to their country of origin. This measure reflects the full impact of program activities to ensure that criminal aliens identified in the country, that are amenable to removal do not remain in the U.S. (statistical tracking note: Measure equals the case status with a departure date within the fiscal year, filtered by criminality and exiting ERO Criminal Alien Program codes.)
Scope of Data	Total number of criminal removals and returns defined by case category 0,3,9 - Returns and case category 6,8,X-Returns. The term 'Returns' include Voluntary Returns, Voluntary Departures and Withdrawals under Docket Control.
Data Source	Data is maintained in the Alien Removal Module of the ENFORCE database. This database is maintained at headquarters and the data entry occurs at Enforcement and Removal Operations (ERO) Field Offices throughout the country. Tools in the Integrated Decision Support System are used to query the Alien Removal Module and produce reports to calculate the final results for this measure.
Data Collection Methodology	Enforcement and Removals Operations field offices are responsible for the entry and maintenance of data regarding the removal/return of illegal aliens. Officers track the status of administrative processes and/or court cases and indicate when actual removals occur in the Alien Removal Module of the ENFORCE database. When an alien is removed/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. Reports generated from the Alien Removal Module are used to determine the total number of illegal aliens removed/returned from the country during the specified time.
Reliability Index	Reliable
Explanation of Data Reliability Check	Headquarters staff validate the completeness and accuracy of the data entered by field offices into the Alien Removal Module through trend analysis to look for aberrations and unusual patterns. Data is analyzed on a weekly basis and compared to statistics from prior months and the previous year. An additional reliability check occurs when data is cross-referenced between field office detention facility reports of the number of removals, and data entered into the database. The Statistical Tracking unit checks for consistency of the results or measuring instrument through validation, back-end testing or reproducibility of the data through alternative methodology.Depending upon the degree of consistency between two measures of the same measure allows the statistician to determine whether the data is considered reliable and or stable. Any inaccuracies will need to be sent to the Unit Chief, who will make the necessary corrections to the tasking query.

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

Performance Measure	Percent of detention facilities found in compliance with the national detention standards by receiving an acceptable inspection rating
Program	Enforcement and Removal Operations (ERO)
Description	This measure gauges the percent of detention facilities that have received an overall rating of acceptable or above within the Enforcement and Removal Operations (ERO) National Detention Standards Program. The National Detention Standards were originally issued in September 2000 to facilitate consistent conditions of confinement, access to legal representation, and safe and secure operations across the immigration detention system. The standards have been updated into a performance based format known as the Performance Based National Detention Standards. Through a robust inspections program, the program ensures facilities utilized to detain aliens in immigration proceedings or awaiting removal to their countries do so in accordance with the Performance Based National Detention Standards.
Scope of Data	Currently all facilities on the authorized facility's list are included in this measure. Authorized facilities include detention centers that have been inspected by ERO/Custody Operations law enforcement personnel, or their Subject Matter Experts (SME), to ensure the facility meets all requirements of the ICE/ERO National Detention Standards provisions.
Data Source	The annual review rating is contained in formal inspection reports provided by the

	Detention Standards Compliance Unit (DSCU) contractor and is further reviewed by the DSCU. The information from these reports will be compiled to determine the agency-wide percentage of facilities receiving acceptable or above rating.
Data Collection Methodology	Data for this measure is collected by annual inspections, which are then evaluated by ERO inspectors. These inspections review the current 38 National Detention Standards that apply to all facilities, and rate whether the facility is in compliance with each standard. Based on these ratings, the compliance for each facility is calculated. This information is communicated in formal reports to the program and the ERO Inspections and Audit Unit and the Detention Standards Compliance Unit at ERO Headquarters, which oversees and reviews all reports. The program reports semi-annually on agency-wide adherence with the Detention Standards based on calculating the number of facilities receiving an acceptable or better rating, compared to the total number of facilities inspected.
Reliability Index	Reliable
Explanation of Data Reliability Check	The program reviews all reports of detention facilities inspections conducted by the contractor. Inspections that receive a final rating of "Acceptable" or above are reviewed by the Detention Standards Compliance Unit (DSCU) and the Inspections and Audit Unit. Inspections that receive deficient or at-risk rating are reviewed by DSCU SMEs.

Performance Measure	Percent of Removal Orders Secured by ICE attorneys that Support ICE's Civil Enforcement Priorities (CEP)
Program	Enforcement and Removal Operations (ERO)
Description	This measure indicates the percent of total removal orders secured by OPLA attorneys that support the agency's civil enforcement priorities (CEP). OPLA attorneys play an integral role in enforcing the nation's immigration laws by prosecuting accused violators and ultimately securing orders of removal against those found to be in the United States illegally. The CEP prioritizes the use of enforcement personnel, detention space, and removal resources to ensure that the removals orders secured promote the established enforcement priorities.The CEP includes aliens who pose a danger to national security or a risk to public safety, recent illegal entrants, and aliens who are fugitives or otherwise obstruct immigration controls.
Scope of Data	The scope of this measure will include all cases with an Immigration Judge (IJ) order date within the reporting period.
Data Source	The information will be entered in the General Counsel Electronic Management System (GEMS) or the Office of the Principal Legal Advisor Case Management System, PLAnet, and the Enforcement Integrated Database (EID)
Data Collection Methodology	OPLA attorneys use GEMS to enter and track information associated with cases before the immigration court. Enforcement Removal Operations (ERO) identifies aliens who pose a danger to national security or a risk to public safety (Priority 1) at the time of case creation and identifies recent entrants and fugitives (Priorities 2 and 3) at the time of removal. "CEP Removal Orders" include all criminal aliens regardless of removal status, and only those Priority 2 and 3 aliens with an executed removal order.
Reliability Index	Reliable
Explanation of Data Reliability Check	OPLA has implemented a review panel of senior managers from Field Legal Operations to review and confirm the accuracy of the data being presented.

Performance Measure	Percent of transnational child exploitation or sex trafficking investigations resulting in the disruption or dismantlement of high-threat child exploitation or sex trafficking organizations or individuals
Program	Homeland Security Investigations (HSI)
Description	This measure reports the percent of transnational child exploitation or child sex trafficking investigations resulting in the disruption or dismantlement of high-threat criminal organizations/individuals. "Child exploitation" is defined as manufacturing and distributing sexual or perverted acts or images of children under the age of 18. "Disruption" is defined as impeding the normal and effective operation of the targeted organization. "Dismantlement" is defined as destroying the organization's leadership, financial base and network to the degree that the organization is incapable of operating and/or reconstituting itself. ICE has established a Child Exploitation Investigations Center (CEIC) to serve as a central coordination point for state, local, and tribal offices, the National Center for Missing and Exploited Children, and other federal law enforcement agencies, as well as international law enforcement agencies dedicated to combating the sexual exploitation of children.
Scope of Data	The scope of this measure includes all validated records of significant child exploitation or sex trafficking investigations that are entered in to the Treasury Enforcement Communication System (TECS) system. "High-threat" language refers to cases flagged and reviewed through ICE's Significant Case Review (SCR) process. Threshold levels are established in the respective case categories to identify those cases investigating the most significant crimes.
Data Source	Specific case information will be entered through the use of the Significant Case Report (SCR) Module in TECS.
Data Collection Methodology	ICE agents utilize TECS to track and manage investigative case data, which begins with the opening of a case and identification of a case category or categories. Substantive case information during the investigative process is entered into TECS, eventually reflecting indictment, conviction, and/or case closure. This data is routinely validated for accuracy, prior to any reporting. To report for this measure, a data request will be sent to the Homeland Security Investigations (HSI) Executive Information Unit (EIU) from the Budget Formulation and Strategic Planning Unit. EIU will return an Excel spreadsheet with approved SCR child exploitation or child sex trafficking cases by year. A percentage of SCR cases with an approved disruption or dismantlement is then derived.
Reliability Index	Reliable
Explanation of Data Reliability Check	All SCR child exploitation or child sex trafficking cases will be approved by a panel represented by 5 HSI Divisions, HSI Operations, International Affairs and Intelligence. The panel will validate the information provided and determine if the nominated cases indeed meet the criteria of significant investigations resulting in a disruption or dismantlement.

Performance Measure	Percent of transnational drug investigations resulting in the disruption or dismantlement of high-threat transnational drug trafficking organizations or individuals
Program	Homeland Security Investigations (HSI)
Description	This measure will report on the percent of transnational drug investigations resulting in the disruption or dismantlement of high-threat transnational drug trafficking organizations/individuals. "Transnational drug trafficking organization" is defined by the U.S. Department of Justice (DOJ) as those organizations on approved Consolidated Priority Organizational Target (CPOT)

	or Regional Priority Organizational Target (RPOT) lists or those who are earning, laundering, or moving more than $10 million a year in drug proceeds. "Disruption" is defined as impeding the normal and effective operation of the targeted organization. "Dismantlement" is defined as destroying the organization's leadership, financial base and network to the degree that the organization is incapable of operating and/or reconstituting itself. To impact the result of this measure, ICE established international partnerships to link global customs and law enforcement agencies.
Scope of Data	The scope of this measure includes all validated records of high-threat transnational drug investigations that are entered into the Treasury Enforcement Communication System (TECS). "High-threat" refers to cases flagged and reviewed through ICE's Significant Case Review (SCR) process. Threshold levels are established in the respective case categories to identify those cases investigating the most significant crimes.
Data Source	Specific case information will be entered through the use of the Significant Case Report (SCR) Module in TECS.
Data Collection Methodology	ICE agents utilize TECS to track and manage investigative case data, which begins with the opening of a case and identification of a case category or categories. Substantive case information during the investigative process is entered into TECS, eventually reflecting indictment, conviction, and/or case closure. This data is routinely validated for accuracy, prior to any reporting. To report for this measure, a data request will be sent to the Homeland Security Investigations (HSI) Executive Information Unit (EIU) from the Budget Formulation and Strategic Planning Unit. EIU will return an Excel spreadsheet with approved SCR cases of transnational drug cases by year. A percentage of SCR cases with approved disruptions or dismantlements is then derived.
Reliability Index	Reliable
Explanation of Data Reliability Check	All SCR transnational drug cases will be approved by a panel represented by 5 HSI Divisions, HSI Operations, International Affairs and Intelligence. The panel will validate the information provided and determine if the nominated cases indeed meet the criteria of significant investigations resulting in a disruption or dismantlement.

Performance Measure	Percent of transnational gang investigations resulting in the disruption or dismantlement of high-threat transnational criminal gangs
Program	Homeland Security Investigations (HSI)
Description	This measure reports on the percent of transnational gang investigations resulting in the disruption or dismantlement of high-threat transnational criminal gangs. "Transnational gang" is defined as members within a transnational criminal organization linked to gang activity as defined by the Racketeering Influenced Corrupt Organization (RICO) and/or the Violent Crime in Aid of Racketeering (VICAR) statutes. "Disruption" is defined as impeding the normal and effective operation of the targeted organization. "Dismantlement" is defined as destroying the organization's leadership, financial base and network to the degree that the organization is incapable of operating and/or reconstituting itself. To impact the result of this measure ICE has developed and implemented anti-gang initiatives focused on violent criminal activities and on crimes with a nexus to the border.
Scope of Data	The scope of this measure includes all validated records of high threat transnational gang investigations that are entered into the Treasury Enforcement Communication System (TECS). "High-threat" refers to cases flagged and reviewed through ICE's Significant Case Review (SCR) process. Threshold levels are established in the respective case categories to identify those cases

	investigating the most significant crimes.
Data Source	Specific case information will be entered through the use of the Significant Case Report (SCR) Module in TECS.
Data Collection Methodology	ICE agents utilize TECS to track and manage investigative case data, which begins with the opening of a case and identification of a case category or categories. Substantive case information during the investigative process is entered into TECS, eventually reflecting indictment, conviction, and/or case closure. This data is routinely validated for accuracy, prior to any reporting. To report for this measure, a data request will be sent to the Homeland Security Investigations (HSI) Executive Information Unit (EIU) from the Budget Formulation and Strategic Planning Unit. EIU will return an Excel spreadsheet with approved SCR transnational gang cases by year. A percentage of approved SCR cases with approved disruptions or dismantlements is then derived.
Reliability Index	Reliable
Explanation of Data Reliability Check	All SCR transnational gang cases will be approved by a panel represented by 5 HSI Divisions, HSI Operations, International Affairs and Intelligence. The panel will validate the information provided and determine which nominated cases indeed meet the criteria of significant investigations resulting in a disruption or dismantlement.

U.S. Secret Service

Performance Measure	Amount of dollar loss prevented by Secret Service cyber investigations (in millions)
Program	Criminal Investigations
Description	This measure is an estimate of the direct dollar loss to the public prevented due to cyber investigations by Secret Service. The dollar loss prevented is based on the estimated amount of cyber losses that would have occurred had the offender not been identified nor the criminal enterprise interrupted. The measure reflects the Secret Service's efforts to reduce cyber related financial losses to the public.
Scope of Data	This measure is an estimate of the direct dollar loss to the public prevented due to cyber crime investigations by the Secret Service. Error is due to lag time in data entry or corrections to historical data.
Data Source	The Cyber Crimes Loss Prevented measure is collected from the Master Central Index (MCI) 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 its cyber investigations through its case management system known as the Master Central Index. Data is input to the Master Central Index system via Secret Service personnel located in field offices throughout the United States and overseas. Data pertaining to this particular measure (loss prevented) are extracted from the Master Central Index system 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	MCI has many features built into it in order to provide the most accurate data

Reliability Check	possible. Along with the mainframe security features, there are many edit checks built into the applications to ensure the accuracy and validity of the data. Only authorized headquarters and field personnel have access to the applications, and they are governed by specific procedures to input case and arrest data. An annual audit is conducted and recurring verification reports are generated and reviewed to reduce errors and ensure data accuracy.

Performance Measure	Financial crimes loss prevented through a criminal investigation (in billions)
Program	Criminal Investigations
Description	An estimate of the direct dollar loss to the public that was prevented due to Secret Service intervention or interruption of a criminal venture through a criminal investigation. This estimate is based on the likely amount of financial crime that would have occurred had the offender not been identified nor the criminal enterprise disrupted, and reflects the Secret Service's efforts to reduce financial losses to the public attributable to financial crimes.
Scope of Data	This measure reports an estimate of the direct dollar loss prevented due to Secret Service intervention/interruption of a criminal venture through a criminal investigation. Error is due to lag time in data entry or corrections to historical data.
Data Source	The Financial Crimes Loss Prevented measure is collected from the Master Central Index (MCI) 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 its multitude of criminal investigations through its case management system known as the Master Central Index. Data is input to the Master Central Index system via Secret Service personnel located in field offices throughout the United States and overseas. Data pertaining to this particular measure (loss prevented) are extracted from the Master Central Index system by designated financial crime case violation codes and the dates these cases were closed. The data is then aggregated up to the highest levels by month, year, office, and Service-wide. This information is then reported through various management and statistical reports to Secret Service headquarters program managers, field offices, and the Department of Homeland Security.
Reliability Index	Reliable
Explanation of Data Reliability Check	MCI 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 financial accounts recovered (in millions)
Program	Criminal Investigations
Description	This measure represents the number of financial accounts recovered during cyber investigations. Financial accounts include bank accounts, credit card accounts, PayPal and other online money transfer accounts.
Scope of Data	This measure represents the number of financial accounts recovered during cyber investigations.
Data Source	The Financial Accounts measure is collected from the Master Central Index (MCI) 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 its cyber investigations through its case management system known as the Master Central Index. Data is input to the Master Central Index system 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 the Master Central Index system 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	MCI 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 cyber crime and cyber forensics both domestically and overseas
Program	Criminal Investigations
Description	This measure represents the number of individuals trained in cyber crime and cyber forensics by the Secret Service. This specialized technical training occurs both domestically and overseas in an effort to strengthen our ability to fight cyber crime.
Scope of Data	This measure captures the total number of individuals trained by the Secret Service in cyber crime and cyber forensics.
Data Source	Data on individuals trained by the USSS is currently collected through internal tracking devices. We are attempting to move towards an enterprise solution to allow for easier dataset extraction and analysis.
Data Collection Methodology	Data is entered through internal tracking devices by authorized Secret Service personnel. Quarterly data is then extracted from the database and aggregated up to the highest levels by month and year. Training data is collected and aggregated by the number of individuals who attend each training class. Because of this, the potential exists for counting unique individuals multiple times if they attend more than one training per fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	Only authorized Secret Service personnel have access to the applications. Once the data has been aggregated, it is double checked for verification and to ensure data accuracy.

Performance Measure	Percent of currency identified as counterfeit
Program	Criminal Investigations
Description	The dollar value of counterfeit notes passed on the public reported as a percent of dollars of genuine currency. This measure is calculated by dividing the dollar value of counterfeit notes passed by the dollar value of genuine currency in circulation. This measure is an indicator of the proportion of counterfeit currency relative to the amount of genuine U.S. Currency in circulation, and reflects our efforts to reduce financial losses to the public attributable to counterfeit currency.
Scope of Data	This measure is an indicator of the proportion of counterfeit currency relative to

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

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

Performance Measure	Percent of protectees that arrive and depart safely (New Measure)
Program	Protection
Description	This measure gauges the percent of travel stops where Secret Service protectees arrive and depart safely. The performance target is always 100%.
Scope of Data	This measure is an indicator of the percentage of travel stops where protectees arrive and depart safely. The number of protective stops protectees arrive and depart safely divided by the total number of protective stops protectees arrive and depart.
Data Source	Protective stops information is collected from the Agent Management & Protection Support System. This system is used by Secret Service protective divisions, and provides a means of record keeping for all protective stops information.
Data Collection Methodology	Results from Protective Operations, as well as any incident that may occur, are immediately reported by detail leaders to the Special Agent in Charge, who submits an After Action Report to Protective Operations program managers, and are disseminated within the organization for further analysis. Analysts collect protective travel stops for domestic protectees, foreign dignitaries, and campaign protectees and aggregate the totals into one measure. The number of incident-free

	protection stops is divided by the total number of protection stops to achieve a percent outcome.
Reliability Index	Reliable
Explanation of Data Reliability Check	Program managers and Operations Research Analysts continually monitor and review performance, including all instances of arrival and departure. Any breach of Protective Operations would be immediately known and subject to a thorough investigation.

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

Performance Measure	Percent of total U.S. Secret Service protection activities that are incident-free for protection of national leaders, foreign dignitaries, designated protectees and others during travel or at protected facilities (Retired Measure)
Program	Protection
Description	This measure gauges the percent of instances where incident free protection is provided to leaders, dignitaries, and persons (protectees, staff/employees, guests, and the public) during travel and inside the White House Complex or the Vice President's Residence. An incident is defined as someone who is assaulted or receives an injury from an attack while receiving Secret Service protection or inside the White House Complex or Vice President's Residence. Anything less than 100% incident free protection is deemed unacceptable.
Scope of Data	This measure is a roll up of three arrival and departure measures: percent of instances protectees arrive and depart safely (domestic), percent of instances protectees arrive and depart safely (foreign dignitaries), and percent of instances

	protectees arrive and depart safely (campaign protectees); and percent of time incident free protection is provided to persons inside the White House Complex and vice President's Residence. Results are based on all available data for all four measures and therefore there is no sampling.
Data Source	This program measure originates from every protective event or visit for designated protectees. The Secret Service conducts after action reviews to gauge performance of specific protective operations and submits After Action Reports. 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 collect protective travel stops for domestic protectees, foreign dignitaries, and campaign protectees and calculate the percentages. These percentages are combined with 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. This creates an overall percent of protective instances.
Reliability Index	Reliable
Explanation of Data Reliability Check	Program managers and Operations Research Analysts continually monitor and review performance, including all instances of arrival and departure. Any breach of Protective Operations would be immediately known and subject to a thorough investigation.

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

Component Acronyms

Below is the list of DHS Components and their Acronyms.

AO – Analysis and Operations
CBP – U.S. Customs and Border Protection
DMO – Departmental Management and Operations
DNDO – Domestic Nuclear Detection Office
FEMA – Federal Emergency Management Agency
FLETC – Federal Law Enforcement Training Centers
ICE – U.S. Immigration and Customs Enforcement
NPPD – National Protection and Programs Directorate
OHA – Office of Health Affairs
OIG – Office of Inspector General
S&T – Science and Technology Directorate
TSA – Transportation Security Administration
USCG – U.S. Coast Guard
USCIS – U.S. Citizenship and Immigration Services
USSS – U.S. Secret Service

This page intentionally left blank.

Homeland
Security

Homeland
Security