

Our Vision

A homeland that is safe, secure, and resilient against terrorism and other hazards.

Our Mission

We will lead efforts to achieve a safe, secure, and resilient homeland. We will counter terrorism and enhance our security; secure and manage our borders; enforce and administer our immigration laws; protect cyber networks and critical infrastructure; and ensure resilience from disasters. We will accomplish these missions while providing essential support to national and economic security and maturing and strengthening the Department of Homeland Security and the homeland security enterprise.

About this Report

The U.S. *Department of Homeland Security Annual Performance Report for Fiscal Years (FY) 2012 – 2014* presents the Department's performance measures and applicable results aligned to our missions, provides the planned performance targets for FY 2013 and FY 2014, and includes information on the Department's Priority Goals. The report is consolidated to incorporate our annual performance plan and annual performance report.

The *FY 2012 – 2014 Annual Performance Report* is one in a series of three reports which comprise the Department's Performance and Accountability Reports:

- ***DHS Annual Financial Report:*** Delivery date – November 14, 2012
- ***DHS Annual Performance Report:*** Delivery date – April 10, 2013
- ***DHS Summary of Performance and Financial Information:*** Delivery date – February 15, 2013

When published, all three reports will be located on our public website at:

http://www.dhs.gov/xabout/budget/editorial_0430.shtm.

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

Table of Contents

Introduction	3
Measure Descriptions and Data Collection Methodologies	4
Mission 1: Preventing Terrorism and Enhancing Security	4
Goal 1.1: Preventing Terrorist Attacks	4
Analysis and Operations.....	4
Departmental Management and Operations	5
Transportation Security Administration.....	6
Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear (CBRN) Materials and Capabilities	10
Domestic Nuclear Detection Office	10
National Protection and Programs Directorate.....	11
Office of Health Affairs	13
Goal 1.3: Manage Risks to Critical Infrastructure, Key Leaders, and Events	13
National Protection and Programs Directorate.....	13
Transportation Security Administration.....	16
U.S. Secret Service.....	18
Mission 2: Securing and Managing Our Borders.....	20
Goal 2.1: Secure U.S. Air, Land, and Sea Borders	20
U.S. Customs and Border Protection	20
Goal 2.2: Safeguard Lawful Trade and Travel.....	24
Transportation Security Administration.....	24
U.S. Coast Guard.....	27
U.S. Customs and Border Protection	27
Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations	31
U.S. Immigration and Customs Enforcement	31
Mission 3: Enforcing and Administering Our Immigration Laws	34
Goal 3.1: Strengthen and Effectively Administer the Immigration System	34
U.S. Citizenship and Immigration Services	34
Goal 3.2: Prevent Unlawful Immigration.....	39
U.S. Citizenship and Immigration Services	39
U.S. Immigration and Customs Enforcement	41
Mission 4: Safeguarding and Securing Cyberspace.....	45
Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment	45
Analysis and Operations.....	45
National Protection and Programs Directorate.....	46
U.S. Secret Service.....	51
Goal 4.2: Promote Cybersecurity Knowledge and Innovation.....	54
Science and Technology Directorate.....	54

Mission 5: Ensuring Resilience to Disasters 56

- Goal 5.1: Mitigate Hazards 56
 - Federal Emergency Management Agency 56
- Goal 5.2: Enhance National Preparedness through a Whole Community Approach to Emergency Management..... 59
 - Federal Emergency Management Agency 59
- Goal 5.3: Ensure Effective Emergency Response..... 62
 - Federal Emergency Management Agency 62
 - National Protection and Programs Directorate..... 68
- Goal 5.4: Rapidly Recover from a Catastrophic Event 70
 - Federal Emergency Management Agency 70

Providing Essential Support to National and Economic Security 72

- Goal: Collect Customs Revenue and Enforce Import/Export Controls 72
 - U.S. Customs and Border Protection 72
- Goal: Ensure Maritime Safety and Environmental Stewardship..... 73
 - U.S. Coast Guard..... 73
- Goal: Conduct and Support Other Law Enforcement Activities..... 77
 - Federal Law Enforcement Training Center 77
 - U.S. Secret Service 77

Cross-Cutting Performance Measures 78

- Analysis and Operations..... 78
 - Federal Law Enforcement Training Center 79

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 are listed alphabetically by Component within each mission and focus area.

Measure Descriptions and Data Collection Methodologies

Mission 1: Preventing Terrorism and Enhancing Security

Goal 1.1: Preventing Terrorist Attacks

Analysis and Operations

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. The survey results are defined by the currently available Office of Management and Budget vetted tool.
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 Reliability Check	Individuals within the DHS IE are responsible for collecting, storing, and reporting data generated by the source above. I&A Performance Management & Evaluation (PME) personnel are responsible for aggregating the data from the DHS IE and reporting the results quarterly. Once the survey responses are received and aggregated, I&A PME staff review the results for consistency and look for any anomalous trends that would signal a data integrity problem. Any issues are researched and if any erroneous data is found, it is corrected or removed from the overall calculation.

Performance Measure	Percent of intelligence reports rated "satisfactory" or higher in customer feedback that enable customers to anticipate emerging threats (Retired Measure)
Program	Analysis and Operations
Description	This measure gauges the extent to which the DHS Intelligence Enterprise is satisfying their customers' needs related to anticipating emerging threats. The survey results are defined by the currently available Office of Management and Budget vetted tool.
Scope of Data	The scope of this measure is feedback received from customer satisfaction surveys

	returned to the DHS-IE (USCG, TSA, etc) that originated the intelligence report. For this performance measure "intelligence report" is defined per Component. Each Component will produce a Component specific Performance Measure Definition Form (PMDF) and define the specific reporting included for data aggregation.
Data Source	The data source for this performance measure will be customer feedback surveys fielded by DHS Intelligence Enterprise (IE). The surveys are either attached to the intelligence report or fielded separately to the customer following the dissemination of each "intelligence report". The surveys will contain a standard question intended to elicit the degree of customer satisfaction with the usefulness of the intelligence report. The question asks customers to rate satisfaction on a five-point rating scale (very satisfied, somewhat satisfied, neither satisfied nor dissatisfied, somewhat dissatisfied, very dissatisfied). Responses "very satisfied" and "somewhat satisfied" will be considered to have met the criteria for "satisfactory". Components will aggregate the results obtained based on the survey metadata.
Data Collection Methodology	Members of the DHS Intelligence Enterprise will attach an electronic survey instrument to each intelligence product disseminated to customers. The survey instrument will provide DHS Intelligence Components with a standard data collection instrument and method to aggregate the results throughout the Agency. For data aggregation purposes, customer satisfaction is defined as responsiveness and timeliness of product. The DHS Intelligence Enterprise will provide the Office of Intelligence and Analysis (I&A) with Component 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.
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 and Evaluation (PME) personnel are responsible for aggregating the data from the DHS IE and reporting the results quarterly. I&A personnel are responsible for aggregating the data from the DHS IE and reporting the results quarterly. I&A will use the individual PMDF's for internal control and data quality. Annually, I&A will review the PMDF's with individual components and ensure the processes identified remain intact.

Departmental Management and Operations

Performance Measure	Percent of law enforcement officials trained in methods to counter terrorism and other violent acts that rate the training as effective
Program	Office of the Secretary and Executive Management
Description	This measure assesses the effectiveness of DHS training to state and local law enforcement officials offered by the DHS Office of Civil Rights and Civil Liberties (CRCL). This training covers three components: 1) Cultural Competency, 2) Community Engagement, and 3) Understanding and Countering Violent Radicalization. A post training survey is administered to assess effectiveness. A pre- and post-test of topic familiarity will also be administered.
Scope of Data	All available evaluation forms completed by participants at all Countering Violent Extremeism training courses hosted by CRCL.
Data Source	Paper evaluation forms are completed by participants of every Countering Violent Extremeism training course hosted by CRCL. Staff collect, collate, and then file evaluation forms with the CRCL Institute. Staff document data from the evaluation forms and calculate reports, including overall effectiveness.
Data Collection Methodology	At completion of training course, attendees complete a 10-12 item questionnaire. A five-point rating scale is used to provide feedback on aspects of the training, including: the effectiveness, presentation style, and the usefulness of the

	information as applied to the respondent’s work. Qualitative questions are on the least and most helpful aspects of the training, suggestions for changes in the content, presentation style, etc. Responses are tabulated and analyzed using Microsoft Excel. The self-assessed pre- and post- test of topic familiarity will also be analyzed and training session outcomes will be compared by geographic area and general audience characteristics. Those who rate the content and delivery of the training as a “4” or a “5” are used to calculate the percent for this measure. Evaluation forms are scanned and electronically stored on the DHS network along with the data in Excel files. Original hard copies are then archived in CRCL filing cabinets.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data is obtained from CRCL Institute staff as training is conducted and verified by staff for accuracy based on the internal tracking system. Once the survey responses are received and aggregated, CRCL 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.

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 Inquiry Program forms, excluding the time DHS waits for all required documents to be submitted.
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	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 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.
--	--

Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear (CBRN) Materials and Capabilities

Domestic Nuclear Detection Office

Performance Measure	Percent of cargo conveyances that pass through radiation detection systems 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 amount of cargo conveyances 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 fixed, mobile, and hand-held radiation detection equipment of the total number of cargo conveyances entering the nation through land ports of entry and by international rail.
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	Weekly reports of new detection portal installations are provided by the installation agent, the Pacific Northwest National Laboratory. This data is provided in tabular form, based on new installations completed in a given week. Baseline land border cargo data is maintained by CBP, and baseline rail cargo data is 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 Domestic Nuclear Detection Office (DNDO) Mission Management Directorate on the Cargo Screening 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 fixed 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.

National Protection and Programs Directorate

Performance Measure	Percent of inspected high-risk chemical facilities in compliance with the Chemical Facility Anti-Terrorism Standards (Retired Measure)
Program	Infrastructure Protection
Description	Measures onsite inspections, conducted by Infrastructure Protection, that provide regulatory oversight of the Nation's high-risk chemical facilities and verify compliance with the Chemical Facility Anti-terrorism Standards (CFATS). This program is in the early stage of implementation.
Scope of Data	Results are based on all available data retained in the Chemical Security Assessment Tools (CSAT)/Chemical Management System (CHEMS) systems for high-risk chemical facilities. This measure accounts for the highest risk chemical facilities having completed authorization inspections verifying that the facility submitted Site Security plan is compliant with the Chemical Facility Anti-Terrorism Standards (CFATS) regulation.
Data Source	Reporting data sources are all internal to DHS/NPPD/IP/ISCD. Reported data is the resulting summaries from queries against internal systems. The Chemical Security Assessment Tools (CSAT) Suite 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). CSAT is a secure web-based system.
Data Collection Methodology	Chemical facility compliance information is maintained in CHEMS, the chemical security management system. The compliance percentage is determined by the number of sites found to be in compliance with CFATS, as compared to the number of sites selected for inspection each year. For a facility to be found in compliance, it must meet each of the 18 risk based performance standards established by CFATS. The total number of proposed to be inspected chemical sites for compliance is determined from a designated subset of the sites that have completed an SVA and developed an SSP that meets the CFATS standards. The period between inspections is based on a risk based priority, with the highest risk

	facilities inspected more frequently. It is expected that at full operational capability, Tier 1 facilities will be inspected annually, Tier 2 facilities every 2 years, and a prioritized selection of 10% of Tier 3 and Tier 4 facilities each year.
Reliability Index	Reliable
Explanation of Data Reliability Check	The accuracy of data captured and reported via the CSAT/CHEMS systems 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 performance standards implemented by the highest risk chemical facilities and verified by DHS (New Measure)
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 HQ staff and inspection cadre posts added information and status to the CSATs system that includes the CHEMS applications as a course of normal operations. The success percentage for this measure will be based upon: the number of compliant RBPS measures of Tier 1 and Tier 2 regulated facilities that have been implemented (not planned) and that have subsequently obtained the DHS approval of the facilities rendered CRBPS (CRBPS) divided by the total number of applicable RBPS measures for facilities receiving a final tiering letter (tiers 1-2 inclusive) (TRBPSFTL). Formula: $CRBPS \div TRBPSFTL (Tier 1 + Tier 2) = \%$.
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.

Office of Health Affairs

Performance Measure	Percent of targeted urban areas that are monitored for biological threats using BioWatch technology (Retired Measure)
Program	Health Threats Resilience
Description	This measure examines the number of areas in which BioWatch technology has been deployed compared to those that were targeted for deployment by the Office of Health Affairs.
Scope of Data	The scope of data is all urban areas targeted for deployment of BioWatch that currently use BioWatch technology to monitor biological threats.
Data Source	The Office of Health Affairs Systems Program Office provides the data.
Data Collection Methodology	The BioWatch Program has a deployment plan that expands current coverage to the top Urban Area Security Initiative (UASI) metropolitan areas. Data are collected through activity reports from existing jurisdictions and will be collected from deployment reports as new jurisdictions come on line. The metric is expressed as a percentage calculated by dividing the number of operational jurisdictions by the target number.
Reliability Index	Reliable
Explanation of Data Reliability Check	The Systems Program Office ensures reliability of data.

Goal 1.3: Manage Risks to Critical Infrastructure, Key Leaders, and Events

National Protection and Programs Directorate

Performance Measure	Percent of countermeasures that are determined to be in compliance with standards when tested in federal facilities (Retired Measure)
Program	Federal Protective Service
Description	This measure determines what percent of countermeasures deployed, when tested, are in compliance with standards, based on established testing protocols and informed by Interagency Security Committee standards, designed to prevent harm and destruction to the building and its contents. This applies to federal buildings where the Federal Protective Service provides security and law enforcement services. Countermeasures include systems such as cameras, x-ray equipment, magnetometers, alarms, and security guards. These tests occur on a regular basis and provide the program decision makers a means of assessing the compliance of existing countermeasures.
Scope of Data	This measure includes all buildings where the Federal Protection Service program provides security law enforcement services. This includes approximately 8,800 federal buildings nationwide. The vast majority of these buildings are either owned or leased by the General Services Administration.
Data Source	The data is stored in the Federal Protective Service Security Tracking System database, maintained at Headquarters.
Data Collection Methodology	Program field personnel conduct the countermeasure compliance tests on a regular basis. Field personnel test five systems during the assessment-cameras, alarms, x-ray equipment, magnetometers, and guard effectiveness. Typically multiple devices are tested within each of the five system areas. Test results by device are gathered by the inspectors are then entered into the database. The results by device are aggregated and the percent in compliance score is calculated based on the number of devices that passed the countermeasures test compared to the number of devices tested.

Reliability Index	Reliable
Explanation of Data Reliability Check	Within the aggregate scores, a trend analysis is conducted at Headquarters to identify anomalies. If found, then the facility level data is reviewed by Headquarters personnel to ensure its validity and accuracy. In addition, testing protocols are periodically verified by Headquarters personnel through surveys and quality assurance auditing to ensure procedures and scoring criteria are accurately applied.

Performance Measure	Percent of high risk facilities that receive a facility security assessment in compliance with the Interagency Security Committee (ISC) schedule (New Measure)
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 facilities that have implemented at least one security enhancement that raises the facility's protective measure index score after receiving an Infrastructure Protection vulnerability assessment or survey
Program	Infrastructure Protection
Description	This measure will show the percent of facilities that have enhanced their security after receiving an Infrastructure Protection vulnerability assessment or survey. Only enhancements, changes or additional protective measures that count towards this measure are ones that result in an increase to the facility's Protective Measures Index (PMI); a set of rigorous criteria that the impact of security and protective measures. Infrastructure Protection recommendations are represented by security gaps or weaknesses identified by low PMI scores in a security assessment. Improvements done "soon after" the recommendations mean that they have occurred within 180 days of a survey or 365 days after a vulnerability assessment.
Scope of Data	The results are based on all available data collected during the fiscal year. "Improvements to security" are defined as any change in the facility's operations or protective measures that result in an increase to the facility's Protective Measures Index (PMI). PMI improvements can be to physical security, security force, security management, information sharing, protective measures, dependencies, robustness, resourcefulness, recovery, or options for consideration.
Data Source	IP personnel conduct voluntary vulnerability assessments and security surveys on

	critical infrastructure facilities to identify protective measures and security gaps or vulnerabilities. The data is collected using a web-based survey/assessment tool, and input into the central database. The facilities then receive a 180-day (for surveys) or 365-day (for vulnerability assessments) follow-up interview via telephone to gather data on improvements that have been made to facility security as a result of the assessment or survey, which is recorded using a web-based tool and input into the database. Personnel at Argonne National Laboratory conduct analysis of the implementation data to determine the percentage of facilities that have made enhancements to security, and in which areas those improvements have been made.
Data Collection Methodology	Data is gathered by Infrastructure Protection personnel in the field with input into the central database. Argonne National Labs personnel extract data on the implementation of security improvements from the follow-up interviews conducted within the last reporting period/year.
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 goes through a three tier quality assurance program the 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 is 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 owner/operators of critical infrastructure and key resources who report that the products provided by Infrastructure Protection enhance their understanding of the greatest risks to their infrastructure
Program	Infrastructure Protection
Description	This measure will show the percent of Level 1 and Level 2 critical infrastructure and key resources owner/operators (e.g., state, local, private) who indicate, via a customer survey administered by Infrastructure Protection (IP), that the products that IP provided them contributed to and/or resulted in their understanding of the greatest risks (prioritized in terms of threat, vulnerability, consequence) posed to their infrastructure.
Scope of Data	The scope of the data will include all the responses received from the electronic survey, which contain responses from L1 and L2 critical infrastructure owners and operators. The customer survey overall results, to the extent feasible, shall have at least a 95% confidence interval with $\pm 5\%$ margin of error, and important subgroup results shall have at least a 95% confidence interval with $\pm 5\%$ margin of error.
Data Source	The electronic surveys are created in a web-based survey software with a cryptographic protocol such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL). TLS, SSL, and other protocols encrypt the survey link and survey pages during all transmissions between the surveyor and respondents. The raw data from the survey will be stored in this software. Analysis will be conducted by the DHS contractor in the software and will also be downloaded into Excel for analysis. The analysis and summary of the data will be provided to the Office of Infrastructure Protection by the DHS contractor.
Data Collection Methodology	A customer satisfaction survey, administered via a web link/electronic survey to a statistically significant survey sample, is used to collect data for this measure. Responses are due two weeks to one month following receipt of the survey. Once responses are reported, data is analyzed and composite results are derived as a

	percentage of the total sample based on the response selected. In addition, the results may be further segmented to differentiate between owners and operators and state and local government officials. All responses are confidential. To overcome sample bias, IP will randomly select survey respondents from the entire IP stakeholder population and only rely on contacts received from valid sources. The survey has initial questions to ensure that only individuals involved in the security and protection of infrastructure can access the survey and can restrict the number of times a respondent can take the survey.
Reliability Index	Reliable
Explanation of Data Reliability Check	The customer survey overall results, to the extent feasible, shall have at least a 95% confidence interval with $\pm 5\%$ margin of error, and important subgroup results shall have at least a 95% confidence interval with $\pm 5\%$ margin of error. The sample selection methodology will depend upon the unit of analysis. For example, the sampling frame will be divided by critical infrastructure sector strata and simple random samples (or, if the sampling frame is large enough, systematic random samples or multi-stage samples) will be drawn from each stratum. Additionally, prior to conducting the survey, PRA approval from OMB needs to be received. During the approval process, a review of the survey questions and the data collection and analysis process is conducted to ensure undue burden is not placed on the public, to ensure a similar duplicate data collection is not being conducted, and to ensure the reliability and accuracy of the data.

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.

Transportation Security Administration

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. Secret Service

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	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 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 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
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.
Scope of Data	Performance data capture the protection of designated leaders, facilities, and other designated individuals. There is no error rate for this measure.
Data Source	This program measure originates from every protective event or visit for designated protectees. The Secret Service conducts after action reviews to gauge performance of specific protective operations. These reviews are used to measure how successfully the Secret Service performed its mission and what can be done to increase efficiency without compromising a protectee or event.
Data Collection Methodology	Results from Protective Operations, as well as any incident that may occur, are immediately reported by detail leaders to the Special Agent in Charge, who submits an After Action Report to Protective Operations program managers, and are disseminated within the organization for further analysis.
Reliability Index	Reliable
Explanation of Data Reliability Check	Program managers and Operations Research Analysts continually monitor and review performance, including all instances of arrival and departure. Any breach of Protective Operations would be immediately known and subject to a thorough investigation.

Mission 2: Securing and Managing Our Borders

Goal 2.1: Secure U.S. Air, Land, and Sea Borders

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 apprehensions on the Southwest Border between the ports of entry
Program	Securing America's Borders
Description	Protection of our Southwest border against threats from illicit cross-border activity is a key element needed to secure our country. This measure calculates the number of apprehensions made of those attempting entry along the Southwest border between ports of entry. DHS's border security strategy is based on a layered approach of strategically positioning personnel, technology, and defensive infrastructure; developing strong partnerships with law enforcement partners on both sides of the border; and increasing consequences to repeat offenders to provide a deterrent effect.
Scope of Data	Results include all apprehensions of deportable illegal aliens made by the Border Patrol within the nine sectors of the Southwest border.
Data Source	This data is captured by agents at the station level, where apprehension data is entered into the e3 (Enforce next generation) Processing system. All data entered via e3 Processing resides in the Enforcement Integrated Database (EID) database, the official system of record for this data.
Data Collection Methodology	Apprehension data is entered into a database, the e3 (Enforce next generation) 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.
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	Percent of people apprehended multiple times along the Southwest border (New Measure)
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	Number of smuggled outbound weapons seized at the ports of entry (New Measure)
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	Number of weapons seized on exit from the United States (Retired Measure)
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.
Scope of Data	All outbound-related weapons 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 weapons seizures are entered into Seized Assets and Case Tracking System (SEACATS) which is a subsystem of TECS, the principal system of record used by CBP. Weapons seizure information is accessed in report format through the BorderStat reporting tool.
Data Collection Methodology	All CBP officers effecting outbound weapons seizures enter the 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 weapons seized data for the different categories of weapons violations.
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.

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.

Goal 2.2: Safeguard Lawful Trade and Travel

Transportation Security Administration

Performance Measure	Percent of air carriers operating flights from foreign airports that serve as last point of departure to the U.S. in compliance with leading security indicators (Retired Measure)
Program	Intermodal Assessments and Enforcement
Description	This measure identifies air carrier operating from foreign airports serving as Last Point of Departure compliance with leading security indicators. A leading security indicator is a key indicator that may be predictive of the overall security posture of an air carrier. These critical indicators are derived from security laws, regulations, and standards and are applied to both U.S.-flagged aircraft operators (operating from foreign airports to any destination) and foreign air carriers operating from foreign airports serving as Last Point of Departure. Identifying compliance with the key indicators assesses air carriers' vulnerabilities. Assessing air carriers' vulnerabilities is part of an overall risk reduction process. Measuring compliance with standards is a strong indicator of system security.
Scope of Data	This measure is germane to U.S. passenger carriers operating regularly scheduled commercial service and public charters from any foreign airport to any other location, foreign or domestic, and is derived from TSA transportation statutes, regulations, standard security programs, and security directives. This measure also applies to all foreign passenger air carriers operating regularly scheduled commercial service and public charters from any foreign airport to the United States and is derived from similar statutory and regulatory documents.
Data Source	Air carrier inspection results are maintained in TSA's Performance and Results Information System (PARIS), which serves as the official source of data repository for TSA's 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 TSA's Office of Global Strategies, in accordance with its risk methodology. When inspections are completed, the results are entered into the Performance and Results Information System and are subsequently used to calculate the results for this measure.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data reliability 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 foreign airports serving as last point of departure in compliance with leading security indicators (Retired Measure)
Program	Intermodal Assessments and Enforcement
Description	TSA is responsible for evaluating security at foreign airports with service to the United States, those airports from which U.S. air carriers operate, and other sites

	as directed by the Secretary of the Department of Homeland Security. Using a 5-point scale, each foreign airport that serves as a last point of departure to the U.S. is evaluated against critical International Civil Aviation Organization (ICAO) aviation and airport security standards. This measure assesses the percent of foreign airports serving as the last point of departure to the U.S. in compliance with these aviation and security standards.
Scope of Data	The data reflect information collected by Transportation Security Specialists (TSSs) during evaluation of each LPD foreign airport's implementation of ICAO aviation security standards. Assessments occur at LPD foreign airports with direct service to the United States. Of the more than 70 security measures contained in ICAO's Annex 17 (Security), the TSSs focus special attention on 17 critical standards across 5 broad categories: (1) Aircraft & Inflight Security (2), Passenger and cabin bag screening (3), Hold bag security (4), Cargo/catering security (3), and Access Control (5). On an annual basis, TSA determines which LPD foreign airports will be assessed using a risk informed approach that includes threat, vulnerability, and consequence ratings. The objective is to assess low-risk airports once every three years; medium-risk airports every two years; and high-risk airports every year.
Data Source	The data to support this measure is contained in Foreign Airport Assessment Program (FAAP) reports prepared by TSSs following each airport assessment. Completed reports are submitted by the TSSs in international field offices to their Regional Managers and stored in a database located at TSA headquarters within the Office of Global Strategies (OGS). Each FAAP report contains data and observations collected during the assessment and highlights any shortfalls in security.
Data Collection Methodology	TSSs use a standard template for collecting and reporting data on the assessments. The template is contained in a TSA Standard Operating Procedure and is reviewed annually to ensure currency and standardization. Each foreign airport is evaluated against the ICAO critical aviation and airport security standards. Following submission of the assessment report, Vulnerability ratings are assigned by International Operations senior leadership to ensure consistent application of the relative ratings (1 through 5, with 1 indicating no shortfalls and 5 identifying instances of egregious noncompliance). Results are entered into the OGS database at TSA headquarters. Each quarter, the measure is calculated by OGS headquarters staff who run a query of the database to identify the airports receiving values of 4 or 5 in any of the ICAO standards.
Reliability Index	Reliable
Explanation of Data Reliability Check	TSSs in the field submit a comprehensive assessment report to their Regional Managers at TSA Headquarters. The report is reviewed by the respective Regional Manager for quality and consistency. Reports are then forwarded through senior leadership in International Operations to the Assistant Administrator, Office of Global Strategies, for final approval. This process may result in inquiries to the appropriate 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 to determine next steps and proposed areas of cooperation and assistance.
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 (New Measure)
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. Assessment 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.
--	---

U.S. Coast Guard

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 on whether a major problem is found during an inspection, requiring a notice of violation or civil penalty. 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. Examining the rate of compliance at high risk facilities provides insight into resiliency in that MTSA facilities are not only required to maintain proper access safeguards, but also exercise approved plans/procedures to prevent and react to security emergencies; and are therefore better suited to resist, adapt, and recover to adversity or disruption.
Scope of Data	This measure includes the results from annual Coast Guard security inspections conducted on all MTSA-regulated facilities. A facility means any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the U.S. and used, operated, or maintained by a public or private entity. 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 subject to SOLAS, 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 46 CFR chapter I. 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.
Data Source	The data source is MISLE (entry by field commands).
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 facilities who did not receive a notice of violation and/or civil penalty by the total number of facilities inspected.
Reliability Index	Reliable
Explanation of Data Reliability Check	Compliance is verified by inspection visits and self-reporting.

U.S. Customs and Border Protection

Performance Measure	Compliance rate for Customs-Trade Partnership Against Terrorism (C-TPAT) members with the established C-TPAT security guidelines (Retired Measure)
Program	Securing and Expediting Trade
Description	This measure provides the overall compliance rate achieved for all validations performed during the Fiscal Year. After acceptance into the Customs-Trade Partnership Against Terrorism (C-TPAT) program, all C-TPAT members must undergo a periodic validation in which U.S. Customs and Border Protection (CBP) examiners visit company locations and verify compliance with an industry-specific set of CBP security standards and required security practices. These

	validations are prepared using a weighted scoring system that is used to develop an overall compliance rate for each company. Compliance with security guidelines enhances the security of cargo shipped to the U.S.
Scope of Data	In accordance with the SAFE Port ACT, all entities importers that enroll to become C-TPAT members are required to submit a security profile and undergo a validation by a C-TPAT Supply Chain Security specialist within 1 year of certification. In addition, members must be revalidated within three years of the initial validation. Certified C-TPAT members can be Suspended/Removed from the program for failure to meet minimum security criteria as documented during a validation visit.
Data Source	CBP maintains an internal automated database commonly referred to as the C-TPAT portal which contains a variety of data pertaining to the C-TPAT member company to include the validation report and C-TPAT status (e.g. certified, validated, suspended, and removed).
Data Collection Methodology	The Supply Chain Security Specialist collects data in a variety of ways to include review of the Company Supply Chain Security Profile which each member must submit and conducting validation visits of member supply chains throughout the world. The results of the validation visit are documented in the C-TPAT Portal utilizing the Validation Report. The compliance rate can be determined at any given time by identifying total number of companies suspended / removed as a result of a validation and dividing by total number of validations performed to date.
Reliability Index	Reliable
Explanation of Data Reliability Check	Validation results and associated documentation are collected by Supply Chain Specialists and reviewed by their supervisor, often assisted by an additional supervisor who had oversight over the actual validation. Validation reports are further reviewed by a Headquarters program manager who analyzes and addresses overall anomalies.

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 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 requested cargo examinations conducted at foreign ports of origin in cooperation with host nations under the Container Security Initiative (Retired Measure)
Program	Securing and Expediting Trade
Description	The measure is an indication of the extent to which potential higher-risk cargo is satisfactorily inspected before it leaves the foreign port of origin. This measure is the percent of requested container examinations resolved or conducted by foreign Customs officials meeting CBP examination standards and requirements divided by the total number of examinations requested by CBP Container Security Initiative (CSI) officials. These examinations would otherwise have taken place at U.S. ports of entry.
Scope of Data	The scope of this measure is all requests for cargo examinations by made CBP CSI officials. Requests are made based on CSI standards which identify potential high-risk cargo. Data for this measure is collected at all CSI ports operating world-wide. This measure has been revised to reflect a percent, rather than a number (quantity) in order to provide context to the raw number of examinations presented under the old formulation. There are several on-going refinements and improvements to the Automated Targeting System (ATS) targeting algorithms that will likely result in significant reductions in the total number of examinations requested, which may also impact the overall percent conducted and enable CSI to reach its targets.
Data Source	ATS is the source of both the targeting data describing potential higher-risk cargo identified for examination and the host port examination data.
Data Collection Methodology	CSI officials at the CSI ports track host port examination data daily by using the Automated Targeting System (ATS), including the number of requests and

	completed examinations. ATS identifies the potential high-risk cargo shipments to be examined and, once the host port completes the examination in a manner meeting CSI requirements, a CSI team member at the host port enters the completed examination data using the intranet-based CSI web portal. CSI supervisors track the examination statistics on an on-going basis using the ATS Examination Findings module.
Reliability Index	Reliable
Explanation of Data Reliability Check	Reliability of the data is verified and evaluated by the CSI Division. Supervisors at the CSI host ports review potential high-risk shipments to ensure that the corresponding host port examination results are recorded daily. CSI Division Headquarters compares monthly examination data to historical volume at the given port and checks to see if it falls within certain parameters. If it does not, CSI Headquarters will ask the CSI Port Team Leader for additional information to review and justify the change in volume. Team Leaders review any identified discrepancies with host port Customs officials to ensure all examination data is accurately recorded.

Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations

U.S. Immigration and Customs Enforcement

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 (New Measure)
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 (New Measure)
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 (New Measure)
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.

Performance Measure	Percent of significant high-risk transnational criminal investigations that result in a disruption or dismantlement (Retired Measure)
Program	Homeland Security Investigations (HSI)
Description	This measure will report on the percentage of significant high-risk investigations that result in a disruption or dismantlement of high risk individuals or transnational organizations that threaten the national security and/or public safety of the United States through the violation of our Nation's Customs and Immigration Laws. Disruption is defined as impeding the normal and effective operation of the targeted organization. Dismantlement is defined as destroying the organization's leadership, financial base and network to the degree that the organization is incapable of operating and/or reconstituting itself.
Scope of Data	Data will be retrieved from the investigative case management system, TECS. Data query results will determine whether a case involved a disruption, dismantlement or both.
Data Source	Specific case information will be entered through the use of the Significant Case

	Report (SCR) Module in TECS.
Data Collection Methodology	A data request will be sent to the HSI Executive Information Unit (EIU) from the Budget Formulation and Strategic Planning Unit. EIU will return an excel spreadsheet with a list of Significant Cases and related Distuptions and Dismantlements.
Reliability Index	Reliable
Explanation of Data Reliability Check	All disruptions and dismantlements 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 cases indeed meet the criteria of a significant case.

Mission 3: Enforcing and Administering Our Immigration Laws

Goal 3.1: Strengthen and Effectively Administer the Immigration System

U.S. Citizenship and Immigration Services

Performance Measure	Average customer satisfaction rating with information provided about legal immigration pathways from USCIS call centers (Retired Measure)
Program	Information and Customer Service
Description	This measure gauges the average satisfaction rating with the information provided to assist prospective immigrants through the citizenship process from USCIS call centers.
Scope of Data	USCIS uses an independent contractor to measure customer satisfaction through a monthly telephone survey of randomly selected National Customer Service Center (NCSC) customers who used one of U.S. Citizenship and Immigration Services' (USCIS) Tier 1 Call Centers. The survey is conducted each quarter until 900 complete surveys are accomplished for a total of 3,600 annually.
Data Source	The data source for identifying the customers for the random selection is the Automatic Number Identification (ANI) system which tracks incoming phone numbers. This data is provided to the independent contractor on a monthly basis. The data source for the survey results is the independent contractor's quarterly reports which are used to calculate the customer satisfaction rating.
Data Collection Methodology	USCIS's independent contractor conducts quarterly surveys of those seeking information about the immigration process to determine their satisfaction with the information provided by USCIS Tier 1 call centers. Using the results of 900 complete surveys each quarter, USCIS calculates the average customer satisfaction rating for this measure. The survey uses a 5-point scale and responses of a 4 - Satisfied or 5 - Highly Satisfied are included in the calculation. The quarterly data are then aggregated at the end of the year for the fiscal year calculation.
Reliability Index	Reliable
Explanation of Data Reliability Check	The Independent Contractor submits the survey results to the Program Manager for review, comment, and approval. USCIS relies on the independent contractor to ensure completeness and reliability of the data; however, the Program Manager reviews the quarterly reports and if there are any anomalies, the Program Manager will work with the contractor to resolve.

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 Form I-485, Application to Register for Permanent Residence or to Adjust Status, approval decisions determined by quarterly quality reviews to have correctly followed established adjudication procedures (Retired Measure)
Program	Adjudication Services
Description	An I-485, Application to Register for Permanent Residence or to Adjust Status, is filed by an individual to apply for permanent residence in the United States or to adjust their current status. The U.S. Citizenship and Immigration Services (USCIS) conducts quality reviews on a quarterly basis to determine the accuracy rate of final approved decisions. Quality reviews are conducted using a team of experienced subject matter experts. This measure assesses the program's ability to process the I-485 to provide immigration benefit services in a fully supportable and accurate manner. Additionally, the results of this quality review process are used to improve the training of adjudicators and the processes used in conducting adjudications.
Scope of Data	This measure is a quarterly statistically valid random sampling of approved I-485 Forms nationwide received at the National Records Center. The sample is drawn from I-485s completed during the last month of the previous quarter. Sample size varies based on the number of forms completed during the previous quarter. For a typical population of ~26,000, ~125 files are sampled. This sample size provides accuracy with a ±1% margin of error. Ensuring a random sample of the entire population allows USCIS to make a statistically valid inference about the population from this sample. Quarterly results are based on approvals completed in the last month of the previous quarter. The annual result is calculated as a stratified sample where each quarter represents a strata.
Data Source	Completed Decisional Quality Review check sheets by a team of subject matter

	experts are entered into an online database and accessed by USCIS Headquarters, Office of Performance and Quality, Quality Management Branch (QMB) who maintains and integrates the information into a consolidated spreadsheet.
Data Collection Methodology	A team of subject matter experts conduct the review of the applicant's original request. The review is documented using a Decisional Quality Review checklist. Those cases where the documentation in the file does not support the decision are set aside. Once all files have been reviewed, at least 2 additional reviewers analyze any flagged applications. If either one of the two reviewers find the decision to be questionable, the file is returned to the original office to resolve any discrepancies. That office is required to advise the QMB of action taken to resolve the discrepancies within 10 working days. If the discrepancy does not impact the decision, no further action is required. QMB analysts gather final results and enter them into a database. A report is published quarterly documenting the reviewed results.
Reliability Index	Reliable
Explanation of Data Reliability Check	Layers of subject matter experts review and concur on correct or questionable decisions. This provides reliability. USCIS is able to obtain a valid random sample to conduct this audit, compile results, and develop corrective action plans to address noted deficiencies.

Performance Measure	Percent of Form N-400, Application for Naturalization, approval decisions determined by quarterly quality reviews to have correctly followed established adjudication procedures (Retired Measure)
Program	Adjudication Services
Description	A N-400, Application for Naturalization, is filed by an individual applying to become a United States citizen. The U.S. Citizenship and Immigration Services (USCIS) conducts quality reviews on a quarterly basis to determine the accuracy rate of final decisions on approved N-400 applications. Quality reviews are conducted using a team of experienced subject matter experts. This measure assesses the program's ability to process the N-400 to provide immigration benefit services in a fully supportable and accurate manner. Additionally, the results of this quality review process are used to improve the training of adjudicators and the processes used in conducting adjudications.
Scope of Data	This measure is a quarterly statistically valid random sampling of all approved and 'oathed' (sworn and signed) N-400 Forms received at the National Records Center. The sample is drawn from N-400s completed during the last month of the previous quarter. Sample size varies based on the number of forms completed during the previous quarter. For a typical population of ~70,000, ~125 files are sampled. This sample size provides accuracy with a ±1% margin of error. Ensuring a random sample of the entire population allows USCIS to make a statistically valid inference about the population from this sample. Quarterly results are based on approvals completed in the last month of the previous quarter. The annual result is calculated as a stratified sample where each quarter represents a strata.
Data Source	Completed Decisional Quality Review check sheets by a team of subject matter experts are entered into an online database and accessed by USCIS Headquarters, Office of Performance and Quality, Quality Management Branch (QMB) who maintains and integrates the information into a consolidated spreadsheet.
Data Collection Methodology	A team of subject matter experts conduct the review of the applicant's original request. The review is documented using a Decisional Quality Review checklist. Those cases where the documentation in the file does not support the decision are set aside. Once all files have been reviewed, at least 2 additional reviewers analyze any flagged applications. If either one of the two reviewers find the decision to be questionable, the file is returned to the original office to resolve any discrepancies. That office is required to advise the QMB of action taken to

	resolve the discrepancies within 10 working days. If the discrepancy impacts the decision, the office changes the decision and notifies QMB. If the discrepancy does not impact the decision, no further action is required. QMB analysts gather final results and enter them into a database. A report is published quarterly documenting the reviewed results.
Reliability Index	Reliable
Explanation of Data Reliability Check	Layers of subject matter experts review and concur on correct or questionable decisions. This provides reliability. USCIS is able to obtain a valid random sample to conduct this audit, compile results, and develop corrective action plans to address noted deficiencies.

Performance Measure	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 to 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 effectiveness in processing complete I-485 to provide immigration benefit services in a timely manner.
Scope of Data	This measure includes all pending I-485 Forms and receipt counts for the past fiscal year. Applications for which no visa number is available are considered pending, but not part of the backlog, and are removed from the scope. Cases are also removed if a Request For Evidence is pending for the regulatory period with the applicant, the applicant has requested a later appearance date, or the required name check is pending with the FBI.
Data Source	Automated counts and manual case counts are reported monthly through the automated Performance Analysis System (PAS) database. The Headquarters Statistics Branch of the DHS Office of Policy and Programs oversees PAS operations. The production system and database reside at the Justice Department Data Center, in Dallas, TX.
Data Collection Methodology	On a monthly basis, USCIS collects performance data on I-485 applications received, completed, and pending through PAS. Receipts are entered into case management systems through lockbox processing or e-filing. For lockbox cases, applications are scanned and data is sent electronically to the Computer Linked Application Information Management System (CLAIMS3). When cases are filed via e-filing, data elements get pushed to CLAIMS3 to populate the data fields. Individual adjudicators count the number of applications approved and denied, and record the information. Each office subsequently aggregates individual reports and enters them into PAS. At Service Centers, most data is collected and entered directly into PAS from automated systems supporting casework, including CLAIMS3. This data is then used to calculate the average cycle time.
Reliability Index	Reliable
Explanation of Data Reliability Check	The USCIS Operations Planning Division, Performance Management Branch conducts monthly data reconciliation and review activities to maximize the integrity of the data reported. The correlation between the amount of work reported, the amount of time taken to do that work, and the utilization factor provides triangular examination for report integrity. Data pulls from inventory systems are also used to measure the balance between reporting completions and system updates.

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 effectiveness in processing N-400 applications, while controlling for a number of external

	factors that can affect the timeline.
Scope of Data	This measure includes all pending N-400 Forms and receipt counts for the past fiscal year. The program excludes those forms that have been exempted due to circumstances beyond their control. Cases are removed from the scope calculation if the applicant has failed the English/Civics requirement and is waiting the statutory period between testing attempts, if the applicant has requested rescheduling, is awaiting a judicial oath ceremony for more than one month, the required name check is pending with the FBI, or if a Request For Evidence is pending for the regulatory period with the applicant.
Data Source	Automated counts and manual case counts are reported monthly through the automated Performance Analysis System (PAS) database. The Headquarters Statistics Branch of the DHS Office of Policy and Programs oversees PAS operations. The production system and database reside at the Justice Department Data Center, in Dallas, TX.
Data Collection Methodology	On a monthly basis, the program collects performance data on N-400 applications received, completed, and pending through PAS. Receipts are entered into case management systems through lockbox processing or via e-filing. For lockbox cases, applications are scanned and data is sent electronically to the Computer Linked Application Information Management System (CLAIMS4). When cases are filed via e-filing, data elements get pushed to CLAIMS4 to populate the data fields. Individual adjudicators count the number of applications approved and denied, and record the information. Each office subsequently aggregates individual reports and enters them into PAS. At Service Centers, most data is collected and entered directly into PAS from automated systems supporting casework, including CLAIMS4. This data is then used to calculate the average cycle time.
Reliability Index	Reliable
Explanation of Data Reliability Check	The USCIS Operations Planning Division, Performance Management Branch conducts monthly data reconciliation and review activities to maximize the integrity of the data reported. The correlation between the amount of work reported, the amount of time taken to do that work, and the utilization factor provides triangular examination for report integrity. Data pulls from inventory systems are also used to measure the balance between reporting completions and system updates.

Performance Measure	Percent of Citizenship and Integration Grant Program grantees that meet annual performance plan goals
Program	Citizenship
Description	This measure reports on the success of grantees in meeting their annual performance goals as of the 3rd quarter. USCIS plays a significant and ongoing role in ensuring the success of grantees by performing the following functions: negotiating with grantees to identify manageable goals and targets to hold them accountable; implementing systems to measure grantee performance; conducting onsite grant monitoring, and prioritizing those grantees in need of technical assistance; providing proactive group technical assistance and guidance and reactive technical assistance to individual grantees deemed in need of such support to ensure grantees are on target to meet performance goals; and providing grantees with regular feedback on their performance including a written assessment of grantee quarterly reports.
Scope of Data	This measure will draw on cumulative performance data for Q1-Q3 of the fiscal year.
Data Source	The measure will be tracked using quarterly grantee performance reports. The quarterly reports contain both quantitative data and a narrative description and are completed by each grantee. These reports are submitted quarterly within 30 days of the conclusion of each quarter. The data contained in each quarterly report is analyzed by the assigned Office of Citizenship program officer. Performance is

	measured in terms of percentage of grantees having achieved their pre-established goals by Q3 based on the original program proposal.
Data Collection Methodology	Due to the lag in the receipt of grantee performance data, the measure will be calculated by taking the total number of grantees meeting all of their performance goals through the 3rd quarter and dividing by the total of number of grantees during the performance period. An individual grantee will be considered to have met its overall annual performance goal if it achieves its stated grantee program goals through the 3rd quarter. The overall measure will be based on 90% of current grantees achieving this performance standard. To align with DHS reporting deadlines, this measure will be reported annually to DHS no later than 30 days after the end of the fiscal year and will be derived from grantee Quarterly Reports for quarters 1-3 of the given fiscal year.
Reliability Index	Reliable
Explanation of Data Reliability Check	The reliability of this measure will be established through uniform data collection and reporting procedures, through on-going follow-up with grantees on their reports, and through grantee monitoring visits. All grantees will receive training at the beginning of the performance period on how to complete the quarterly report forms. Office of Citizenship will provide written feedback on every filed quarterly report, and will ask grantees for clarification if there are questions about information found in the reports. Office of Citizenship will annually conduct in-person monitoring visits to approximately 1/3 of grantees. During these visits, staff will review records (e.g. student intake records, classroom attendance sheets, records of test scores, copies of filed N-400s) that were used to compile the data for the quarterly reports.

Goal 3.2: Prevent Unlawful Immigration

U.S. Citizenship and Immigration Services

Performance Measure	Accuracy rate of USCIS’s manual processing of Systematic Alien Verification for Entitlements (SAVE) Program referrals (Retired Measure)
Program	Immigration Status Verification
Description	The measure tracks the accuracy of SAVE manual verifications using a quality review which is a monthly review of verification work performed by Status Verifiers (SV) to determine whether SAVE referrals are resolved correctly. Specifically, they determine whether the response provided to by USCIS reflects the immigration status on record for persons seeking benefits from other governmental agencies using the SAVE program.
Scope of Data	Each month, a random sample of completed SAVE manual referrals consisting of either 2nd Step or 3rd Step cases is within the scope of data for this report. The appropriate sample sizes are taken to achieve a confidence level of 95 percent.
Data Source	A random sample of completed cases is taken from the Status Verification System (SVS) database and forwarded to verifiers for re-verification. The results are reported to the Quality Assurance (QA) section for analysis with results reported to supervisors for review and consultation with the QA section for completion and drafting of a summary of findings.
Data Collection Methodology	Based on historical data available, QA projects expected case volumes for each month in the fiscal year and samples that population to calculate the results of the report. Sample sizes are determined according to the expected monthly volumes for the audit being conducted and confidence parameters.
Reliability Index	Reliable
Explanation of Data Reliability Check	Cases are subject to a QA secondary review and vetting of results to ensure the accuracy of the findings. Findings are reviewed with supervisors from the appropriate unit to ensure accurate reporting.

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 Reliability Check	E-Verify transaction data are extracted quarterly from the VIS by the contractor 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 conducted that result in a potential finding of Fraud
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 conducted that result in a potential finding of fraud
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.

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	Dollar value of fines assessed for employers who have violated the I-9 requirements (Retired Measure)
Program	Homeland Security Investigations (HSI)
Description	The fines are a product of Form I-9 inspections, where an employer has violated the I-9 requirements. This fine amount is the final number, reported only after the appeals process or court hearings are concluded.
Scope of Data	Dollar value is a sum of individual case financial data maintained in ICE financial systems. The number of cases and individual case details are included in the weekly report with case count for validation of each entry.
Data Source	Data is compiled weekly by the Burlington Finance Center and reported to ICE Headquarters. Fines are reported in Excel by case number, company name, final order amount, and amount collected to date.
Data Collection Methodology	Meth: This financial data represents the total final order amount of the employer worksite enforcement fine and billed by the Burlington Finance Center. This data is calculated and reported weekly by the Burlington Finance Center.
Reliability Index	Reliable
Explanation of Data Reliability Check	Fine amounts are queried from ICE financial systems which are subject to audit control standards. Weekly reports are analyzed each week and compared to statistics from prior months and years for completeness and accuracy using trend analysis to ensure data quality.

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 arrested or sanctioned for criminally hiring illegal labor (Retired Measure)
Program	Homeland Security Investigations (HSI)
Description	This measure indicates the number of employers that are arrested or have sanctions imposed against them as a result of criminally hiring illegal labor into our workforce. Fines and sanctions serve as an important deterrent against employers hiring illegal labor.
Scope of Data	The scope of this measure includes all employer investigations resulting in a fine, sanction, or arrest.
Data Source	Specific case information is entered and maintained through TECS identifying the number of criminal arrests, sanctions, and/or amount of monetary fines levied against companies for a specific time period.
Data Collection Methodology	A data is pulled from TECS into an excel spreadsheet with the number of criminal arrests, sanctions, and/or amount of monetary fines levied against companies for a specific time period. This information is aggregated for the fiscal year to determine the number of employers arrested or sanctioned for criminally hiring illegal labor.
Reliability Index	Reliable
Explanation of Data Reliability Check	Case information in TECS is verified and audited by the HSI Data Quality Unit on a monthly basis.

Performance Measure	Number of employers audited, sanctioned, or arrested for violating immigration-related employment laws or otherwise brought into compliance with those laws (New Measure)
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 aliens arrested or charged who will be electronically screened through Secure Communities
Program	Enforcement and Removal Operations (ERO)
Description	Biometric information sharing between the Department of Justice fingerprint database (IAFIS) and the DHS immigration database (IDENT) allows a single query by a participating local law enforcement agency to check both systems and confirm the identification and immigration status of a subject. This measure gauges the percent of all aliens arrested in the United States that are screened through Secured Communities.
Scope of Data	The scope of the data is the total number of estimated criminal alien annual Law Enforcement Agency arrests in jurisdictions with IDENT/IAFIS Interoperability.
Data Source	The source of this data is the Law Enforcement Support Center (LESC) and ICE Enforcement and Removal Operations. An individual who is transferred from one correctional facility to another correctional facility and has fingerprints submitted at multiple locations are scrubbed from the database to only be counted once.
Data Collection Methodology	The data is calculated based on a merge of LESC data and ICE enforcement data. The annual percent is calculated by taking the total number of estimated criminal alien annual LEA arrests in jurisdictions with IDENT/IAFIS interoperability divided by the total estimated criminal alien annual LEA arrests in the United States.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data for this measure is calculated once a year for each county in the country. Everytime a new county deploys the technology, the percentage represented by that county is added to the cumulative total. Therefore, data reliability is maintained through limited modification. The data is maintained in a dashboard and is reviewed on a monthly basis for accuracy.

Performance Measure	Percent of detention facilities found in compliance with the national detention standards by receiving an inspection rating of acceptable or greater on the last inspection
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.

Mission 4: Safeguarding and Securing Cyberspace

Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment

Analysis and Operations

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. The survey results are defined by the currently available Office of Management and Budget vetted tool.
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	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 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.
-------------------	--

National Protection and Programs Directorate

Performance Measure	Average amount of time required for initial response to a request for assistance from public and private sector partners to prevent or respond to major cyber incidents (in minutes) (Retired Measure)
Program	Cybersecurity and Communications
Description	This measure assesses the average amount of time it takes DHS to initially respond to a request for technical assistance from a public (.gov) or private (.com) sector partner in order to prevent or respond to a major cyber incident.
Scope of Data	Request for assistance" is defined as the following: requests for technical assistance, malware analysis requests, digital media analysis requests, and requests for mitigation strategies from both private and public sector partners.
Data Source	The US-CERT Remedy Database (Helpdesk Worklog)
Data Collection Methodology	To determine the average time required for initial response to a request for assistance, the United States Computer Emergency Readiness Team (US-CERT) will use its internal Request for Technical Assistance (RTA) process which tracks the date and time of a request for technical assistance and the date and time US-CERT and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) initially responds to the requestor, i.e. provides the RTA template. The amount of time between the request for technical assistance and the initial response to the requestor will be calculated and the average across all requests will be used to calculate the actual result reported.
Reliability Index	Reliable
Explanation of Data Reliability Check	Data is valid and reliable as it is produced by many users and deposited in a single empirical data source, the Remedy system. The Python script ensures that data is pulled consistently each time by any individual tasked in the recovery and reporting of the data.

Performance Measure	Percent of cybersecurity mitigation strategies provided by DHS for unique vulnerabilities that are timely and actionable
Program	Cybersecurity and Communications
Description	The DHS National Cyber Security Division will follow up with cyber customers, to whom mitigation strategies were provided, in order to determine the timeliness and effectiveness of those strategies. A customer survey will be used to acquire data on areas such as timeliness, clarity, effectiveness, and sufficiency of mitigation strategies. This measures a program that is early stages of implementation.
Scope of Data	This measure is limited to customer feedback from the stakeholder survey attached to the following products: Security Awareness Reports, Critical Infrastructure Information Notices, and ICS-CERT Advisories.
Data Source	The data source for this performance measure is a stakeholder survey disseminated with the reports identified above. The surveys contains the standard Departmental question intended to elicit the degree of customer satisfaction with the usefulness of the intelligence report. The question asks customers to rate satisfaction on a five-point rating scale (very satisfied, somewhat satisfied, neither satisfied nor dissatisfied, somewhat dissatisfied, very dissatisfied). Responses

	"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 NCSO Front Office. The spreadsheet will contain several elements to include, but not limited to, the unique product identifier, date disseminated, date survey results received, score for each question, identifier for customer.
Data Collection Methodology	The United States Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) attach a survey to the bottom of the following products: Security Awareness Reports, Critical Infrastructure Information Notices and ICS-CERT Advisories. Two questions will be used to collect data for this measure: "Was this product timely?" and "Was this product actionable?" The responses are weighted and the answers to the two questions will be averaged and then divided by the total number of responses. A third question will be included in the survey to identify stakeholders for whom the vulnerability and associated mitigation strategy are not applicable (i.e. the vulnerability applies to an application or operating system that a given stakeholder does not use). The denominator will be adjusted to account for stakeholders who self-identify with the population for whom the vulnerability and associated mitigation strategy are not applicable.
Reliability Index	Reliable
Explanation of Data Reliability Check	Survey responses will be collected and maintained by NCSO Front Office and shared with US-CERT and ICS-CERT as part of their ordinary course of business. Data will be validated by program manager reviews in US-CERT and ICS-CERT, as applicable, and by the NCSO Front Office.

Performance Measure	Number of cybersecurity vulnerability and resiliency assessments and self-assessments facilitated by DHS (New 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 CSEP 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 Federal Executive Branch civilian networks monitored for cyber intrusions with advanced technology (Retired Measure)
Program	Cybersecurity and Communications
Description	This measure assesses DHS's increased vigilance for malicious activity across 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. This measures a program that is early stages of implementation.
Scope of Data	The scope of the data is the coverage of the 116 agencies formally identified by OMB. The percentage is determined by the number of agencies whose networks are at least partially monitored at Trusted Internet Connection (TIC) or Internet Service Provider locations, divided by the 116 identified agencies.
Data Source	The source of this data is two-fold: The equation denominator - the list of the 116 official agencies which comprise the Federal Executive Branch civilian network - is provided by OMB in Appendix C of OMB Circular A-11. In the event Appendix C is updated, DHS complies with the most current Appendix C list. The equation numerator - those agencies with traffic monitored by EINSTEIN 2 sensors - is tracked by the NCPS program office (Network Security Deployment). How that list is compiled and updated is explained in detail in the Data Collection Methodology.
Data Collection Methodology	For the 19 Trusted Internet Connection Access Providers (TICAPs) : 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 the National Cybersecurity & Protection System (NCPS) program managers. For the 97 Departments and Agencies with EINSTEIN 2 coverage at Internet Service Provider (ISP) locations: To begin EINSTEIN 2 coverage through an ISP, a Department or Agency and the participating ISP sign a "Banner Language" Memorandum of Agreement providing a formal agreement. These agreements are tracked by NCPS, and used to monitor the number of Departments and Agencies with ISP coverage. No FY13-15 targets as predictive reliability decreases in those years and a new methodology for calculating this measure will be presented for FY13- the amount of total traffic covered by DA sensors will be tracked and calculated.

Reliability Index	Reliable
Explanation of Data Reliability Check	The completion of EINSTEIN installations and Banner Language MoAs are validated by the respective program managers during the review process.

Performance Measure	Percent of incidents detected by the U.S. Computer Emergency Readiness Team for which targeted agencies are notified within 30 minutes (New Measure)
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 organizations that have implemented at least one cybersecurity enhancement after receiving a cybersecurity vulnerability assessment or survey (New Measure)
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 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 unique vulnerabilities detected during cyber incidents where mitigation strategies were provided by DHS (Retired Measure)
Program	Cybersecurity and Communications
Description	This measure indicates the percent of unique, known cyber vulnerabilities, detected during cyber incidents, where DHS provides a mitigation strategy to address the vulnerabilities and prevent the incident from recurring.
Scope of Data	The scope of data includes all unique high vulnerabilities that meet the US-CERT Priority Information Requirements (PIR), have a workable solution, and are under the realm of responsible disclosure.
Data Source	The US-CERT Remedy Database (Helpdesk Worklog).
Data Collection Methodology	When United States Computer Emergency Readiness Team (US-CERT) becomes aware of a unique high vulnerability, the person who receives the information will check it against the Priority Information Requirements (PIRs). If it meets one of the criteria, they will inform the US-CERT Senior Watch Officer who will record it in the PIR spreadsheet, and follow up with US-CERT analysts and the production team. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) collects information in its ticketing system and will track vulnerabilities for which mitigations are issued to the community.
Reliability Index	Reliable
Explanation of Data Reliability Check	The data is valid and reliable as it is produced by many users and deposited in a single empirical data source, the Remedy system. The SQL script ensures that data is pulled consistently each time by any individual tasked in the recovery and reporting of the data.

U.S. Secret Service

Performance Measure	Amount of dollar loss prevented by Secret Service cyber investigations (in millions) (New Measure)
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 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	Financial crimes loss prevented by the Secret Service Electronic Crimes Task Forces (in millions) (Retired Measure)
Program	Criminal Investigations
Description	This measure is an estimate of the direct dollar loss to the public prevented due to investigations by Secret Service Electronic Crimes Task Forces (ECTFs) throughout the United States. The estimate is based on the likely amount of electronic financial crime that would have occurred had the offender not been identified nor the criminal enterprise disrupted. It reflects the Secret Service's efforts to reduce financial losses to the public attributable to electronic crimes. The program provides manpower on a temporary basis to support protective assignments; Field agents provide a "surge capacity" of protective manpower, without which the Secret Service could not accomplish its protective mandate in a cost-effective manner. Although these temporary assignments occur every year, they increase during a presidential campaign requiring the Secret Service to decrease its performance measure targets in campaign years.
Scope of Data	The scope of this measure includes all investigations by ECTFs which were closed in the fiscal year being reported. Any 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 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 Electronic Crimes Task Force 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	The Master Central Index 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) (New Measure)
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 (New Measure)
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	Terabytes of data forensically analyzed and protected from future malicious use (New Measure)
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.

Goal 4.2: Promote Cybersecurity Knowledge and Innovation

Science and Technology Directorate

Performance Measure	Percent of planned cybersecurity products and services transitioned to commercial and open sources (New Measure)
Program	Research, Development, and Innovation
Description	This measure reflects the percent of Science & Technology Directorate, projects that identify and complete planned transitions of a cyber security product and/or service to a commercial or open source. The percent reported is reviewed using the number of planned transitions stated in CSD'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 all Phase III research projects and programs efforts will be included in developing this measure (The program groups its research into Phase I/II/III, with Phase III research addressing the most advanced technology readiness levels and hence ready for transition). The data will be both quantitative and qualitative, i.e. absolute numbers of projects/programs and several judgments of the quality of the transition effort, 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 program and program review documentation as the reference material to develop an annual "measures analysis paper," where the numbers of Phase III projects are listed, they are discussed, table summaries of are listed, and analytical explanation and justification for the determination of the final qualitative measure will be provided.
Data Collection Methodology	The percent reported is reviewed using the number of intended transitions stated in budget execution plan for the fiscal year, and the explanation that is provided in each quarterly data call. The 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 and financial responsibility transferred from S&T to the intended partner, customer, end-user, etc. Independent peer research managers evaluations will focus on the status of new or improved cyber security products or services transitioned to provisional or final availability, accessible through commercial, GSA schedule or open source vehicles. It will consider successful transition of those within reach of transition, how well the program has prepared the transition process (prior planning with users, completion of development, project evaluation and red team completed, etc.).
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 (New 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.

Mission 5: Ensuring Resilience to Disasters

Goal 5.1: Mitigate Hazards

Federal Emergency Management Agency

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 through their BCEGS database to the program; however, the data are reviewed by FEMA's Mitigation program to ensure results are consistent over time. If significant fluctuations in quarterly and annual results occur, the program will work with ISO to address issues with data reliability.

Performance Measure	Percent of households surveyed reporting they have taken steps to mitigate damage to property and protect themselves in the event of a disaster
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	Reliable
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 U.S. population (excluding territories) covered by planned mitigation strategies
Program	Mitigation
Description	This is a point in time metric that determines the percent of U.S. population (excluding territories) covered by approved or approvable local Hazard Mitigation Plans. The population of each community with approved or approvable local Hazard Mitigation Plans is used to calculate the percentage of the national population. The FEMA Mitigation program gathers and analyzes critical data to aid in future mitigation efforts and enable communities to be better informed and protected. FEMA Mitigation helps communities reduce risk through sound land-use planning principles (such as planned mitigation strategies), floodplain management practices, and financial assistance.
Scope of Data	The scope of this measure includes all United States jurisdictions excluding territories.
Data Source	Data are derived from Regional Reports and are entered into 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.

Goal 5.2: Enhance National Preparedness through a Whole Community Approach to Emergency Management

Federal Emergency Management Agency

Performance Measure	Number of corrective actions completed to improve performance following National Level Exercises (since FY 2007)
Program	Preparedness
Description	This measure will count completed corrective actions assigned to DHS for action resulting from National Level Exercises. A National Level Exercise (NLE) helps the Federal Government prepare and coordinate a multiple-jurisdictional integrated response to a national catastrophic event. A NLE is the capstone exercise conducted as the final component of each National Exercise Program cycle and requires the participation of all appropriate department and agency principals, other key officials and all necessary staffs and operations centers, and operational elements at both the national and regional/local levels. The capstone exercise satisfies the biennial national exercise requirement established in 6 USC 748(b) (3). Corrective actions identified from the exercise are assigned to the respective Agency for completion and validation.
Scope of Data	The scope of this measure includes all agreed upon action items (since FY 2007) assigned to DHS as a result of a National Level Exercise. This is an ongoing cumulative measure.
Data Source	Agreed upon action items are consolidated and incorporated into an improvement plan. All action items are then entered into the FEMA's Corrective Action Program (CAP) System database.
Data Collection Methodology	CAP is a component of FEMA's Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP serves as the doctrine for design, conduct, and evaluation of National Exercise Program exercises. Each DHS Component has a designated Action Officer who is responsible for tracking and updating the implementation status of a corrective action for their respective organization. The number of completed Corrective Actions assigned to DHS is calculated by adding the total number of corrective actions listed in the Improvement Plans for the National Level Exercise which have been assigned to DHS since FY 2007 and marked as "Completed" within the CAP System.
Reliability Index	Reliable
Explanation of Data Reliability Check	Each department and agency is responsible for verifying their organization's Point of Contact (POC) for the CAP System, monitoring their respective corrective actions, and updating the status as "open, complete, validated, or cancelled". Each department and agency, including FEMA, can run reports from the CAP System to obtain status data on corrective actions for their agency. The verification that corrective actions have been successfully implemented can only be determined through experience in another exercise or real world event. This can take several years to determine and so is not included in this measure.

Performance Measure	Percent of high-priority core planning capabilities rated as proficient by states and territories (New Measure)
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 that, aside from a fire drill, participated in a preparedness exercise or drill at their workplace, school, or home in the past two years (New Measure)
Program	Preparedness
Description	This measure calculates the percent of households responding to a survey who indicate that, aside from a fire drill, they have participated in a preparedness exercise or drill like the ShakeOut in their workplace, school, or home in the past two years. The survey collects individual disaster preparedness data from a random sample of households across the nation.
Scope of Data	As part of the Nationwide Household Survey, a total of about 2,000 or more telephone interviews are conducted during the spring each year on individual and household preparedness. The survey contacts individuals throughout the United States and the six territories.
Data Source	The FEMA National Survey is conducted by National Preparedness Directorate (NPD) contractors who collect the data in the statistical analysis program SPSS and provide 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,

	aside from a fire drill, participated in a preparedness exercise or drill like the ShakeOut in their workplace, school, or home in the past two years. Results from the survey are collected in SPSS. When processing the data from the random digit dialing surveys, results are weighted according to geography, age, gender and race to account for potential biases such as over- and under-representation of certain population segments. This adjusted the sample's demographic distributions to match the distribution in the American Community Survey 5-Year estimates for 2005 through 2009 population 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 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 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.

Performance Measure	Percent of households surveyed reporting they have taken steps to be prepared in the event of a disaster (Retired Measure)
Program	Preparedness
Description	This measure tracks the percent of surveyed households who report that they have taken specific actions, such as attend skills training, gathered disaster supplies, and/or developed a disaster plan to prepare for disasters relevant to their community.
Scope of Data	As part of the National Disaster Preparedness Survey, more than 2,700 telephone interviews are conducted from May to July of each year on the steps being taken to be prepared in the event of a disaster. The survey covers the United States and the six territories.
Data Source	The results of the survey are recorded in a statistical analysis program called SPSS. Responses to the questions specific to this measure are extracted from SPSS by the independent contractor and provided to the program for analysis.
Data Collection Methodology	This measure calculates the percent of households surveyed who reported taking steps in 2 out of 3 key categories of preparedness: 1) Be informed, 2) Make a Plan, and 3) Get a Kit. Calculation is based on a random telephone/cell national household survey of over 2,000 respondents that are weighted to match U.S. population distributions according to U.S. Census population estimates. Data is collected by relevant demographic factors in order to provide information on significant differences by factors such as income, age, education, race/ethnicity, disability.
Reliability Index	Reliable
Explanation of Data Reliability Check	Survey responses are analyzed and checked for completeness and reliability through several layers of reviews by the contractor and then reviewed by National Preparedness personnel.

Performance Measure	Percent of states with a Threat and Hazard Identification and Risk Assessment (THIRA) that meets current DHS guidance (New Measure)
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.

Goal 5.3: Ensure Effective Emergency Response

Federal Emergency Management Agency

Performance Measure	Percent of essential incident command functions (enabled through response teams and operations centers) that are established within 12 hours (Retired Measure)
Program	Response
Description	This measure gauges the percent of time that response teams and operations centers are established in order to successfully perform essential incident command functions to respond to disasters effectively and in a unified manner within 12 hours of being notified of deployment.
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.
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. FEMA's 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 NWC database is used as the system of record and is archived for historical reference. Program personnel review the data after each deployment to ensure data entered are accurate. Any anomalies are research against other data to confirm time of notification.

Performance Measure	Percent of incident management and support actions necessary to stabilize a jurisdiction within 72 hours or by the agreed upon time (New Measure)
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 (New Measure)
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. FEMA's 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 jurisdictions with access to the FEMA National Shelter System which allows users to locate and monitor open congregate shelters (Retired Measure)
Program	Recovery
Description	This measure reflects the percent of states with a signed Memorandum of Agreement (MOA) to utilize the FEMA's National Shelter System (NSS) to monitor disaster shelter activity. The NSS is a comprehensive, web-based database created to support federal, state, and local government agencies and voluntary organizations responsible for Mass Care and Emergency Assistance. The FEMA NSS allows users to identify, track, analyze, and report on data for virtually any facility associated with the congregate care of people and/or household pets following a disaster.
Scope of Data	The scope of this measure is based on the number of States that have signed a MOA with FEMA to utilize the FEMA National Shelter System (NSS). The FEMA NSS is available to all 50 States and U.S. territories for preparedness and operations. Federal, state, and local government officials are provided access to the FEMA NSS based upon a signed MOA with FEMA for use of the system.
Data Source	The FEMA National Shelter System (NSS) is a web-based reporting tool for use by federal, state, and local officials to locate and monitor open congregate shelters

	and numbers of sheltered individuals. The FEMA Headquarters Individual Assistance Division monitors all presidentially declared disasters that occur in the 50 States and U.S. territories each fiscal year. Memorandums with States are signed by the FEMA Regional Administrator. The original MOA is maintained in the Region and a copy is sent to FEMA Headquarters and retained by the Recovery Directorate Individual Assistance Division.
Data Collection Methodology	The program uses the number of MOAs executed with states as a percentage of the 50 states. The number of MOAs is based upon executed MOAs as indicated by the date of the last signature by the parties on the signature page of the MOA and the date specified in the MOA as the period the MOA will remain in effect.
Reliability Index	Reliable
Explanation of Data Reliability Check	FEMA staffs in the Recovery Directorate verify the number of signed, current Memorandums of Agreement quarterly.

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 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 time that critical communications for response operations are established within 12 hours (Retired Measure)
Program	Response
Description	This measure reflects the percent of time that critical communications are established for FEMA's on-site emergency responders within 12 hours of the deployment of Mobile Emergency Response Support (MERS). MERS is FEMA's critical communications capability for response operations and provides self-sufficient, mobile telecommunications, life support, logistics, operational support and power generation for all-hazards disaster response activities. The six MERS

	Detachments are located throughout the U.S. to rapidly respond to all incidents. Detachments support National Special Security Events as well as other planned special events and activities and provide a cost-effective solution to National Response Framework requirements allowing staff at the Joint Field Offices to focus on immediate response and recovery activities. MERS Operations Centers specialists support FEMA's network of operations centers providing situational awareness down to the incident site level.
Scope of Data	The scope of this measure includes all significant activities or events that require the deployment of MERS.
Data Source	MERS notification and arrival time are tracked by FEMA's National Response Coordination Center (NRCC) database and recorded in the Activities Log portion of the database, which is maintained as the document of record for all incidents.
Data Collection Methodology	Upon notification, the MOC begins tracking the movement of MERS teams and their work to establish capabilities. These activities are documented in FEMA's NRCC database. The NRCC database is used and maintained as the system of record for all incidents. FEMA's Response personnel query the activities/events log module of the database to extract pertinent data. This data is then analyzed by comparing the time it took to establish communications to the time teams were initially notified of deployment. Response personnel evaluate data based on the total number of actual real-world or exercise deployments, rather than a specific number of deployments throughout the year. Thus, the denominator varies based on the disaster activity in any given year. Response personnel then calculate how frequently the evaluated teams established critical communications within 12 hours.
Reliability Index	Reliable
Explanation of Data Reliability Check	FEMA's NRCC database is used as the system of record and is archived for historical reference. Program personnel review the data after each deployment to ensure data entered are accurate. Any anomalies are researched against other data to confirm time of notification.

Performance Measure	Percent of urban search and rescue teams arriving on scene within 12 hours of deployment notification (Retired Measure)
Program	Response
Description	Urban Search and Rescue (US&R) teams have a requirement to arrive on scene within 12 hours of deployment notification to save and sustain lives and minimize suffering in a timely manner in communities overwhelmed by acts of terrorism, natural disasters, or other emergencies. This standard applies to task forces travelling by ground and by air. The optimum traveling method for the task forces is determined at the time of mobilization. This measure includes the task force members and their support equipment as well as the commanding element (Incident Support Team).
Scope of Data	The scope of this measure includes all significant activities or events that require the deployment of one or more US&R teams.
Data Source	US&R team notification and arrival time are tracked by FEMA's National Response Coordination Center (NRCC) database and recorded in the Activities Log portion of the database, which is maintained as the document of record for all incidents.
Data Collection Methodology	Upon notification, FEMA's NRCC staff record on-site arrival times of teams in the NRCC database. Once the team arrives on scene, team leaders contact the NRCC to update their status. Response personnel query the database to extract pertinent data. This data is then analyzed by comparing the time it took to arrive on site to the time teams were initially notified of deployment. Response personnel evaluate data based on the total number of actual real-world or exercise deployments. The denominator varies based on the disaster activity in any given year. Response personnel then calculate frequency of US&R capabilities

	established within 12 hrs.
Reliability Index	Reliable
Explanation of Data Reliability Check	FEMA's NRCC database is used as the system of record and is archived for historical reference. Program personnel review the data after each deployment to ensure data entered are accurate. FEMA also uses a vehicle tracking tool to provide visual real-time data of team location/arrival times. Response personnel examine this data to verify the arrival times.

National Protection and Programs Directorate

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, processes 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 high-risk urban areas designated within the Urban Areas Security Initiative (UASI) able to demonstrate increased Emergency Communications capabilities (Retired Measure)
Program	Cybersecurity and Communications
Description	This measure gauges the percent of high-risk urban areas within the UASI that display a five percent or more increase in their overall communications capabilities, based on the SAFECOM Interoperability Continuum. This measures a program that is early stages of implementation.
Scope of Data	Includes data collected by OEC from the States with Urban Area Security Initiative regions as of July 2008 (publication date of the NECP). This was done in Fall 2010 as part of the States' annual Statewide Communications Interoperability Plan (SCIP) reports.
Data Source	Statewide Interoperability Coordinators (SWIC) provided the final data from 60 UASIs to OEC.
Data Collection Methodology	This measure will account only for those UASIs (out of 60) that display a five percent or more increase in their overall communications capabilities, based on

	the SAFECOM Interoperability Continuum. The Office of Emergency Communications (OEC) utilizes the SAFECOM Interoperability Continuum to identify key capabilities that we believe enable successful emergency communications. The capability factors are 1) utilization of strong governance structures, 2) utilization of SOPs and formal agreements, 3) what technology is used, 4) whether the technology is used regularly, and 5) training and exercises. OEC has a 3-year Paperwork Reduction Act approval for data collection starting in FY 2011. During FY 2011, OEC will work to establish baselines, against which UASI progress will be assessed starting in FY 2012.
Reliability Index	Unreliable. The Office of Emergency Communications did not have the mechanism to collect the data required to report results for this measure. The measure is being retired as the program does not have the ability to develop a reliable methodology to collect the needed data.
Explanation of Data Reliability Check	The 60 UASIs self-assess and self-report the data to their State coordinator (the SWIC), who is responsible for verifying the completeness and accuracy of the results before officially submitting to OEC.

Performance Measure	Percent of urban area interoperable communications capabilities that are rated at the most advanced levels (New 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	Reliable
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.

Goal 5.4: Rapidly Recover from a Catastrophic Event

Federal Emergency Management Agency

Performance Measure	Percent of eligible applicants provided temporary housing (including non-congregate shelters, hotel/motel, rental assistance, repair and replacement assistance, or direct housing) assistance within 60 days of a disaster (Retired Measure)
Program	Recovery
Description	This measure tracks the percent of eligible applicants seeking temporary housing assistance and provided temporary housing assistance within 60 days of a disaster. FEMA temporary housing assistance includes transitional sheltering assistance (hotel/motel), rental assistance, repair and replacement assistance, or direct housing (temporary housing units).
Scope of Data	The scope of this measure is based on actual, eligible applicant data from presidentially declared disasters. FEMA may provide assistance to individuals and households who qualify for such assistance under section 408 of the Stafford Act and in accordance with Title 44 CFR 206.113 eligibility factors.
Data Source	Individuals affected by a disaster can apply to FEMA for disaster assistance online through disasterassistance.gov or via tele-registration. Initial applicant data is recorded in the National Emergency Management Information System (NEMIS), in accordance with Title 44 CFR 206.113. Basic eligibility, as determined through the Registration Intake process, may trigger an on-site housing inspection to verify damages. After the inspection data is loaded into NEMIS, the qualified applicants eligibility for housing assistance is determined. The FEMA National Processing Service Centers are the central repository for data collection; eligibility data is transmitted to the FEMA Finance Center for disbursement of financial rental assistance, repair assistance, and/or replacement assistance. Data for direct assistance for temporary emergency housing is collected by FEMA staff and captured in the Direct Assistance Replacement Assistance Consideration (DARAC) portal in NEMIS.
Data Collection Methodology	Data is collected from NEMIS to identify the number of survivors receiving Rental Assistance, Transitional Sheltering Assistance, Home Repair Assistance, Replacement Assistance and Temporary Housing Units. Applicants are counted only once using the following hierarchy of assistance category: Rent Financial assistance for rental of alternate housing unit; Transitional Sheltering Direct assistance in the form of hotel lodging; Home Repair Financial assistance for repair of primary residence; Replacement Financial assistance for replacement of primary residence; Temporary Housing Unit Direct assistance in the form of temporary housing units (manufactured housing, etc.). The number of eligible applicants provided temporary housing assistance within 60 days is determined by the number of days between the date of registration and the date housing assistance was enabled.
Reliability Index	Reliable
Explanation of Data Reliability Check	Information provided by applicants is compared with public records in order to verify identity, occupancy, and property ownership. This information, as well as insurance coverage, is verified during field housing inspections. Applicants may be required to submit additional insurance settlement information to the FEMA National Processing Service Centers (NPSC) for manual review by FEMA staff before they are eligible for certain financial assistance. The NPSC Quality Control Section reviews a sample of manual eligibility determinations processed by the NPSCs through the National Emergency Management Information System (NEMIS) for accuracy.

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 (New Measure)
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 (New Measure)

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.

Providing Essential Support to National and Economic Security

Goal: Collect Customs Revenue and Enforce Import/Export Controls

U.S. Customs and Border Protection

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.

Goal: Ensure Maritime Safety and Environmental Stewardship

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 Reliability Check	The program manager 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. 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
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	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	Checks on data input are made by individual case owners during the case

Reliability Check	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.
-------------------	---

Goal: Conduct and Support Other Law Enforcement Activities

Federal Law Enforcement Training Center

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 three 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.

U.S. Secret Service

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.

Cross-Cutting Performance Measures

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.

Federal Law Enforcement Training Center

Performance Measure	Percent of Partner Organizations that agree the Federal Law Enforcement Training Center 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 Center (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 that respond to the Partner Organization Satisfaction Survey Items 30 and 31, respectively: "FLETC's basic training programs address the right skills needed for my officers/agents to perform their law enforcement duties," and "FLETC's advanced training programs address the right skills needed for my officers/agents to perform their law enforcement duties." FLETC collaborates with more than 80 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. Each respondent (for example, the Partner Organization Training Academy representative on-site or a knowledgeable agency representative off-site) enters survey data through Vovici and saves the responses online when the survey is completed.
Data Collection Methodology	The FLETC Partner Organizations (POs) are surveyed using the Partner Organization Satisfaction Survey. The measure uses an average of survey Item 30 and 31. Item 30 begins "The FLETC's basic training programs"; Item 31 begins "The FLETC's advanced training programs." Each item ends with "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 Items 30 and 31 divided by the number of POs that responded to each of the respective items. POs that responded "Not Applicable" to either Item 30 and/or 31 were excluded from the calculations for the respective item(s).
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.
--	--



Homeland
Security



Homeland
Security