# Annual Performance Report

Fiscal Years 2007 - 2009

## Appendix B

Verification and Validation of Performance Measures

Homeland Security

Pursuant to OMB Circular A-136, this year's Finance and Performance reporting is following an Office of Management and Budget (OMB) Pilot Program for Alternative Approaches to Performance and Accountability Reporting. The pilot is an alternative to the consolidated Performance and Accountability Report (PAR) published in previous years. DHS anticipates this approach will improve its performance reporting by presenting performance information in a more accessible and informative format, and that performance information will be more complete given additional time to collect actual year-end performance data. Additionally, the pilot approach will ensure performance results and plans are integrated with the President's Budget.

The pilot consists of three separate reports:

- **Annual Financial Report (AFR)**. The AFR consists of the Secretary's Message, Management's Discussion and Analysis, Financial Statements and Notes, the Audit Report, Major Management Challenges, and other required information. The AFR was published on 15 November 2007, and is available at the DHS website.

- **Annual Performance Report (APR)**. The APR contains more detailed performance information as required by the Government Performance and Results Act (GPRA). The APR reports fiscal year (FY) 2007 results and presents the DHS Performance Plan for FY 2009. The APR is transmitted with the Congressional Budget Justification (CBJ) on 4 February 2008 and is posted on the DHS website.

- **Highlights Report**. The Highlights report summarizes key performance and financial information and is available at the DHS website just prior to publication of the President's Budget.

The Department of Homeland Security's FY 2007 Annual Performance Report is available at the following website: http://www.dhs.gov/xabout

For more information or to obtain additional copies, contact:

Department of Homeland Security
Office of the Chief Financial Officer/PA&E
245 Murray Lane SW
Mailstop 0200
Washington, DC 20528

par@dhs.gov
(202) 447-0333

# Table of Contents

To easily locate a measure by name, an alphabetical list of all measures is provided in the index at the back of the report.

## Introduction

This Appendix provides, in tabular format, a detailed listing of the means used to verify and validate all performance measures in the Annual Performance Report. Verification and validation descriptions are grouped by Component as identified in the Table of Contents. Programs are listed alphabetically by Component, and performance measures are listed alphabetically within a program. To easily locate a performance measure by name, an alphabetical list of all measures is provided in the Index at the back of the report.

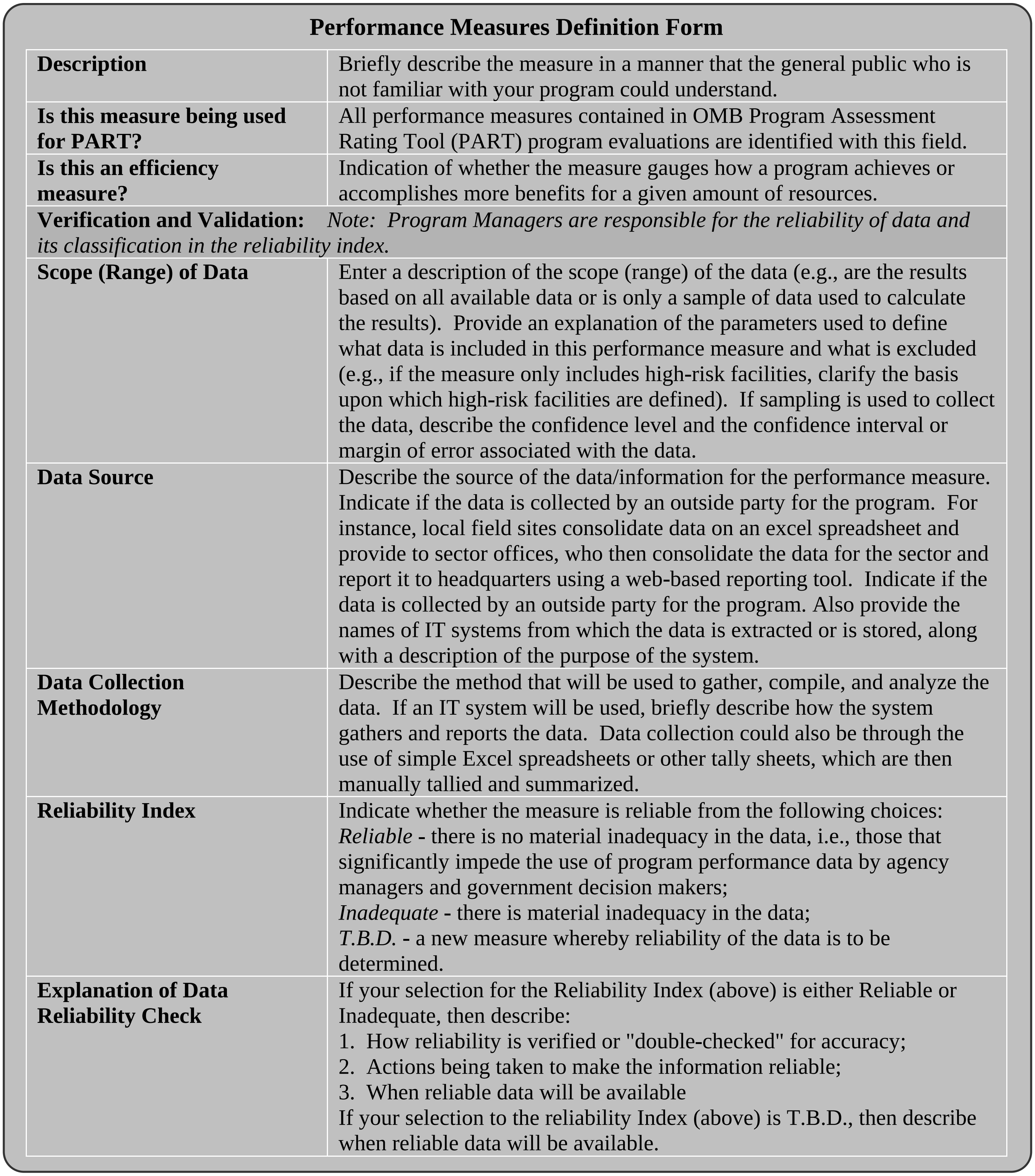
The performance measures listed in this Appendix include both measures that are being retired from the Department of Homeland Security (DHS) Performance Plan, and new measures that are making their initial debut in the DHS Performance Plan. New and retired measures are noted within the tables in this Appendix and in similar tables in the Annual Performance Report. A new DHS Performance Plan measure does not necessarily mean that the program has not been using this measure to gauge performance, but this is the first year it has been included in the DHS Performance Plan. Likewise, a retired plan measure, although not in the DHS Performance Plan going forward, may still be used by the program for management purposes.

The Department recognizes the importance of collecting complete, accurate, and reliable performance data, as this helps determine progress toward achieving program and Department goals and objectives. Program Managers are responsible for the reliability of performance measurement information for programs under their cognizance. To encourage completeness and reliability, DHS evaluates the verification and validation information for each performance measure during its annual Resource Allocation Planning (RAP) process. This review evaluates the quality of descriptive information for each performance measure. The figure on the next page is a copy of the form used by the programs to ensure performance measures are complete and reliable.

For each performance measure presented in the Annual Performance Report, a description of the measure, the source of the data, how it is collected, and an assessment of the reliability of data is provided. Figure 1 provides a description of the DHS Performance Measure Definition Form fields used to gather and report this information. Reliability is determined by Office of Management and Budget (OMB) guidance. At a minimum, performance data are considered reliable if Program Managers and decision makers use the data on an ongoing basis in the normal course of their duties. In addition, performance data are considered reliable if transactions and other data that support reported performance measures are properly recorded, processed, and summarized to permit the preparation of performance information in accordance with criteria stated by management. Performance data need not be perfect to be reliable, particularly if the cost and effort to secure the best performance data possible will exceed the value of any data so obtained.

The Department has reviewed performance measures for conformance to the standard of completeness and reliability as specified for federal agencies in *OMB Circular A-136, Financial Reporting Requirements, Section II.3.4.4 Assessing the completeness and reliability of performance data;* and *OMB Circular A-11, Preparation, Submission and Execution of the Budget*, *Section 230.2 (e*), *Assessing the completeness and reliability of performance data.* Performance information contained within this report is complete and reliable in accordance with these standards.

**Figure 1. Completeness and Reliability Framework**



### Performance Measures Definition Form

| | |
|---|---|
| **Description** | Briefly describe the measure in a manner that the general public who is not familiar with your program could understand. |
| **Is this measure being used for PART?** | All performance measures contained in OMB Program Assessment Rating Tool (PART) program evaluations are identified with this field. |
| **Is this an efficiency measure?** | Indication of whether the measure gauges how a program achieves or accomplishes more benefits for a given amount of resources. |
| **Verification and Validation:** *Note: Program Managers are responsible for the reliability of data and its classification in the reliability index.* | |
| **Scope (Range) of Data** | Enter a description of the scope (range) of the data (e.g., are the results based on all available data or is only a sample of data used to calculate the results). Provide an explanation of the parameters used to define what data is included in this performance measure and what is excluded (e.g., if the measure only includes high-risk facilities, clarify the basis upon which high-risk facilities are defined). If sampling is used to collect the data, describe the confidence level and the confidence interval or margin of error associated with the data. |
| **Data Source** | Describe the source of the data/information for the performance measure. Indicate if the data is collected by an outside party for the program. For instance, local field sites consolidate data on an excel spreadsheet and provide to sector offices, who then consolidate the data for the sector and report it to headquarters using a web-based reporting tool. Indicate if the data is collected by an outside party for the program. Also provide the names of IT systems from which the data is extracted or is stored, along with a description of the purpose of the system. |
| **Data Collection Methodology** | Describe the method that will be used to gather, compile, and analyze the data. If an IT system will be used, briefly describe how the system gathers and reports the data. Data collection could also be through the use of simple Excel spreadsheets or other tally sheets, which are then manually tallied and summarized. |
| **Reliability Index** | Indicate whether the measure is reliable from the following choices:<br>*Reliable* - there is no material inadequacy in the data, i.e., those that significantly impede the use of program performance data by agency managers and government decision makers;<br>*Inadequate* - there is material inadequacy in the data;<br>*T.B.D.* - a new measure whereby reliability of the data is to be determined. |
| **Explanation of Data Reliability Check** | If your selection for the Reliability Index (above) is either Reliable or Inadequate, then describe:<br>1. How reliability is verified or "double-checked" for accuracy;<br>2. Actions being taken to make the information reliable;<br>3. When reliable data will be available<br>If your selection to the reliability Index (above) is T.B.D., then describe when reliable data will be available. |

## Customs and Border Protection

| | |
|---|---|
| Performance Measure | Number of trade accounts with access to ACE functionality to manage trade information. |
| Program and Organization | Automation Modernization - Customs and Border Protection |
| Description | This measures the extent to which the Automated Commercial Environment (ACE) is made available to and used by members of the trade community (importers, brokers, carriers, etc.) to process and manage trade-related information. |
| Scope | This measure represents the cumulative number of ACE accounts associated with the trade community, (i.e., those outside CBP) from the introduction of the accounts feature in ACE. The number of trade accounts end-state (expected universe of accounts associated with trade community users) is an unknown variable due to marketplace dynamics. However, targets for this performance measure have been determined based on trend data. |
| Data Source | Data is manually gathered monthly by the CBP Modernization Office personnel as they establish new accounts for companies moving goods through borders nation-wide. The data related to new accounts is recorded and contained in an Excel spreadsheet entitled "FBO Data.xls." |
| Collection Method | The data is collected in a spreadsheet and displayed graphically. The CBP Modernization Office team performs analysis of the reported data to assess program performance and the attainment of Program Objectives, and to identify corrective actions if necessary. |
| Reliability | Reliable |
| How Data is Verified | Accounts are tracked by contractor teams establishing accounts and verified by the government CBP Modernization Office leaders. Verification of ACE performance data is done through a variety of tools and techniques, including comparative analysis between multiple reports generated from ACE. For example, a particular data point may be appear in multiple ACE reports. Inconsistent data appearing on any of those multiple reports is investigated. Comparative analysis with reports created outside ACE. Data sourced outside ACE is sometimes used to verify ACE-generated data to ensure consistency and standard reporting. Validation occurs to ensure that the report query instructions are sourcing the correct data fields, and that the data contained in those fields is defined correctly. |

| | |
|---|---|
| Performance Measure | Percent of CBP workforce using ACE functionality to manage trade information. |
| Program and Organization | Automation Modernization - Customs and Border Protection |
| Description | The number of Customs and Border Protection people using Automated Commercial Environment (ACE), compared to the targeted adoption rate shows that internal personnel have easier, timelier, access to more complete and sophisticated information than in the past. |
| Scope | The data represents the percentage of CBP personnel using ACE expressed as a percentage of the total CBP population with trade management-related job duties. The total population of CBP Users is a nationwide human resource statistic. The time span for this measure includes the introduction of the accounts feature in ACE (2004). |
| Data Source | The source for the number of CBP users is a function of the ACE system. User statistics are tracked automatically by the system. |
| Collection Method | ACE tracks and reports the number of users, over time, by user type. The CBP Modernization Office team performs analysis of the reported data to assess program performance and the attainment of Program Objectives, and to identify corrective actions if necessary. |
| Reliability | Reliable |
| How Data is Verified | User data is created with each user log-on and use. Reports are generated by the system to capture this data and provide an audit trail. The Program Management |

| | |
|---|---|
| | Office team regularly reviews these reports and associated user logs to analyze and resolve anomalies. Verification of ACE performance data is done through a variety of tools and techniques, including comparative analysis between multiple reports generated from ACE. For example, a particular data point may appear in multiple ACE reports. Inconsistent data appearing on any of those multiple reports is investigated. Comparative analysis with reports created outside ACE. Data sourced outside ACE is sometimes used to verify ACE-generated data to ensure consistency and standard reporting. Validation occurs to ensure that the report query instructions are sourcing the correct data fields and that the data contained in those fields is defined correctly. |

| | |
|---|---|
| Performance Measure | Percent of network availability. |
| Program and Organization | Automation Modernization - Customs and Border Protection |
| Description | The CBP network provides the basis for linking all IT systems for communications and access to mission critical systems. High levels of system availability are needed to accomplish CBP's mission. This measure represents the percent of network availability to users. |
| Scope | Information is recorded for the following CBP applications: Automated Commercial Environment, Immigration and Customs Enforcement, United States-Visit , Customs and Border Protection Network, Passenger Name Record (PNR) Network and others as requested, including, Routers; Switches; Network nGenus probes; Network Analysis Module Traffic data and RMON1 and RMON2 data; new Packet Shapers for traffic analysis; server Agent or Simple Network Management Protocol (SNMP) messaging; other communications devices with SNMP capability on the device. Concord eHealth live can collect performance data from the applications like Oracle/Windows IIS, Apache, others. |
| Data Source | SNMP data source is directly retrieved from managed device every five minutes |
| Collection Method | To find the resources, eHealth uses SNMP agents to search for the IP addresses that are specified. It then obtains the information from the Management Information base (MIB) of each device and creates elements based on that data. The results are sent, and eHealth stores all the information into its database and its poller configuration. The e-health poller automatically collects performance and availability statistics data from the network, systems and applications through the polling process. Once the polling process collects the statistical data it is saved on the eHealth servers and backup tapes. |
| Reliability | Reliable |
| How Data is Verified | eHealth provides two administrative interfaces that are used to manage the poller elements. OneClickEH and the eHealth Console. These tools are used to add new elements, organize elements, update element information, and resolve polling errors. The Network Management Toolset adopted by CBP/DHS Network Operations Center provides 24x7 staff with real-time data on the availability and utilization of critical network infrastructure devices. This polling and reporting is based on the Simple Network Management Protocol (SNMP), an industry standard method for gathering information from network devices for the purpose of managing those devices or reporting on availability of those devices. While we have had no reason to question the accuracy of information provided by this industry-standard and industry-tested set of protocols, we can validate our toolsets finding against those of our Managed Service Providers, who maintain their network management infrastructure with no ties to our own. |

| | |
|---|---|
| Performance Measure | Percent of time the Traveler Enforcement Communications System (TECS) is available to end users. |
| Program and Organization | Automation Modernization - Customs and Border Protection |
| Description | TECS is a CBP mission-critical law enforcement application system designed to identify individuals and businesses suspected of or involved in violation of federal law. TECS is also a communications system permitting message transmittal between DHS law enforcement offices and other National, State, and local law |

| | |
|---|---|
| | enforcement agencies. TECS provides access to the FBI's National Crime Information Center (NCIC) and the National Law Enforcement Telecommunication Systems (NLETS) with the capability of communicating directly with state and local enforcement agencies. NLETS provides direct access to state motor vehicle departments. As such, this performance measure quantifies, as a percentage in relation to an established service level objective, the end-user experience in terms of TECS service availability. |
| Scope | The range of data is a sample population consisting of active end-user application monitoring at 18 of the busiest airports as defined by US-VISIT Ports of Entry Documentation. This capability is currently being expanded to 54 Ports of Entry (POEs). The data reflect the combined availability of underlying system, task, subsystems and processes which make up the TECS applications, such as the Customer Information Control System - a transaction processing system, and the IBM Message Queuing subsystems, the mainframe system, and other components of TECS. |
| Data Source | The data source is a web-based application that enables users to track and analyze the performance of business processes and network infrastructure, and diagnose the cause of end-user performance as well as process monitoring and automation. |
| Collection Method | The Computer Associates Event and Automation tool for mainframe systems (CA OPS/MVS) monitors all system log and task activity at a low level within the operating system, and has been customized to timestamp and log all down and up times associated with a subsystem or process as well as the host system. |
| Reliability | Reliable |
| How Data is Verified | All data logged are reviewed for accuracy and comments are added by Computer Operations staff as part of their procedures. Discrepancies caused by rare events such as overall system hangs or failures in CA OPS/MVS are corrected by Operations personnel. |

| | |
|---|---|
| Performance Measure | Total number of linked electronic sources from CBP and other government agencies for targeting information. |
| Program and Organization | Automation Modernization - Customs and Border Protection |
| Description | This measure counts the number of electronic sources to which CBP information technology systems are linked to share information for targeting purposes. The measure reflects the ability to accurately and efficiently identify a potential risk to border security in any conveyance entering the U.S. is improved by linking data sources from CBP automated systems and other government agencies, through ACE, as a single source for border decision makers. |
| Scope | Databases are considered linked if they provide transactional data or new source data that enhances existing data for risk assessment purposes. These linkages are to databases both within and outside of DHS. |
| Data Source | The number of linked data sources is identified and manually tabulated, and reported by the Targeting and Analysis Systems Program Office (TASPO). This measure is formally documented and located in the Microsoft SharePoint server portal at TASPO under the Performance Measures site. |
| Collection Method | On a quarterly basis, the TASPO office manually tabulates the list of electronic sources from which data is being linked. The list is summed and the total number of sources is graphed over time. |
| Reliability | Reliable |
| How Data is Verified | The TASPO team will systematically verify the number of systems linked to ACE that supports targeting, or risk assessment. This verification is done quarterly by a Database Administrator (DBA) at TASPO. The DBA follows the data stream to ensure that each electronic source indicated on the list is still linked and continues to provide data that is being used. In addition, the DBA conducts further analysis to find new linkages between electronic sources. The results of this analysis are formally documented and stored on the Microsoft SharePoint server portal at TASPO under the Performance Measures site. |

| | |
|---|---|
| Performance Measure | Border miles under effective control (including certain coastal sectors). |
| Program and Organization | Border Security and Control between Ports of Entry - Customs and Border Protection |
| Description | This measure depicts the number of border miles under control where the appropriate mix of personnel, technology, and tactical infrastructure has been deployed to reasonably ensure that when an attempted illegal alien is detected, identified and classified, that the Border Patrol has the ability to respond and that the attempted illegal entry is brought to a satisfactory law enforcement resolution. As the Border Patrol continues to deploy additional resources based on risk, threat potential, and operational need, the number of miles under control will increase. |
| Scope | There are a total of 8,607 border miles for which the Border Patrol is responsible. This measure reports those miles that are under effective control. |
| Data Source | The Operational Requirements Based Budget Program (ORBBP) database, a web-based application, maintained at the Headquarters Office of Border Patrol (OBP) is the official source of this data. |
| Collection Method | Every quarter the 143 Border Patrol stations throughout the United States use the standard methodology for this measure to determine the number of miles of border that are under effective control in their areas of responsibility. Stations report this data through the web-based application, Operational Requirements Based Budget Program (ORBBP), to sector headquarters where the information is verified and consolidated. The 20 sector headquarters then provide their consolidated data using the web-based application to Headquarters Office of Border Patrol (OBP) twice a year. Headquarters OBP reviews all the sector reports and produces a consolidated OBP report to determine the total number of miles under effective control. |
| Reliability | Reliable |
| How Data is Verified | The Patrol Agents-in-Charge of all 143 Border Patrol stations review and verify their miles under effective control by comparison to operational statistics, third party indicators, intelligence and operational reports, resource deployments and discussions with senior Border Patrol Agents. This information is again verified at the sector level through the same type of review by the Assistant Chief Patrol Agents, and the Chief Patrol Agent, before it is consolidated for the sector report. Once the sector data is provided to Headquarters, Office of Border Patrol, it is again verified through a similar process by the Operations Planning and Analysis Division, and the Southwest Border and Northern/Coastal Border Operations Divisions (as appropriate), and the Chief of the Border Patrol. |

| | |
|---|---|
| Performance Measure | Border miles with increased situational awareness aimed at preventing illegal entries per year. (New performance plan measure for FY 2008.) |
| Program and Organization | Border Security and Control between Ports of Entry - Customs and Border Protection |
| Description | This measure indicates the number of border miles where the situational awareness has increased, or improved, to prevent illegal entries into the U.S. The Border Patrol uses the following levels to describe border security from the least secure to the most secure: Remote/Low Activity; Less Monitored; Monitored; and Controlled. Border regions classified as Remote/Low Activity are generally characterized by rugged and inaccessible terrain. By raising the border security status to Less Monitored (or higher), the Border Patrol improves its situational awareness and border security. |
| Scope | There are a total of 8,607 border miles for which the Border Patrol is responsible. This measure includes all border miles where the situational awareness has increased from the Remote/Low Activity level to any higher level of categorization of awareness. |
| Data Source | The Operational Requirements Based Budget Program (ORBBP) database, a web-based application, maintained at the Headquarters Office of Border Patrol (OBP) is the official source of this data. |
| Collection Method | Every quarter the 143 Border Patrol stations throughout the United States use the |

| | |
|---|---|
| | standard methodology for this measure to determine the number of miles of border that are at this level of situational awareness in their areas of responsibility. Stations report this data through ORBBP to sector headquarters where the information is verified and consolidated. The 20 sector headquarters then provide their consolidated data using the web-based application to Headquarters Office of Border Patrol (OBP) twice a year. Headquarters OBP reviews all the sector reports and produces a consolidated OBP report to determine the consolidated results for this measure. |
| Reliability | Reliable |
| How Data is Verified | The Patrol Agents-in-Charge of all 143 Border Patrol stations review and verify their miles at this level of situational awareness by comparison to operational statistics, third party indicators, intelligence and operational reports, resource deployments and discussions with senior Border Patrol Agents. This information is again verified at the sector level through the same type of review by the Assistant Chief Patrol Agents, and the Chief Patrol Agent, before it is consolidated for the sector report. Once the sector data is provided to Headquarters Office of Border Patrol, it is again verified through a similar process by the Operations Planning and Analysis Division and the Southwest Border and Northern/ Coastal Border Operations Divisions (as appropriate), and the Chief of the Border Patrol. |

| | |
|---|---|
| Performance Measure | Number of Border Patrol Agents trained in rescue and emergency medical procedures. |
| Program and Organization | Border Security and Control between Ports of Entry - Customs and Border Protection |
| Description | This measure will examine the number of agents trained and certified in rescue and emergency medical procedures. One of the Border Patrol's Border Safety Initiative (BSI) objectives is to increase the number of agents trained and certified in rescue and emergency medical procedures at the field agent level to improve the Border Patrol's capabilities to prevent and respond to humanitarian emergencies in order to create a safer and more secure border region. |
| Scope | All Border Patrol Agents trained and certified to respond to rescue and medical emergencies within the Southwest Border area of responsibility are included in this measure. To be trained and certified in rescue and emergency medical procedures, one must attend the certified 8-hour training offered by the Special Operations Division, Office of Border Patrol. |
| Data Source | The data for this measure is contained in the Border Patrol Enforcement Tracking System (BPETS). Data is entered by the Special Operations Division from student training records. |
| Collection Method | Training records are collected by the Supervisory Border Patrol Agent responsible for the training. These records are then entered into the Border Patrol Enforcement Tracking System (BPETS) by the Special Operations Division, Office of Border Patrol. |
| Reliability | Reliable |
| How Data is Verified | Training records are collected by the Supervisory Border Patrol Agents responsible for the training. These records are then entered into the Border Patrol Enforcement Tracking System (BPETS) by the Special Operations Division, Office of Border Patrol. In addition, the sectors are required to submit quarterly reports regarding training. Data from these reports is then compared to the training records to ensure the data is accurate and to rectify any discrepancies. |

| | |
|---|---|
| Performance Measure | Percent of apprehensions at Border Patrol checkpoints. |
| Program and Organization | Border Security and Control between Ports of Entry - Customs and Border Protection |
| Description | This measure examines the effectiveness of checkpoint operations in apprehensions as they relate to border enforcement activities and serves as a barometer for measuring operational effectiveness. Checkpoints are temporary |

| | |
|---|---|
| | and permanent facilities used by the Border Patrol to monitor traffic on routes of egress from border areas, and are an integral part of the Border Patrol's defense-in-depth strategy. As such, activities that occur at checkpoints serve as measures not only of checkpoint operational effectiveness, but as barometers of the effectiveness of the Border Patrol's overall national border enforcement strategy to deny successful illegal entries into the United States. This measure will examine one checkpoint activity, apprehensions, and compare it to the Border Patrol apprehensions nationwide. This comparison will measure checkpoint effectiveness in terms of apprehensions, as well as provide insights into the overall effectiveness of the Border Patrol's national strategy. |
| Scope | A summary of records is completed and the percentages are obtained from the actuals entered from the Checkpoint Activity Report (CAR) completed daily by Border Patrol Agents for all checkpoints in operation. A summary of records is completed for all apprehensions nationwide obtained from Enforcement Case Tracking System (ENFORCE). All Border Patrol checkpoints collect data on a daily basis for inclusion in this measure. |
| Data Source | Summary records from the Checkpoint Activity Report (CAR), a web-based application resident in the Border Patrol Enforcement Tracking System (BPETS). |
| Collection Method | The Border Patrol Agents at the checkpoints enter the data into the Checkpoint Activity Report (CAR), which is a web-based application contained in Border Patrol Enforcement Tracking System (BPETS). The data is immediately available to the Operations Planning and Analysis Division, Office of Border Patrol (OBP) for review and compilation into a consolidated report. |
| Reliability | Reliable |
| How Data is Verified | Multiple levels of review of Checkpoint Activity Report/Enforcement Case Tracking System/Border Patrol Enforcement Tracking System (CAR/ENFORCE/BPETS) data are conducted by Supervisory Border Patrol Agents first at the station level (primary), and by second level Supervisory Border Patrol Agents at the sectors, before a final review reliability check is conducted at Headquarters OBP. Data are analyzed for compliance of established data protocols and accuracy. |

| | |
|---|---|
| Performance Measure | Percent of narcotic seizures at Border Patrol checkpoints compared to Border Patrol seizures nationwide. (Retired plan measure.) |
| Program and Organization | Border Security and Control between Ports of Entry - Customs and Border Protection |
| Description | This measure will examine the percentage of narcotic seizures at Border Patrol Checkpoints compared to the percentage of narcotic seizures nation-wide. The Border Patrol checkpoint operations are an integral part of the Border Patrol's defense-in-depth strategy. As such, these activities serve as measures for both the checkpoint operational effectiveness and the value of the Border Patrol's overall national border enforcement strategy to deny successful illegal entries into the United States. This comparison will measure checkpoint effectiveness in terms of narcotics seizures as well as provide insights into the overall effectiveness of the Border Patrol's national strategy. |
| Scope | The number of narcotic seizure events at the 35 permanent and 75 tactical (non-permanent) Border Patrol checkpoints are compared to the number of narcotic seizure events by Border Patrol nationwide to determine what percentage of events take place at Border Patrol checkpoints. |
| Data Source | The number of narcotic seizure events is obtained through the Checkpoint Activity Report (CAR). The number of narcotic seizure events nationwide are obtained through Enforcement Case Tracking System/Border Patrol Enforcement Tracking System (ENFORCE/BPETS). ENFORCE is the Enforcement Case Tracking System which is the official database of record utilized of each individual arrested by the Border Patrol. BPETS is used as a collection mechanism for other required information to monitor Border Patrol operations. |
| Collection Method | Seizure event data are recorded daily by Border Patrol Agents using the CAR at |

| | |
|---|---|
| | each checkpoint in operation as well as in Enforcement Case Tracking System/Border Patrol Enforcement Tracking System (ENFORCE/BPETS) and used to collect Border Patrol statistics. The data is immediately available to the Operations Planning and Analysis Division, Office of Border Patrol (OBP) for review and compilation into a consolidated report. |
| Reliability | Reliable |
| How Data is Verified | Multiple levels of review of Checkpoint Activity Report/Enforcement Case Tracking System/Border Patrol Enforcement Tracking System (CAR/ENFORCE/BPETS) data are conducted by Supervisory Border Patrol Agents, first at the station level (primary), and by second level Supervisory Border Patrol Agents at the sectors, before a final review reliability check is conducted at Headquarters OBP. Data are analyzed for compliance of established data protocols and accuracy. |

| | |
|---|---|
| Performance Measure | Percent of traffic checkpoint cases referred for prosecution to the U.S. Attorney's office. |
| Program and Organization | Border Security and Control between Ports of Entry - Customs and Border Protection |
| Description | This measure will examine the percent of border related cases brought by the Border Patrol and originating from traffic checkpoint operations that are referred to one of the 92 U.S. Attorneys located throughout the United States, Puerto Rico, and the Virgin Islands for prosecution, compared to the total number of apprehensions at traffic checkpoints. This measure will depict the effectiveness of Border Patrol checkpoint operations in identifying and prosecuting dangerous criminals, thus enhancing overall public safety. All apprehensions by the Office of Border Patrol (OBP) are considered arrests (administrative or criminal). The number of cases referred for prosecution by OBP and being tracked in this measure are criminal arrests only. |
| Scope | The number of cases referred is drawn from all apprehension activity at all Border Patrol checkpoints. Cases referred meeting the criteria for prosecution referral include Alien Smuggling, Drugs/Narcotics, Fraudulent Documents and Other activities (which captures all other criminal cases referred). |
| Data Source | The Checkpoint Activity Report (CAR), generated by the Operations Planning and Analysis Division, Office of Border Patrol for all Border Patrol sectors, is the source of data for this measure. |
| Collection Method | The number of cases referred to the U.S. Attorneys for prosecution and the number of apprehensions are recorded daily by Border Patrol Agents in the Checkpoint Activity Report (CAR). The number of cases referred to prosecutions related to checkpoint enforcement activity is compared to all apprehension activity at Border Patrol checkpoints to determine what percent of all apprehensions are referred for prosecution as criminal cases. The cases referred are broken down into four categories: Alien Smuggling, Drugs/Narcotics, Fraudulent Documents and Other activities (captures all other criminal cases referred). The number of cases referred does not represent the number of cases accepted for prosecution. While cases referred may meet the Border Patrol criteria for referral, they may not fully meet guidelines for prosecution by the U.S. Attorneys. |
| Reliability | Reliable |
| How Data is Verified | Multiple levels of review of the Checkpoint Activity Report/Enforcement Case Tracking System/Border Patrol Enforcement Tracking System (CAR/ENFORCE/BPETS) data are conducted by Supervisory Border Patrol Agents, first at the station level (primary), and by second level Supervisory Border Patrol Agents at the sectors, before a final review reliability check is conducted at Headquarters, Office of Border Patrol. Data are analyzed for compliance of established data protocols and accuracy. |

| | |
|---|---|
| Performance Measure | Total number of cumulative miles of permanent tactical infrastructure constructed. |
| Program and Organization | Border Security and Control between Ports of Entry - Customs and Border Protection |
| Description | This measure reports the total number of cumulative miles of tactical infrastructure constructed. Tactical Infrastructure consists of barriers built to deter or delay illegal entries into the United States. Tactical infrastructure includes pedestrian fencing, all-weather roads, vehicle fence and permanent lighting installed in the border areas to support border enforcement activities. |
| Scope | Permanent tactical infrastructure is defined by Border Patrol as permanent fencing, all-weather roads, vehicle fence and permanent lighting installed in the border areas to support enforcement activities and serves as an important piece of Border Patrol's strategy to gain operational control. The placement of additional permanent infrastructure is measured as a cumulative total for miles of fencing, lighting, vehicle fencing, or all-weather roads installed. |
| Data Source | Permanent tactical infrastructure implementation plans and installation progress as reported by Asset Management and Border Patrol field personnel. |
| Collection Method | Weekly reports are submitted by each sector location and purchases are inputted into the Systems, Applications and Products (SAP) application, tracked in the Operational Requirements Based Budget Program (ORBBP), and reported in the Enforcement Case Tracking System (ENFORCE). |
| Reliability | Reliable |
| How Data is Verified | Various management controls are in place to review data in ORBBP, SAP, ENFORCE, and the Border Patrol Enforcement Tracking System (BPETS). |

| | |
|---|---|
| Performance Measure | Advanced Passenger Information System (APIS) Data Sufficiency Rate. (Percent) (Retired plan measure.) |
| Program and Organization | Border Security Inspections and Trade Facilitation at Ports of Entry - Customs and Border Protection |
| Description | Accurate transmittal of advance passenger information data for law enforcement queries facilitates decision making and targeting capabilities to identify high risk passengers prior to arrival. New APIS reporting requirements went into effect in FY 2006 that greatly increased the number of reportable data elements from five to over 20, including several that must be manually provided, placing greater responsibility for accuracy at the embarkation point. All data elements must be transmitted correctly for the passenger record to be counted as accurate. CBP is working with carriers to improve collection procedures and input forms to increase the APIS rate. |
| Scope | Air carriers landing at all international airports who are carrying passengers entering the United States record and report information in advance of passenger arrival for every international commercial flight. This information is transmitted from air carriers to the CBP National Data Center by lists known as passenger and crew manifests. This advance information is collected for all passengers arriving into the United States by commercial carrier. |
| Data Source | The airline passenger and crew manifest data. |
| Collection Method | Passenger and crew manifest information is electronically transmitted from commercial air carriers to the CBP National Data Center. Air carriers present arrival and departure General Declarations to CBP Officers. CBP Officers enter flight information, including onboard passenger and crew counts, into the Automated Commercial System (ACS). The passenger and crew counts from ACS are automatically compared to the number of records received in the air carriers electronic manifest transmission. This provides the percentage of records received. Additionally the system identifies incomplete records or invalid data, such as a missing name or an invalid date of birth. Records with incomplete or invalid data are subtracted data and an automated report is generated by the Interagency Border Inspection System (IBIS) that calculates and providing a sufficiency rate. |
| Reliability | Reliable |

| | |
|---|---|
| How Data is Verified | APIS data is initially entered by air carriers, verified by CBP Officers during daily operations and further assessed for completeness and accuracy by National APIS Account Managers by reviewing missing data reports and performing outreach with carriers. |

| | |
|---|---|
| Performance Measure | Air passenger apprehension rate for major violations. (New performance plan measure for FY 2008.) |
| Program and Organization | Border Security Inspections and Trade Facilitation at Ports of Entry - Customs and Border Protection |
| Description | This measure provides a statistically valid estimate of the apprehension rate of air passengers for major violations at the international airports. The data are derived from the results of inspections for major violations among air passengers traveling to the U.S. from international airports. A major violation involves serious criminal activities such as air passengers transporting illegal drugs, guns, or other banned substances into the U.S. The measure uses statistical sampling methods to estimates potential threats and gauges the effectiveness of Customs and Border Protection (CBP) Officers in interdicting those threats among air passengers arriving at international airports. |
| Scope | CBP Officers working at the 19 largest international airports gather statistically random data on the proportion of air passengers who are responsible for a major violation, defined as a Category 1 violation in COMPEX. COMPEX is a traveler compliance program that uses randomized statistical sampling to determine the level of threat at international airports. Passengers are selected in a random sample that totals 12,000 passengers annually (1,000 passengers per month) at each of the 19 airports. This sample size was selected to obtain an overall 95 percent probability of finding a serious violation. |
| Data Source | The data used to calculate the air apprehension rate for major violations is obtained from the Traveler Enforcement Communications System (TECS), one of the principal systems of record used by CBP. |
| Collection Method | CBP Officers working at international airports gather data on violations while processing air passengers entering the U.S. These data are entered into TECS by each responsible officer at the time of occurrence of the violation. Once entered, this data cannot be erased or altered. Data is extracted from TECS by analysts at CBP Headquarters to calculate the number of overall major violations found by CBP Officers. This number is compared to the number of major violations predicted, based on the number found in the random sample, to determine the overall Apprehension Rate. |
| Reliability | Reliable |
| How Data is Verified | Verification of data is conducted by making extractions from the Operations Management Report (OMR), Automated Targeting System (ATS), and the Traveler Enforcement Communications System (TECS). The extracted data are reviewed against hard-copy records to verify the accuracy of the reported data and identify any anomalies or inconsistencies. |

| | |
|---|---|
| Performance Measure | Air passengers compliant with laws, rules, and regulations (%). |
| Program and Organization | Border Security Inspections and Trade Facilitation at Ports of Entry - Customs and Border Protection |
| Description | This measure is the compliance rate of international air passengers with all of the laws, rules, and regulations that CBP enforces at the Ports of Entry, with the exception of agriculture laws and regulations. It is also referred to as the Air Compex Rate. It results from a statistical sampling technique that is outcome/result driven. The measure estimates the threat approaching the port of entry and the effectiveness of officer targeting toward that threat. The measure is valid because it encompasses enforcement actions taken at a port of entry and a statistically valid random sampling of passengers who are considered low risk and would not otherwise be examined. These data are used to determine the actual percentage of travelers who are compliant with all of the laws, rules, regulations, |

| | |
|---|---|
| | and agreements enforced by CBP. |
| Scope | CBP Officers working at the 19 largest International Airports gather statistically random data on the proportion of air travelers in compliance with Customs regulations. Passengers are selected in a random sample that totals 12,000 passengers annually (1,000 passengers per month) at each of the 19 airports. This sample size was selected to obtain an overall 95 percent probability of finding a serious violation. |
| Data Source | The percent of compliant passengers in the Air/Land Passenger environment is obtained from Traveler Enforcement Communications System (TECS), Category I violations, and Category II violations. |
| Collection Method | CBP Officers working at International compliance rate data while processing passengers entering the U.S. These data are entered into the TECS by each Officer at the time of occurrence of the violation. Individual compliance rate data entered in TECS is then extracted by a specialist at Headquarters to an Excel spreadsheet where the compliance rate is calculated by applying a statistically valid formula (including confidence intervals on the results) to determine the rate of compliance. |
| Reliability | Reliable |
| How Data is Verified | Verification of the data is conducted by making extractions from the Operations Management Report (OMR), Automated Targeting System (ATS), and the TECS. These data extractions are then reviewed by the headquarters program officers against hard copy records to verify the accuracy of the reported data and identify any anomalies or inconsistencies. |

| | |
|---|---|
| Performance Measure | Average CBP exam reduction ratio for Customs-Trade Partnership Against Terrorism (C-TPAT) member importers compared to Non-C-TPAT importers. (Retired plan measure.) |
| Program and Organization | Border Security Inspections and Trade Facilitation at Ports of Entry - Customs and Border Protection |
| Description | By enrolling in C-TPAT, members follow security procedures to secure the supply chain. This results in reduced exams and thereby helps facilitate the flow of trade. This performance measures indicates the impact of C-TPAT exam reduction benefits on C-TPAT importer exams. The ratio measures the exam reduction ratio of C-TPAT member importers compared to Non-C-TPAT importers. |
| Scope | Data includes national commercial cargo importations and exam results which occur at all Ports of Entry. |
| Data Source | The Automated Commercial System (ACS) is a mainframe database system that stores a variety of information related to trade. This system is maintained at the Customs and Border Protection (CBP) National Data Center. |
| Collection Method | All commercial importations and exam results are recorded in ACS. The software programs Dataquery and Datareporter are used to extract this information from ACS and the data used to calculate the number of cargo exams conducted on C-TPAT member shipments versus non-member shipments. |
| Reliability | Reliable |
| How Data is Verified | Entry of exam data has several checks built into its processing, including maintenance of an audit trail within ACS, mandatory supervisory review of exam override actions, random samples associated with compliance measurement and the self-inspection program. |

| | |
|---|---|
| Performance Measure | Border vehicle passengers in compliance with agricultural quarantine regulations (percent compliant). |
| Program and Organization | Border Security Inspections and Trade Facilitation at Ports of Entry - Customs and Border Protection |
| Description | The measure shows CBP's success at maintaining a high level of security in the land border environment by measuring the degree of compliance with U.S. Department of Agriculture (USDA) agricultural quarantine regulations and other |

| | |
|---|---|
| | mandatory agricultural product restrictions. CBP randomly samples border vehicle passengers for compliance with all USDA laws, rules, and regulations using USDA guidance on sampling procedures. |
| Scope | Agricultural specialists report agricultural violations at all land border ports into the Work Accomplishment Data System (WADS) managed and maintained by the U.S. Department of Agriculture (USDA) Animal, Plant, and Health Inspection Service (APHIS). This data is used to calculate the overall compliance of all passengers entering the U.S. through the land border ports of entry with the USDA Agricultural Quarantine Regulations |
| Data Source | Data are taken from the Work Accomplishment Data System (WADS), maintained by the U.S. Department of Agriculture (USDA), and entered by Customs and Border Protection Agricultural Specialists. |
| Collection Method | The program collects data used for this measure through Agricultural Quarantine Inspection (AQI) Monitoring activities. Violation data are recorded at the ports of entry (POEs) by Agriculture Specialists for both commercial and privately - owned vehicles. Every violation is recorded in WADS to capture the pertinent information required to identify the plant, pest, disease, and/or health risk using the detailed identification process built into the WADS coding system. USDA uses this information to identify new risks, look for patterns in violations, and track seasonal activity. |
| Reliability | Reliable |
| How Data is Verified | National and regional managers work with the ports to continually monitor and improve data quality. USDA APHIS conducts a detailed quarterly review of all data entered into WADS at the ports of entry to identify coding errors, missing data, and errors in processing that might impact the accuracy of the data used in the new threat analysis and risk management process. A report is issued quarterly and CBP and USDA APHIS work together to resolve operational issues and correct identified errors. |

| | |
|---|---|
| Performance Measure | Compliance rate for Customs-Trade Partnership Against Terrorism (C-TPAT) members with the established C-TPAT security guidelines. |
| Program and Organization | Border Security Inspections and Trade Facilitation at Ports of Entry - Customs and Border Protection |
| Description | After acceptance into the C-TPAT program, all C-TPAT members must undergo a periodic validation in which 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. This measure provides a summary of the overall Compliance Rate achieved for all validations performed during the Fiscal Year. |
| Scope | 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 one 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, removed. |
| Collection Method | 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 after 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 | Reliable |
| How Data is Verified | 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 | International air passengers in compliance with agricultural quarantine regulations (percent compliant). |
| Program and Organization | Border Security Inspections and Trade Facilitation at Ports of Entry - Customs and Border Protection |
| Description | The measure shows CBP's success at maintaining a high level of security in the international air environment by measuring the degree of compliance with U.S. Department of Agriculture (USDA) agricultural quarantine regulations and other mandatory agricultural product restrictions. CBP randomly samples international air passengers for compliance with all USDA laws, rules, and regulations using USDA guidance on sampling procedures |
| Scope | Agricultural specialists report agricultural violations at all international airports into the Work Accomplishment Data System (WADS) managed and maintained by the U.S. Department of Agriculture (USDA) Animal, Plant, and Health Inspection Service (APHIS). This data is used to calculate the overall compliance of all passengers entering the U.S. through international airports with the USDA Agricultural Quarantine Regulations. |
| Data Source | Data are taken from the WADS (Work Accomplishment Data System), maintained by United States Department of Agriculture (USDA) and entered by CBP Agricultural Specialists. |
| Collection Method | The program collects data used for this measure through Agricultural Quarantine Inspection (AQI) Monitoring activities. Violation data are recorded at international airports by Agriculture Specialists for all arriving passengers into the U.S. Every violation is recorded in WADS to capture the pertinent information required to identify the plant, pest, disease, and/or health risk using the detailed identification process built into the WADS coding system. USDA uses this information to identify new risks, look for patterns in violations, and track seasonal activity. |
| Reliability | Reliable |
| How Data is Verified | National and regional managers work with the ports to continually monitor and improve data quality. USDA APHIS conducts a detailed quarterly review of all data entered into WADS at the international airports to identify coding errors, missing data, and errors in processing that might impact the accuracy of the data used in the new threat analysis and risk management process. A report is issued quarterly and CBP and USDA APHIS work together to resolve operational issues and correct identified errors. |

| | |
|---|---|
| Performance Measure | Land border apprehension rate for major violations. (New performance plan measure for FY 2008.) |
| Program and Organization | Border Security Inspections and Trade Facilitation at Ports of Entry - Customs and Border Protection |
| Description | This measure provides a statistically valid estimate of the apprehension rate of land vehicle passengers for major violations who enter through U.S. land border ports of entry. The data are derived from the results of inspections for major violations among land vehicle passengers. A major violation involves serious criminal activities such as transporting illegal drugs, guns, or other banned substances into the U.S. The measure uses statistical sampling methods to estimates potential threats and gauges the effectiveness of Customs and Border Protection (CBP) Officers in interdicting those threats among people crossing into |

| | |
|---|---|
| | the U.S. at land borders. |
| Scope | CBP Officers working at the top 25 largest land border ports of entry gather statistically random data on the proportion of land vehicle passengers who are responsible for a major violation, defined as a Category 1 violation in COMPEX. COMPEX is a traveler compliance program that uses randomized statistical sampling to determine the level of threat at the land border ports. Passengers are selected in a random sample that totals 12,000 passengers annually (1,000 passengers per month) at each of the 25 land border ports . This sample size was selected to obtain an overall 95 percent probability of finding a serious violation. |
| Data Source | The data used to calculate the Land Border Apprehension Rate for Major Violations is obtained from the Traveler Enforcement Communications System (TECS), one of the principal systems of record used by CBP. |
| Collection Method | CBP Officers working at land ports of entry gather data on violations while processing vehicles entering the U.S. These data are entered into TECS by each responsible officer at the time of occurrence of the violation. Once entered, this data cannot be erased or altered. Data is extracted from TECS by analysts at CBP Headquarters (HQ) to calculate the number of overall major violations found by CBP Officers. This number is compared to the number of major violations predicted, based on the number found in the random sample, to determine the overall Apprehension Rate. |
| Reliability | Reliable |
| How Data is Verified | Verification of data is conducted by making extractions from the Operations Management Report (OMR), Automated Targeting System (ATS), and the TECS. The extracted data are reviewed against hardcopy records to verify the accuracy of the reported data and identify any anomalies or inconsistencies. |

| | |
|---|---|
| Performance Measure | Land border passengers compliant with laws, rules, and regulations (%). |
| Program and Organization | Border Security Inspections and Trade Facilitation at Ports of Entry - Customs and Border Protection |
| Description | This measure is the compliance rate of land border vehicle passengers with all of the laws, rules, and regulations that CBP enforces at the Ports of Entry, with the exception of agricultural laws and regulations. It is also referred to as the Land Compex Rate. It results from a statistical sampling technique that is outcome/result driven. This measure estimates the threat approaching the port of entry and the effectiveness of officer targeting toward that threat. The measure is valid because it encompasses enforcement actions taken at a port of entry and a statistically valid random sampling of passengers who are considered low risk and would not otherwise be examined. These data are used to determine the actual percent of passengers who are compliant with all of the laws, rules, regulations, and agreements enforced by CBP. |
| Scope | CBP Officers working at the 25 largest land ports of entry gather statistically random data on the proportion of land vehicle passengers in compliance with Customs regulations. Passengers are selected in a random sample that totals 12,000 passengers annually (1,000 passengers per month) at each of the 25 land border ports. This sample size was selected to obtain an overall 95 percent probability of finding a serious violation. |
| Data Source | The percent of compliant passengers in the Land Passenger environment is obtained from Traveler Enforcement Communications System (TECS). |
| Collection Method | CBP Officers working at land ports of entry gather compliance rate data while processing vehicles entering the U.S. These data are entered into the Traveler Enforcement Communications System (TECS) by each Officer at the time of occurrence of the violation. Individual compliance rate data entered in TECS is then extracted by a specialist at Headquarters CBP to an excel spreadsheet where the compliance rate is calculated by applying a statistically valid formula (including confidence intervals on the results) to determine the rate of compliance. |
| Reliability | Reliable |
| How Data is Verified | Verification of the data is conducted by making extractions from the Operations |

| | |
|---|---|
| | Management Report (OMR), Automated Targeting System (ATS), and the Traveler Enforcement Communications System (TECS). The extracted data are reviewed against hardcopy records to verify the accuracy of the reported data and identify any anomalies or inconsistencies. |

| | |
|---|---|
| Performance Measure | Number of foreign cargo examinations resolved in cooperation with the Container Security Initiative. |
| Program and Organization | Border Security Inspections and Trade Facilitation at Ports of Entry - Customs and Border Protection |
| Description | This measure provides an indicator of the benefit of locating CBP Officers at foreign locations that are cooperating with CBP under the Container Security Initiative (CSI). It provides the number of container examinations processed or mitigated by foreign Customs officials that were identified by CBP CSI as higher-risk, and accepted as meeting CBP examination standards and requirements. These examinations would otherwise have taken place at U.S. ports of entry. It is an indication of the number of higher-risk cargo shipments identified and examined prior to embarkation from foreign ports to U.S. destinations. |
| Scope | The measure will be the number of foreign examinations resolved through the use of host nation intelligence. Data for this measure is collected at the CSI ports operating worldwide, which is currently 58 sites. All examinations that qualify are included in the calculation for this measure. |
| Data Source | A Container Security Initiative port team member inputs this data into an intra - net web-based spreadsheet daily. Total numbers are extracted weekly from this spreadsheet for required reports to the CSI Division. The Automated Targeting System (ATS) was used by the port members to input mitigated data. |
| Collection Method | CSI Port Team Leaders track statistics using the existing web-based portal. Data is input daily and reported weekly. This statistical data is then reported via the ATS Exam Findings module. |
| Reliability | Reliable |
| How Data is Verified | Reliability of the data is verified and evaluated by the CSI Division. CSID Headquarters compares the data to historical volume at the given port and checks to see if it falls within certain perimeters. If it does not, CSID Headquarters will ask the CSI Port Team Leader for additional information to justify the increase in volume from previous years. Reliable data is currently available. |

| | |
|---|---|
| Performance Measure | Percent of active commissioned canine teams with 100% detection rate results in testing of the Canine Enforcement Team. (Retired plan measure.) |
| Program and Organization | Border Security Inspections and Trade Facilitation at Ports of Entry - Customs and Border Protection |
| Description | The Canine Enforcement Program conducts twice-yearly testing of the Canine Enforcement Teams to maintain an operating standard of full detection. To meet both new and existing threats, the canine program has trained and deployed canine teams in a broad array of specialized detection capabilities. Any team exhibiting a weakness in detection capability for an area in which it has been trained must undergo additional training in order to bring it to a level of full detection. |
| Scope | Customs and Border Protection detector dogs, with the exception of those detected to explosive detection, are evaluated once a year. Explosive detector dogs are evaluated twice a year. The only dogs excluded from this measure are those who are injured or ill. Dogs are tested in the actual work environment at their assigned port of entry on a set number of odors. Any team exhibiting a weakness in detection capability for an area in which it has been trained (such as narcotics, chemicals, explosives, weapons, and human smuggling) is temporarily decommissioned and must immediately undergo additional training to bring it to a full level of detection. Once re-trained, the teams are retested against the full battery of tests for its detection areas. Any team then failing the detection test is decommissioned and immediately taken out of service. To pass evaluations, detector dogs must successfully detect 100 percent of all trained odors. |

| | |
|---|---|
| Data Source | Once a detector dog has successfully completed an evaluation at their assigned port of entry, the evaluator will notify Program Managers, Canine Enforcement Program (CEP), of the completed evaluation. CEP Program Managers maintain the detector dog evaluation /certification information on a spreadsheet located in canine folder. Data recorded include detection areas for which training is received, training completion date, dogs' name, and identification number for all dogs that complete the training. |
| Collection Method | CEP Program Managers schedule detector dogs for evaluations. The evaluator will notify CEP Program Managers of the completed evaluation. The evaluation is captured on CBP Form 312. The officer and the canine are scored separately. The CBP Form is kept on file at each port of entry for 90 days. A typical test consists of a set number of training aids similar to those to be detected, such as drugs or explosive materials, being concealed in locations specified by the testing protocol. To pass, detector dogs must successfully detect 100 percent of all hidden training aids. |
| Reliability | Reliable |
| How Data is Verified | Once the evaluation process is completed on each detector dog, the detector dog receives weekly training and evaluations to ensure the dog maintains 100 percent detection capability on trained odors. This training is conducted by a CBP canine trainer assigned to the port of entry. The port of entry maintains the training records and evaluation forms (CBP Form 312). |

| | |
|---|---|
| Performance Measure | Percent of sea containers screened for contraband and concealed people. |
| Program and Organization | Border Security Inspections and Trade Facilitation at Ports of Entry - Customs and Border Protection |
| Description | The measure shows the progress towards increasing security by measuring the percent of sea containers arriving at seaports that were screened for contraband and concealed people using Non-intrusive (NII) technology. NII technology consists of x-ray imaging and electro-magnetic imaging equipment that is very effective at inspecting trucks, containers, and packages for shapes, density, and hidden cargo. It is very effective at identifying weapons, narcotics, smuggled humans, and concealed cargo. NII equipment is not effective at identifying radioactive or weapons-grade materials. NII equipment and radiation portal monitor (RPM) equipment use very different technologies that accomplish distinctly different things. They complement each other and work together to fully screen cargo. |
| Scope | All containers that arrive at a Seaport that handles the importation of sea containers into the U.S. are included in this measure. |
| Data Source | Operations Management Reports (OMR) Data Warehouse. |
| Collection Method | All sea borne containerized cargo that is being imported into the U.S. through Ports of Entry are recorded in the Traveler Enforcement Communications System (TECS). In addition, any time a CBP officer inspects sea cargo, that inspection action is also entered into TECS. On a weekly basis the data are migrated to a permanent data warehouse where they are verified and compiled. The measure is calculated based on the percent of NII examinations performed on sea containers compared to the total number of sea containers imported in the U.S. |
| Reliability | Reliable |
| How Data is Verified | Verification is regularly done by port supervisors. Data are reviewed for anomalies, outliers, and inconsistencies in data records. Any discrepancies are investigated and resolved as necessary. |

| | |
|---|---|
| Performance Measure | Percent of truck and rail containers screened for contraband and concealed people. |
| Program and Organization | Border Security Inspections and Trade Facilitation at Ports of Entry - Customs and Border Protection |
| Description | The measure shows the progress towards increasing security by measuring the percent of truck and rail containers that were screened for contraband and concealed people using Non-Intrusive (NII) technology. NII technology consists |

| | |
|---|---|
| | of x-ray imaging and electro-magnetic imaging equipment that is very effective at inspecting trucks, containers, and packages for shapes, density, and hidden cargo. It is very effective at identifying weapons, narcotics, smuggled humans, and concealed cargo. NII equipment is not effective at identifying radioactive or weapons-grade materials. NII equipment and radiation portal monitor (RPM) equipment use very different technologies that accomplish distinctly different things. They complement each other and work together to fully screen cargo. |
| Scope | All containers that arrive at Land Border Ports of Entry that handle the importation of truck or rail containers into the U.S. are included in this measure. |
| Data Source | Operations Management Reports (OMR) Data Warehouse. |
| Collection Method | All land border cargo that is being imported into the U.S. through Ports of Entry are recorded in the Traveler Enforcement Communications System (TECS). In addition, any time a CBP officer inspects land based cargo, that inspection action is also entered into TECS. On a weekly basis the data are migrated to a permanent data warehouse where they are verified and compiled. The measure is calculated based on the percent of NII examinations performed on land truck or rail containers compared to the total number of land truck or rail containers imported in the U.S. |
| Reliability | Reliable |
| How Data is Verified | Check Verification is regularly done by port supervisors. Data are reviewed for anomalies, outliers, and inconsistencies in data records. Any discrepancies are investigated and resolved as necessary. |

| | |
|---|---|
| Performance Measure | Percent of worldwide U.S. destined containers processed through Container Security Initiative (CSI) ports. |
| Program and Organization | Border Security Inspections and Trade Facilitation at Ports of Entry - Customs and Border Protection |
| Description | This measure is the percent of worldwide U.S.-destined containers (and their respective bills of lading) processed through CSI ports as a deterrence action to detect and prevent weapons of mass effect and other potentially harmful materials from leaving foreign ports headed to U.S. ports. Note: Processed cargo may include any of the following: 1) U.S.-destined cargo manifest/bills of lading data reviewed using the Automated Targeting System (ATS), 2) further research conducted, 3) collaboration with host country and intelligence representatives, and 4) examination of the container. |
| Scope | This measure will utilize the annual volume of U.S. destined containers processed through all CSI ports, which is currently at 58 sites. |
| Data Source | Two sources are used to develop this statistic. The first is the data input into the Statistical Web-portal by each port to document the shipping volume (as expressed through Bills of Lading) processed through the port. The second is the total annual volume arriving in the U.S. as tracked by the Port Import Export Reporting Service (PIERS) subscription service. |
| Collection Method | CSI Port Team already tracks and documents the shipping volume processed through each port using the Statistical Web-portal. The data is input daily and reported weekly by CSI to Office of Field Operations (OFO) Headquarters. Data on the total annual volume arriving in the U.S. will be extracted from PIERS. |
| Reliability | Reliable |
| How Data is Verified | The CSI Division (CSID) is responsible for verifying the statistics regarding shipping volume in the respective ports. The PIERS data is a subscription service with independently verified data. PIERS data is compared to historical data that is contained in the CSID Statistical Web-portal to identify any changes in shipment volumes. |

| | |
|---|---|
| Performance Measure | Number of airspace incursions along the southern border. (Extending the physical zone of security beyond the borders) |
| Program and Organization | CBP Air and Marine - Customs and Border Protection |
| Description | This measure shows the number of airspace incursions along the southern border. A consistent standard of less than 10 incursions each year is an aggressive standard we strive to maintain. The measure monitors Air and Marine efforts in reducing, with the intent of ultimately denying, the use of border air space for acts of terrorism or smuggling using intelligence and threat assessments. The number of Targets of Interest (TOI) has been reduced over time as strategic surveillance and tactical responses by CBP interceptors and patrols, work with the Border Patrol on the ground, to deter the use of air routes into the United States. Air and Marine continues to gather and analyze intelligence on past and current threat patterns to forecast and disseminate information about potential and emerging threats. The targeted goals for this measure are to maintain this low level of border incursions at a minimum and reduce it if possible, until there are no border incursions. |
| Scope | This measure monitors Air and Marine efforts in reducing, with the intent of ultimately denying, the use of border air space for acts of terrorism or smuggling using intelligence and threat assessments. The number of TOI has been reduced over time as strategic surveillance and tactical responses by CBP interceptors and patrols work with Border Patrol on the ground to deter the use of air routes into the U.S. Air and Marine continues to gather and analyze intelligence on past and current threat patterns to forecast and disseminate information about potential and emerging threats. The targeted goals for this measure are to maintain a minimum level of border incursions, and reduce it if possible, until there are no border incursions. |
| Data Source | Performance data are captured routinely as part of the normal work process. Data are reported through the Traveler Enforcement Communications System (TECS) and input to the Air and Marine Operations Report (AMOR). Data are available in real- time and are continuously validated within Air and Marine. The program uses these routine reports to measure efficiency and effectiveness. The current data system enables the program to measure the activities necessary to manage and improve performance. |
| Collection Method | Systems Application Products (SAP), Computerized Aircraft Reporting Material Control (CARMAC), Air Program Administrative Tracking System (APATS), and Customs Automated Maintenance and Inventory Tracking System (CAMITS) generated reports in conjunction with analyst-developed Excel spreadsheets are routinely used to determine the locations and costs associated with relocation of assets. Airspace incursions are identified by Air and Marine Operations Center (AMOC). Once identified, this information is transmitted to the closest air branch for air support. The results are then entered into the TECS and AMOR systems, and tallies are summarized of all incursions on a monthly basis. |
| Reliability | Reliable |
| How Data is Verified | Data reliability is routinely reconciled (a comparison of information in the systems) manually by contractor and FTE staff on a monthly and/or quarterly basis. All flights are provided a unique identifier to eliminate the possibility of double counting. Flight hours recorded are reconciled back against maintenance logs to assure all flights have been recorded. Air and Marine is identifying data bridges between SAP and CARMAC, APATS and CAMITS to increase reliability and decrease human error opportunities. There is no date available when these bridges may become available. |

| | |
|---|---|
| Performance Measure | Percent of air support launches accomplished to support border ground agents to secure the border. |
| Program and Organization | CBP Air and Marine - Customs and Border Protection |
| Description | A primary and important measure for Air and Marine is its capability to launch an aircraft when a request is made for aerial support. This measure captures the percent of all requests made for air support to which Air and Marine was able to respond. |
| Scope | The primary and most important performance measured for Air and Marine, or any air force, is its capability and/or capacity to provide (or launch) an aircraft when a request is made for aerial support. This industry standard immediately lets management know where problems or gaps exist and what is needed to correct the problem. These gaps may take days to years to remedy, but constant awareness of this measurement highlights problems. The program only monitors the following three reasons for not providing 100 percent air support: (1) aircraft unavailable due to maintenance; (2) correct type of aircraft needed for mission unavailable; (3) correct type of aircraft available, but incorrect crew or crew-size unavailable to launch. |
| Data Source | Performance data are reported through the Traveler Homeland Enforcement Communication System (TECS) and input to the Air and Marine Operations Reporting (AMOR) System. |
| Collection Method | Data is input into the AMOR system daily by Air and Marine Operations Center (AMOC) personnel requesting the launch and verified by their Supervisors. (Communications are continuous throughout the mission and times are recorded by AMOC.) This database contains a report writing module which allows users to extract canned or preconfigured reports such as no launch. The database has been programmed to allow the user to define data ranges, such as all air locations, specific air locations etc. The no launch report summarizes all requests made and all launches made against those requests. The program then divides the number of launches into the number of requests to calculate its results. |
| Reliability | Reliable |
| How Data is Verified | Input is routed to and approved by supervisors daily. Data reliability is routinely reconciled manually by contractor and FTE staff on a monthly and/or quarterly basis. |

| | |
|---|---|
| Performance Measure | Percent of at-risk miles under strategic air surveillance. (Strategic air coverage) |
| Program and Organization | CBP Air and Marine - Customs and Border Protection |
| Description | The measure is represented by the percent of at-risk miles under strategic air surveillance and is evaluated according to up-to-the-minute information and intelligence. This measure describes the area of the U.S. border determined to be under the span of control of Air and Marine assets. The program uses a multi-level layer to aerial response and support to accomplish this goal:<br>1) Strategic surveillance for the P-3 and Unmanned Aerial Systems (UAS) aircraft, 2) Intelligence driven support for the rapid deployment of forces, and<br>3) Strategic and tactical support to ground law enforcement such as Office of Border Patrol and Immigration and Customs Enforcement. |
| Scope | The measure is the percent of border miles at-risk that is under surveillance by CBP patrol-type aircraft (including UAS). Measuring surveillance is an evolving metric. In FY 2003 and FY 2004 metrics were based on the measurement of 7200 P-3 flight hours provided in support of drug enforcement. In FY 2005, the UAS was introduced and added to these total hours. Effective FY 2007, the measure is represented by the miles of "at risk borders" (border miles that have no or minimal flight coverage) under strategic air surveillance in response to the anti-terrorism mission. |
| Data Source | Systems Application Products (SAP), Computerized Aircraft Reporting Material Control (CARMAC), Air Program Administrative Tracking System (APATS), Customs Automated Maintenance Inventory Tracking System (CAMITS) generated reports in conjunction with analyst developed Excel spreadsheets are |

| | |
|---|---|
| | used to generate this data. |
| Collection Method | Data for this measure is collected daily from flights and UAS as part of the normal work process. Data are reported through the Traveler Enforcement Communications System (TECS) and input to the Air and Marine Operations Report (AMOR). Data are available in real-time and is continuously validated. The program routinely extracts reports to measure progress made in support of Border Patrol Ground agents and the capacity to increase air coverage in areas of threat based on intelligence.  Maintenance records as to the availability of aircraft are maintained in CARMAC. |
| Reliability | Reliable |
| How Data is Verified | The reliability of data is routinely reconciled (a comparison of information in the TECS and AMOR systems) manually by contractor and program staff on a monthly and/or quarterly basis. |

## Domestic Nuclear Detection Office

| | |
|---|---|
| Performance Measure | Number of individual Urban Area Security Designs completed for the Securing the Cities Program. |
| Program and Organization | Domestic Nuclear Detection - Domestic Nuclear Detection Office |
| Description | This measure is one of several for informing the program leadership of the reduction in risk to the interior layer of the global nuclear detection architecture. An Urban Area Security Design will consist of a strategy for encountering and identifying illicit radioactive or nuclear materials in or near high risk urban areas or regions. The design will provide an acquisition plan with types, quantities, and placements of radiation/nuclear materials detectors, and describe interfaces to other Federal systems that collectively will enhance the security of the interior layer against a terrorist attack. |
| Scope | The scope of this measure is all high risk urban areas in the United States. |
| Data Source | Source information is contained in reports from the Securing the Cities program management. Status on progress is maintained in a spreadsheet and controlled by the Securing the Cities program office. |
| Collection Method | The program and regional partners, at the culmination of a successful design, will enter into a cooperative agreement (or other contractual mechanism) to begin implementation of the design. This data is collected by the program’s Securing the Cities staff and the status is updated in the spreadsheet. |
| Reliability | Reliable |
| How Data is Verified | The efficacy of regional strategies is evaluated by subject matter experts (principally program and other Federal staff) prior to the award of any funds to State and local agencies for implementation of strategies. |

| | |
|---|---|
| Performance Measure | Percent of cargo, by volume, that passes through radiation portal monitors upon entering the Nation. |
| Program and Organization | Domestic Nuclear Detection - Domestic Nuclear Detection Office |
| Description | The program is responsible for acquiring all radiation detection equipment to be deployed to the Nation's ports of entry (POEs). Radiation portal monitors are one of the principle pieces of equipment used to meet this requirement. While Customs and Border Protection (CBP) maintains the responsibility for operating the systems, this measure reflects the capability that the program provides to CBP in support of this mission. |
| Scope | All containerized cargo entering the U.S. |
| Data Source | Port volume reports of containers entering the U.S. are provided by CBP field offices. Volume data are maintained in the spreadsheet. Additionally, weekly reports of new portal installations are provided by the installation agent, the Pacific Northwest National Laboratory (PNNL). This data is provided in tabular form, based on new installations completed in a given week. |
| Collection Method | Volume data is entered into the spreadsheet on a daily basis by the field offices at the port of entry. Weekly progress reports are provided by PNNL and sent to both the program and CBP which summarize installation progress for the last week and any changes to the overall volume of cargo being scanned. The percent of cargo passing through portal monitors is calculated based on the volume of containers entering through each lane at each port and is matched against those lanes that are covered by a portal monitor. |
| Reliability | Reliable |
| How Data is Verified | Volume data is reviewed and verified by CBP field supervisors on a daily basis. Portal monitor installation information is monitored and verified by the program and CBP Program Managers, and validated by field inspections when necessary. |

## Federal Emergency Management Agency

| | |
|---|---|
| Performance Measure | Percent of customers satisfied with Individual Recovery Assistance. |
| Program and Organization | Disaster Assistance - Federal Emergency Management Agency |
| Description | The percent of Americans affected by disaster or other emergency who indicate satisfaction with the Individual Disaster Recovery Assistance provided by FEMA to help them return to normal and function quickly and efficiently. |
| Scope | The customer is the individual disaster applicant who has registered with FEMA and received assistance. The calculation is based on a random sample of applicants who were surveyed between October 1st and September 30th and who responded positively to the question, “Overall, how would you rate the information and support you received from FEMA since the disaster occurred Would you say it's been: Excellent, Good, Satisfactory, Below Average or Poor?” While on a per disaster basis, statistical validity is not always feasible, cumulative annual results typically provide a confidence level of 98 percent with a margin of error of +/- 2 percent. |
| Data Source | Customer satisfaction data are derived from statistical reports from regular surveys of the customer population in the Individual Assistance (IA) program. For this performance measurement, a random sample of applicant data is extracted from the National Emergency Management Information System (NEMIS) database and imported to the survey tool. Based on the date of registration, two segments of applicants are called: the first after the first fifteen days of registration, and the second thirty days after the close of the application period. |
| Collection Method | Customer satisfaction survey data is collected by telephone for each Individual Assistance declaration. |
| Reliability | Reliable |
| How Data is Verified | To verify data, surveyors are monitored for quality assurance by listening to their calls to be sure the disaster applicant is not influenced in their response and by simultaneously viewing the data entry screens for accurate collection of information by using Systems Management Server (SMS) software. |

| | |
|---|---|
| Performance Measure | Percent of customers satisfied with Public Recovery Assistance. |
| Program and Organization | Disaster Assistance - Federal Emergency Management Agency |
| Description | The percent of communities affected by disaster or other emergencies who indicate satisfaction with the Public Disaster Recovery Assistance provided by FEMA to help them return to normal and function quickly and efficiently. Assistance includes debris removal, emergency protective measures, and repair or replacement of damaged infrastructure. |
| Scope | To track improvement in the operations of the Public Assistance Program and to identify areas in need of additional attention, FEMA conducts a series of Program Evaluation and Customer Satisfaction Surveys for each Fiscal Year to gather data on customer satisfaction with performance in specific program areas, represented by performance standards and their targets. The performance standards are: Overall Program and Process, Project Worksheet (PW) Process, Information Dissemination, Public Assistance Administrative Burden, Timely Service and Staff Performance. Grantees (State) and sub-grantees (local applicants) are the two types of customers for whom this report analyzes satisfaction. The annual report, which is derived from the Customer Service Survey, summarizes customer satisfaction results from disasters surveyed during the past fiscal year and compares them to the Public Assistance program’s performance targets and the previous fiscal year’s survey. |
| Data Source | Customer satisfaction data are derived from statistical reports from regular surveys of the customer population in the Public Assistance program. Customer satisfaction surveys are sent to all Grantees and Sub-Grantees who received a Public Assistance Grant in the previous year. Grantees are typically State-level emergency management officials, such as State Director, Governors Authorized |

| | |
|---|---|
| | Representative (GAR), and State Public Assistance Officer (PAO). Sub-grantees are typically State, local or tribal governments, or private nonprofit organizations applying for Public Assistance funds and carrying out the day-to-day recovery efforts. There are an average of 143 sub-grantees and one grantee per disaster and an average of 55 disasters per year. |
| Collection Method | The customer survey data is collected by an independent contractor via telephone and mail surveys. The number of responses is based upon the number of Federally declared disaster in the previous fiscal year. State and local applicants involved in a federally declared disaster are invited to participate in the customer survey process. Surveys are mailed to Grantees and Sub-grantees. Completed surveys are received via the mail or the internet and entered in the SAS statistical software program by an independent contractor. Responses typically range from Very Satisfied to Very Dissatisfied. |
| Reliability | Reliable |
| How Data is Verified | Survey data are collected, analyzed and reported by outside contractors using methods that guarantee both validity and reliability. The verification of the reliability of information collected is considered complete based on the data collection method used, which includes the allowance for all grantees and sub-grantees to respond to the survey with no sampling and the voluntary basis for responses from grantees and sub-grantees. |

| | |
|---|---|
| Performance Measure | Percent of response teams reported at operational status. |
| Program and Organization | Disaster Operations - Federal Emergency Management Agency |
| Description | This measure gauges the percent of FEMA's response teams indicating they are ready to respond quickly and effectively to acts of terrorism, natural disasters, and other emergencies. The measure tracks the readiness of three types of teams: the 28 task forces of Urban Search and Rescue (US&R); the five Mobile Emergency Response Support (MERS) detachments; and the two Federal Incident Response Support Teams (FIRSTs). |
| Scope | The three types of teams mentioned above are included in the measure. Operational readiness is defined for each team type as teams having the necessary staffing, equipment and training required for response to a disaster or incident. The criteria and source data for this determination is particular to each team type. |
| Data Source | Staffing and equipment levels are provided by status reports that are collected periodically. Urban Search and Rescue derived source data from Task Force Self-Evaluations. The Federal Incident Response Support Teams (FIRSTs) data is collected and tracked in reports maintained by the Field Operations Section Chief and staff. |
| Collection Method | Urban Search and Rescue (USR) task forces receive comprehensive self - evaluations by March 1 of each year. Task force Program Managers must complete and return the self-evaluations to the USR Program Office at FEMA by June 1. USR Program Office staff compiles task force submission in a spreadsheet, which is utilized for reporting data for this performance measure. The Federal Incident Response Support Teams (FIRSTs) collects and tracks data continuously using reports maintained by the Field Operations Section Chief and staff. |
| Reliability | Reliable |
| How Data is Verified | For Urban Search and Rescue task forces, hard copies of submitted self-assessments are verified and archived at the Program Office. Additionally, results are assessed with respect to the monthly online readiness questionnaires completed by each task force for consistency. The data collected and tracked by the Federal Incident Response Support Teams (FIRSTs) is verified by the Field Operations Section Chief. |

| | |
|---|---|
| Performance Measure | Percent of analyzed capabilities performed acceptably in exercises. (New performance plan measure for FY 2008.) |
| Program and Organization | Grants Program - Federal Emergency Management Agency |

| | |
|---|---|
| Description | Exercises form a critical part of the backbone of national emergency preparedness. During an exercise, a jurisdiction is required to implement its critical capabilities under circumstances as close as possible to an actual emergency. Historically exercises were evaluated using critical tasks; now they are evaluated using capabilities as described by the Homeland Security Exercise and Evaluation Program. Exercises expose areas of strength, weaknesses in plans and abilities, and areas of possible improvement. As such, exercises are the most cost-effective and accessible means of demonstrating whether or not a jurisdiction has attained a desired level of emergency capabilities. |
| Scope | The data set consists of all available after-action reports (AARs) which meet Homeland Security Exercise and Evaluation Program (HSEEP) criteria and are posted to the Office of Grants and Training (GT) secure portal. GT funds and supports exercises at the national, Federal, State, and local levels and requires that these exercises follow HSEEP guidance and processes. Vendors are required to post HSEEP-AARs to the GT portal for every direct support exercise. State and local jurisdictions are encouraged to post HSEEP-compliant AARs for all exercises funded or supported by the State Homeland Security Grant Program (SHSGP) and the HSEEP. GT conducts analysis of each analyzed capability in the exercise AARs and places the performance of each capability in a category such as acceptable, partially acceptable, or unacceptable. |
| Data Source | Supporting data is derived from homeland security exercise AARs that are submitted to the GT portal for GT review. Vendors are required to post HSEEP - compliant AARs to the GT portal for every direct support exercise. State and local jurisdictions are encouraged to post HSEEP - compliant AARs for all exercises funded or supported by the State Homeland Security Grant Program (SHSGP) and the HSEEP. All AARs in the data sample follow the prescribed HSEEP format which requires an AAR to include analysis of how jurisdictions participating in the exercise performed on capabilities. |
| Collection Method | GT reviews HSEEP-compliant AARs submitted by participating State and local jurisdictions. Capability analyses included in the AARs are evaluated using Exercise Evaluation Guides and the Target Capabilities List (TCL) to determine whether the jurisdictions performance met expectations or required improvement. Jurisdictions performance on each capability is analyzed by comparing the results documented in the AAR to the expected outcome described in the EEG. For each of the 37 target capabilities in the TCL, the percent performed acceptably is calculated by dividing the number of instances in which a capability was performed acceptably by the total number of instances a capability was exercised. The resulting percentage represents the percent of analyzed capabilities performed acceptably in exercises. |
| Reliability | Reliable |
| How Data is Verified | The quality and consistency of after-action reports (AAR) is ensured through the HSEEP exercise evaluation process. A team of independent, expert evaluators is recruited and trained for each exercise to assess capability performance in accordance with HSEEP EEGs. This process ensures that multiple evaluations of capability performance are included in AARs. Exercise planners also develop standard forms to capture observation and data analysis to ensure certain areas of observation are completed by all evaluators. GT Program Managers and support staff review raw data and calculations to ensure completeness and accuracy of the results. |

| | |
|---|---|
| Performance Measure | Percent of jurisdictions demonstrating acceptable performance on applicable critical tasks in exercises using Grants and Training approved scenarios. (Retired plan measure.) |
| Program and Organization | Grants Program - Federal Emergency Management Agency |
| Description | This measure gauges the percent of analyzed capabilities performed acceptably by jurisdictions during exercises based on Homeland Security Exercise and Evaluation (HSEEP) criteria. Increased percentages of capabilities performed |

| | |
|---|---|
| | acceptably demonstrates strengthened nationwide preparedness and mitigation against acts of terrorism, natural disasters, and other emergencies. Measuring improvements in jurisdictions’ performance on capabilities over time reflects the impact of Grants and Training preparedness activities on jurisdictions’ overall preparedness levels. To measure preparedness levels, capability analyses included in exercise after-action reports (AARs) are evaluated using HSEEP Exercise Evaluation Guides (EEGs) to determine whether the jurisdiction’s performance met expectations or required improvement. Jurisdictions’ performance on capabilities is analyzed by comparing the results documented in the AAR to the expected outcome described in the EEG. |
| Scope | The data set consists of all available after-action reports (AARs) which meet Homeland Security Exercise and Evaluation Program (HSEEP) criteria and are posted to the National Preparedness Directorate (NPD) secure portal. NPD funds and supports exercises at the national, Federal, State, and local levels and requires that these exercises follow HSEEP guidance and processes. Vendors are required to post HSEEP-compliant AARs to the NPD portal for every direct support exercise. State and local jurisdictions are encouraged to post HSEEP-compliant AARs for all exercises funded or supported by the State Homeland Security Grant Program (SHSGP) and the HSEEP. NPD conducts analysis of each analyzed capability in the exercise AARs and places the performance of each capability in a category such as acceptable, partially acceptable, or unacceptable. |
| Data Source | At the conclusion of a direct support exercise, each exercise participant is asked to complete a paper survey measuring his or her satisfaction with exercise components on a scale of 1 (Very Unsatisfied) to 5 (Very Satisfied). Questions include whether the exercise was well - structured and organized, whether the scenario was plausible and realistic, whether the facilitators were effective, and whether the exercise tools were valuable. These surveys are then sent to DHS in hard copy or scanned into a computer and sent electronically as pictures or PDF files. |
| Collection Method | NPD reviews HSEEP-compliant AARs submitted by participating State and local jurisdictions. Measure calculated based on exercise participants responses to paper surveys measuring satisfaction with exercise support. Participants rate their satisfaction with exercise design, scenario, contribution to capabilities, etc. immediately following exercises. Ratings are based on scale of 1 (Very Unsatisfied) to 5 (Very Satisfied) and typically include 4-8 questions. Respondents’ answers are averaged to produce an overall satisfaction rating for that participant. Overall participant ratings are averaged to calculate a satisfaction rating for an exercise. Finally, all satisfaction ratings for exercises conducted in the same fiscal year are averaged to produce an overall satisfaction rating for direct support exercises. A rating of 4 or 5 is considered satisfied." Surveys are sent to DHS, where analysts compile the results into spreadsheets to calculate overall satisfaction ratings. |
| Reliability | Reliable |
| How Data is Verified | The quality and consistency of after-action reports (AAR) is ensured through the HSEEP exercise evaluation process. A team of independent, expert evaluators is recruited and trained for each exercise to assess critical task performance in accordance with HSEEP EEGs. This process ensures that multiple evaluations of capability performance are included in AARs. Exercise planners also develop standard forms to capture observation and data analysis to ensure certain areas of observation are completed by all evaluators. NPD Program Managers and support staff review raw data and calculations to ensure completeness and accuracy of the results. |

| | |
|---|---|
| Performance Measure | Percent of participating urban area grant recipients reporting measurable progress made towards identified goals and objectives to prevent and respond to terrorist attacks. (Retired plan measure.) |
| Program and Organization | Grants Program - Federal Emergency Management Agency |

| | |
|---|---|
| Description | This measure gauges the percent of urban area grant recipients with measurable progress toward the goals and objectives identified in their individual Urban Area Homeland Security Strategies as monitored by Preparedness Officers. Measurable progress by urban areas in achieving their goals and objectives improves nationwide preparedness and mitigation against acts of terrorism, natural disasters, or other emergencies. Demonstrating progress towards identified goals and objectives illustrates improvements in the abilities of urban area homeland security grant recipients to prevent, protect against, respond to, and recover from terrorist attacks. Measurement of progress towards identified goals and objectives is based on programmatic monitoring conducted by Preparedness Officers. |
| Scope | Urban Area Security Initiative grantees develop and maintain an Urban Area Homeland Security Strategy that identifies goals and objectives to improve homeland security capabilities. Eligible urban areas are determined based on the estimated relative risk of a successful terrorist attack using a common definition for the footprint of an urban area. The number of eligible urban areas in FY 2007 was 45, each with a corresponding strategy. Grantees complete a Biannual Strategy Implementation Report (BSIR) every six months. In the BSIR, grant recipients outline how they are spending grant money, tie funded projects to goals and objectives identified in the Urban Area Homeland Security Strategy, and estimate the overall impact of grant funding on addressing identified goals and objectives. |
| Data Source | Data for this measure is derived from programmatic monitoring conducted by preparedness officers. Preparedness Officers use analysis forms that contain fields for progress toward planning, organization, equipping, training, exercising, and other factors. Each Urban Area is evaluated by Preparedness Officers once every two years. The scores are manually entered into an Access database and the results are also manually extracted into an Excel document. |
| Collection Method | Staff conducts programmatic monitoring activities including review of BSIR data to determine what progress Urban Areas are making toward their identified goals and objectives. All BSIR data is collected through a standard web-based Grant Reporting Tool. In programmatic monitoring, Preparedness Officers evaluate progress by the urban area on its identified goals. Each goal is evaluated on progress in the categories of plans, organization, equipment, training, exercises, and other factors supporting that goal. Progress in each category is rated using a 5 point scale. Scores for progress in the categories are averaged to provide an overall measure of progress for each goal. The scores for each goal are then averaged to provide a measure of progress for the urban area as a whole against the goals it identified in the Urban Area Homeland Security Strategy. The scores are manually entered into an Access database and the results are also manually extracted into an Excel document. |
| Reliability | Reliable |
| How Data is Verified | The Grants Program Directorate (GPD) ensures data reliability and consistency by issuing detailed guidance to grantees on developing State Homeland Security Strategies and reporting information through BSIRs. GPD also develops an annual monitoring plan and provides detailed protocols for monitoring to staff. In addition, all information provided by grantees in State Homeland Security Strategies and BSIRs, as well as monitoring reports, undergo a review and approval process by GPD. |

| | |
|---|---|
| Performance Measure | Percent of State and local homeland security agency grant recipients reporting measurable progress towards identified goals and objectives to prevent and respond to terrorist attacks. (Retired plan measure.) |
| Program and Organization | Grants Program - Federal Emergency Management Agency |
| Description | This measure gauges the percent of state and local homeland security agency grant recipients with measurable progress toward the goals and objectives identified in their individual State Homeland Security Strategies. Measurable progress by States in achieving their goals and objectives improves nationwide preparedness |

| | |
|---|---|
| | and mitigation against acts of terrorism, natural disasters, or other emergencies. Demonstrating progress towards identified goals and objectives illustrates improvements in the abilities of State and local homeland security grant recipients to prevent, protect against, respond to, and recover from terrorist attacks. Measurement of progress towards identified goals and objectives is based on programmatic monitoring conducted by Preparedness Officers. |
| Scope | The Grant Programs Directorate (GPD) requires grant recipients to develop a State Homeland Security Strategy that identifies goals and objectives to improve homeland security capabilities. Each State and territory develops and maintains a State Homeland Security Strategy, resulting in 56 such strategies, each with corresponding goals and objectives. In addition, all grant recipients must complete a Biannual Strategy Implementation Report (BSIR) every six months in an award year. In the BSIRs, grant recipients outline how they are spending grant money, tie funded projects to goals and objectives identified in the State Homeland Security Strategy, and estimate the overall impact of grant funding on addressing identified goals and objectives. |
| Data Source | Data for this measure is collected by Preparedness Officers during their regular evaluation for the fiscal year. The scores are manually entered into an Access database and the results are also manually extracted into an Excel document. |
| Collection Method | All BSIR data is collected through a standard web-based Grant Reporting Tool. All information provided by grantees in State Homeland Security Strategies and BSIRs, as well as monitoring reports, undergo a review and approval process by GPD. In programmatic monitoring, Preparedness Officers evaluate progress by the State or territory on each of its identified goals. Each goal is evaluated on progress in the categories of plans, organization, equipment, training, exercises, and other factors supporting that particular goal. Progress in each of these categories is rated using a 5 point scale. Scores for progress in the categories are averaged to provide an overall measure of progress for each goal. The scores for each goal are averaged to provide a measure of progress for the state or territory against the goals it identified in the State Homeland Security Strategy. The scores are manually entered into an Access database and the results are manually extracted into an Excel document. |
| Reliability | Reliable |
| How Data is Verified | GPD ensures data reliability and consistency by issuing detailed guidance to grantees on developing State Homeland Security Strategies and reporting information through BSIRs. GPD also develops an annual monitoring plan and provides detailed protocols for monitoring to staff. Throughout the grant period, the staff conducts programmatic monitoring activities including review of data provided in BSIRs in order to determine what progress the State or territory is making toward its identified goals and objectives. |

| | |
|---|---|
| Performance Measure | Percent of State and local homeland security agency grant recipients reporting significant progress towards identified goals and objectives. (New performance plan measure for FY 2008.) |
| Program and Organization | Grants Program - Federal Emergency Management Agency |
| Description | This measure reflects grantee progress against goals and objectives identified in homeland security strategies. |
| Scope | All 56 States and Territories are monitored each fiscal year. The National Preparedness Directorate (NPD) Preparedness Officers (POs) collect the progress scores for each objective and average the score to come up with one final progress number. That number will be compared against the previous year's monitoring visit to chart progress. A movement of 0.1 in total average progress will show "significant" progress. |
| Data Source | Data for each State is tracked in an access database. |
| Collection Method | Although all 56 State and Territories are being monitored on an annual basis, the only way to make sure that we are comparing similar results is to only include the States and Territories who did not update their strategy between consecutive |

| | |
|---|---|
| | monitoring visits. If a grantee updates their strategy (which they can do at anytime), we would expect their progress to decrease as new objectives are added. FY 2006 was the first year in which NPD conducted programmatic monitoring in order to track progress made in achieving goals and objectives stated in the most recently approved State Homeland Security Strategies. |
| Reliability | Reliable |
| How Data is Verified | NPD analyzes all of the data that is collected during the monitoring visits. We will pull - out those States that updated their strategies since their previous monitoring visit and run the numbers on the remaining States to determine how many States and Territories made significant progress since their last monitoring visit. |

| | |
|---|---|
| Performance Measure | Percent of urban area grant recipients reporting significant progress towards identified goals and objectives. (New performance plan measure for FY 2008.) |
| Program and Organization | Grants Program - Federal Emergency Management Agency |
| Description | This measure reflects grantee progress against the goals and objectives identified in their Urban Area homeland security strategies. This measure will be collected during the monitoring visits conducted by the FEMA/National Preparedness Directorate (NPD) Preparedness Officers (PO). Each objective is measured on a 0-5 scale with 0 meaning zero progress and 5 meaning the objective has been completed. The term "significant" means a 0.1 increase in the average progress of all of the objectives in the grantee's strategy. |
| Scope | Each Urban Area is monitored every two fiscal years. The NPD POs will collect the progress scores for each objective and average the score to come up with one final progress number. That number will be compared against the previous monitoring visit to chart progress. A movement of 0.1 in total average progress will show "significant" progress. |
| Data Source | NPD POs will monitor the Urban Areas and enter their results into an Access Database which serves as the basis for the monitoring report. |
| Collection Method | Only 50 percent of all Urban Areas are monitored each year. Therefore, we will be using a different pool of candidates for each fiscal year target. Also, the only way to make sure that we are comparing similar results is to only include the Urban Areas who did not update their strategy since their previous monitoring visit. If a grantee updates their strategy (which they can do at anytime), we would expect their progress to decrease as new objectives are added. |
| Reliability | Reliable |
| How Data is Verified | NPD analyzes all of the data that is collected during the monitoring visits by looking at the results of each of the Access databases and the final monitoring reports. |

| | |
|---|---|
| Performance Measure | Percent reduction in firefighter injuries in jurisdictions receiving Assistance to Firefighter Grants funding compared to the national average. (New performance plan measure for FY 2008.) |
| Program and Organization | Grants Program - Federal Emergency Management Agency |
| Description | This measure compares the percent reduction in fighter injuries in jurisdictions that receive Assistance to Firefighter Grants (AFG) to the average percent reduction in firefighter injuries nationwide. The measure assesses improvements in firefighter safety in jurisdictions that receive AFG funding. Comparing AFG-funded jurisdictions to the national average shows the impact of AFG awards on reducing firefighter injuries. The measure specifically focuses on line-of-duty firefighter injuries, not any injury that a firefighter may have. |
| Scope | The National Fire Protection Association (NFPA) conducts an annual voluntary survey of fire departments on line of duty fire fighter injuries. Line of duty categories collected include: fire, ground, responding or returning, on-scene non fire, training, and other on-duty. The NFPA surveys approximately 8000 departments representing a cross section of the urban, suburban, rural, volunteer, paid, and combination departments. If any large departments (Chicago, Miami, |

| | |
|---|---|
| | etc.) do not respond, NFPA contacts them and conducts the survey via telephone interview to ensure there are no major gaps in the sample data. The data range for AFG specific information is all AFG grant-funded jurisdictions. There are approximately 5500 jurisdictions that receive AFG funding each year. The NFPA survey is sent to jurisdictions that serve populations of 50,000 or more and departments that protect smaller populations. Over the past 5 years the response rate from all jurisdictions averages out to: 44.11 percent. |
| Data Source | Information on firefighter injuries nationwide is provided by fire departments through the National Fire Incident Reporting System and the NFPA annual survey. NFIRS is an electronic data collection system. It is used to report a variety of information related to each call that a department responds to. Congress mandated that USFA collect this type of data gain a better understanding of what the United States fire related risks. The NFPA survey is conducted to in order to collect similar information. There is overlap in the types of information collected. The survey is sent in a hard copy format with an option to respond electronically. They are multiple choice type questions with data input fields. AFG collects data on active firefighters and firefighter injures via the application process. All applicants are required to enter their counts in the application. AFG requires, as a condition of award acceptance, that they report for a period of 12 months. |
| Collection Method | The NFPA conducts an annual voluntary survey of fire departments on line of duty fire fighter injuries. NFIRS is the standard national reporting system used by U.S. fire departments to report fires and other incidents to which they respond and to maintain records of these incidents in a uniform manner. NFIRS compares the results of the NFPA survey with their own data. NFIRS data is derived from incident reports received directly from fire departments and allows NFIRS to determine national trends. The corroboration of trends indicated by NFPA and NFIRS is the data verification. Reporting to NFIRS is voluntary, but follows a prescribed format. AFG collects data on active firefighters and firefighter injures via the application process. All applicants are required to enter their counts in the application. Jurisdictions report this information in the data fields of the application itself for the past three years. Therefore every jurisdiction that is awarded has submitted this data. |
| Reliability | Reliable |
| How Data is Verified | Data is reported annually by the National Fire Protection Association and is based on the results of a survey representing a cross section of urban, suburban, rural, volunteer, paid, and combination departments. If any large departments do not respond, NFPA contacts them and conducts the survey by telephone to ensure there are no major gaps in the sample data. The National Fire Incident Reporting System (NFIRS) is the standard national reporting system used by U.S. fire departments to report fires and other incidents to which they respond and to maintain records of these incidents in a uniform manner. The AFG collects data on active firefighters and firefighter injures via the application process. All applicants are required to enter their counts in the application. All jurisdictions have to report their information when applying. If they don't fill in these fields then the application is not processed. All awarded jurisdictions will have provided the requested information. |

| | |
|---|---|
| Performance Measure | Ratio of the Nation's on-scene fire incident injuries to total number of active firefighters. (Retired plan measure.) |
| Program and Organization | Grants Program - Federal Emergency Management Agency |
| Description | This measure reports the percent of firefighters injured on the scene as compared with the total number of the Nation's firefighters. This measure assesses improvements in firefighter safety in jurisdictions receiving Assistance to Firefighters Grant (AFG) funds to maximize the health and safety of firefighting personnel against fire and fire-related hazards by providing assistance to fire departments and by training the Nation's fire department personnel to prevent, protect against, respond to, and recover from fire-related events. The ratio of |

| | |
|---|---|
| | firefighter injuries to active firefighters reflects the effectiveness of AFG funds in promoting firefighter safety through its support for firefighter training, wellness programs, and protective equipment. |
| Scope | The National Fire Protection Association (NFPA) conducts an annual voluntary survey of fire departments on line of duty fire fighter injuries. Line of duty categories collected include: fire, ground, responding or returning, on-scene non fire, training, and other on-duty. The NFPA surveys approximately 8,000 fire departments across the nation representing a cross section of the urban, suburban, rural, volunteer, paid, and combination departments. If any large departments (Chicago, Miami, etc.) do not respond, then NFPA contacts them by telephone and conducts the survey via telephone interview to ensure there are no major gaps in the sample data. The NFPA survey is sent out to jurisdictions that protect populations of 50,000 or greater as well as departments that protect smaller populations. |
| Data Source | Information on firefighter injuries was provided by fire departments through the National Fire Incident Reporting System (NFIRS) and the National Fire Protection Association annual survey. NFIRS, a voluntary electronic reporting and data collection system, is used to report a variety of information related to each call that a department responds to. Congress mandated that the U.S. Fire Administration (USFA) collect this type of data in order to get a better picture of what the U.S.'s fire related risks are. The AFG requires, as a condition of award acceptance, that they report for a period of 12 months. |
| Collection Method | The NFPA conducts an annual voluntary survey of fire departments on line of duty fire fighter injuries. The NFIRS is the standard national reporting system used by U.S. fire departments to report fires and other incidents to which they respond and to maintain records of these incidents in a uniform manner. Reporting to NFIRS is voluntary, but follows a prescribed format. The program asks AFG recipients to complete a voluntary survey on the number of firefighter injuries and the total number of active firefighters in each jurisdiction receiving AFG funds. Data collected from survey responses is then combined to determine an overall ratio of firefighter injuries to total number of active firefighters for AFG recipients. |
| Reliability | Reliable |
| How Data is Verified | Data is reported annually by the NFPA and is based on the results of a survey representing a cross section of urban, suburban, rural, volunteer, paid, and combination departments. If any large departments do not respond, NFPA contacts them and conducts the survey by telephone to ensure there are no major gaps in the sample data. The NFIRS is the standard national reporting system used by U.S. fire departments to report fires and other incidents to which they respond and to maintain records of these incidents in a uniform manner. NFIRS compares the results of the NFPA survey with their own data. NFIRS data is derived from incident reports received directly from fire departments and allows NFIRS to determine national trends. The corroboration of trends indicated by NFPA and NFIRS is the data verification. |

| | |
|---|---|
| Performance Measure | Average time in hours to provide essential logistical services to an impacted community of 50,000 or fewer. |
| Program and Organization | Logistics Management - Federal Emergency Management Agency |
| Description | This measure reports the average response time in hours to provide essential logistical services to a community of 50,000 or fewer, in the event of a natural disaster or other emergency. FEMA provides logistical services to communities which include ice, water, meals ready to eat, and other commodities. Start time is measured from the driver pick up time and end time is measured as delivery to the destination. |
| Scope | Life-saving, life-sustaining disaster commodities tracked in this measure include: water, ice, emergency meals, plastic sheeting, tarps, generators, cots, and blankets. The initial request(s) for these commodities are generated by the completing an |

| | |
|---|---|
| | Action Request Forms and entering it into the eTasker system. Response time is measured from the moment the initial request is entered into the system until the order is received by the Joint Field Office. |
| Data Source | Logistics Management Directorate is currently implementing the Total Assets Visibility (TAV) and eTasker systems to assist with data collection. eTasker is a role-based application which is designed to provide users with an automated, standardized system for requesting commodities through FEMA Headquarters, along with other technological advances, as a major component of a Total Logistics Management System that allows FEMA to track disaster assets from mobilization, to arrival, demobilization, and departure. TAV, utilizing the Global Positioning System, provides transparency and visibility of required commodities throughout the supply chain, from source to end-user. |
| Collection Method | Data is collected from the Resource Tracking spreadsheet maintained by personnel assigned during deployments. 100 percent of the spreadsheet rows are queried for data and included in the calculation as follows: 1) Rows with Actual Shipping Times and Actual Arrival Times; and 2) Rows with Actual Shipping Times and Estimated Arrival Times. |
| Reliability | Reliable |
| How Data is Verified | The new electronic tracking system Logistics Management has implemented ensures data is captured and reported accurately. The electronic reporting capability of these systems allows users to sort various data in a short amount of time. Data is verified by physical inspection to ensure delivery is completed. |

| | |
|---|---|
| Performance Measure | Percent of the national population whose safety is improved through the availability of flood risk data in Geospatial Information System (GIS) format. |
| Program and Organization | Mitigation - Federal Emergency Management Agency |
| Description | This measure reports the cumulative percent of the national population that has updated digital flood risk data available online for their community. This digital data replaces old-fashioned paper flood maps. There are some communities, representing eight percent of the population, with little to no flood risk that will not be mapped. |
| Scope | This performance measure is based on the cumulative percentage to date of the national population living in communities that have received preliminary digital flood maps. The National Flood Insurance Program and FEMA’s Flood Map Modernization Program are organized around community participation; a community's population is counted when they receive preliminary digital flood maps from FEMA. Using a series of such factors as population and growth, housing units, flood insurance policies and claims, and repetitive flood losses, FEMA has assigned every county in the nation a risk factor. This risk factor is the value used by FEMA to make decisions about effective allocation of Flood Map Modernization study funds and priorities nationwide. |
| Data Source | In order to calculate the data for this performance measure (as well as to host numerous other applications), FEMA operates the Mapping Information Platform (MIP). The MIP is a management platform for all flood map study projects nationwide, providing a base from which Program Managers and the public can determine the current status of Map Modernization. Based on data in the MIP, FEMA counts a community's population when they receive preliminary digital flood maps. |
| Collection Method | FEMA uses the Mapping Information Platform (MIP) to calculate this performance measure, collecting data from all of the FEMA Regional map modernization contracts, grants, and major mapping activities. The MIP is a management platform for all flood map study projects nationwide, providing a database from which Program Managers and the public can determine the current status of Map Modernization as well as this performance measure. |
| Reliability | Reliable |
| How Data is Verified | FEMA’s Flood Map Modernization Program uses a three-tier approach to data verification. Tier 1 is the internal quality assurance check of the status of the |

| | |
|---|---|
| | preliminary maps used by the Map Modernizations National Service Provider contractor. Tier 2 is an external validation of the primary source data through the Status of Studies report, reviewed by FEMA Regional staff. Tier 3 relies on FEMA's national headquarters contract with an independent, third party company to check for program and data quality assurance. |

| | |
|---|---|
| Performance Measure | Potential property losses, disasters, and other costs avoided. |
| Program and Organization | Mitigation - Federal Emergency Management Agency |
| 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. Losses are avoided to property (buildings and infrastructure) through the provision of: 1) Financial and technical assistance to States, territories, tribes, and communities to implement pre-identified, cost-effective mitigation measures (via Hazard Mitigation Assistance grants); 2) Sound floodplain management; and 3) State-of-the-art building science technologies, guidance and expertise for natural and man-made hazards (Disaster-Resistant Building Sciences), thus protecting American citizens from disasters through assistance, education, and technology. |
| Scope | 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 | National Emergency Management Information System (NEMIS) and e-grants 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 (DFO) 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 CRS data. The CIS 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. |
| Collection Method | The methodology used to estimate the annual flood losses that are avoided resulting from the NFIPs mitigation requirements are based on estimates of the number of Post-FIRM structures in SFHAs, 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 average benefit cost ratio of 2 for projects). All mitigation activities, except for Management Costs/Technical Assistance, were included. In support of the this approach, the Multi-Hazard Mitigation Council released a report in December of 2005 that stated that mitigation saves society an average of four dollars for every dollar spent. |
| Reliability | Reliable |
| How Data is Verified | 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 (IFMIS) funding reports. |

| | |
|---|---|
| Performance Measure | Percent of Federal Departments and Agencies with fully operational Continuity of Operations (COOP) capabilities. |
| Program and Organization | National Continuity Programs - Federal Emergency Management Agency |
| Description | FEMA works with Federal departments and agencies to develop and exercise |

| | |
|---|---|
| | plans that ensure the continuation of federal operations and the continuity and survival of an enduring constitutional government. FEMA collects the results of exercises and self-assessments to measure the percentage of departments and agencies that have in place the necessary plans and capabilities. |
| Scope | FEMA determines the percentage of 30 Federal departments and agencies listed for Continuity of Government Conditions (COGCON) matrix with fully operational COOP capabilities. Criteria is derived from the Federal Preparedness Circular (FPC) 65, Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Operations and other guidance documents and matrices. COOP capable is being able to perform essential functions from an alternate location. Agencies perform self assessments of COOP plans using the COOP self assessment tool. This ensures the agencies are aware of their COOP capability. Criteria include: Federal Departments and Agencies participation in annual federal COOP training and/or exercises to demonstrate their ability to achieve full operational COOP capability; participation in quarterly alert and notification tests; deployment of emergency relocation teams; and testing of their ability to perform essential functions from an alternate facility. |
| Data Source | The data sources for the percentage of federal departments and agencies with fully operational capabilities include: reports generated from the FEMA Operations Center (FOC), self-assessments by the Federal D/As, participation in training events and exercises, real world events and activities, and assessments conducted by FEMA. A report is generated by the FOC showing who positively responded to the alert and notification tests. The agencies are evaluated using a COOP self assessment tool. Also their COOP Plan is evaluated before an exercise using the COOP self assessment tool. |
| Collection Method | Internal and Inter-Agency exercises provide the ability to evaluate strengths and weaknesses of the overall continuity programs by using the COOP self assessment tool. This information is notated in After Action Reports generated after training and exercises. Also, The FOC generates a Qualification and Exception Report that gives the percentage of responses/non-responses from the alert and notification testing. |
| Reliability | Reliable |
| How Data is Verified | The reliability of communications data will be verified by continuous communications testing plans with other D/As and the quarterly alert and notification results form the FOC’s Qualification and Exception Reports. The training and exercise data is verified by the FEMA 75 - 5 training registration forms, Training Information Access Database maintained by EMI, and Federal Department and Agency After Action Reports from exercise events. This data will be verified through periodic assessments involving interviews with the Federal D/As to analyze the validity and accuracy of the self-generated reports and through regularly scheduled government wide evaluated COOP exercises, such as Forward Challenge. |

| | |
|---|---|
| Performance Measure | Percent of fully operational Continuity of Government (COG) capabilities. |
| Program and Organization | National Continuity Programs - Federal Emergency Management Agency |
| Description | The percentage of federal departments and agencies that have developed and exercised plans to ensure the continuity of government operations and essential functions in the event of crisis or disaster. |
| Scope | This measure assesses the percent of Federal Executive Branch Departments and Agencies (D/As) with operational Continuity of Government (COG) capability based on the priorities of (1) program training and (2) communications capabilities established by the Enduring Constitutional Government Coordination Council (ECGCC). The following indicators have been adopted: (1) Training opportunities provided to designated D/A personnel, based on three essential categories with an annual training calendar and five year training plan, and documentation support to D/As, which is measured based on the essential policy and operations doctrine in the domestic COG documentation requirements.; and |

| | |
|---|---|
| | (2) percentage of applicable D/As with designated interagency communications capability. Each category of documentation is weighted to determine an overall percentage value. |
| Data Source | The data sources used to validate the above performance measure include but are not limited to the Corrective Action Program and the operations information systems. |
| Collection Method | The classified communications capabilities data base is maintained on a spreadsheet. The training component of the performance measure is collected from the Training Plan and the proposed and actual Annual Training Calendars, which are developed from an analysis of the Mission Essential Task List (METL), Professional Qualification Standards, and various feedback tools (which are completed for every event). |
| Reliability | Reliable |
| How Data is Verified | Surveys of communications capabilities are verified by technical representatives from an independent organization. Information is classified and will be available for properly cleared personnel upon completion of initial site surveys. The proposed and actual training calendars are maintained by FEMA. Feedback mechanisms are in place for every training event and maintained in a Corrective Action/Remedial Action data base. |

| | |
|---|---|
| Performance Measure | Percent increase in knowledge, skills, and abilities (KSAs) of State and local homeland security preparedness professionals receiving training. |
| Program and Organization | National Preparedness - Federal Emergency Management Agency |
| Description | This measure evaluates the gain in knowledge, skills, and abilities (KSA) of students through pre and post course assessments. This measure gauges the percent improvement in KSAs of State and local homeland security professionals after the completion of training, which demonstrates strengthened first responder preparedness and mitigation with respect to acts of terrorism, natural disasters, and other emergencies. Measuring these improvements indicates the impact of training services on the Nation's preparedness level. |
| Scope | Supporting data includes evaluations of all trainee's knowledge, skills, and abilities in a particular homeland security/preparedness subject area both before and after delivery of the training courses. Courses are offered throughout the year and include training at FEMA facilities, local sites, and online distance learning. Individuals receiving training are State and local personnel representing one or more of the following response disciplines: emergency management, emergency medical services, fire service, governmental administrative, hazardous materials, health care, law enforcement, public health, public safety communications, public works, and the private sector. |
| Data Source | Supporting data is derived from evaluation forms administered by training partners. Each individual trainee completes these forms that assess subject-matter knowledge, skills, and abilities at the beginning and conclusion of each training course. |
| Collection Method | Before and after each training course, trainees are asked to assess their knowledge, skills, and abilities in the subject area in which they are receiving training. Trainee responses are entered either manually by training partners or are transmitted electronically to the program via a database. For each participant, pre- and post-evaluations are compared to determine the percent increase in knowledge, skills, and abilities due to delivery of training. Pre- and post-course assessments are compared to determine the percentage increase in trainees' knowledge, skills, and abilities related to the training course subject area. These individual percentage increases are then averaged across all trainee responses. |
| Reliability | Reliable |
| How Data is Verified | Self-reported trainee evaluations are somewhat subjective but constitute an efficient method of collecting information on all trainees' progress in improving their knowledge, skills, and abilities. The program collects self-assessments on 100 percent of the professionals enrolled in training courses, improving data |

| | |
|---|---|
| | consistency and reliability. In addition, the risk of including clearly erratic or unreliable evaluation responses in the data set is mitigated through a review process. Program supervisors review data tabulations performed by analysts before releasing results. Data is estimated because partners are not required to submit data until 30 days after the end of the quarter and it takes 15 days to compile and verify the data for reporting. Supervisors review data tabulations performed by analysts before releasing results. |

| | |
|---|---|
| Performance Measure | Percent of Federal, State, local and tribal Governments compliant with the National Incident Management System (NIMS). |
| Program and Organization | National Preparedness - Federal Emergency Management Agency |
| Description | This measure tracks the percent of critical partners who are compliant with the National Incident Management System (NIMS). Federal Agencies were required to identify a point of contact within their agency to act as a liaison with NIMS Integration Center (NIC), create a NIMS Implementation Plan, incorporate NIMS into their respective Emergency operations Plans, and train all appropriate personnel in the NIMS standard training curriculum. States are required to submit self-certification of compliance based on 23 compliance requirements in the NIMCAST system. The program monitors the previous year's submission of NIMS implementation within States. Selective data audits, field monitoring and continuous refinements on reporting metrics to identify inconsistencies and errors are used to ensure reliability. |
| Scope | Federal Agencies, State, local and tribal governments were required to implement the NIMS into their response programs beginning in FY 2005 based on annual requirements sent to the directors of each agency and the Governors of all 56 States and territories. These requirements specify actions that agencies and the 56 State and Territorial governments and their subordinate jurisdictions must take to be NIMS compliant. |
| Data Source | Federal and State NIMS Compliance Assistance Support Tool (NIMCAST) report data. |
| Collection Method | NIMS compliance determination relies on Federal, State, local, and tribal Governments' self-assessment as reported to FEMA via NIMCAST. Once reported to FEMA, this information is submitted to the White House for its review. |
| Reliability | Reliable |
| How Data is Verified | Federal departments and agencies rely on quarterly meetings where peer review and critique ensure more effective NIMS implementation. FEMA's Headquarters office monitors and verifies NIMS compliance for the 56 States and Territories. |

| | |
|---|---|
| Performance Measure | Percent of Radiological Emergency Preparedness Program communities with a nuclear power plant that are fully capable of responding to an accident originating at the site. |
| Program and Organization | National Preparedness - Federal Emergency Management Agency |
| Description | This measure reports the percent of U.S. communities surrounding a nuclear power plant that are prepared and capable of responding to and recovering from an accident or terrorist attack. This assessment is based on first responder performance in exercises conducted at the facilities. |
| Scope | There are currently 64 operating commercial nuclear power plants. Approximately 400 State and local government jurisdictions are involved in radiological emergency planning and preparedness around these 64 sites. |
| Data Source | The program bases its findings and determinations of the adequacy of State and local radiological emergency preparedness and planning on the results of exercises at all 64 licensed commercial nuclear power plants. The program has been working with the State and local governments surrounding nuclear power plants for over 25 years. |
| Collection Method | The method of collection is by evaluating exercises at each nuclear power plant every 2 years. These exercises test the capabilities of State and local governments |

| | |
|---|---|
| | to protect the health and safety of the public in the event of an emergency at the plant. The results of these exercises are documented and REPP uses them in its reasonable assurance determinations to the Nuclear Regulatory Commission (NRC). |
| Reliability | Reliable |
| How Data is Verified | The program makes findings and determinations as to the adequacy and capability of implementing offsite plans, and communicates those finding and determinations to the NRC. The NRC reviews these findings and determinations in conjunction with the NRC onsite findings for the purpose of making determinations on the overall state of emergency preparedness. |

| | |
|---|---|
| Performance Measure | Percent of respondents reporting they are better prepared to deal with disasters and emergencies as a result of training. |
| Program and Organization | National Preparedness - Federal Emergency Management Agency |
| Description | The percent of students attending training at the Emergency Management Institute (EMI) and FEMA's Employee Development program who responded to a survey and indicated that they are better prepared to deal with disasters and emergencies as a result of the training they received. This training provides Federal, State, local and tribal officials having key emergency responsibilities with the knowledge and skills needed to strengthen nationwide preparedness and respond to, recover from, and mitigate against acts of terrorism, natural disasters, and other emergencies. |
| Scope | Approximately 14,000 students attend courses at Emergency Management Institute (EMI) resident training facilities every year, and an additional 3 million complete distance learning courses. Participants include Federal, State, local and tribal officials and responders. Typically, 35 percent of the long term follow-up evaluation questionnaires are completed and returned. EMI has only one dedicated permanent facility (in Emmitsburg, MD), but it currently also uses the Noble Training Center in Anniston, AL. EMI records fourteen categories of professions of the officials they train: Management, Training/Education, Scientific/Engineering, Investigation, Fire Prevention, Fire Suppression, Health, Disaster Response/Recovery, Hazard Mitigation, Emergency Preparedness, etc. EMI cross-references this with fifteen types of official experience: Incident Command, Administration/Staff Support, Supervision, Budget/Planning, Program Development/Delivery, Research Development, Law Enforcement, etc. |
| Data Source | Data are obtained from post-course evaluations sent to students. These forms are paper surveys and are distributed by mail to students, who must fill them out and return them to EMI. |
| Collection Method | All students are asked to complete post-course or end-of-course evaluation questionnaires at the conclusion of their training. Approximately 3 months following the training course, students are asked to complete a long term evaluation questionnaire. When the paper forms are returned to EMI, the information is manually entered into a Microsoft Access database for storage, use, and analysis by senior EMI officials. |
| Reliability | Reliable |
| How Data is Verified | Typically, 35 percent of the long term follow-up evaluation questionnaires are completed and returned. The data is reliable because it is collected directly from the students receiving the training. All data is collected and reviewed by a contractor for completeness prior to report compilation and production. |

| | |
|---|---|
| Performance Measure | The per capita loss of life due to fire in the U.S. |
| Program and Organization | U.S. Fire Administration - Federal Emergency Management Agency |
| Description | This measure is based on data that analyzes the reduction in the rate of loss of life from fire-related events by one percent per year. It examines the fatalities in the U.S. per million population using modified targets based on the review of historical data. The National Fire Protection Association (NFPA) reports data in September for the previous year. NFPA Survey data are analyzed to produce the report on fire related civilian fatalities. |

| | |
|---|---|
| Scope | The annual civilian fire death rate is based upon the total number of civilian fire deaths that occur within the U.S. during the calendar year, and U.S. Census Bureau population estimates for that year. Civilian fire death rates are measured in deaths per million population. A death is defined as a civilian fatality as reported to the National Fire Protection Association's (NFPA) National Fire Experience Survey (NFPA Survey) for a given calendar year. Estimates from the NFPA Survey are generally available in Sept. for the preceding year (e.g., fatality estimates for Calendar Year 2006 were available in Sept 2007). |
| Data Source | The data sources used in calculating this performance measure are fire department responses to the NFPA Fire Experience Survey, and U.S. Census Bureau population estimates. The NFPA survey is a probability sample survey conducted annually, and provides data to derive unbiased national estimates of U.S. civilian fire fatalities. Census Bureau population estimates are generated annually, estimating total U.S. population on July 1 of the relevant year. |
| Collection Method | NFPA Survey data are analyzed to produce estimates of fire related civilian fatalities which are used for numerator data; Census Bureau population estimates are used for denominator data. |
| Reliability | Reliable |
| How Data is Verified | Loss of life data from the National Fire Incident Report System (NFIRS) are also compiled and reviewed by the National Fire Data Center. Statistical weighting and comparison of these data as well as with National Centers for Health Statistics (NCHS) mortality data are done to check for accuracy. A comparison of these data sets to the NFPA fatality data is conducted for consistency and relative veracity. |

## Federal Law Enforcement Training Center

| | |
|---|---|
| Performance Measure | Percent of Partner Organizations (POs) that respond "agree" or "strongly agree" on the Partner Organization Satisfaction Survey (POSS) to their overall satisfaction with the training provided by the FLETC. |
| Program and Organization | Law Enforcement Training - Federal Law Enforcement Training Center |
| Description | This performance measure reflects the percentage of POs that responded on the POSS agree or strongly agree to the overall satisfaction with the training the Federal Law Enforcement Training Center (FLETC) provides their officers or agents to prevent terrorism and other criminal activity against the U.S. and our citizens. |
| Scope | This measure focuses on training satisfaction of each of the FLETC’s 83 Partner Organizations (PO). Surveys are completed by agency leaders after a student finishes training at FLETC. |
| Data Source | The source of the data is from the FLETC Partner Organization Satisfaction Survey (POSS) administered via a web-based program (Perseus) which tabulates and calculates the survey results. The measure uses the question, “Overall, my agency is satisfied with the training the FLETC provides.” |
| Collection Method | The FLETC Partner Organizations (POs) are surveyed using the Partner Organization Satisfaction Survey (POSS) which is accessed via the Perseus web based program. The survey uses a modified a six-point Likert scale (Strongly Agree, Agree, Slightly Agree, Slightly Disagree, Disagree, and Strongly Disagree). Data is entered through this system and stored at the end of each completed survey. Strategic Planning and Analysis Division personnel access the data via the Perseus web site, import the data into the Statistical Package for the Social Sciences (SPSS) to generate descriptive statistics, and then into MS Excel to generate data charts and tables. |
| Reliability | Reliable |
| How Data is Verified | The survey was developed using contemporary survey methods comparable to those used by the military services and other major training organizations. FLETC leaders conduct verbal sessions with Partner Organization (PO) key representatives to confirm and discuss their responses. Throughout the year other formal and informal inputs are solicited from the PO representatives by FLETC staff and used to validate the survey results. No known integrity problems exist. |

| | |
|---|---|
| Performance Measure | Percent of Partner Organizations (POs) that respond "agree" or "strongly agree" that FLETC training programs address the right skills needed for their officers/agents to perform their law enforcement duties. |
| Program and Organization | Law Enforcement Training - Federal Law Enforcement Training Center |
| Description | This performance measure reflects the percent of POs that responded on the Partner Organization Satisfaction Survey (POSS) agree or strongly agree that FLETC training programs address the right skills needed for their officers/agents to perform their law enforcement duties to prevent 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 | This measure focuses on whether or not FLETC training addresses the right skills needed for officers/agents to perform law enforcement duties. Once a student finishes training, surveys are completed by agency leaders, as applicable, from each of FLETC’s 83 Partner Organizations (PO). |
| Data Source | The source of the data is from the FLETC Partner Organization Satisfaction Survey (POSS) administered via a web-based survey program (Perseus) which tabulates and calculates the survey results. The measure uses the average of two questions: The FLETC's basic training programs address the right skills needed for my officers/agents to perform their law enforcement duties and the FLETC's advanced training programs address the right skills needed for my officers/agents |

| | |
|---|---|
| | to perform their law enforcement duties. |
| Collection Method | The FLETC Partner Organizations (POs) are surveyed using the Partner Organization Satisfaction Survey (POSS) which is accessed via the Perseus web based program. The measure uses the questions: The FLETC's basic training programs address the right skills needed for my officers/agents to perform their law enforcement duties and the FLETC's advanced training programs address the right skills needed for my officers/agents to perform their law enforcement duties. The survey uses a modified six-point Likert scale (Strongly Agree, Agree, Slightly Agree, Slightly Disagree, Disagree, and Strongly Disagree). Data is entered through this system and stored at the end of each completed survey. Strategic Planning and Analysis Division personnel access the data via the web site, import the data into the Statistical Package for the Social Sciences (SPSS) to generate descriptive statistics, and then into MS Excel to generate data charts and tables. |
| Reliability | Reliable |
| How Data is Verified | The survey was developed using contemporary survey methods comparable to those used by the military services and other major training organizations. 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. |

| | |
|---|---|
| Performance Measure | Percent of students that express "excellent" or "outstanding" on the Student Feedback - Program Survey. |
| Program and Organization | Law Enforcement Training - Federal Law Enforcement Training Center |
| Description | This performance measure reflects the percent of Federal Law Enforcement Training Center (FLETC) students who, on the student feedback survey, indicate the degree of training quality received was excellent or outstanding. Results from the survey are used to improve training to ensure students receive the right skills and knowledge, presented in the right way and at the right time to prevent terrorism and other criminal activity against the U.S. and our citizens. |
| Scope | The Student Feedback Program Survey is distributed by FLETC staff to all students at the conclusion of their training program. The percent is calculated as the number of students that rate their overall training experience as "excellent" or "outstanding" divided by the total number of students responding. |
| Data Source | The data for this measure is collected from the Student Feedback Program Survey Question 19, “Overall, I believe the quality of the training presented in this program has been: Outstanding, Excellent, Good, Satisfactory, and Poor.” The Student Information System (SIS) data base, maintained by the FLETC Chief Information Officer Directorate (CIO), is a compilation of results from the Student Feedback Program surveys. |
| Collection Method | From the Student Feedback Program Survey, using a modified 5-point Likert scale, students respond to question 19 listed above. Completed surveys are collected at the conclusion of each program and scanned into the Student Information System (SIS) by the Educational Aides, contracted to the FLETC Services Division. The percent reported in this measure is determined by dividing the number of students that rate the program as excellent or outstanding by the total number of students responding. |
| Reliability | Reliable |
| How Data is Verified | Quarterly quality checks are conducted by Evaluation and Analysis Division (EAD) personnel to ensure the data is reliable and valid. The data is scrubbed consistent with acceptable survey practices, for example, to verify that all surveys were scanned, to eliminate any duplication and to confirm accuracy of class identification. No known integrity problems exist. |

# Inspector General

| | |
|---|---|
| Performance Measure | Percent of recommendations made by the Office of Inspector General (OIG) that are accepted by the Department of Homeland Security. |
| Program and Organization | Audit, Inspections, and Investigations Program - Inspector General |
| Description | The Office of Inspector General (OIG) audits programs for fraud, waste, and abuse. OIG also reviews programs to promote economy, efficiency, and effectiveness. The criteria used to select programs for audit include: statutory and regulatory requirements; adequacy of internal control systems; newness; changed conditions; potential dollar magnitude; etc. Where appropriate, OIG audit and inspection reports include recommendations which, if accepted and implemented, will improve the respective program. The OIG tracks the recommendations that are issued until they have been implemented. |
| Scope | This measure encompasses all DHS programs and operations that are selected by the OIG for an audit, inspection, or evaluation based on how vulnerable the operation is to fraud, waste, abuse and mismanagement, or if there is a legislative or regulatory audit requirement. |
| Data Source | The source of data is an electronic database maintained by OIG which records all recommendations and whether they have been accepted, implemented, or declined. |
| Collection Method | OIG collects information on and tracks all the formal recommendations made to the Department and whether or not the recommendations have been accepted and implemented in its database. The Department provides requested information in response to formal communication from OIG headquarters regarding recommendations, acceptance and implementation. These responses are recorded and compiled in the OIG database. In tracking this information, OIG auditors, inspectors and investigators will employ the use of Microsoft office products, Visio, IDEA, Teammate and other software applications to collect and report their findings. |
| Reliability | Reliable |
| How Data is Verified | Auditors and inspectors apply GAO’s risk-based framework for data reliability assessments (which includes tests on sufficiency, competency and relevancy) to determine whether the Government Auditing Standards for evidence are met. The PCIE (what does this stand for) sets quality standards for investigations and maintaining the resulting data, which are validated through (what kind/done by whom) investigative process. |

## Management Directorate

| | |
|---|---|
| Performance Measure | Number of internal control processes tested for design and operational effectiveness. (New performance plan measure for FY 2008.) |
| Program and Organization | Departmental Management and Operations - Management Directorate |
| Description | The measure indicates the number of tests completed to gauge the effectiveness of our financial management processes, in order to ensure internal controls prevent waste, fraud, and abuse. |
| Scope | The Department has 13 financial management processes that are tested for this measure. Examples of these processes include Financial Reporting, Fund Balances with Treasury, Property Management, etc. All major Components of DHS are subject to annual testing of these processes. |
| Data Source | Data is compiled by the components and reviewed by Internal Control Program Management Office (IC PMO) for use in supporting the Secretary's Assurance Statement. The IC PMO maintains an access data base which compiles component results for analysis by the Department. |
| Collection Method | Each DHS Component Head submits an assurance package to the IC PMO. The IC PMO reviews the assurance statement package to assess compliance with OMB A-123. At the conclusion of the review, the IC PMO prepares a summary report of information submitted to the databases for use in preparation of the Secretary's Assurance Statement. This statement is published in our Annual Financial Report. |
| Reliability | Reliable |
| How Data is Verified | Conclusions reached by the IC PMO are reviewed by the DHS Senior Management Council and a final recommendation is made to the Secretary for final review. |

| | |
|---|---|
| Performance Measure | Number of President's Management Agenda (PMA) initiatives whose score improved over the prior year or were rated green in either status or progress. (Retired plan measure.) |
| Program and Organization | Departmental Management and Operations - Management Directorate |
| Description | The PMA is the Administration's initiative to increase the efficiency and effectiveness of Federal Government management. This measure assesses standards and evaluation criteria in the following areas: 1) Human Capital; 2) Competitive Sourcing/Procurement; 3) Improved Financial Performance; 4) Expanded Electronic Government; and 5) Performance Improvement. On a quarterly basis, each Federal agency is rated by the Office of Management (OMB) and Budget as red, yellow, or green on their current status in meeting standards, and progress in meeting or maintaining standards for each area. |
| Scope | This measures the Department's performance as an agency in each of the five PMA initiatives. |
| Data Source | The source of information is quarterly reports issued by OMB, scoring DHS in each of the five initiative areas. |
| Collection Method | OMB reports to DHS on its overall performance in each initiative area in both status and progress. This report is used to determine the number of areas increasing status year to year and the number of PMA areas with a green progress score. The Office of Program Analysis & Evaluation (PA&E) creates a report summing the number of PMA initiatives whose score improved over the prior year or were rated green in either status or progress, to determine these results. |
| Reliability | Reliable |
| How Data is Verified | OMB develops the base report and conducts internal reviews to ensure accurate reflection of the current status. The DHS Office of Program Analysis and Evaluation makes and double checks the final calculation. |

| | |
|---|---|
| Performance Measure | Percent improvement in favorable responses by DHS employees agency-wide (strongly agree/agree) on the section of the Federal Human Capital Survey that addresses employee sense of accomplishment. (Retired plan measure.) |
| Program and Organization | Departmental Management and Operations - Management Directorate |
| Description | Every two years the U.S. Office of Personnel Management conducts a survey to gauge employee perceptions on whether they are effectively led and managed, if they have opportunities to grow professionally and advance in their careers, and if their contributions are truly valued and recognized. This measure reflects the survey findings regarding DHS employee perceptions on the quality of their work environment. |
| Scope | This measure reflects the survey findings regarding DHS employee perceptions on the quality of their work environment by assessing the number survey respondents who are DHS employees and who either agree or strongly agree with the following statement: "My work gives me a feeling of personal accomplishment." |
| Data Source | The source of information is the most recent Federal Human Capital Survey, which the Office of Personnel Management conducts every two years. Every other year, the Department conducts an internal human capital survey, intended to supplement the OPM survey and address issues specific to DHS. |
| Collection Method | The Office of Personnel Management publishes the results of its survey in January of the following year. This measure specifically examines the results of DHS employee assessments of the following statement, as it pertains to their individual situation: "My work gives me a feeling of personal accomplishment.” |
| Reliability | Reliable |
| How Data is Verified | The Office of Personnel Management conducts, analyzes, and publishes the data obtained from the Federal Human Capital Survey. |

| | |
|---|---|
| Performance Measure | Percent of DHS strategic objectives with programs that meet their associated performance targets. (Retired plan measure.) |
| Program and Organization | Departmental Management and Operations - Management Directorate |
| Description | This measure is defined as the total number of DHS strategic objectives with programs that meet their associated performance targets. Performance data is tabulated against the strategic objectives of the DHS Strategic Plan. Each program is linked to the DHS strategic goals and objectives and has specific performance measures. DHS demonstrates the value and outcomes of its services through the results of program performance measures. The performance outcomes of DHS programs essentially tell how the Department is impacting citizens, stakeholders, and customers and meeting its mission. |
| Scope | This measure includes all measures published in the current years Annual Performance Report relating to each of the programs within the Department. |
| Data Source | The Department's Future Year Homeland Security Program System (FYHSP) captures all data. The source of information is are reports from the FYHSP system, which Program Managers update quarterly. These reports detail whether or not programs have met their performance targets. |
| Collection Method | DHS Components report quarterly on performance targets and update the FYHSP system with actual results. All data is due in the system no later than thirty days after the end of the quarter. The Office of Program Analysis and Evaluation (PA&E) produces reports from the FYHSP system to calculate the result. |
| Reliability | Reliable |
| How Data is Verified | Annual performance data for each program are validated through the Component's Planning offices, vetted through their leadership, and supported by the PA&E. Many of the measures are validated through the Office of Management and Budget (OMB) Program Assessment Rating Tool (PART) process. |

| | |
|---|---|
| Performance Measure | Percent of favorable responses by DHS employees on the Federal Human Capital Survey. (New performance plan measure for FY 2008.) |
| Program and Organization | Departmental Management and Operations - Management Directorate |

| | |
|---|---|
| Description | Every two years, the U.S. Office of Personnel Management (OPM) conducts a survey to gauge employees' perceptions on whether they are effectively led and managed, if they have opportunities to grow professionally and advance in their careers, and if their contributions are truly valued and recognized. This measure reflects the responses of DHS employees on the 39 questions that the OPM has determined make up the four Human Capital Assessment and Accountability Framework (HCAAF) Indices: Leadership and Knowledge Management; Results-Oriented Performance Culture; Talent Management; and Job Satisfaction. OPM created the HCAAF to guide agencies in addressing human capital management issues and to measure their performance in these areas. |
| Scope | The measure includes the responses of all DHS employees who participate in the Federal Human Capital Survey to the 39 questions (out of approximately 84) that make up the Human Capital Assessment and Accountability Framework Indices. |
| Data Source | The source of information is the most recent Federal Human Capital Survey, which the Office of Personnel Management (OPM) distributes every two years to full-time permanent federal employees. The survey is available online. |
| Collection Method | The Office of Personnel Management (OPM) publishes the results of its survey in January following the year it is distributed. OPM targets 39 specific questions as relevant to the Human Capital Assessment and Accountability Framework Indices, which OPM created to provide standards of success for agencies to measure their progress and achievements in managing their workforces. OPM calculates the indices by tracking the percent of positive responses by DHS employees and publishes them as part of the survey results. The measure is then calculated by averaging the four indices. |
| Reliability | Reliable |
| How Data is Verified | The Office of Personnel Management conducts, analyzes, and publishes the data obtained from the Federal Human Capital Survey. Personnel within the Office of Program Analysis and Evaluation calculate the average of the four indices and the Office of Human Capital validates it. |

| | |
|---|---|
| Performance Measure | Percent of President's Management Agenda initiatives that receive a green progress score from the Office of Management and Budget. (New performance plan measure for FY 2008.) |
| Program and Organization | Departmental Management and Operations - Management Directorate |
| Description | The Management Directorate oversees the progress of the Department of Homeland Security on achieving improvements in the President’s Management Agenda (PMA) across all initiative areas. The initiative areas are assessed quarterly by the Office of Management and Budget (OMB) and assigned a progress score of red, yellow, or green. The performance measure is calculated by taking the total number of green progress scores divided by the total number of progress scores across four quarters. |
| Scope | This measures the Department's performance as an agency in each of the eight PMA initiatives: 1) Human Capital; 2) Competitive Sourcing/Procurement;<br>3) Improved Financial Performance; 4) Expanded Electronic Government;<br>5) Performance Improvement; 6) Faith Based and Community Initiatives; 7) Real Property; and 8) Eliminating Improper Payments. OMB rates the Department quarterly against specified criteria, as red, yellow, or green in both status and progress. This measure will focus on the progress score. The measure will report as of fiscal year end standings, and after every quarter. |
| Data Source | The progress scores are provided to the Department of Homeland Security by OMB within the first month of the following quarter of the period of performance. The scores are also posted by OMB at www.results.gov. |
| Collection Method | The data for this measure looks at the proposed milestones that were met for each quarter as judged by examiners at OMB and approved by the Deputy Director for Management. The percent of green scores will be manually tabulated using Microsoft Excel. The data is provided by OMB and will be used to calculate progress against the measure by the front office of the Under Secretary for |

| | |
|---|---|
| | Management. |
| Reliability | Reliable |
| How Data is Verified | OMB develops the base report and conducts internal reviews to ensure accurate reflection of the current status. The DHS Office of Program Analysis and Evaluation makes and double checks the final calculations. |

| | |
|---|---|
| Performance Measure | Total instances of material weakness conditions identified by the independent auditor in their report on the DHS financial statements. |
| Program and Organization | Departmental Management and Operations - Management Directorate |
| Description | The number reported is the total instances of material weakness conditions in both the DHS Office of Financial Management and DHS components. A material weakness is a deficiency significant enough to be reported outside the agency. |
| Scope | The scope of material weakness identification through an annual independent audit includes the financial statement, balance sheet, custodial activity, and consideration of internal controls over financial reporting, certain supplemental information, performance measures, and compliance with certain provisions of applicable laws, regulations, contracts and grant agreements that could have a direct and material effect on the financial statement. Material weaknesses reported through the independent audit against the DHS Office of Financial Management and the DHS components are included in this measure. |
| Data Source | The source of data is the signed independent auditor's report on the status and instances of material weakness throughout the Department. |
| Collection Method | The Office of the Program Analysis and Evaluation will review the auditors' findings and will derive the total instances of material weakness conditions. |
| Reliability | Reliable |
| How Data is Verified | The Office of Financial Management verifies the review and determination of results. |

| | |
|---|---|
| Performance Measure | Percent of major IT projects that are within 10% of cost/schedule/performance objectives. |
| Program and Organization | Office of the Chief Information Officer - Management Directorate |
| Description | This measure gauges the percent of major IT investments that are on schedule, on cost, and delivering their planned performance. These indicators are the industry accepted critical factors for assessing project management effectiveness, and ultimately the success of IT investments. |
| Scope | All major investments (Levels 1, 2, and 3 Information Technology) that are in development milestone decision phases (Capability Development and Demonstration, Production and Deployment) must submit Earned Value Management (EVM) data indicating investment program variances. |
| Data Source | Components provide data on IT Investments via the Periodic Reporting Excel template or through the Periodic Reporting System (PRS), a system that enables users to submit Periodic Reports for their investments. |
| Collection Method | DHS requests quarterly data from Component Periodic Reporting Points of Contact, who distribute the data call to relevant Program Managers. Data are entered into the Periodic Reports, vetted, and approved by Components, and then submitted to DHS. The DHS Chief Information Office reconciles the data submitted against headquarters records, analyzes the data, and produces a variety of reports for both internal and external customers. |
| Reliability | Reliable |
| How Data is Verified | Per regulations, components review the data reported to DHS for accuracy and reliability prior to submittal. Future EVM data reported on appropriate contracts will need to meet the DHS requirements for compliance and surveillance reviews against the American National Standards Institute/Electronic Industries Alliance (ANSI/EIA) standard. |

## National Protection and Programs Directorate

| | |
|---|---|
| Performance Measure | Government Emergency Telecommunications Service (GETS) call completion rate during periods of network congestion. (Retired plan measure.) |
| Program and Organization | Cyber Security and Communications - National Protection and Programs Directorate |
| Description | This measure gauges the probability a National Security or Emergency Preparedness (NS/EP) user will be able to use the public telephone network, landline or wireless, to communicate with the intended user/location/system/etc. during emergency events. Call completion is the measure through which end-to-end communication is measured. "Priority Services" currently consists of GETS, and Wireless Priority Service (WPS) components, and will eventually include a Next Generation Network (NGN) component. |
| Scope | NS/EP call completion rate represents expected probability an NS/EP user completes the call under all-hazard scenarios. The range is 0 to 100 percent representing no call completed to all calls completed respectively. Data is captured during the reporting period when the Public Switched Network experiences major congestion. Such congestion is typically due to the occurrence of a natural or manmade disaster such as a hurricane, earthquake, or terrorist event. |
| Data Source | Reports from Priority Service InterExchange Carriers and integrated by Priority service program office. |
| Collection Method | The information is collected within priority service IXC information systems and provided to NS/EP communications government employees. |
| Reliability | Reliable |
| How Data is Verified | 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; for WPS more recently. All data collected is in accordance with best industry practices and is compared with previous collected data as a validity check |

| | |
|---|---|
| Performance Measure | Percent of planned Einstein sensors deployed on-time annually throughout the Federal government. (New performance plan measure for FY 2008.) |
| Program and Organization | Cyber Security and Communications - National Protection and Programs Directorate |
| Description | This measure assesses the percent of planned Einstein sensor deployments that are completed on time. With the full implementation of these sensors, visibility into the potentially malicious cyber activity and throughout the Federal cyberspace will dramatically increase. The sensors will provide more comprehensive situational awareness information to better understand the current environment and identify vulnerabilities, risks, and mitigation actions. |
| Scope | The data includes the actual number of Einstein sensors installed and the planned number of Einstein sensor installations per year. The planned number of sensors is derived from the program's Einstein implementation plan, and the target values are based upon this plan. The plan assumes the federal civilian government network as of FY 2007 and this is used as the baseline for this measure. Limitations of the measure include, (1) Einstein is a voluntary program with no requirements for agencies to participate, (2) participation in Einstein and subsequent sensor deployment requires a somewhat lengthy process which includes a Memorandums of Understanding (MOU) signed by both parties, and (3) as the total number of installations increases, staff are increasingly focused on supporting existing sensor and customers, and expansion is dependant on the provision of required resources. |
| Data Source | The number of Einstein sensor installations is provided by the United States Computer Emergency Readiness Team (US-CERT). The number of sensors installed is determined through the existing MOUs and US-CERT installation |

| | |
|---|---|
| | logs. These logs are maintained by US-CERT in a database/system. The number of planned sensors is determined using the Einstein implementation plan/schedule, as defined in FY 2007. |
| Collection Method | Einstein installation logs are used to determine the number of sensors installed in each given fiscal year. The number of installations is compared to the planned installations and a ratio of actual to planned installations is derived. This is a cumulative measure. Achieving the aggressive targets is dependant on sufficient resource allocation and the ability of the program to arrange and codify agreements with Federal Agencies to install the sensors. |
| Reliability | Reliable |
| How Data is Verified | The number of Einstein installations is logged by the US-CERT program team. The information will be validated to be reliable across several US-CERT Program Managers' reviews. |

| | |
|---|---|
| Performance Measure | Percent of States and Urban Areas whose current interoperable communications abilities have been fully assessed. (New performance plan measure for FY 2008.) |
| Program and Organization | Cyber Security and Communications - National Protection and Programs Directorate |
| Description | This performance measure is based on the percent of States and Urban Areas that be have been fully assessed and approve of the national baseline capability "gaps" and/or the future emergency communications requirements. The National Communications Baseline Assessment capability assessment framework presents the broad range of capabilities needed by emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters |
| Scope | States and Urban Areas (131 total) that have been assessed in the NCBA. |
| Data Source | The Office of Emergency Communication's (OEC) Office of the Director and Multi-Jurisdictional Communications Services Division will collect the data from Government and contractor personnel providing assistance to states and urban areas and maintain it in a database/excel spreadsheet. Detailed reports will also be generated for each State/urban area. |
| Collection Method | Reporting mechanism for Areas to approve 'gaps' and 'requirements' will be developed in FY 2008. |
| Reliability | Reliable |
| How Data is Verified | All data is gathered by Program Managers and verified by OEC leadership. |

| | |
|---|---|
| Performance Measure | Percent of targeted stakeholders who have implemented the Control Systems Security Self Assessment Tool (CS2SAT) to conduct vulnerability assessments. (New performance plan measure for FY 2008.) |
| Program and Organization | Cyber Security and Communications - National Protection and Programs Directorate |
| Description | This measure evaluates the use of the CS2SAT tool to help asset owner and operators conduct assessments to identify and mitigate vulnerabilities in their control systems. This measure will require the program to track the distribution of the CS2SAT tool to the owner/operator level. Information regarding the implementation of this tool will be collected across control system owners/operators at the annual Process Control Systems Forum and the International Instrumentation Symposium. This measure will be computed as follows: number of targeted stakeholders that have implemented the CS2SAT divided by the total number of targeted stakeholders |
| Scope | The program is targeting private sector users such as asset owners and operators, and federally managed energy agencies/departments determined based on estimated risk level of the stakeholder, stakeholder receptivity to the product, and level of impact the tool may have on stakeholder protection and prevention needs. Public sector targeted facilities include the various facilities managed by the Bureau of Reclamation, Army Corps of Engineers, Tennessee Valley Authority, and Bonneville Power Administration. Private sector customers will be |

| | |
|---|---|
| | incorporated into the measure as distribution to these markets mature. The tool is marketed sector through a third-party private sector vendor based on a combination of the estimated level of impact of the tool for the stakeholder and the estimated level of risk for the stakeholder's sector. Federal government users may obtain the tool free of charge from the CSSP program office. |
| Data Source | The data will be collected by the Control Systems Security Program (CSSP). Data regarding the implementation of this tool will be collected across control system owners/operators at the annual Process Control Systems Forum and the International Instrumentation Symposium. The CSSP records and maintains this data in a spreadsheet. The data is based on feedback from all CS2SAT targeted users |
| Collection Method | Standard feedback evaluation criteria will be defined and implemented by the CSSP to obtain information from CS2SAT users. Relevant data will be collected, tracked and compiled using a standard spreadsheet for data collection. It will then be aggregated and summarized for reporting. This measure will be computed as follows: number of targeted stakeholders that have implemented the CS2SAT divided by the total number of targeted stakeholders. |
| Reliability | Reliable |
| How Data is Verified | The number of CS2SAT stakeholders is maintained by CSSP. The percent use will be self-reported to CSSP by identified stakeholders. The information is validated to be reliable across several CSSP Program Managers' reviews. |

| | |
|---|---|
| Performance Measure | Percent of targeted stakeholders who participate in or obtain cyber security products and services. (Retired plan measure.) |
| Program and Organization | Cyber Security and Communications - National Protection and Programs Directorate |
| Description | This measure assesses the impact of National Cyber Security Division (NCSD) activities targeting multiple stakeholders and NCSD's success in building effective partnerships with its stakeholders. As NCSD is able to reach a greater number of organizations and individuals, their awareness of the need to and the means of protecting cyber space increases and they act to implement NCSD recommendations to improve cyber space. |
| Scope | This measure counts the overall number of cyber security products and services NCSD produces and delivers, for the purpose of reducing vulnerabilities and minimizing the severity of cyber attacks. The stakeholders who receive these products and services include Federal agencies; state, local and tribal governments; non-governmental organizations such as industry and academia; and individual users. |
| Data Source | Data are obtained by all of the National Cyber Security Division (NCSD) branches in order to make up a single sample size. The data to be used in the sample size include: number of active users/subscribers to alerts/bulletins/web pages, number of other agency participants in NCSD-held/delivered/chaired interagency or working groups/conferences/workshops/ training/speeches/briefings; number of requests for and/or downloads of the developed and delivered methodologies/guidance/frameworks and major reports/plans. |
| Collection Method | The data/information will be collected internally within NCSD from each branch using a standardized Excel data collection spreadsheet. It will then be aggregated into a summary sheet for reporting. |
| Reliability | Reliable |
| How Data is Verified | Each National Cyber Security Division (NCSD) branch is responsible for capturing required data at the time of each event (if appropriate) or obtains it from web sites, repositories, system logs, and other sources. Each branch is also responsible for working with outside stakeholders to obtain required data, if necessary. The data is reviewed by branch management to validate its accuracy. |

| | |
|---|---|
| Performance Measure | Priority services call completion rate during emergency communications periods. (New performance plan measure for FY 2008.) |
| Program and Organization | Cyber Security and Communications - National Protection and Programs Directorate |
| Description | National Security/Emergency Preparedness (NS/EP) call completion rate is the probability an NS/EP user will be able to use the public telephone network, landline or wireless, to communicate with the intended user/location/system/etc. during emergency events. Call completion is the measure through which end-to-end communication is measured. "Priority Services" currently consists of Government Emergency Telecommunications (GETS) and Wireless Priority Service (WPS) components, and will eventually include a Next Generation Network (NGN) component. |
| Scope | NS/EP call completion rate represents expected probability an NS/EP user completes the call under all-hazard scenarios. The range is 0 to 100 percent representing no call completed to all calls completed respectively. Data is captured during the reporting period when the Public Switched Network experiences major congestion. Such congestion is typically due to the occurrence of a natural or man-made disaster such as a hurricane, earthquake, or terrorist event. |
| Data Source | Reports from GETS InterExchange Carriers and the WPS service providers and integrated by the GETS/WPS program management office. |
| Collection Method | The information is collected within the priority service IXC and WPS information systems and provided to NS/EP communications government FTEs and integrated by the GETS/WPS program management office. |
| Reliability | Reliable |
| How Data is Verified | 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; for WPS more recently. 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 Critical Infrastructure and Key Resource (CIKR) sector specific planning protection implementation actions on track. (New performance plan measure for FY 2008.) |
| Program and Organization | Infrastructure Protection - National Protection and Programs Directorate |
| Description | The National Infrastructure Protection Plan (NIPP) defines a set of 23 core metrics applied across the 17 CIKR sectors, for a total of 391 total metrics. These metrics track the success of actions taken to further protection and partnership building activities are being conducted within each sector. Specifically the metrics track the implementation of planned sector accomplishments in Sector Partnerships, Information Sharing, Security Goals, Asset Identification, Risk Assessments, Prioritization, Implement Protective Programs, and Effectiveness. Subject matter experts score each sector's responses to the 23 metrics; the program then employs an algorithm to determine overall scores and success for each metric. An action is initiated upon the allocation of resources toward that action or through an agreement, e.g. Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), etc. This measure evaluates annually the percent of the 391 total protection action metrics that were scored as being on track. |
| Scope | This measure includes 391 core sector metrics developed for and required by the NIPP Risk Management Framework. The content of metrics stem from two key sources: (a) Sector Governance/Coordination measures demonstrate progress of the evolving collaboration among Sector Specific Agencies (SSAs), Government Coordinating Councils (GCCs), and Sector Coordinating Councils (SCCs), as well as the progress made in developing and using appropriate information - sharing and analysis mechanisms within the sector; (b) NIPP Risk Management Framework measures demonstrate progress at each step of the NIPP Risk Management Framework. These metrics include (1) metrics from the 17 CIKR |

| | |
|---|---|
| | sector specific plans and (2) activities and initiatives from the National Annual CIKR Security Report, the Sector Annual CIKR Security Reports, and the 17 Government Coordinating Councils. |
| Data Source | Sector Specific Agencies provide the program responses to questions relating the 23 NIPP Risk Management Framework at meetings of the Government and Sector Coordinating Councils, technical sessions with sectors reps, and National and Sector Annual CIKR Protection reporting processes. Once the data is collected it is stored in a database located at program headquarters. |
| Collection Method | This measure represents responses to a set of 23 core metrics by each of the 17 CIKR sectors, or 391 total individual metrics. Each metric reflects an action or milestone for the sector. The program collects data on a quarterly basis. Each Sector Specific Agency responds to its 23 metric questions for its sector. Responses are scored by a panel of sector subject matter experts; the panel ensures that metrics can be compared across sectors. Scores are fed into a complex algorithm that produces an overall scoring for each metric and sector (some metrics are weighed more heavily than others in the algorithm). An algorithm is used to score determine if action target has been met (i.e., whether the action has met the target criteria, at a minimum initiated). An action is initiated upon the allocation of resources toward that action or through an agreement, (e.g., an MOU, MOA, etc.). This measure evaluates annually the percent of the protection action metrics scored as being on track. |
| Reliability | Reliable |
| How Data is Verified | The measures used to develop this overarching measure include descriptive, process, output, and outcome metrics that help measure progress in the implementation of the 17 sectors' SSPs. The measures developed in the 17 Sector Specific Plans (SSPs) are derived by both the Federal Sector Specific Agencies responsible for their respective sectors as well as by the official coordinating bodies (the GCCs and SCCs) and the private sector owners and operators. These measures are reviewed by program staff at the headquarters level who verify and validate the information. |

| | |
|---|---|
| Performance Measure | Percent of high priority Critical Infrastructure and Key Resources (CIKR) where a vulnerability assessment has been conducted and enhancement(s) have been implemented. (New performance plan measure for FY 2008.) |
| Program and Organization | Infrastructure Protection - National Protection and Programs Directorate |
| Description | This measure tracks the number of the Nation's high priority CIKR sites at which at least one vulnerability assessments (VA) has been conducted and a protective enhancement has been implemented. High-priority CIKR include assets categorized in Tier 1 (assets deemed to be at highest risk) and other CIKR assets Infrastructure Protection (IP) plans to assess in the fiscal year. Vulnerability assessments are conducted to identify physical, cyber, and human-related vulnerabilities at an asset and dependencies/interdependencies on other assets and sectors. During vulnerability assessments the program's assessors identify suitable protective measures and enhancements needed to reduce or mitigate vulnerability of the asset and identify what enhancements have been implemented at the site (such as bollards, razor wire, closed-circuit television cameras, etc.). The assessments are also used to assist federal stakeholders and private sector owners in making optimal resource allocation decisions for future enhancements. |
| Scope | The scope of this measure is all vulnerability assessments (VA) which have been conducted in the past year on Tier 1 assets and other CIKR assets planned in the fiscal year. |
| Data Source | The program (Office of Infrastructure Protection (OIP)) collects data on assessments conducted through the program as well assessments conducted by other Federal, State, local, and private sector security partners. Data on non-DHS/IP conducted assessments will be collected by DHS/IP Sector Specialists and provided to OIP's Protective Security Compliance Division. Data is maintained in a database housed in a U.S. national laboratory facility. |

| | |
|---|---|
| Collection Method | The program determines the appropriate type of assessment and methodology to be used. Using common threat scenarios, the assessment identifies physical, cyber, and human-element related vulnerabilities and dependencies with other assets. The assessment analyzes the benefits of existing protective programs and provides recommendations to remediate unresolved vulnerabilities. A program is determined to have had a VA conducted if a comprehensive review, Buffer Zone Protection Plan (BZPP), or a self-assessment has been conducted. After the assessments are completed, the protective security advisor follows up with an owner/operator of the facility to determine whether the facility has incorporated a recommended enhancement. The Protective Security Advisor (PSA) determines through this follow-up whether the site has implemented a security enhancement. |
| Reliability | Reliable |
| How Data is Verified | Data is verified by the Protective Security Advisors who interface with CIKR owners and operators and verify that VAs have been conducted. Advisors also confirm that reported enhancements have been implemented and all data is reviewed and approved by supervisors to ensure data integrity. |

| | |
|---|---|
| Performance Measure | Percent of high-priority critical infrastructure for which a Buffer Zone Protection Plan (BZPP) has been implemented. (Retired plan measure.) |
| Program and Organization | Infrastructure Protection - National Protection and Programs Directorate |
| Description | This measure reports the percent of the Nation's high priority critical infrastructure for which a Buffer Zone Protection Plan (BZPP) has been implemented to reduce specific vulnerabilities by developing protective measures that extend from the critical infrastructure site to the surrounding community to deter terrorist activities. |
| Scope | This measure includes the percent of BZPPs implemented for all CIKR assets for which development of a BZPP is deemed appropriate. The total number of assets on the BZPP list will vary from year to year and may change during the fiscal year in response to a criteria change, such as a budget reallocation, threat information, and agency focus. The total number of assets on the list forms the baseline for this performance measure |
| Data Source | The source of this data is the BZPP Progress Report which is maintained by the Risk Management Division (RMD) Field Operations Branch and is updated weekly. |
| Collection Method | Data is collected from written reports that are received from State and local government agencies, assessments made during on - site visits and data collected from the Federal Emergency Management Agency's Office of Grants and Training. Data is maintained in a database housed in a U.S. national laboratory facility. |
| Reliability | Reliable |
| How Data is Verified | The verification process is done by the RMD Field Operations Branch Manager who reviews the collected data for accuracy |

| | |
|---|---|
| Performance Measure | Percent of high-priority critical infrastructure/key resources (CIKR) sites at which a vulnerability assessment (VA) has been conducted. (Retired plan measure.) |
| Program and Organization | Infrastructure Protection - National Protection and Programs Directorate |
| Description | Percent of the Nation's high priority critical infrastructure of key resource sites for which assessments of vulnerability have been conducted in order to identify suitable protective measures needed to reduce vulnerability from acts of terrorism, and make corresponding resource allocation decisions. |
| Scope | The scope of this measure is all high-priority critical infrastructure/key resources (CIKR) sites and all associated vulnerability assessments which have been conducted in the past 2 years. |
| Data Source | Data is obtained from vulnerability assessments and self vulnerability assessments and is provided to the Risk Management Division (RMD) by the Assessment teams or the owner/operators in the case of self assessments. Data is maintained in a database housed in a U.S. national laboratory facility. |

| | |
|---|---|
| Collection Method | The method of collection for VAs conducted is from multiple sources - DHS/Infrastructure Protection, other DHS components such as Transportation Security Administration, U.S. Coast Guard, etc.; Federal partners Sector Specific Assessments (SSAs) which are verified through the National Infrastructure Protection Plan (NIPP) process; visits and validation of State/Local and Owner/Operator assessments by our Protective Security Advisors (PSAs) that are stationed in 60 cities around the country where our high priority CIKR reside. Reports are generated to determine the percent of assessments conducted. |
| Reliability | Reliable |
| How Data is Verified | Data is verified by the Protective Security Advisors who interface with CIKR owners and operators and verify that VAs have been conducted. |

| | |
|---|---|
| Performance Measure | Percent of identified high-priority critical infrastructure/key resources sites at which at least two suitable protective actions (PA) have been implemented. (Retired plan measure.) |
| Program and Organization | Infrastructure Protection - National Protection and Programs Directorate |
| Description | Percent of the Nation's critical infrastructure or resource sites, which have been designated high risk and highly valued, for which a minimum of two protective actions that are designed to reduce vulnerability from acts of terrorism have been implemented. |
| Scope | The scope of this measure is all high-priority critical infrastructure/key resources (CIKR) sites and all associated protective actions (PA) implemented during a three year period. |
| Data Source | A computer - based tracking log is maintained by the Risk Management Division which tracks PA implementation information for designated high priority CIKR sites |
| Collection Method | The Risk Management Division conducted site security visits and information obtained by the Protective Security Advisors (PSAs) in addition to data calls to the Sector Specific Agencies (SSAs) as the SSAs mature are used to track the receipt of PA implementation information for the designated high-priority CIKR sites. |
| Reliability | Reliable |
| How Data is Verified | PSAs compare CIKR PA implementation information against site security visit information obtained by the Risk Management Division to verify information. |

| | |
|---|---|
| Performance Measure | Percent of inspected high-risk chemical facilities in compliance with risked based performance standards. (New performance plan measure for FY 2008.) |
| Program and Organization | Infrastructure Protection - National Protection and Programs Directorate |
| Description | The program conducts onsite inspections to provide regulatory oversight of the Nation's high-risk chemical facilities and verify compliance with the Chemical Facility Anti-terrorism Standards (CFATS). Inspections are conducted in intervals commensurate with the defined risk tiering of each facility. Compliance means that chemical facilities have been inspected to validate the facility's Site Security Plan (SSP) and that the SSP is in accordance with the Risk-Based Performance Standards set forth by DHS, or that the facility is seeking/will seek remedies to identified security gaps. |
| Scope | This measure accounts for the highest risk chemical facilities based on calculations of overall threat, consequence, and vulnerability. The facilities are separated into 4 tiers based on risk criteria such as proximity to population centers, transportation networks (highways, etc.), commercial natural resources; population density; type of chemicals produced/stored, etc. Criteria are analyzed for each site and "scored" based on risk analysis algorithms. Tier 1 are highest risk facilities. As the regulation has only recently been initiated, inspections will encompass the highest risk facilities first and then expand to other Tier levels in later fiscal years. It is estimated that many of the high risk facilities are already in compliance with the CFATS standards so initial percentages are high, but that with the inclusion of lower Tier facilities compliance percentages may fluctuate |

| | |
|---|---|
| | and then increase in later years. |
| Data Source | Site compliance information is gathered by the program's cadre of Chemical Site inspectors. Data is stored in the Chemical Security Assessment Tool (CSAT) to identify facilities that meet the Departments criteria for high risk chemical facilities as well as the methodology to conduct security vulnerability assessment (SVAs) and to develop site security plan (SSPs). CSAT is a secure web-based system that includes a suite of four tools: (1) facility registration; (2) a Top - Screen questionnaire; (3) a SVA tool; and (4) a SSP template. |
| Collection Method | Percent of chemical sites inspected each year that have completed an SVA and developed an SSP with sufficient allocated resources to meet the CFATS standards. Information from the inspections, including facility compliance information, is transferred into CSAT. |
| Reliability | Reliable |
| How Data is Verified | Information is reviewed by IRCD, OIP, and NPPD management |

| | |
|---|---|
| Performance Measure | Average biometric watch list search times for Department of State BioVisa queries. (New performance plan measure for FY 2008.) |
| Program and Organization | US-VISIT - National Protection and Programs Directorate |
| Description | This measure is used to determine the average amount of time required to complete an automated search processed through the US-VISIT Automated Biometric Identification System (known as IDENT) in response to queries from Consular Offices worldwide where fingerprints are captured as part of the BioVISA process. The service level agreement with Department of State is less than 15 minutes to provide critical identity and watch list information in a timely manner to not impede traveler processing. In light of past performance, US-VISIT has set an internal target of processing BioVisa searches within 5 minutes. |
| Scope | This measure covers all BioVisa queries. The measure covers IDENT processing time only. |
| Data Source | IDENT system transaction records. |
| Collection Method | Data is extracted from the IDENT system via a standard query through the IDENT reporting tool. Search times within IDENT for all BioVisa queries for a the reporting period are averaged. |
| Reliability | Reliable |
| How Data is Verified | Data is generated daily and actual performance against targets are reviewed monthly with IDENT stakeholders. Data aberrations are researched. |

| | |
|---|---|
| Performance Measure | Average biometric watch list search times for queries from U.S. ports of entry. (New performance plan measure for FY 2008.) |
| Program and Organization | US-VISIT - National Protection and Programs Directorate |
| Description | The average response time of biometric watch list queries processed through the Automated Biometric Identification System (known as IDENT) in response to queries from ports of entry (POE) where fingerprints are captured. The service level agreement with Customs and Border Protection is less than 10 seconds to provide identity and watch list information to inspectors timely to facilitate traveler processing. |
| Scope | The measure covers IDENT processing time only. |
| Data Source | IDENT system transaction records. |
| Collection Method | Data is extracted from the IDENT system via a standard query through the IDENT reporting tool. Search times within IDENT for all POE queries for the reporting period are averaged. |
| Reliability | Reliable |
| How Data is Verified | Data is generated daily and data trends are reviewed monthly. Data aberrations are researched. |

| | |
|---|---|
| Performance Measure | Number of biometric watch list hits for travelers processed at ports of entry. (Retired plan measure.) |
| Program and Organization | US-VISIT - National Protection and Programs Directorate |
| Description | This measure reflects US-VISIT's support to Customs and Border Protection (CBP) in identifying persons of interest and taking appropriate actions at U.S. ports of entry. A hit occurs when the biometric data provided by a traveler matches biometric data contained in a biometric watch list. This measure provides a count of the number of verified US-VISIT Automated Biometric Identification System (known as IDENT) biometric watch list hits in secondary for which there were no associated DHS system biographic enforcement information (biographic hits). This represents individuals for whom derogatory information exists, but was not revealed by a biographic-based check. The increase in FY 2008 is based on the addition of the Criminal Master File (FBI records). After 2008, the number is projected to decline as travelers with derogatory information forego attempts to enter the country and are deterred from entering the country. |
| Scope | Provides a count of the number of verified US-VISIT IDENT System biometric watch list hits at ports of entry for which there were no associated Traveler Enforcement Communications System (TECS) biographic hits. TECS is a text-based automated system operated by CBP that contains information and lookouts on suspect individuals, businesses, and vehicles. TECS terminals are normally located at ports of entry and are used by CBP Officers to check incoming travelers. TECS plays an essential role in the screening of travelers entering the U.S. and in supporting the screening requirements of other federal agencies. |
| Data Source | Data is drawn from the US-VISIT Consolidated Report Data file, which reports data extracted from the IDENT system Biometric Hit database. The data reflects biometric watch list hits that have no associated biographic watch list records (i.e., there was no corresponding watch list record in TECS). |
| Collection Method | Data is extracted from the IDENT system via a standard query through the IDENT reporting tool by the IDENT and OM Team. |
| Reliability | Reliable |
| How Data is Verified | The information is collected, reported, and analyzed daily. Data aberrations are researched. Watch list hits and resulting adverse actions are reported based on site specific processing for entry transactions (including land border ports). The data is consolidated for weekly, monthly, and quarterly reporting. This specific metric (number of biometric watch list hits for travelers processed at ports of entry) is a cumulative total for the number of biometric watch list hits for the reporting period. Watch list hits are identified by DHS automated fingerprint identification system (IDENT). |

| | |
|---|---|
| Performance Measure | Number of biometric watch list hits for visa applicants processed at consular offices. (Retired plan measure.) |
| Program and Organization | US-VISIT - National Protection and Programs Directorate |
| Description | This measure reflects US-VISIT's support to the Department of State in creating a virtual border that identifies persons of interest and denies them a visa before they arrive in the United States. A hit occurs when the biometric data provided by a visa applicant matches biometric data contained in a biometric watch list. The Department of State has deployed a biometric capture capability, known as the BioVisa Program, in all consular offices as of October 26, 2004. This measure provides a count of the number of BioVisa non-immigrant/immigrant visa applications resulting in biometric-only hits. This measure represents individuals who applied for a U.S. visa for whom derogatory information exists, but was not revealed by a name-only check. The increase predicted in FY 2008 is also based on the additional FBI information to the US-VISIT system. |
| Scope | The scope of this measure is all Bio Visa non-immigrant/immigrant visa applications in all consular offices worldwide |

| | |
|---|---|
| Data Source | Data source for this measure is the US-VISIT Consolidated Report Data File, which reports data extracted from the Automated Biometric Identification System (known as IDENT) Biometric hit log. |
| Collection Method | Data is extracted from the IDENT system by the US-VISIT Law Enforcement and Intelligence Group via a standard query through the IDENT reporting tool. |
| Reliability | Reliable |
| How Data is Verified | Verification is done by vetting data collected from consular offices through both the Department of State and US-VISIT to determine accuracy. The information is provided, reviewed, analyzed, and collected for weekly, monthly, and quarterly reporting and review. |

| | |
|---|---|
| Performance Measure | Percent of biometrically screened individuals inaccurately identified as being a on a US-VISIT watch list. (New performance plan measure for FY 2008.) |
| Program and Organization | US-VISIT - National Protection and Programs Directorate |
| Description | US-VISIT provides biometric identity services to other DHS entities through the Automated Biometric Identification System (known as IDENT) to screen foreign visitors to determine whether those individuals are on a watch list. Accuracy of US-VISIT information is a key indicator of the quality of the information furnished to its customers. This measure attempts to assess the accuracy of data provided by the IDENT system by tracking the rate at which individuals screened against the watch list returns a false positive identification (false acceptance). In other words, the rate at which individuals that are not on the watch list are misidentified as being on a watch list. |
| Scope | IDENT False Acceptance Rate (FAR) data reported here includes all watch list query transactions received by the IDENT system. |
| Data Source | Data on incidents of false acceptance are determined through human fingerprint examinations. The results of these human examinations are stored in the IDENT database. Data on total number of IDENT system queries is obtained from IDENT system transaction records. Data is extracted from the IDENT system via a standard query through the IDENT reporting tool. |
| Collection Method | The IDENT Watch list FAR is a measure of the positive hits returned by the system for individuals known to not be on the watch list. Calculation of the measure is done as such: FAR equals the number of ambiguous automated hits not on the watch list divided by the total number of IDENT queries for a specific reporting period. |
| Reliability | Reliable |
| How Data is Verified | Data is generated daily and data trends are reviewed monthly during a program status review with key user agency participation. Data aberrations are researched. |

| | |
|---|---|
| Performance Measure | Percent of in-country overstay leads deemed credible and forwarded to Immigration and Customs Enforcement for further investigation. (New performance plan measure for FY 2008.) |
| Program and Organization | US-VISIT - National Protection and Programs Directorate |
| Description | An in-country overstay is defined as non-immigrant foreign traveler whose authorized period of admission granted at arrival in the United States has expired without an apparent subsequent departure, arrival, or status update recorded in the Arrival Departure Information System (ADIS) database. The program uses ADIS to identify Priority In-Country Overstay records for possible law enforcement action by Immigration and Customs Enforcement (ICE) and then manually validates these records. The result of this process is vetted ADIS records that are likely to represent the travelers who are overstaying their authorized period of admission and are thus subject to adverse actions. These vetted records are then sent to ICE for further investigation. An upward trend indicates that US-VISIT is increasing the number of credible law enforcement leads identified for manual review, and thus assisting ICE investigations of illegal overstays. |
| Scope | This measure applies to all US-VISIT in-country overstay transactions pertaining to persons overstaying the terms of their visas by 90 days or more. |

| | |
|---|---|
| Data Source | The data source is the Lead Trac database, which is used to track the status of the analytical activity of the US-VISIT Data Integrity Group during the vetting process. |
| Collection Method | The data is collected in the current Lead Trac system and will be collected in TRACS (the Lead Trac replacement) and on Data Integrity Services spread sheets. The percent of in-country overstay leads deemed credible and forwarded to Immigration and Customs Enforcement equals 100 times [the number of priority in-country overstay leads forwarded to government staffs] divided by [the number of priority in-country overstay records closed by dig staff plus the number of records closed by automated vetting plus the number of leads forwarded to government staffs]. |
| Reliability | Reliable |
| How Data is Verified | These data are checked manually on desktop computers by the analysis section of the Data Integrity Services. |

| | |
|---|---|
| Performance Measure | Ratio of adverse actions to total biometric watch list hits at ports of entry. (Retired plan measure.) |
| Program and Organization | US-VISIT - National Protection and Programs Directorate |
| Description | This measure captures efforts by US-VISIT to work with its partner agencies to improve the value of the information provided. The decision not to admit is considered an adverse action. This measure represents individuals for whom the derogatory information revealed by the biometric check was sufficient to deny admission or take law enforcement action. Each watch list hit constitutes a piece of critical information provided to decision-makers that they would not have otherwise. |
| Scope | The scope of this measure is based on all visitors processed though the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Automated Biometric Identification System (known as IDENT) at ports of entry. Adverse actions are those that a traveler would view as a negative outcome since his travels or ultimate destination is being interrupted and include the following categories: Expedited Removals, I-275 Withdrawals, Visa Waiver Program Refusals, Notices to Appear, Extraditions, Transferred Over To (law enforcement agencies), and Criminal Prosecutions |
| Data Source | Data is drawn from the US-VISIT Consolidated Report Data file, which reports data extracted from the IDENT system. |
| Collection Method | Data is extracted from the IDENT system by the IDENT Operations and Maintenance team via a standard query through the IDENT reporting tool. |
| Reliability | Reliable |
| How Data is Verified | Data is generated daily and data trends are reviewed monthly. Data aberrations are researched. Watch list hits and resulting adverse actions are reported based on site specific processing for entry transactions (including land border ports). The data is consolidated for weekly, monthly, and quarterly reporting and review. Data trends are researched by the US-VISIT Performance Measurement Group within the Office of Budget. |

# Office of Health Affairs

| | |
|---|---|
| Performance Measure | Number of agencies who have agreed to provide information to the National Biosurveillance Integration Center (NBIC). |
| Program and Organization | Medical and Biodefense Programs - Office of Health Affairs |
| Description | This measure will determine how many Federal agencies are participating in NBIC by determining the number of information sharing and access agreements (ISAA) that are in place. An ISAA is a tool that facilitates and formalizes information access or exchange between two or more parties, and can take many forms. Agency participation and information exchange must be paced to allow adequate consideration of major issues and documentation of the exchange details. Currently, details pertaining to privacy rights, system compatibility issues, and information security are being negotiated. |
| Scope | The present scope of this measure is those Federal, State, local and private entities with which the NBIC has formed partnerships. Over the long term the center will establish partnerships with multiple Federal agencies as well as State, local, and private entities. The initial five partners form the core of NBIC and will bring direct expertise, data streams, analytical skills, and defined product needs to the system. In future years, it is envisioned that additional Federal, State, local, and private entities will contribute relevant information to strengthen the knowledge base and speed of the analysis. |
| Data Source | A hard-copy file is maintained that defines the level of agency participation, data submittal, and product needs in the form of Memorandums of Understanding, Interagency Agreements, Memorandums of Agreement, cooperative agreements, and other similar documents. |
| Collection Method | Copies of documentation are collected and maintained from the various participating agencies. |
| Reliability | Reliable |
| How Data is Verified | The NBIC retains hard and soft copy of all final agreements. It will review these agreements annually to ensure currency and also to ensure that agreements are directly applicable to specifically identified partners as defined in the NBIC Concept of Operations and the Strategic Plan. |

| | |
|---|---|
| Performance Measure | Number of biological monitoring units employed in high-risk indoor facilities within BioWatch jurisdictions. (New performance plan measure for FY 2008.) |
| Program and Organization | Medical and Biodefense Programs - Office of Health Affairs |
| Description | This performance measure captures the number of monitoring units, designed to detect the release of biological agents, within the facilities or complexes of a BioWatch jurisdictions A BioWatch jurisdiction includes the largest metropolitan areas in the United States. The higher number of units employed, the larger number of people protected from a potential biological attack. |
| Scope | This measure includes the number of biological monitoring units that are employed (operating and providing actionable information) in high risk indoor facilities within BioWatch jurisdictions. A high risk indoor facility is any building or complex that a jurisdiction considers to be vulnerable to a biological attack. |
| Data Source | The Systems Program Office has a BioWatch point of contact at all jurisdictions. This point of contact is responsible for providing the Systems Program Office updates regarding any additions or changes in the number and location of each biological monitoring unit. |
| Collection Method | The number of biological monitoring units that is employed at each jurisdiction varies from one to the other. This number is determined by the Systems Program Office based on data collected from Los Alamos National Labs. The BioWatch point of contact at each jurisdiction informs the Systems Program Office each time a new biological monitoring unit is employed. The Systems Program Office reports on the total number of biological monitoring units in indoor high risk |

| | |
|---|---|
| | facilities on a quarterly basis. |
| Reliability | Reliable |
| How Data is Verified | The Systems Program Office conducts an annual assessment of each jurisdiction and ensures that all biological monitoring units employed have been reported. This assessment also verifies the accuracy of the internal records. |

| | |
|---|---|
| Performance Measure | Number of biological monitoring units employed in the top threat cities. (Retired plan measure.) |
| Program and Organization | Medical and Biodefense Programs - Office of Health Affairs |
| Description | The data measures the total number of bioaerosol collectors employed in the U.S. in cities determined to be at the highest risk. These collectors serve to determine the characteristic and extent of a potential terrorist airborne health threat to the public and protect the public by enabling early response actions to identify airborne materials in the event of an attack. |
| Scope | This measure reports on all bioaerosol collectors employed in the top threat cities at the end of each year. Additional collectors will continue to be employed in the ten top threat cities to improve the spatial coverage and to provide the capability for the local jurisdiction to provide coverage for special venues and events. Placement of additional collectors will be decided in close collaboration with the jurisdictions that provide input as to where additional coverage is necessary. |
| Data Source | The jurisdictions receiving the collectors report via spreadsheet on the actual number of collectors deployed. |
| Collection Method | Data collection for this measure relies on reporting from the jurisdictions on a quarterly basis of additional collectors deployed. The program will collect this data into a master spreadsheet. Laboratory analysis reports will provide confirmation as the number of samples analyzed correlates to the number of collectors operating. |
| Reliability | Reliable |
| How Data is Verified | The Systems Engineering and Development onsite contractor conducts an annual evaluation of all BioWatch sites at which time they also inventory the deployed BioWatch collectors. This serves as an independent double-check to ensure that the information on deployed collectors is correct. |

| | |
|---|---|
| Performance Measure | Percent of annual milestones that are met for the National Biosurveillance Integration Center. (Retired plan measure.) |
| Program and Organization | Medical and Biodefense Programs - Office of Health Affairs |
| Description | This measure reports the percent of milestones met each year by the program. In FY 2007, the National Biosurveillance Integration Center (NBIC) met all four of its milestones. This achievement has helped NBIC to develop information streams from other federal agencies in order to provide biosurveillance data, design analytic methodology, develop information technology tools to support biosurveillance analysis and enable rapid deployment. The benefits of meeting all four goals are embodied in the ongoing daily reporting provided to senior decision and policy makers in DHS and other engaged partner agencies on health issues of significance to homeland security. |
| Scope | The scope of this measure is the number of NBIC milestones. The Center will be established and improved over a five year timeframe. The program plan includes multiple yearly milestones for the development of information streams, analytical methodology development, product development, information technology tool development and spiral upgrades. In each of the five years, NBIC will measure its progress against specific milestones. The information streams will initially include seven Federal agency partners, and will expand to include an additional four Federal agency partners plus State, local and tribal entities, private/commercial entities, and international allies and organizations engaged in biosurveillance and public health. |
| Data Source | The source of this data will come from an independent analysis of the progress of the system development. This will be derived by two methods. First, a series of |

| | |
|---|---|
| | semiannual program reviews are conducted and a firsthand review of the protocols, design documentation, and active agency agreements are performed. |
| Collection Method | The NBIC Program Manager conducts program reviews annually which are verified independently by the Office of Health Affairs on the progress of the system, protocols, and methodologies. |
| Reliability | Reliable |
| How Data is Verified | The on-site contractor and the IT development contractors examine the milestones contained in contract deliverables and the NBIC master Work Breakdown Structure (WBS) to ensure all milestones are listed, reviewed, and properly accounted for. All of these entities then report to the NBIC Program Manager who in turn validates completion to the Director, NBIC. |

| | |
|---|---|
| Performance Measure | Percent of the population in BioWatch jurisdictions covered by outdoor biological monitoring units. (New performance plan measure for FY 2008.) |
| Program and Organization | Medical and Biodefense Programs - Office of Health Affairs |
| Description | This performance measure calculates the percent of the population in the BioWatch jurisdictions that is covered by outdoor biological monitoring units. Population covered by these units can be warned and identified for treatment prior to becoming symptomatic as a consequence of an outdoor release of biological agent. A BioWatch jurisdiction includes the largest metropolitan areas in the U.S. This measure is an estimate based on performance (e.g., probability of detection) and range (e.g., protection area) of the monitoring units. |
| Scope | This measure includes the population within BioWatch jurisdictions and estimates the coverage provided by biological monitoring units. Currently, the BioWatch Program covers more than 30 of the largest metropolitan areas within the U.S. According to the Metropolitan Statistical Area (MSA) census data, BioWatch jurisdictions represent approximately 50 percent of the U.S. MSA census population |
| Data Source | Population data is obtained from the U.S. Census Bureau. Historical meteorological data used in model calculation is obtained from National Oceanic and Atmospheric Administration. The data is combined and simulated at Los Alamos National Laboratory. |
| Collection Method | Data is collected from sophisticated modeling tools that incorporate historical meteorological conditions, hypothetical biological agent release scenarios, the performance of BioWatch's biological monitoring units, and their actual location. Based on inputs to the model, an estimate is produced of the percent of population covered. This information in then summarized and provided to the BioWatch System Program Office |
| Reliability | Reliable |
| How Data is Verified | Local teams are responsible to ensure that units in the field are fully operational. These units are checked by the BioWatch jurisdictions on a daily basis to ensure they are working properly. The program does an annual verification to ensure that units reported employed by local authorities are actually operational. The model used to provide estimates is validated by external parties. |

| | |
|---|---|
| Performance Measure | Percent of the U.S. population covered by biological collectors/detectors. (Retired plan measure.) |
| Program and Organization | Medical and Biodefense Programs - Office of Health Affairs |
| Description | This measure shows the progress towards increasing security by measuring the percent of the continental U.S. population covered by Biowatch collectors. These collectors serve to determine the characteristic and extent of a potential terrorist airborne health threat to the public and protect the public by enabling early response actions to identification of airborne materials in the event of an attack. |
| Scope | This measure is based on a model for the entire U.S. population that assesses threats, delivery methods, population densities and vulnerabilities, environmental factors and spatial coverage of each unit in the system. |
| Data Source | Sophisticated modeling tools available through the National Laboratories are used |

| | |
|---|---|
| | to determine if the collector/sensor locations are sufficient based on historical meteorological conditions, hypothetical terrorist release scenarios, and actual Global Positioning System coordinates of deployed collectors/sensors taken as they are put into operation. |
| Collection Method | Historical meteorological data will be obtained from National Oceanic and Atmospheric Administration, release scenarios will be obtained from the National Laboratories, and Global Positioning System coordinates will be obtained from the BioWatch jurisdictions.  The data is then input into a model to determine the percent of the of the U.S. population covered. |
| Reliability | Reliable |
| How Data is Verified | This data is based on sophisticated modeling tools which are verified, validated, and vetted consistently and have been used in placing collectors and performing event reconstruction.  BioWatch contractors gather, collect, and enter information into the model to generate the data.  This data is sent to the Systems Program Office, and all information inputted into the model is double checked for accuracy.  This process is overseen and reviewed a third time by the Office of Health Affairs' budget division and leadership. |

| | |
|---|---|
| Performance Measure | Probability of detecting the release of a biological agent.  (Retired plan measure.) |
| Program and Organization | Medical and Biodefense Programs - Office of Health Affairs |
| Description | This measure demonstrates Biowatch's ability to detect an aerosol release of a biological agent. This measure is calculated using modeling and statistical data that account for several key factors, including the number of detectors, coverage area, environmental factors, population concentration, and meteorological data. |
| Scope | The scope of this measure is all of the collectors, detectors, measures and devices contributing to the detection of biological agents in the U.S. |
| Data Source | Sophisticated modeling tools available through the National Laboratories are used to determine if the collector/sensor locations are sufficient based on historical meteorological conditions, hypothetical terrorist release scenarios and actual GPS coordinates of deployed collectors/sensors taken as they are put into operation. |
| Collection Method | Historical meteorological data will be obtained from National Oceanic and Atmospheric Administration, release scenarios will be obtained from the National Laboratories, and Global Positioning System coordinates will be obtained from the BioWatch jurisdictions.  The data is then input into a model to determine the probability of detecting the release of a biological agent. |
| Reliability | Reliable |
| How Data is Verified | This data is based on sophisticated modeling tools which are verified, validated, and vetted consistently and have been used in placing collectors and performing event reconstruction.  BioWatch contractors gather, collect, and enter information into the model to generate the data.  This data is sent to the Systems Program Office and all information inputted into the model is double checked for accuracy.  This process is overseen and reviewed a third time by the Office of Health Affairs' budget division and leadership. |

| | |
|---|---|
| Performance Measure | Time between an indoor monitoring unit exposure to a biological agent and the declaration of a confirmed positive result.  (New performance plan measure for FY 2008.) |
| Program and Organization | Medical and Biodefense Programs - Office of Health Affairs |
| Description | This performance measure calculates the time between an indoor monitoring unit exposure to a biological agent and the declaration of a confirmed positive sample result by the local laboratory official.  There are a number of factors that influence the time gauged by this measure, such as the number of units and the type of technology.  For instance, the higher the number of autonomous indoor biological monitoring units employed, the shorter the time will be between the release of a biological agent and the declaration of a confirmed positive sample result.  An autonomous indoor biological monitoring unit is a type of sensor that collects airborne particles and performs sample analysis.  By performing the sample |

| | |
|---|---|
| | analysis at the monitoring site, automated detection systems significantly reduce the time between a biological release and detecting confirming that an event has occurred. |
| Scope | This measure is a system-wide average of the elapsed time between an indoor release of a biological agent and the declaration by the local laboratory official of a confirmed positive result. This measure includes the number and type of indoor biological monitoring units employed. |
| Data Source | The Systems Program Office is in charge of developing the standard operating timeline for indoor biological units |
| Collection Method | The Systems Program Office has developed standard operating timelines for indoor biological monitoring units. The timeline is designed by calculating the sampling period, the time to analyze the samples and the agent identification. Agent identification is the process by which a species or subspecies of the agent found in a sample is determined. The Systems Program Office reports quarterly on the time between an indoor monitoring unit exposure to a biological agent and the declaration of a confirmed positive sample result. |
| Reliability | Reliable |
| How Data is Verified | The data is verified annually as part of the BioWatch Evaluation and Exercise Program that is conducted by the Chemical/Biological Early Detection Systems Program Office personnel. The jurisdictions are evaluated on a wide range of operational parameters including performance time lines. |

| | |
|---|---|
| Performance Measure | Time between an outdoor monitoring unit exposure to a biological agent and the declaration of a confirmed positive result. (New performance plan measure for FY 2008.) |
| Program and Organization | Medical and Biodefense Programs - Office of Health Affairs |
| Description | This performance measure calculates the time between an outdoor monitoring unit exposure to a biological agent and the declaration of a confirmed positive sample result by the local laboratory official. There are a number of factors that influence the time gauged by this measure, such as the number of units and the type of technology. For instance, the higher the number of autonomous outdoor biological monitoring units employed, the shorter the time will be between the release of a biological agent and the declaration of a confirmed positive sample result. An autonomous outdoor biological monitoring unit is a type of sensor that collects airborne particles and performs sample analysis. By performing the sample analysis at the monitoring site, automated detection systems significantly reduce the time between a biological release and detecting confirming that an event has occurred. |
| Scope | This measure is a system-wide average of the elapsed time between an outdoor release of a biological agent and the declaration by the local laboratory official of a confirmed positive result. This measure includes the number and type of outdoor biological monitoring units employed. |
| Data Source | The Systems Program Office is in charge of developing the standard operating timeline for outdoor biological units |
| Collection Method | The Systems Program Office has developed standard operating timelines for outdoor biological monitoring units. The timeline is designed by calculating the sampling period, the time to analyze the samples and the agent identification. Agent identification is the process by which a species or subspecies of the agent found in a sample is determined. The Systems Program Office reports quarterly on the time between an outdoor monitoring unit exposure to a biological agent and the declaration of a confirmed positive sample result. |
| Reliability | Reliable |
| How Data is Verified | The data is verified annually as part of the BioWatch Evaluation and Exercise Program that is conducted by the Chemical/Biological Early Detection Systems Program Office personnel. The jurisdictions are evaluated on a wide range of operational parameters including performance time. |

## Office of Intelligence and Analysis/Operations Coordination

| | |
|---|---|
| Performance Measure | Number of Homeland Intelligence Reports (HIRs) disseminated. (New performance plan measure for FY 2008.) |
| Program and Organization | Analysis and Operations Program - Office of Intelligence and Analysis/Operations Coordination |
| Description | The number of Homeland Intelligence Reports (HIRs) disseminated is a formal mechanism monitoring the distribution of Homeland Intelligence Reports (HIRs). The HIRs provide emergent intelligence information with Intelligence Community (IC) standards to necessary stakeholders. A higher number of HIRs provides the Intelligence Community as well as Federal, State, local, tribal, and private sector partners greater information to protect the public interest. |
| Scope | This output measurement tracks the number of HIRs disseminated by IA and differs from finished intelligence. Intelligence reporting is a single snapshot of relevant, operational data that may require follow-on analysis - the dot. Finished intelligence represents analytic conclusions drawn from the collection, processing, analysis, and dissemination cycle-connecting the dots. |
| Data Source | The information required for HIR production comes from a variety of classified and unclassified data sources. These sources, harvested from DHS component information, are compiled into HIRs for State, local, and tribal governments, as well as the Intelligence Community. |
| Collection Method | IA collects HIR data through electronic classified and unclassified methods. |
| Reliability | Reliable |
| How Data is Verified | The Production Management Division has established stringent controls for the distribution of HIRs including a single point for Agency distribution. The reported performance measure is the actual output of HIRs produced. The Production Management division records the serialized HIR number at reporting of HIR distribution; therefore, the number is reported definitively. |

| | |
|---|---|
| Performance Measure | Percent of active Homeland Security Information Network (HSIN) users. |
| Program and Organization | Analysis and Operations Program - Office of Intelligence and Analysis/Operations Coordination |
| Description | Percent of active HSIN users is derived by dividing the number of users who have accessed the system during the reporting period (the quarter) divided by the number of total HSIN user accounts. |
| Scope | Includes Federal, State, local, tribal, etc. users that have accessed the system during the reporting period. |
| Data Source | The HSIN software engineering group uses the Urchin software application to identify the number of unique users in a given reporting period. A unique user is one who has logged onto the system at least once during the reporting period. Someone who has logged in 50 times using the same log-in information is counted as 1 unique user. |
| Collection Method | Urchin counts and stores the number of total log-ins on a daily basis. At the end of the reporting period, the system compiles the statistics. The Operations Maintenance Manager of the Technical Design Agent (TDA) team selects the statistics needed from a drop-down selection of configurable data reports. The number of unique users is distinguished from the total number of HSIN user accounts. The number of unique users (active users) is divided by the total number of HSIN accounts to get the percent of active HSIN users. TDA submits a quarterly HSIN Metrics report to the Joint Program Management Office that includes this metric. |
| Reliability | Reliable |
| How Data is Verified | The tools used to run the usage report have undergone configuration and testing to ensure accurate data is supplied. The percent calculated in the quarterly metrics report submitted by TDA is rechecked for accuracy by the Operations Performance Management team. |

| | |
|---|---|
| Performance Measure | Percent of Component-to-Component information sharing relationships documented through information sharing and access agreements (ISAAs). |
| Program and Organization | Analysis and Operations Program - Office of Intelligence and Analysis/Operations Coordination |
| Description | It is important that DHS Components (major organizational entities) share information with one another, especially with their critical information sharing stakeholders. This formal sharing is granted broadly from Component to Component, rather than system by system access. This measure does not assume that DHS Components must have access to all DHS information, rather that they must have formal access to their critical information-sharing partners. This measure will determine the percent of information sources accessible to DHS internal components by determining the number of Information Sharing and Access Agreements (ISAA) that are in place relative to the number of critical information sharing partners that Components should have access to. An ISAA is a tool that facilitates and formalizes information access or exchange between two or more parties, and can take many forms, e.g., Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), Letter of Understanding (LOU), etc. |
| Scope | The scope of this measure encompasses the sharing of DHS-originated information between DHS Components and specifically, counts the number information sharing relationships between DHS Components and how many of those relationships have been documented using information sharing and access agreements (ISAAs). This measure is a ratio of two parts. The numerator examines the number of documented information sharing relationships between DHS components (as indicated by ISAAs). ISAAs facilitate the exchange of information between two or more parties. ISAAs take many forms including formal legal agreements or unsigned documents that adhere to the DHS ISAA Methodology (as defined by clarifying guidance to the Secretary's February 2007 Policy for Internal Information Exchange and Sharing Memorandum (One DHS Memo). The denominator of the measure estimates the number of Component-to-Component information sharing relationships at DHS as identified by reference to policy documents. |
| Data Source | The Office of Intelligence and Analysis (IA) maintains in an MS Access database a master repository of ISAAs between DHS components. The repository supports the calculation of the numerator. The data source for the denominator is component strategic policy documents, validated through interviews with each component's information sharing action officer. Information sharing relationships must: (a) satisfy an ongoing information requirement, vice an ad-hoc request; (b) be essential to the conduct of the recipient components mission; (c) be DHS-originated information and (d) be obtained from a DHS component. |
| Collection Method | All Components must forward copies of their ISAAs to IA for inclusion in the master repository. IA will conduct annual data calls to validate the accuracy of the master repository and subsequently measure progress toward documenting information sharing relationships via ISAAs. Data will be collected annually, not quarterly. The program will research and analyze each components strategic policy documents, and work with Component representatives to ensure all relevant documents are identified. |
| Reliability | Reliable |
| How Data is Verified | Program personnel knowledgeable with the requirements of the One DHS Memo, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), and other subsequent Intelligence and Analysis produced guidance analyze the data gathered for the measure. IA personnel (a) conduct initial research to identify Component-to-Component information sharing relationships and (b) review submitted ISAAs against published One DHS memo guidance as a double-check to ensure the document is a valid ISAA for reporting and tracking purposes. Information sharing stakeholder relationships identified by IA are validated by component subject matter experts including (but not necessarily limited to) each components information sharing action officer(s). |

## Science and Technology Directorate

| | |
|---|---|
| Performance Measure | Percent of milestones that are met, as established in the fiscal year's budget execution plan. |
| Program and Organization | Borders and Maritime Security - Science and Technology Directorate |
| Description | The program has established a set of milestones that are necessary for achieving the goals and objectives of the program. These milestones are presented in the program's portion of the Science and Technology (S&T) Directorate's fiscal year budget execution plan, which details the allocation of dollars and projected accomplishments for the year. |
| Scope | The scope encompasses the approved programmatic and technical milestones for all Directorate programs and projects. |
| Data Source | The S&T Directorates Enterprise Portfolio Management Initiative (EPMI) database is the designated repository for all project-level planning and actual status information. Its purpose is to provide ready access to individual and aggregate project data for reporting, planning, status reviews and analysis. |
| Collection Method | Project managers update EPMI milestone data on at least a quarterly basis from project status reports provided by performers, and from personal knowledge of project management status that can be objectively corroborated by artifacts such as signed documents. |
| Reliability | Reliable |
| How Data is Verified | The percent reported is reviewed using the status of funding, the number of milestones stated in the execution plan, and the explanation that is provided in each quarterly performance data call. Division Directors review the data submitted by Program Managers to ensure accuracy/consistency, approve the status and submit to the S&T Strategy, Policy and Budget/Chief Financial Officer's Office. Information is verified by the Directorate's financial officers, and additional information is requested of programs if discrepancies occur. |

| | |
|---|---|
| Performance Measure | Percent of transition program funding dedicated to developing technologies in direct response to Department of Homeland Security components' requirements. |
| Program and Organization | Borders and Maritime Security - Science and Technology Directorate |
| Description | This measure represents the percent of Science and Technology (S&T) transition funding that directly supports the development of technologies requested by the Department Components such as Customs and Border Protection, to ensure that operational end users are provided with the technology and capabilities they need to detect and prevent terrorist attacks, means of terrorism, and other illegal activities. |
| Scope | The percent of funding that is reported for this measure is calculated based on the amount of funding committed or obligated towards those programs in the S&T Federal Financial Management System (FFMS). |
| Data Source | The dataset is generated based on requirements gathered from the S&T Integrated Product Teams (IPT) and the Borders and Maritime Security program. The data is the amount of funding based on expenditures and obligations that link back to the IPT requirements. The S&T FFMS is the financial record of the Directorate and the official source of financial information regarding commitments and obligations that have received funds certification. |
| Collection Method | The Borders and Maritime Security program receives its information through the FFMS and PRISM financial systems. These systems provide a weekly report on the commitments, obligations, and expenditures of funding. |
| Reliability | Reliable |
| How Data is Verified | Once the FFMS system calculates this percent, S&T headquarters validates the number. The Borders and Maritime Security Program Managers compare the percent of obligations and expenditures to program plans that indicate the amount of transition funding for Border and Maritime Security. |

| | |
|---|---|
| Performance Measure | Percent completion of an effective restoration technology to restore key infrastructure to normal operation after a chemical attack. |
| Program and Organization | Chemical and Biological - Science and Technology Directorate |
| Description | This measure gauges the percent of work accomplished out of the total effort needed to prototype an effective technology that can restore key infrastructure to normal operations after a chemical attack. |
| Scope | This measure tracks the development of effective restoration technologies, which are capability requirements that have been translated into specific system requirements, then developed into prototypes and guidance, and transitioned to Environmental Protection Agency for further use and capability expansion.  Scope of effort being measured provides capability for Washington DC and New York City regions. |
| Data Source | Assessment is made based on completion of milestones, each of which quantitatively describes an advance toward the final desired end state.  Milestones are documented in interagency monthly meetings, roadmaps, Technology Transition Agreements, and/or Memorandum of Agreements/Interagency Agreements, which serve as the contract between the Science and Technology (S&T) Directorate and the customer. |
| Collection Method | The program obtains and compiles written documentation from interagency partners of central relevance to component milestones, as well as minutes of record generated at regular meetings of approximately monthly periodicity. |
| Reliability | Reliable |
| How Data is Verified | Data are assessed on regular basis by the Division Head or designee within the Office of the Division Head, using data from the EPMI database as well as reports, meeting minutes, and interagency assessment documents submitted by the Program Manager. |

| | |
|---|---|
| Performance Measure | Percent of milestones that are met, as established in the fiscal year’s budget execution plan. |
| Program and Organization | Chemical and Biological - Science and Technology Directorate |
| Description | The program has established a set of milestones that are necessary for achieving the goals and objectives of the program. These milestones are presented in the program’s portion of the Science and Technology (S&T) Directorate’s fiscal year budget execution plan, which details the allocation of dollars and projected accomplishments for the year. |
| Scope | The scope encompasses the approved programmatic and technical milestones for all Directorate programs and projects. |
| Data Source | The S&T Directorates Enterprise Portfolio Management Initiative (EPMI) database is the designated repository for all project-level planning and actual status information.  Its purpose is to provide ready access to individual and aggregate project data for reporting, planning, status reviews and analysis. |
| Collection Method | Project managers update EPMI milestone data on at least a quarterly basis from project status reports provided by performers, and from personal knowledge of project management status that can be objectively corroborated by artifacts such as signed documents. |
| Reliability | Reliable |
| How Data is Verified | The percent reported is reviewed using the status of funding, the number of milestones stated in the execution plan, and the explanation that is provided in each quarterly performance data call.  Division Directors review the data submitted by Program Managers to ensure accuracy/consistency, approve the status and submit to the S&T Strategy, Policy and Budget/Chief Financial Officer’s Office. Information is verified by the Directorates financial officers and additional information is requested of programs if discrepancies occur. |

| | |
|---|---|
| Performance Measure | Number of cyber security data sets collected and approved. |
| Program and Organization | Command, Control and Interoperability - Science and Technology Directorate |
| Description | This measure tracks the cumulative number of data sets available in the protected repository, a secure library that is made available to specified researchers. Each data set contains information about real network and system traffic that researchers can use to design, produce, and evaluate new cyber security solutions. The program continues the ongoing collection, refreshing, and sharing of data sets, and addition of new partners as applicable for the Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT) repository. This is important because the repository needs to continually add new and pertinent data so that the cyber security research community can have the most recent information to respond to new attacks. |
| Scope | The total number of stored data sets is collected for this measure. The datasets consist of real network and Internet traffic information that may include, but is not limited to, net flow, critical infrastructure data, and network management data. |
| Data Source | The data sets originate in the academic world, but there is potential to have other dataset providers from various public and private sectors. Researchers (PREDICT users) must be approved for access to a particular data set by a review board. Once this is done, the data hosting site and the researcher are notified and work together to retrieve the data set. The data providers are responsible for maintaining their dataset. |
| Collection Method | The independent contractor supporting the program submits monthly reports on the number of data sets stored. Data is collected and reviewed using an Excel spreadsheet. Reliable data is provided by the PREDICT Coordinating Center that is run by RTI International, a non-profit organization with extensive experience in handling sensitive research data. As part of its contract with DHS, the Coordinating Center collects statistical information including the number of data sets, and provides this information to DHS in monthly reports, and on an as needed basis. |
| Reliability | Reliable |
| How Data is Verified | DHS conducts regular audits of the PREDICT project to ensure compliance with PREDICT operating procedures and contractual provisions |

| | |
|---|---|
| Performance Measure | Number of proof-of-concept reconnaissance, surveillance and investigative technologies demonstrated. (New performance plan measure for FY 2008.) |
| Program and Organization | Command, Control and Interoperability - Science and Technology Directorate |
| Description | This measure identifies the number of proof-of-concept (feasibility of) technologies demonstrated that aid in the discovery, investigation, and prosecution of terrorists and criminals. Proof of concept is considered a milestone in the development of a fully functioning prototype. |
| Scope | Proof-of-concept assessments are used by the Program Manager for the Reconnaissance, Surveillance, and Investigative Technologies subprogram or Division executives to determine the necessity of a continued investment. The program will only include those activities that involve this milestone. |
| Data Source | The data source is quarterly/monthly performance reports (depending on the agreement in the contract) by performers submitted to Program Managers indicating that an assessment has been completed. Proof of concept assessments are performed based on direction from the Program Managers. |
| Collection Method | The Program Managers receive the initial information from the performers (based on the above data source), and identify which projects have produced a proof of concept assessment. The official Directorate-wide collection of this data is conducted by a query of all Division Program Managers and their staffs to provide updated data per quarter based on the above data source. |
| Reliability | Reliable |
| How Data is Verified | The Command, Control and Interoperability Division staff provides their status to the Division Director, who in turn reviews the information and compares it to planned milestones for the year. |

| | |
|---|---|
| Performance Measure | Percent of milestones that are met, as established in the fiscal year's budget execution plan. |
| Program and Organization | Command, Control and Interoperability - Science and Technology Directorate |
| Description | The program has established a set of milestones that are necessary for achieving the goals and objectives of the program. These milestones are presented in the program's portion of the Science and Technology (S&T) Directorate's fiscal year budget execution plan, which details the allocation of dollars and projected accomplishments for the year. |
| Scope | The scope encompasses the approved programmatic and technical milestones for all Directorate programs and projects. |
| Data Source | The S&T Directorates Enterprise Portfolio Management Initiative (EPMI) database is the designated repository for all project-level planning and actual status information. Its purpose is to provide ready access to individual and aggregate project data for reporting, planning, status reviews and analysis. |
| Collection Method | Project managers update EPMI milestone data on at least a quarterly basis from project status reports provided by performers, and from personal knowledge of project management status that can be objectively corroborated by artifacts such as signed documents. |
| Reliability | Reliable |
| How Data is Verified | The percent reported is reviewed using the status of funding, the number of milestones stated in the execution plan, and the explanation that is provided in each quarterly performance data call. Division Directors review the data submitted by Program Managers to ensure accuracy/consistency, approve the status and submit to the S&T Strategy, Policy and Budget/Chief Financial Officer's Office. Information is verified by the Directorates financial officers and additional information is requested of programs if discrepancies occur. |

| | |
|---|---|
| Performance Measure | Percent of States that have initiated or completed a statewide interoperability plan, such as the Statewide Communications Interoperability Plan (SCIP). (Retired plan measure.) |
| Program and Organization | Command, Control and Interoperability - Science and Technology Directorate |
| Description | This measure tracks how well the Office for Interoperability and Compatibility is fostering the development of statewide plans to implement interoperable public safety communications. |
| Scope | The range of data includes all 50 states. |
| Data Source | The Office of Interoperability and Compatibility contracts with several policy academies that assist States in developing interoperability plans. As part of the grant process, States must develop an interoperability plan. In addition, the Preparedness grant process may yield additional statewide plans. |
| Collection Method | The policy academies are required to submit reports to the Office of Interoperability and Compatibility. The Office of Interoperability and Compatibility will collect available statewide interoperability plans. Data will be collected and reported using an Excel spreadsheet. |
| Reliability | Reliable |
| How Data is Verified | The SAFECOM program has directly supported the development of Statewide plans in three states. SAFECOM has also established a Cooperative Agreement with the National Governors Association (NGA) to help 10 States develop or enhance their Statewide plans over 2 years. The NGA will report to SAFECOM regularly and provide final copies of the plans. Further, the Department of Homeland Security Office of Grants and Training (GT) required every state to develop and adopt a Statewide plan by the end of 2007 to remain eligible for interoperability grants. SAFECOM will obtain copies of those plans as they are submitted, and the information will be included in the calculation of the performance measure. |

| | |
|---|---|
| Performance Measure | Number of new or improved technologies available for transition to the customers at a Technology Readiness Level (TRL) 6 or above. |
| Program and Organization | Explosives - Science and Technology Directorate |
| Description | The number of technologies includes those that have reached a maturity level of TRL 6 or above; this indicates that a technology is ready for demonstration. These technologies are potentially ready for transition to the primary customer. |
| Scope | Technology Readiness Level (TRL) 6 is an assessment by Program Managers and Division staff to quantify a technology, subsystem, or prototype readiness level or maturity for demonstration in a relevant environment. These assessments are most meaningful and used by the Program Manager or Division executives to support management oversight and determination of execution status for continued investment, or transition to a customer for further development or acquisition. |
| Data Source | Technology Readiness Level (TRL) assessments are performed in conjunction with technical and program reviews, quarterly performer reports, and discussions with performers on a monthly basis. Program managers and Division staff use the Department of Defenses definitions of TRLs from the Defense Acquisition Guidebook to identify the TRL level the technology has achieved based on the aforementioned reviews and reports. |
| Collection Method | The collection is conducted by a formal query of all Division Program Managers and their staff to provide updated status as of the annual reporting date on current status of technologies, subsystems or prototypes (based on the above data source). The Division Directors staff reviews the information from Program Managers and identifies which technologies have matured to Technology Readiness Level (TRL) 6 status and should be considered for transition to the appropriate customer. |
| Reliability | Reliable |
| How Data is Verified | The Explosives Division staff provides their assessment to the Division Director and Chief Scientist, who in turn reviews the information and compares it to the Technology Readiness Level definitions to ensure that the data are accurate. |

| | |
|---|---|
| Performance Measure | Percent of milestones that are met, as established in the fiscal year’s budget execution plan. |
| Program and Organization | Explosives - Science and Technology Directorate |
| Description | The program has established a set of milestones that are necessary for achieving the goals and objectives of the program. These milestones are presented in the program’s portion of the Science and Technology (S&T) Directorate’s fiscal year budget execution plan, which details the allocation of dollars and projected accomplishments for the year. |
| Scope | The scope encompasses the approved programmatic and technical milestones for all Directorate programs and projects. |
| Data Source | The S&T Directorate’s Enterprise Portfolio Management Initiative (EPMI) database is the designated repository for all project-level planning and actual status information. Its purpose is to provide ready access to individual and aggregate project data for reporting, planning, status reviews and analysis. |
| Collection Method | Project managers update EPMI milestone data on at least a quarterly basis from project status reports provided by performers, and from personal knowledge of project management status that can be objectively corroborated by artifacts such as signed documents. |
| Reliability | Reliable |
| How Data is Verified | The percent reported is reviewed using the status of funding, the number of milestones stated in the execution plan, and the explanation that is provided in each quarterly performance data call. Division Directors review the data submitted by Program Managers to ensure accuracy/consistency, approve the status and submit to the S&T Strategy, Policy and Budget/Chief Financial Officer’s Office. Information is verified by the Directorates financial officers and additional information is requested of programs if discrepancies occur. |

| | |
|---|---|
| Performance Measure | Percent of milestones that are met, as established in the fiscal year's budget execution plan. |
| Program and Organization | Human Factors - Science and Technology Directorate |
| Description | The program has established a set of milestones that are necessary for achieving the goals and objectives of the program. These milestones are presented in the program's portion of the Science and Technology (S&T) Directorate's fiscal year budget execution plan, which details the allocation of dollars and projected accomplishments for the year. |
| Scope | The scope encompasses the approved programmatic and technical milestones for all Directorate programs and projects. |
| Data Source | The S&T Directorate's Enterprise Portfolio Management Initiative (EPMI) database is the designated repository for all project-level planning and actual status information. Its purpose is to provide ready access to individual and aggregate project data for reporting, planning, status reviews and analysis. |
| Collection Method | Project managers update EPMI milestone data on at least a quarterly basis from project status reports provided by performers, and from personal knowledge of project management status that can be objectively corroborated by artifacts such as signed documents. |
| Reliability | Reliable |
| How Data is Verified | The percent reported is reviewed using the status of funding, the number of milestones stated in the execution plan, and the explanation that is provided in each quarterly performance data call. Division Directors review the data submitted by Program Managers to ensure accuracy/consistency, approve the status and submit to the S&T Strategy, Policy and Budget/Chief Financial Officer's Office. Information is verified by the Directorates financial officers and additional information is requested of programs if discrepancies occur. |

| | |
|---|---|
| Performance Measure | Number of analyses/simulations completed on critical infrastructure decision support systems that provide actionable information to help protect U. S. critical infrastructure. (New performance plan measure for FY 2008.) |
| Program and Organization | Infrastructure and Geophysical - Science and Technology Directorate |
| Description | This measure represents the cumulative number of analyses/simulations completed on critical infrastructure decision support systems. These systems provide a rational, scientifically-informed approach for prioritizing critical infrastructure protection strategies and resource allocations using modeling, simulation, and analyses to assess vulnerabilities, consequences, and risks; develop and evaluate protection, mitigation, response, and recovery strategies and technologies; and provide real-time support to decision makers during crises and emergencies. This measure demonstrates the availability of actionable information to help protect the U.S.'s critical infrastructure from acts of terrorism, natural disasters, and other emergencies. |
| Scope | The critical infrastructure decision support systems have defined standards that signal the completion of an analysis/simulation. The measure examines the total number of completed analyses/simulations. |
| Data Source | The critical infrastructure decision support systems generate reports for each analysis/simulation that is completed. |
| Collection Method | Analysis is performed on the output of each analysis/simulation, and a report is generated by the analysts within the National Laboratory consortium. Official copies of the reports are delivered to the DHS Program Manager. |
| Reliability | Reliable |
| How Data is Verified | The DHS Science and Technology (S&T) Directorate and the system team verify the resultant data via different methods depending upon the analyses performed. These methods vary from detailed technical review by internal and external Subject Matter Experts, and comparison against similar studies and analysis against real-world events. In more recent analyses, the team has begun to use parameter sensitivity and uncertainty analyses for more prominent studies, resulting in a better understating of the "tipping points" that modeled space and |

| | |
|---|---|
| | regions that may require better data or more analyses. Issues identified by the S&T Directorate are brought to the team and resolution is either sought or determined to be inappropriate or unnecessary. |

| | |
|---|---|
| Performance Measure | Number of scenarios completed on the Critical Infrastructure Protection - Decision Support System (CIP-DSS) that provide actionable information to help protect U.S. critical infrastructure. (Retired plan measure.) |
| Program and Organization | Infrastructure and Geophysical - Science and Technology Directorate |
| Description | This measure reports the cumulative number of scenarios developed and stored in the Critical Infrastructure Protection-Decision Support System (CIP-DSS). The CIP-DSS provides a rational, scientifically-informed approach for prioritizing critical infrastructure protection strategies and resource allocations using modeling, simulation, and analyses to assess vulnerabilities, consequences, and risks; develop and evaluate protection, mitigation, response, and recovery strategies and technologies; and provide real-time support to decision makers during crises and emergencies. This measure demonstrates the availability of actionable information to help protect the U.S.'s critical infrastructure from acts of terrorism, natural disasters, and other emergencies. |
| Scope | The Critical Infrastructure Protection - Decision Support System (CIPDSS) program has defined standards that signal the completion of a modeling capability of specific scenario. The measure examines the total number of completed scenarios. |
| Data Source | The Critical Infrastructure Protection - Decision Support System generates reports for each scenario that is analyzed. |
| Collection Method | Analysis is performed on the output of each model, and a report is generated by the analysts within the National Laboratory consortium. Official copies of the reports are delivered to the DHS Program Manager. |
| Reliability | Reliable |
| How Data is Verified | The DHS S&T Directorate and the CIPDSS Team verify the resultant data via different methods depending upon the analyses performed. These methods vary from detailed technical review by internal and external Subject Matter Experts, comparison against similar studies and analysis against real-world events. In more recent analyses, the CIPDSS team has begun to use parameter sensitivity and uncertainty analyses for more prominent studies, resulting in a better understating of the tipping points that modeled space and regions that may require better data or more analyses. Issues identified by the S&T Directorate are brought to the CIPDSS Team and resolution is either sought or determined to be inappropriate or unnecessary. |

| | |
|---|---|
| Performance Measure | Percent of milestones that are met, as established in the fiscal year’s budget execution plan. |
| Program and Organization | Infrastructure and Geophysical - Science and Technology Directorate |
| Description | The program has established a set of milestones that are necessary for achieving the goals and objectives of the program. These milestones are presented in the program’s portion of the Science and Technology (S&T) Directorate’s fiscal year budget execution plan, which details the allocation of dollars and projected accomplishments for the year. |
| Scope | The scope encompasses the approved programmatic and technical milestones for all Directorate programs and projects. |
| Data Source | The S&T Directorate’s Enterprise Portfolio Management Initiative (EPMI) database is the designated repository for all project-level planning and actual status information. Its purpose is to provide ready access to individual and aggregate project data for reporting, planning, status reviews and analysis. |
| Collection Method | Project managers update EPMI milestone data on at least a quarterly basis from project status reports provided by performers, and from personal knowledge of project management status that can be objectively corroborated by artifacts such as signed documents. |

| | |
|---|---|
| Reliability | Reliable |
| How Data is Verified | The percent reported is reviewed using the status of funding, the number of milestones stated in the execution plan, and the explanation that is provided in each quarterly performance data call. Division Directors review the data submitted by Program Managers to ensure accuracy/consistency, approve the status and submit to the S&T Strategy, Policy and Budget/Chief Financial Officer's Office. Information is verified by the Directorates financial officers and additional information is requested of programs if discrepancies occur. |

| | |
|---|---|
| Performance Measure | Percent of milestones that are met, as established in the fiscal year's budget execution plan. |
| Program and Organization | Innovation - Science and Technology Directorate |
| Description | The program has established a set of milestones that are necessary for achieving the goals and objectives of the program which focuses on Homeland Innovative Prototypical Solutions (HIPS) and High Impact Technology Solutions (HITS). These milestones are presented in the program's portion of the Science and Technology (S&T) Directorate's fiscal year budget execution plan, which details the allocation of dollars and projected accomplishments for the year. The majority of the projects initiated within Innovation are high-risk and therefore the target is appropriate for this type of research. |
| Scope | The scope encompasses the approved programmatic and technical milestones for all Directorate programs and projects. |
| Data Source | The S&T Directorates Enterprise Portfolio Management Initiative (EPMI) database is the designated repository for all project-level planning and actual status information. Its purpose is to provide ready access to individual and aggregate project data for reporting, planning, status reviews and analysis. |
| Collection Method | Project managers update EPMI milestone data on at least a quarterly basis from project status reports provided by performers, and from personal knowledge of project management status that can be objectively corroborated by artifacts such as signed documents. |
| Reliability | Reliable |
| How Data is Verified | The percent reported is reviewed using the status of funding, the number of milestones stated in the execution plan, and the explanation that is provided in each quarterly performance data call. Division Directors review the data submitted by Program Managers to ensure accuracy/consistency, approve the status and submit to the S&T Strategy, Policy and Budget/Chief Financial Officer's Office. Information is verified by the Directorates financial officers and additional information is requested of programs if discrepancies occur. |

| | |
|---|---|
| Performance Measure | Percent of milestones that are met, as established in the fiscal year's budget execution plan. |
| Program and Organization | Laboratory Facilities - Science and Technology Directorate |
| Description | The program has established a set of milestones that are necessary for achieving the goals and objectives of the program. These milestones are presented in the program's portion of the Science and Technology (S&T) Directorate's fiscal year budget execution plan, which details the allocation of dollars and projected accomplishments for the year. |
| Scope | The scope encompasses the approved programmatic and technical milestones for all Directorate programs and projects. |
| Data Source | The S&T Directorates Enterprise Portfolio Management Initiative (EPMI) database is the designated repository for all project-level planning and actual status information. Its purpose is to provide ready access to individual and aggregate project data for reporting, planning, status reviews and analysis. |
| Collection Method | Project managers update EPMI milestone data on at least a quarterly basis from project status reports provided by performers, and from personal knowledge of project management status that can be objectively corroborated by artifacts such as signed documents. |

| | |
|---|---|
| Reliability | Reliable |
| How Data is Verified | The percent reported is reviewed using the status of funding, the number of milestones stated in the execution plan, and the explanation that is provided in each quarterly performance data call. Division Directors review the data submitted by Program Managers to ensure accuracy/consistency, approve the status and submit to the S&T Strategy, Policy and Budget/Chief Financial Officers office. Information is verified by the Directorates financial officers and additional information is requested of programs if discrepancies occur. |

| | |
|---|---|
| Performance Measure | Number of Department of Homeland Security official technical standards introduced per year. |
| Program and Organization | Testing and Evaluation and Standards - Science and Technology Directorate |
| Description | This measure gauges the number of standards introduced for adoption by the Department of Homeland Security per year. Note that not all standards that are introduced are adopted. The Standards Council and our working groups identify standards and examine their suitability for adoption. Only those standards with clear requirements and applicability are adopted. |
| Scope | The range of data includes the total number of standards introduced for adoption in a fiscal year. Standards are submitted to the Office of Standards for adoption by the DHS Standards Council throughout the year. The standards cover the full range of homeland security needs. The standards can come from within the Science and Technology (S&T) Directorate, other parts of DHS. The S&T Directorate chartered and currently operates the DHS Standards Council. |
| Data Source | DHS S&T Standards Working groups or Components within DHS submit an adoption form via memorandum to the DHS Standards Council recommending adoption. The official adoption form is the data source used to identify the number received by the Council. |
| Collection Method | The data (adoption forms) will be collected by the Office of Standards and tracked by the operational lead, the S&T Directorate, who manages, stores, and monitors using an internal database for standards. |
| Reliability | Reliable |
| How Data is Verified | The Standards Program Manager (from the S&T Directorate) and staff review the database and cross - reference with the official Council minutes that record how many forms are submitted. |

| | |
|---|---|
| Performance Measure | Percent of milestones that are met, as established in the fiscal year's budget execution plan. |
| Program and Organization | Testing and Evaluation and Standards - Science and Technology Directorate |
| Description | The program has established a set of milestones that are necessary for achieving the goals and objectives of the program. These milestones are presented in the program's portion of the Science and Technology (S&T) Directorate's fiscal year budget execution plan, which details the allocation of dollars and projected accomplishments for the year. |
| Scope | The scope encompasses the approved programmatic and technical milestones for all Directorate programs and projects. |
| Data Source | The S&T Directorate's Enterprise Portfolio Management Initiative (EPMI) database is the designated repository for all project-level planning and actual status information. Its purpose is to provide ready access to individual and aggregate project data for reporting, planning, status reviews and analysis. |
| Collection Method | Project managers update EPMI milestone data on at least a quarterly basis from project status reports provided by performers, and from personal knowledge of project management status that can be objectively corroborated by artifacts such as signed documents. |
| Reliability | Reliable |
| How Data is Verified | The percent reported is reviewed using the status of funding, the number of milestones stated in the execution plan, and the explanation that is provided in each quarterly performance data call. Division Directors review the data |

| | |
|---|---|
| | submitted by Program Managers to ensure accuracy/consistency, approve the status and submit to the S&T Strategy, Policy and Budget/Chief Financial Officer's Office. Information is verified by the Directorates financial officers and additional information is requested of programs if discrepancies occur. |

| | |
|---|---|
| Performance Measure | Percent of standards introduced that are adopted by Department of Homeland Security and partner agencies. |
| Program and Organization | Testing and Evaluation and Standards - Science and Technology Directorate |
| Description | This measure reports the percentage of standards and protocols for products, services, and systems that are adopted by the Department and its partner agencies, thus ensuring high levels of effectiveness among the technologies and capabilities end users need to detect and prevent terrorist attacks, means of terrorism, and other illegal activities. |
| Scope | Adopted standards are those that have been introduced (formally submitted) and have received formal approval from the DHS Standards Council or other Federal agencies. |
| Data Source | The sources for the data include Office of Standards, the DHS Standards Council and other relevant standards bodies (e.g., Interagency Council on Standards Policy which coordinates Federal standards), who have adopted the standards developed by this program. The performance data will be collected regularly. The DHS Standards council meets on a monthly basis and decides whether to adopt the standards submitted over the past month. This data provides information necessary for the reporting of this measure. |
| Collection Method | The S&T Directorates Standards Office maintains the Standards database, whose purpose is to maintain and track the development, recommendation and adoption of standards. |
| Reliability | Reliable |
| How Data is Verified | The Standards Program Manager (from the Science and Technology Directorate) and staff review the database and cross-reference with the official Council minutes that record how many standards were formally adopted. |

| | |
|---|---|
| Performance Measure | Percent of milestones that are met, as established in the fiscal year's budget execution plan. |
| Program and Organization | Transition - Science and Technology Directorate |
| Description | The program has established a set of milestones that are necessary for achieving the goals and objectives of the program. These milestones are presented in the program's portion of the Science and Technology (S&T) Directorate's fiscal year budget execution plan, which details the allocation of dollars and projected accomplishments for the year. |
| Scope | The scope encompasses the approved programmatic and technical milestones for all Directorate programs and projects. |
| Data Source | The S&T Directorates Enterprise Portfolio Management Initiative (EPMI) database is the designated repository for all project-level planning and actual status information. Its purpose is to provide ready access to individual and aggregate project data for reporting, planning, status reviews and analysis. |
| Collection Method | Project managers update EPMI milestone data on at least a quarterly basis from project status reports provided by performers, and from personal knowledge of project management status that can be objectively corroborated by artifacts such as signed documents. |
| Reliability | Reliable |
| How Data is Verified | The percent reported is reviewed using the status of funding, the number of milestones stated in the execution plan, and the explanation that is provided in each quarterly performance data call. Division Directors review the data submitted by Program Managers to ensure accuracy/consistency, approve the status and submit to the S&T Strategy, Policy and Budget/Chief Financial Officer's Office. Information is verified by the Directorates financial officers and additional information is requested of programs if discrepancies occur. |

| | |
|---|---|
| Performance Measure | Percent of SAFETY Act applications that have been processed and feedback provided to applicant when package has been disapproved. |
| Program and Organization | Transition - Science and Technology Directorate |
| Description | As part of the Homeland Security Act of 2002, Public Law 107-296, Congress enacted the SAFETY (Support Anti-Terrorism by Fostering Effective Technologies) Act to provide certain protections for sellers of qualified anti-terrorism technologies and others in the supply and distribution chain. Specifically, the SAFETY Act creates certain liability limitations for claims arising out of, relating to, or resulting from an act of terrorism where qualified anti-terrorism technologies have been deployed. This measure indicates the percent of applications for which the Department granted liability protection out of all those evaluated. This liability protection helps to encourage the development of effective technologies aimed at preventing, detecting, identifying, or deterring acts of terrorism, or limiting the harm that such acts might otherwise cause. |
| Scope | The range of data includes the total number of full SAFETY Act applications received by the Science and Technology Directorate. |
| Data Source | The source of the data will be from the www.safetyact.gov web site, where all full applications are stored. Applications are submitted electronically and via U.S. mail. Each application is given a unique identifier and is tracked electronically. |
| Collection Method | The measurement data is collected from the website, reviewed, and reported in an Excel spreadsheet. |
| Reliability | Reliable |
| How Data is Verified | The information is captured through the website (www.safetyact.gov) designed specifically for application processing and information. The website "feeds" the information to the programs business process management software system. From this system, various weekly reports are generated in hard copy, which are reviewed and verified by the Program Director. |

| | |
|---|---|
| Performance Measure | Number of Science, Technology, Engineering, and Mathematics (STEM) students supported. (New performance plan measure for FY 2008.) |
| Program and Organization | University Programs - Science and Technology Directorate |
| Description | The number of the Science, Technology, Engineering, and Mathematics (STEM) students supported may include undergraduates, graduate students, and post-docs. The University Centers can make the awards for scholars and fellowships in their disciplinary areas. The University Centers of Excellence are mission-focused University consortiums that leverage the multi-disciplinary capabilities of Universities to address the DHS needs. |
| Scope | The range of data includes scholarships, fellowships and internships for undergraduate and graduate students as well as postdoctoral awards. |
| Data Source | The data source will be the numbers of students supported with University Programs funds. The Scholars and Fellows Programs and select MSI Programs are administered by Oak Ridge Institute for Science and Education (ORISE). ORISE will provide semi-annual updates to University Programs on the number of STEM students. University Programs also awards grants directly to academic institutions to provide scholarships and fellowships to STEM students. Participating Colleges and universities will provide annual updates on the number of students supported. |
| Collection Method | University Programs will track and maintain the data on supported students based on the reports submitted by ORISE and the participating universities. On a quarterly basis, University Programs will respond to the Department's data call on status. Note that most awards are made annually based on the academic calendar. The program will run the reports from Education Measures tracking tool. |
| Reliability | Reliable |
| How Data is Verified | The Deputy Director of University Programs will review and validate the quarterly reports. |

| | |
|---|---|
| Performance Measure | Percent of milestones that are met, as established in the fiscal year's budget execution plan. |
| Program and Organization | University Programs - Science and Technology Directorate |
| Description | The program has established a set of milestones that are necessary for achieving the goals and objectives of the program. These milestones are presented in the program's portion of the Science and Technology (S&T) Directorate's fiscal year budget execution plan, which details the allocation of dollars and projected accomplishments for the year. |
| Scope | The scope encompasses the approved programmatic and technical milestones for all Directorate programs and projects. |
| Data Source | The S&T Directorates Enterprise Portfolio Management Initiative (EPMI) database is the designated repository for all project-level planning and actual status information. Its purpose is to provide ready access to individual and aggregate project data for reporting, planning, status reviews and analysis. |
| Collection Method | Project managers update EPMI milestone data on at least a quarterly basis from project status reports provided by performers, and from personal knowledge of project management status that can be objectively corroborated by artifacts such as signed documents. |
| Reliability | Reliable |
| How Data is Verified | The percent reported is reviewed using the status of funding, the number of milestones stated in the execution plan, and the explanation that is provided in each quarterly performance data call. Division Directors review the data submitted by Program Managers to ensure accuracy/consistency, approve the status and submit to the S&T Strategy, Policy and Budget/Chief Financial Officer's Office. Information is verified by the Directorates financial officers and additional information is requested of programs if discrepancies occur. |

| | |
|---|---|
| Performance Measure | Percent of peer review adjectival ratings on University Programs' management and research and education programs that are "very good" or "excellent." (Retired plan measure.) |
| Program and Organization | University Programs - Science and Technology Directorate |
| Description | The percent of those Department-funded University research, development, and education programs through the Centers of Excellence that are reviewed each year by relevant experts, and are rated as very good or excellent for quality, relevance, and effectiveness, to ensure that operational end users will have the technology and capabilities they need to detect and prevent terrorist attacks, means of terrorism, and other illegal activities in the future. |
| Scope | External expert panels will assess all University Programs on a rotating basis and rate them on quality, relevance, and effectiveness. At a minimum, experts will review each Center of Excellence by the end of its second full year of inception. |
| Data Source | The external reviewers provide their results to the University Programs office. The University Programs office collects all input and tracks internally. |
| Collection Method | The program will compile the summary ratings of the review panel for the programs under evaluation in a given fiscal year. The data is compiled within a spreadsheet within the University Programs office. The office creates a report based on the data. |
| Reliability | Reliable |
| How Data is Verified | Internal verification procedures have been established to ensure the ratings are reported accurately. The Director of University Programs reviews the data and the report and verifies the final scoring and percent of peer review adjectival ratings. |

## Transportation Security Administration

| | |
|---|---|
| Performance Measure | Baggage security screening assessment results. (New performance plan measure for FY 2008.) |
| Program and Organization | Aviation Security - Transportation Security Administration |
| Description | This measures the percentage of the time that Transportation Security Officers (TSO's) correctly identify prohibited material in baggage during covert tests, in order to reduce the probability of a successful terrorist or other criminal attack to the air transportation system. The target and actual results are classified and are not releasable to the public at this time for security reasons. |
| Scope | Covert tests for baggage screening at the baggage security screening checkpoints of the Nation's commercial airports are conducted by Transportation Security Administration (TSA) in an unannounced systematic manner at select airports that are tested multiple times. The covert tests are designed to evaluate whether screeners properly identify prohibited items placed in the traveler's baggage, and whether the screeners follow Standard Operating Procedures until the issues are fully resolved. |
| Data Source | Data is reported into the Online Learning Center monthly by each airport. |
| Collection Method | Observational data is collected during special operation covert tests using rigorous standard operating procedures to introduce up-to-date, real life, terrorist threat objects to the screener workforce to identify vulnerabilities. |
| Reliability | Reliable |
| How Data is Verified | Post-test reviews are conducted by all special operation teams on classified reports. These reports are issued to senior TSA management and identify reasons for failure and recommend corrective action. |

| | |
|---|---|
| Performance Measure | Level of public confidence in the ability of the flight crew to keep air travel secure and to defend the aircraft and its passengers from individuals with hostile intentions (as measured on a scale of 1-5). (Retired plan measure.) |
| Program and Organization | Aviation Security - Transportation Security Administration |
| Description | The annual Bureau of Transportation Statistics (BTS) Omnibus Survey is an annual household survey used to measure customer satisfaction and confidence of transportation systems. Participants are randomly selected by the Department of Transportation using a statistical model. The survey is administered to the American public, and response is voluntary. Selected participants who choose to provide feedback will provide insight into the public's confidence of transportation systems. The scores range from 1 to 5, with 5 representing total confidence. Confidence in the flight crew is an indication that the training program is improving aviation security by adding another layer of protection. |
| Scope | The Department of Transportation (DOT) collects random nationwide telephone survey data. A statistically significant sample is collected and responses are weighted and analyzed. The survey is administered to the American public, and response is voluntary. Selected participants who choose to provide feedback will provide insight into the public's confidence of transportation systems. |
| Data Source | The Bureau of Transportation Statistics, DOT, conducts an annual statistically valid randomly selected household telephone survey. |
| Collection Method | The DOT uses standard survey methodology. After computing the data, DOT provides the data to TSA on a CD-ROM, at which point TSA analyzes the data to compile a trend analysis report. The BTS Omnibus Survey data is expected every April of the following year. |
| Reliability | Reliable |
| How Data is Verified | The questions have been psychometrically validated and the information validated by DOT and provided to TSA on a CD-ROM for analysis. |

| | |
|---|---|
| Performance Measure | Passenger security screening assessment results. (New performance plan measure for FY 2008.) |
| Program and Organization | Aviation Security - Transportation Security Administration |
| Description | This measures the percentage of the time that passenger Transportation Security Officers (TSO's) correctly identify prohibited material during covert tests, in order to reduce the probability of a successful terrorist or other criminal attack to the air transportation system. The target and actual results are classified for security reasons and are not releasable to the public at this time. |
| Scope | The Passenger Screening Test measure is a compilation of measures that show the effectiveness of Transportation Screening Officers (TSO) to detect a variety of possible threats to aviation security hat are presented at the Security Screening Checkpoint. These threats include guns, knives, and IEDs among others. |
| Data Source | Data is reported into the Online Learning Center monthly by each airport. |
| Collection Method | Tests are administered by Transportation Security Administration (TSA) staff, specifically Screening Managers and/or Training Coordinators at each airport. The test item is inserted into the start of the passenger screening process and its progress monitored through the system. A successful test is obtained when the test item is correctly identified at each stage of the screening process. Any other result is a failure. |
| Reliability | Reliable |
| How Data is Verified | Data is provided to the TSA Office of Inspections for analysis and further independent review. |

| | |
|---|---|
| Performance Measure | Percent level in meeting Federal Air Marshal Service (FAMS) coverage target for each individual category of identified risk. |
| Program and Organization | Aviation Security - Transportation Security Administration |
| Description | This measure reflects the performance levels of Office of Law Enforcement, Federal Air Marshal Service (OLE/FAMS) coverage of targeted critical flights based upon impact (geographical location), vulnerability (aircraft destructive potential), threats, and intelligence relative to the availability of resources. Coverage is provided by specially trained armed law enforcement officers referred to as Federal Air Marshals (FAMs). These FAMs are deployed to fly missions on commercial U.S. aircraft for both domestic and international flights that have been identified as Targeted Critical Flights under 10 individual risk categories that are found in the OLE/FAMS Concept of Operations. Coverage is provided using a risk-based management approach for mission planning. |
| Scope | Coverage is provided using a risk-based management approach for mission planning. Coverage is provided to those flights that have been identified as Targeted Critical Flights for deployment under 10 individual risk categories that were identified in the FAMS Concept of Operations (CONOPS). Specific information related to the identification of these risk categories, targeted coverage and the resources needed to provide this coverage is classified. |
| Data Source | Data is obtained from the FAMS AirCrew Database. |
| Collection Method | The Systems Operations Control Division (SOCD) automated scheduling system employs aviation industry accepted Semi- Automated Business Reservation Environment (SABRE) systems that archive all information on the Targeted Critical Flights covered on a daily basis. On a monthly basis (or as needed) the SOCD accesses the SABRE database through SQL queries and Crystal Reports to identify FAMS performance in both scheduling and flying missions on each cover level of the Targeted Critical Flights. Calculation: Total missions divided by total critical flights for each of 10 risk categories; expressed as a percentage of target goals, then combined into a single overall metric. The range is the deviation between the max and minimum of the 10 individual risk categories, with a smaller range being preferable. |
| Reliability | Reliable |
| How Data is Verified | Data in support of this measure is closely monitored by FAMS management and the OLE/FAMS Office of Flight Operations. FAMS senior managers/leadership |

| | |
|---|---|
| | reviews the previous month's performance by the 5th of each month and validates the coverage levels, and/or provides guidance on any actions that should be taken to increase any performance measure if deemed appropriate. In addition, FAMS procedures require ongoing quality control steps that include monthly validation checks of between 400 and 500 randomly selected individual flights by Headquarters personnel auditors to validate a reported FAM coverage on a targeted critical flight. |

| | |
|---|---|
| Performance Measure | Percent of air carriers in compliance with leading security indicators. (New performance plan measure for FY 2008.) |
| Program and Organization | Aviation Security - Transportation Security Administration |
| Description | This measure identifies overall air carrier compliance with leading security indicators. A leading security indicator is a key indicator, that, when taken into account, may be predictive of the overall security posture of an air carrier (these critical indicators are derived from criteria based on factors like a single point of failure, operational vs. administrative, human factors related). The indicators are guided by security rules, regulations, and standards. Identifying compliance with the key indicators assesses air carrier vulnerabilities. Assessing air carrier vulnerabilities is part of an overall risk reduction process, as in measuring compliance with standards as a strong indicator of system security. |
| Scope | In support of risk-based approach to regulatory oversight, the data demonstrates percent compliance over all critical prompt response to the leading security indicators for air carriers Nation-wide. The critical air carrier inspection prompts are defined as part of FY 2007 Inspection Plan. |
| Data Source | Information obtained from the Performance and Results Analysis System (PARIS), which serves as the official source of data repository for the Office of Compliance's Regulatory activities. |
| Collection Method | Inspectors enter reports into PARIS. Headquarters personnel then compile quarterly reports of these inspection records. Calculation: The quotient of (in compliance critical prompt response total) divided by (total of in- and not-in-compliance critical prompt response from approved air carrier inspections (begun during the reporting period)). The total is multiplied by 100 to gain percent compliance. |
| Reliability | Reliable |
| How Data is Verified | Data is entered and stored in the Performance and Results Information System (PARIS). Headquarters personnel conduct data reviews of randomly selected records. |

| | |
|---|---|
| Performance Measure | Percent of airports in compliance with leading security indicators. (New performance plan measure for FY 2008.) |
| Program and Organization | Aviation Security - Transportation Security Administration |
| Description | This measure identifies overall airport compliance with leading security indicators. A leading security indicator is a key indicator, that, when taken into account, may be predictive of the overall security posture of an airport (these critical indicators are derived from criteria based on factors like a single point of failure, operational vs. administrative, human factor related). The indicators are guided by security rules, regulations, and standards. Identifying compliance with the key indicators assesses airport vulnerabilities. Assessing airport vulnerabilities is part of an overall risk reduction process, as in measuring compliance with standards as a strong indicator of system security. |
| Scope | In support of a risk-based approach to regulatory oversight, the data demonstrates percent compliance over all critical indicator/prompt responses to the leading security indicators for airports. The critical airport inspection prompts are defined as part of FY 2007 Inspection Plan; however, the data is collected based on current critical prompts identified as part of the Domestic Port Inspections conducted nationwide. |
| Data Source | Information obtained from the Performance and Results Analysis System |

| | |
|---|---|
| | (PARIS), which serves as the official source of data repository for the Office of Compliance's Regulatory activities. |
| Collection Method | Inspectors enter reports into PARIS. Headquarters personnel then compile quarterly reports of these inspection records. Calculation: The quotient of (in compliance critical prompt response total) divided by (the total of in - and not in compliance critical prompt response totals from approved airport inspections (begun during the reporting period)). The total is multiplied by 100 to gain percent compliance. |
| Reliability | Reliable |
| How Data is Verified | Data is entered and stored in the Performance and Results Information System (PARIS). Headquarters personnel conduct data reviews of randomly selected records. |

| | |
|---|---|
| Performance Measure | Percentage of screeners scoring above the national standard level of Threat Image Projection (TIP) performance. (Retired plan measure.) |
| Program and Organization | Aviation Security - Transportation Security Administration |
| Description | The Transportation Security Administration (TSA) established a standard level of TIP performance. The measure reflects the percentage of screeners performing above the standard. Transportation Security Officers (TSOs) receive ongoing training and performance assessments to ensure that their skills are being developed to address the variety of threats that may be presented. As threats change and evolve, the TIP program develops new images and training to address the expanded needs of the TSO workforce, allowing TSA to maintain a high level of screener performance that ensures aviation security. As threats change and evolve, the TIP program develops new images and training to address the expanded needs of the TSO workforce, allowing TSA to maintain a high level of screener performance that ensures aviation security. |
| Scope | This measure includes data from TSOs who view at least 50 x-ray projections per month |
| Data Source | Data is obtained through TIP, a component of every x-ray machine in operation at every federalized airport. TIP projects threat images, including images of guns, knives, and explosives, onto bags as they are screened during actual operations. TSOs are responsible for identifying the threat image and calling for the bag to be searched. Once prompted, TIP identifies to the screener whether the threat is real and then records the TSO's performance in a database that could be analyzed for performance trends. |
| Collection Method | Every federalized airport uploads data monthly to the TIP database server for compilation. The data is then consolidated and imported to an Oracle database for analysis by TSA. |
| Reliability | Reliable |
| How Data is Verified | TIP Image Presentation data and daily counts of images are monthly aggregated against monthly data files to ensure internal consistency. |

| | |
|---|---|
| Performance Measure | Percent of Mass Transit agencies that are in full compliance with industry agreed upon standards to improve security. (New performance plan measure for FY 2008.) |
| Program and Organization | Surface Transportation Security - Transportation Security Administration |
| Description | The program assesses and evaluates the security posture of the mass transit and passenger rail modes through the Baseline Assessment for Security Enhancement (BASE) program. Security assessments commenced during FY 2007 with a focus on the 50 largest mass transit and passenger rail agencies based on passenger volume, which carries 75 percent of mass transit rail volume. The BASE program assesses security posture in comprehensive Security and Emergency Management Action Items, including security plans, training, exercises, public awareness, and other specific security areas. The Action Items encompass activities and measures that are critical to an effective security program. Security Inspectors conduct the assessments in partnership with the mass transit and passenger rail agencies' |

| | |
|---|---|
| | security chiefs and directors. The results of the security assessments inform development of risk mitigation programs and resource allocations, most notably security grants. |
| Scope | The BASE program assessments are voluntary, so the scope of data is limited to the 50 largest participating mass transit agencies, based on passenger volume. Transit agencies are defined as mass transit, light rail, passenger rail, buses, and other commuter transit systems. The BASE results reports, maintained by the program and the assessed mass transit agencies, contain comprehensive information on each of the Security and Emergency Management Action Item areas that make up the BASE evaluation. The timing on the data collection effort is a limiting factor since the program's Transportation Security Inspectors (TSIs) are working in support of several modes (Mass Transit, Passenger Rail and Freight Rail). Also, mitigation efforts are largely tied to the Transit Security Grant program (TSGP). BASE results inform priorities of the TSGP and mass transit and passenger rail systems apply the results to inform preparation of project requests under the TSGP. TSGP awards generally trail assessment program results by approximately 1 year. |
| Data Source | TSIs conduct the assessments in partnership with the mass transit and passenger rail agencies' security chiefs and directors. The TSIs are also involved in documenting the assessment results (by placing the information in a central data base on the Transportation Security Administration (TSA) computer system), which is in turn analyzed across the spectrum by staff members at TSA Headquarters. The data is then collated to determine certain trends and weaknesses within the Security and Emergency Management Action Item areas. Initial participation in the assessments and data collection efforts has been strong – 56 assessments have been completed overall, covering 45 of the top 50 agencies. |
| Collection Method | The TSIs conduct the BASE assessments alongside members of the transit system being assessed. This process can take a few days up to a few weeks, depending on the system's size. The TSI team works through each of the assessment categories and determines the overall score using a 5-point scale from 0 to 4. TSIs use a standard checklist to ensure that each transit system is assessed and scored using the same criteria. Once all assessment areas are compiled, the transit system is briefed on the outcome and provided the complete report. This data then gets compiled along with the other systems that have been assessed to produce overall national results in each Action Item category. This result leads to the analysis of weak and strong areas, not only of the individual systems, but also of the collective mass transit and passenger rail mode nationally. TSA-assisted assessments will be repeated approximately every 18-24 months to measure progress in the enhancement of security. |
| Reliability | Reliable |
| How Data is Verified | The data that is reported to TSA Headquarters by the TSIs who actually conducted the assessment after briefing the assessed mass transit or passenger rail agency on the results. TSIs use a common, standard checklist during the assessment process. A consistency check to correct variations between individual TSIs has been completed. The report is reviewed for quality by senior TSI Program staff, then made available to TSA Mass Transit staff for review. These processes may result in inquiries to the appropriate inspectors for clarifying information. Ultimately, results are maintained by individual agency as well as consolidated into a national report of security posture in the Security and Emergency Management Action Items. Analysis for strengths and weaknesses, consistency or divergence from other agencies, trends, and smart practices are derived from these qualitative reviews. |

| | |
|---|---|
| Performance Measure | Percent of national critical surface transportation assets or systems that have been assessed. (Retired plan measure.) |
| Program and Organization | Surface Transportation Security - Transportation Security Administration |
| Description | This measure indicates the increase in risk information available for use in reducing risk to the surface transportation sector. The risk information is used by owner/operators of transportation systems to manage risk more effectively, or by government agencies to identify common risks and best practices to be addressed by standards. The assets and systems on the “Top 100” nationally critical surface transportation assets and systems list are assessed for vulnerability and mitigation measures developed. The assessments are conducted by or on behalf of, or are accepted by, Transportation Security Administration (TSA) and other Federal agencies, who share summary information among themselves and with the owner-operators of the transportation systems that are assessed. |
| Scope | The universe consists of all surface assets and systems listed on the Top 100 nationally critical Transportation Assets List (which contains well over 100 listings, including aviation as well as surface-mode assets and systems). The list is used as a starting place to assess the top transportation assets and systems. Each year additional assessments of items listed in the Top 100 are conducted. The Top 100 list was revised in spring 2007, per Executive Order. The new number of items in the Top 100, i.e., the denominator of this percentage, may change. |
| Data Source | The data source is assessments of transportation assets and systems conducted by or on behalf of, or are accepted by, both TSA and various other Federal agencies. Assessments may consist of, but are not limited to, site visits and field examinations. TSA tracks assessments and information is shared within Federal agencies through mechanisms such as participation in the Federal Risk Assessment Working Group (FRAWG). Sponsored by DHS Science and Technology, FRAWG is a federal risk assessment information clearinghouse that shares information about completed assessments through meetings and a web site that memorializes the assessment date and location information. |
| Collection Method | TSA collects data from its own assessments as well as from assessments conducted by or on behalf of, or accepted by, other federal agencies. |
| Reliability | Reliable |
| How Data is Verified | TSA periodically contacts representatives of various organizations, both inside of and external to TSA, to discuss with them what transportation assessment activities have been conducted These assessment activities are then reported on the master Top 100 assessments list provided to TSA leadership. |

| | |
|---|---|
| Performance Measure | Percent reduction in risk from toxic inhalation hazard bulk cargoes in rail transportation. (New performance plan measure for FY 2008.) |
| Program and Organization | Surface Transportation Security - Transportation Security Administration |
| Description | The Toxic Inhalation Hazard (TIH) Risk Reduction Program strives to reduce the risk posed by TIH materials, the most toxic chemicals transported by rail in the U.S., including chlorine and anhydrous ammonia. Through a partnership with American and Canadian railroads, Transportation Security Administration (TSA) gathers railcar movement data, focusing on the time a loaded rail car is standing unattended in a DHS-designated High Threat Urban Area (HTUA). This period of time is referred to as "dwell time". TSA uses a risk calculation comprised of four elements: 1) the amount of "dwell time" in hours; 2) the specific HTUA; 3) the Population Proximity Factor; and 4) whether the car is attended or unattended. The level of risk will be compared to the baseline risk level, which is calculated from the period prior to the adoption of TSA/Department of Transportation issued Security Action Items developed to enhance the security of TIH shipments. |
| Scope | Railroad carriers provide car movement data on all railcar traffic which includes time and location to Railinc Corp., an information clearing house wholly owned by the Association of American Railroads (AAR). At no cost, Railinc transmits the car movement data on loaded TIH cars to a TSA third party contractor. The |

| | |
|---|---|
| | contractor verifies, validates, and provides risk analysis of the data to TSA. The contractor also provides the end product, which includes risk scores and percent change. The "attended status" variable is not an actual but a projection from a random sample consisting of 1,400 inspections in 2007 performed by TSA inspectors. |
| Data Source | Railroad carriers currently provide car movement data to Railinc for ordinary business purposes. The contractor validates the car movement data to determine number of “dwell time” hours. TSA provides the contractor with variables including the HTUA score and the PPF value. HTUAs are identified using DHS's Urban Area Security Initiative data. The HTUA score is a value between one and five using a logarithmic scale based on the population within a specific HTUA. The PPF value is between one and three and captures the population density within a one-mile radius of an unattended TIH railcar in a HTUA. The attended/unattended percentage is based on a sample size of 1,400 inspections conducted in 2007 by TSA rail inspectors on field visits to verify the reported attended/unattended status on a sample of TIH railcars. The contractor then compiles the data and calculates the final risk reduction score. The data is stored and maintained by the contractor. |
| Collection Method | Railroad carriers provide car movement data which includes time and location to Railinc Corp., an information clearing house wholly owned by the Association of American Railroads (AAR). At no cost, Railinc transmits the car movement data on loaded TIH cars to a TSA third party contractor. The contractor verifies, validates, and provides risk analysis of the data to TSA. Currently, the TSA contractor is working to comply with information security requirements so it is not processing risk information. TSA receives validated and verified information from the contractor via CD-ROM and incorporates all risk information into an excel spreadsheet and tabulates the risk information itself. |
| Reliability | Reliable |
| How Data is Verified | TSA inspects the status of TIH cars for attended/unattended for risk purposes which also validates the accuracy of data. These inspections are performed on a sample of the identified TIH rail cars. The TSA contractor verifies the accuracy of the data provided by Railinc by identifying anomalies and inconsistencies and verifying them with the specific rail carrier. |

| | |
|---|---|
| Performance Measure | Percent of customers satisfied with the intelligence products provided. (New performance plan measure for FY 2008.) |
| Program and Organization | Transportation Security Support - Transportation Security Administration |
| Description | This measure shows the overall level of customer satisfaction with intelligence products produced and disseminated by the program. |
| Scope | The scope of these data is each satisfaction survey question is scored as a percentage of the total number of surveys received quarterly, and the customer satisfaction score represents the percentage of respondents who agree and strongly agree with the statement, “Overall I am satisfied with this product.” |
| Data Source | The source of these data is the TSA Office of Intelligence Customer Satisfaction Survey. |
| Collection Method | The calculation of satisfaction is derived by tabulating the responses to our Customer Satisfaction Survey. For January 2007, satisfaction is based on the percentage of yes (positive) responses. Beginning in February 2007, the percentage is based on percentage of respondents who agree or strongly agree with the statement, “Overall I am satisfied with this product.” |
| Reliability | Reliable |
| How Data is Verified | These data records are considered reliable. |

| | |
|---|---|
| Performance Measure | Percentage of systems certified based on Federal Information System Management Act (FISMA), as accepted by DHS and accredited as designated by CIO. (Retired plan measure.) |
| Program and Organization | Transportation Security Support - Transportation Security Administration |
| Description | This measure ensures that all IT systems are certified and able to provide quality support to the Nation's transportation systems. A certified IT system undergoes a security accreditation, which is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. |
| Scope | The data calculation is based on an aggregation of 11 certification values which includes: Federal Information Processing Standard (FIPS) 199, contingency plan and testing, privacy impact assessment, e-authentication, risk assessment, system security plan, security testing and evaluation plan, security assessment report, Authorization to Operate (ATO) letter, and annual assessments. This measure includes all operational Transportation Security Administration (TSA) systems. |
| Data Source | TSA updates a DHS database called the DHS Trusted Agent Federal Information System that contains all of the information derived from an aggregation of 11 certification values and related information. |
| Collection Method | Data is obtained by TSA Information Systems Security Officers (ISSOs) through the certification accreditation process which is entered into the DHS Trusted Agent Federal Information System Management Act (FISMA) application. A DHS database called the DHS Trusted Agent Federal (TAF) Information System provides continuous updates. The number of systems that pass 11 criteria (Sensitive But Unclassified (SBU) artifacts) divided by the number of systems operational yields the percentage of systems certified based on the FISMA, as accepted by DHS and accredited as designated by the TSA CIO. |
| Reliability | Reliable |
| How Data is Verified | Data is based upon the successful fulfillment of FIPS 199, contingency plan and testing, privacy impact assessment, e-authentication, risk assessment, system security plan, security testing and evaluation plan, security assessment report, ATO letter and annual assessments. Performance is based on National Institute of Standards and Technology (NIST) standards. |

| | |
|---|---|
| Performance Measure | Percent of individuals undergoing a Transportation Threat Assessment and Credentialing (TTAC) security threat assessment (STA). |
| Program and Organization | Transportation Threat Assessment and Credentialing - Transportation Security Administration |
| Description | This measure indicates the percentage of TTAC's total defined population that is receiving an STA. Thorough vetting will decrease vulnerabilities of sensitive transportation systems by limiting access of potentially dangerous individuals who are identified by TTAC vetting and credentialing programs. The populations currently include international flight crews, aviation workers, hazardous material drivers, and non-U.S. citizens receiving flight instruction at the Federal Aviation Administration's (FAA) certified flight schools in the U.S. and abroad. In the future, TTAC programs will also cover domestic airline passengers, surface and maritime workers. |
| Scope | Data is collected detailing the number of new individuals vetted and the number of individuals perpetually vetted for all functional vetting programs. TTAC's total defined population receiving an STA currently includes international flight crews, aviation workers, hazardous material drivers, and non-U.S. citizens receiving flight instruction at the Federal Aviation Administrations (FAA) certified flight schools in the U.S. and abroad. |
| Data Source | Classified Reports and monthly vetting and credentialing data. This data source is a classified database maintaining vetting and credentialing monthly report data and assessments. |
| Collection Method | Each TTAC program details and reports through Transportation Security |

| | |
|---|---|
| | Administration's (TSA) Management Review metrics reporting process the number of individuals vetted. For each program, vetting is a process in which individuals are cleared as able to access the transportation system and are therefore not considered a threat. The assessment of vetting programs may come from the existing programs such as HAZMAT, Alien Flight Student Pilot (AFSP), Crew Vetting (CV) and, Registered Traveler (RT) and other vetting programs.<br>Calculation: The percent of individuals attempting to gain access to the transportation system that are vetted by a TTAC program. |
| Reliability | Reliable |
| How Data is Verified | Data collected reports the number of individuals vetted by each program, and is closely monitored by TTAC and is reported monthly in TSA's Management Review metrics report. |

## United States Citizenship and Immigration Services

| | |
|---|---|
| Performance Measure | Actual cycle time to process form I-129 (Petition for Nonimmigrant Worker). |
| Program and Organization | Adjudication Services - United States Citizenship and Immigration Services |
| Description | This measure reports the average amount of time it takes for U.S. Citizenship and Immigration Services (USCIS) to provide a decision regarding an I-129, Petition for Nonimmigrant Worker, that an employer has filed to petition for an alien to come to the U.S. temporarily as a nonimmigrant worker. |
| Scope | This measure includes all pending I-129 Forms received by USCIS that are pending determination. |
| Data Source | Automated counts and manual case counts, which are reported monthly through the automated Performance Analysis System (PAS) database. |
| Collection Method | On a monthly basis, USCIS collects performance data on applications received, completed, and pending through its 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. |
| Reliability | Reliable |
| How Data is Verified | The USCIS Operations Planning Division, Performance Management Branch conducts monthly data reconciliation and review activities to maximize the integrity of the data reported. USCIS uses PAS and CLAIMS data on a daily basis. In addition, the Director meets regularly with the Director of the Performance Management Division and senior agency managers to review performance on backlog elimination and reducing case cycle times, and to provide direction for future activities. Executive staff meetings, at which cycle time data and any existing/projected backlogs are often discussed, are held weekly. Performance information is used in conjunction with other data, such as application receipts and revenue projections, to manage and plan for future staffing and workload requirements, and inform decisions in other areas of USCIS operations. |

| | |
|---|---|
| Performance Measure | Actual cycle time to process form N-400 (Application for Naturalization). |
| Program and Organization | Adjudication Services - United States Citizenship and Immigration Services |
| Description | This measure reports the amount of time it takes to make a decision on an N-400, Application for Naturalization. In FY 2007, the target increased from 6 months to 7 months to allow the oath to occur in jurisdictions where it is administered by the U.S. District Courts. |
| Scope | The scope includes all pending N-400 Forms, excluding those forms that have been exempted due to circumstances beyond United States Citizenship and Immigration Services (USCIS) control. Cases are removed from the backlog calculation if the applicant has failed the English/Civics requirement and is waiting the statutory period between testing attempts, 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, which are reported monthly through the automated Performance Analysis System (PAS) database. |
| Collection Method | On a monthly basis, USCIS collects performance data on applications received, completed, and pending through its 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. |
| Reliability | Reliable |
| How Data is Verified | The USCIS Operations Planning Division, Performance Management Branch conducts monthly data reconciliation to maximize the integrity of the data reported. USCIS uses PAS and CLAIMS data on a daily basis. In addition, the Director meets regularly with the Director of the Performance Management Division and senior agency managers to review performance on backlog elimination and reducing case cycle times, and to provide direction for future activities. Executive staff meetings, at which cycle time data and any existing/projected backlogs are often discussed, are held weekly. Performance information is used in conjunction with other data, such as application receipts and revenue projections, to manage and plan for future staffing and workload requirements, and inform decisions in other areas of USCIS operations. |

| | |
|---|---|
| Performance Measure | Actual cycle time to process form I-485 (Application to Register for Permanent Residence or to Adjust Status). |
| Program and Organization | Adjudication Services - United States Citizenship and Immigration Services |
| Description | The average amount of time it takes to provide a decision regarding an I-485, Application to Adjust Status. |
| Scope | The scope includes all pending I-485 Forms, excluding those forms that have been exempted due to circumstances beyond United States Citizenship and Immigration Services (USCIS) control. Applications for which no visa number is available are considered pending, but not part of the backlog. Cases are also removed from the backlog calculation 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, which are reported monthly through the automated Performance Analysis System (PAS) database. |
| Collection Method | On a monthly basis, USCIS collects performance data on applications received, completed, and pending through its 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. |
| Reliability | Reliable |
| How Data is Verified | The USCIS Operations Planning Division, Performance Management Branch, conducts monthly data reconciliation and review activities to maximize the integrity of the data reported. USCIS uses PAS and CLAIMS data on a daily basis. In addition, the Director meets regularly with the Director of the Performance Management Division and senior agency managers to review performance on backlog elimination and reducing case cycle times, and to provide direction for future activities. Executive staff meetings are held weekly. Performance information is used in conjunction with other data, such as application receipts and revenue projections, to manage and plan for future staffing and workload requirements, and inform decisions in other areas of USCIS operations. |

| | |
|---|---|
| Performance Measure | Percent of asylum reform referrals (at local offices) completed within 60 days of receipt. |
| Program and Organization | Adjudication Services - United States Citizenship and Immigration Services |
| Description | Asylum is a form of protection that allows refugees to remain in the U.S. Before asylum was reformed in 1995, applicants could obtain work authorization simply by filing for asylum, which made the system vulnerable to abuse. Since asylum reform, work authorization is obtained only if asylum is granted or no negative decision has been made within 180 days. If the United States Citizenship and Immigration Services (USCIS) finds an applicant ineligible for asylum and the applicant is not in valid/legal status, USCIS refers the application to an immigration judge for final determination in the course of removal proceedings. Immigration courts require approximately 120 days to complete adjudications. To meet the 180 day threshold for a decision, USCIS aims to refer 75 percent of ineligible applications to immigration courts within 60 days of filing. Recognizing that some cases should be exempt due to their complexity or the unavailability of staff at certain times, the program has exempted 25 percent of its workload from this requirement. |
| Scope | All asylum reform referrals received at all local offices are the basis for this measure. The data represent the percentage of the total asylum reform referrals that local offices complete within 60 days. This data is limited by staffing shortages and case complexities that require the office to exempt 25 percent of its referral pool from consideration. |
| Data Source | RAPS - The Refugees, Asylum, and Parole System is an Integrated Data Base Management System/Relational (IDMS/R) resident on a mainframe computer at the Justice Data Center - Dallas. |
| Collection Method | Asylum Officers update RAPS with their decision on an I-589 Asylum claim. RAPS calculates the date the case is filed to the date a Notice to Appear (NTA) is served, minus any delays caused by the applicant. RAPS generates a weekly, monthly, and annual report that measures the timeliness of case processing by asylum officers by separating out those cases referred to the Immigration Judge within 60 days, from those cases referred to the Immigration Judge in more than 60 days. |
| Reliability | Reliable |
| How Data is Verified | Supervisors at each of the eight Asylum Offices are responsible for verifying the accuracy of data. Current policy requires 100 percent supervisory review of system entries. |

| | |
|---|---|
| Performance Measure | Number of Significant Citizenship Outreach Events. (New performance plan measure for FY 2008.) |
| Program and Organization | Citizenship - United States Citizenship and Immigration Services |
| Description | This measure describes the number of significant outreach events designed to support immigrant integration. These actions serve a multitude of purposes to assist in accomplishing this goal, such as educating immigrants and encouraging their civic integration, informing stakeholders about the Office’s mission and the importance of promoting civic integration, educating counterparts from outside the U.S. government about Federal integration efforts, and bringing on new partners to help encourage integration. Significant outreach events include conferences, ceremonies, meetings, media appearances, trainings, and presentations. Outreach efforts encourage immigrants to become more integrated into American civic culture. |
| Scope | The frequency of outreach actions across the country. The Office of Citizenship budget cannot accommodate travel to every event to which it may be invited to make a presentation or attend. |
| Data Source | The data is from a weekly report prepared in Headquarters. |
| Collection Method | The Offices WIC Report is compiled weekly. Events mentioned in the WIC Report (in the Top Projects Accomplished (Past Week)) section) which fall under the previously defined category of significant outreach action will be totaled up, |

| | |
|---|---|
| | and the number will be marked on an internally maintained EXCEL spreadsheet. The total number of significant outreach actions for each quarter (13 weeks) will then be turned in. |
| Reliability | Reliable |
| How Data is Verified | To ensure reliability and quality control, the Office of Citizenship will implement a supervisory review of the weekly WIC Report of activity, and the quarterly report on the number of outreach actions. |

| | |
|---|---|
| Performance Measure | Percent of targeted language populations with access to citizenship educational materials in their native language. |
| Program and Organization | Citizenship - United States Citizenship and Immigration Services |
| Description | The percent of targeted language populations with online access to "Welcome to the United States: A Guide for New Immigrants" in their native language. This guide contains information to help immigrants settle into life in the U.S., and basic civics information that introduces immigrants to the U.S. system of government. The guide gives immigrants tips on getting involved in their communities, meeting their responsibilities, and exercising their rights as permanent residents. First distributed in English in 2004, the guide is now available in 11 languages (English, Spanish, Chinese, Vietnamese, Korean, Russian, Arabic, Tagalog, Portuguese, French, and Haitian Creole). Outreach to three additional populations (speakers of Polish, Urdu, and Basic Literacy English) is planned through FY 2009. This measure is used as a proxy outcome due to the economic and logistic difficulties associated with using a more direct outcome measure, such as level of community involvement and volunteerism. |
| Scope | The number of targeted languages into which the new immigrant guide (Welcome to the United States: A Guide for New Immigrants) has been translated and made available to the public, calculated by dividing the number of targeted languages into which the guide has been translated and made available by the total number of targeted languages. The list of targeted languages available to the public is available at www.uscis.gov under Resources for New Immigrants. |
| Data Source | The United States Citizenship and Immigration Services (USCIS) Office of Citizenship tracks the inventory of targeted languages available to the public. The inventory is stored on a spreadsheet and is maintained by the Headquarters Office. |
| Collection Method | The program keeps an inventory on a spreadsheet of both the total number of targeted languages and the number of languages into which the guide has been translated and made available to the public. As a new guide is published, the section in charge within USCIS updates the spreadsheet. |
| Reliability | Reliable |
| How Data is Verified | The list of targeted languages available to the public is available at www.uscis.gov under Resources for New Immigrants. |

| | |
|---|---|
| Performance Measure | Number of immigration application form types where procedure and/or legislative changes are proposed to counteract fraud. (Retired plan measure.) |
| Program and Organization | Immigration Security and Integrity - United States Citizenship and Immigration Services |
| Description | The number of types of immigration transactions where proposed procedural or legislative changes have been offered in order to combat fraud as a result of the fraud assessments that have been conducted. These fraud assessments help to ensure the security and integrity of the immigration system by identifying needed improvements to procedures or legislation. |
| Scope | Cases accepted over the previous six months will be selected using a random sampling formula provided by DHS Office of Immigration Statistics. The Benefit Fraud Assessment (BFA) sampling size of 230-260 cases for each form type will be determined from a Rate of Occurrence not more than 20 percent, confidence level of 95 percent, and reliability factor of +/- 5 percent. Fraud Detection and National Security (FDNS) Information Officers and Intelligence Research Specialists will determine if the BFA cases reach the minimum threshold of fraud, |

| | |
|---|---|
| | defined as entailing any manifestations that amount to an assertion not in accordance with the facts, an untrue statement of fact, or an incorrect/false representation of material to the adjudication of the application/petition. |
| Data Source | Benefit Fraud Assessment final reports in which the Office of Fraud Detection and National Security (FDNS) manually documents and tracks proposed policy, procedural and legislative changes. Tracking of proposed procedural and/or legislative changes to counteract fraud are a result of Benefit Fraud Assessments. If a proposal requires a change to USCIS policy, a memorandum is written for the internal memorandum clearance process. If a proposal involves regulatory change, it goes through the proposed rule process. |
| Collection Method | Through the FDNS data system, FDNS collects and tracks leads and cases of suspected and validated fraud through referral to ICE and return to USCIS for final adjudication. The annual and quarterly performance data reported will be based on the number of cases in the FDNS data system compared to the number of applications in the Computer Linked Application Information Management System and the Refugees, Asylum, and Parole System for certain form types for the same period. This will provide a statistically valid estimate of the amount of fraud present in these form types as the cases identified in the BFA were determined in a statistically valid manner, as described in the Scope section. |
| Reliability | Reliable |
| How Data is Verified | There is one hundred percent review of all determinations and proposed procedural and/or legislative changes by the program headquarters. |

| | |
|---|---|
| Performance Measure | Percent of fraud cases found in conducting Benefit Fraud Assessments on USCIS form types. (Retired plan measure.) |
| Program and Organization | Immigration Security and Integrity - United States Citizenship and Immigration Services |
| Description | The Office of Fraud Detection and National Security conducts Benefit Fraud Assessments (BFA) using statistically random samplings of immigration form types, pulled from pending and completed cases, that historically have been identified as fraud prone or high risk-oriented. BFA results are used to develop and propose procedural and legislative changes to counteract fraud. This measure is being used to assess administrative functionality, and will be changed in the future to assess the marginal effect that procedural and/or legislative changes, resulting from the BFA's, have had on the fraud rate for the various form types. |
| Scope | Cases accepted over the previous six months will be selected using a random sampling formula provided by DHS Office of Immigration Statistics. The Benefit Fraud Assessment (BFA) sampling size of 230-260 cases for each form type will be determined from a Rate of Occurrence not more than 20 percent, confidence level of 95 percent, and reliability factor of +/- 5 percent. Fraud Detection and National Security (FDNS) Information Officers and Intelligence Research Specialists will determine if the BFA cases reach the minimum threshold of fraud, defined as entailing any manifestations that amount to an assertion not in accordance with the facts, an untrue statement of fact, or an incorrect/false representation of material to the adjudication of the application/petition. |
| Data Source | The Office of Fraud Detection and National Security (FDNS) tracks proposed procedural and/or legislative changes to counteract fraud as a result of Benefit Fraud Assessments. Internal manual tracking is used to document proposed changes made in BFA final reports. If a proposal requires a change to United States Citizenship and Immigration Services (USCIS) policy, a memorandum is written for the internal memorandum clearance process. If a proposal involves regulatory change, it goes through the proposed rule process. |
| Collection Method | All data collection and analysis will be reviewed by Headquarter FDNS to ensure uniformity and consistency, and to make the final determination on each inquiry. The FDNS data system will facilitate tracking of leads and cases of suspected and validated fraud through referral to ICE, and return to USCIS for final adjudicative decision. The quarterly reporting of performance will be based on the number of |

| | |
|---|---|
| | cases in the FDNS data system compared to the number of applications in the Computer Linked Application Information Management System and the Refugees, Asylum, and Parole System for certain form types for the same period. Since cases identified in the BFA were determined in a statistically valid manner, this will provide a statistically valid estimate of the amount of fraud present in these form types. FDNS will expand the BFA process to additional form types in future years, and will also expand data mining capabilities to help immediately identify suspect applications and petitions. |
| Reliability | Reliable |
| How Data is Verified | 100 percent review of all determinations and proposed procedural and/or legislative changes by Headquarters FDNS, as well as coordination and approval of cognizant USCIS offices and other agencies involved and/or affected. |

| | |
|---|---|
| Performance Measure | Percent of suspected fraud leads where the principal application/petition is ultimately denied. (New performance plan measure for FY 2008.) |
| Program and Organization | Immigration Security and Integrity - United States Citizenship and Immigration Services |
| Description | This measure assesses the proportion of suspected fraudulent petitions/applications that are verified as fraudulent by the Office of Fraud Detection and National Security (FDNS) or Immigration & Customs Enforcement (ICE), and ultimately denied. When the United States Citizenship and Immigration Services (USCIS) field adjudicators determine that applications/petitions may be fraudulent, the files are forwarded to FDNS. After the initial review by FDNS, if administrative investigation is validated, a lead is opened and FDNS conducts additional research. When the results of the research indicate that prosecutorial and/or administrative investigation is warranted, a case is opened and an investigation is conducted, either by ICE or FDNS. Results are provided to the adjudicator handling the application/petition for use in final determination to grant or deny the benefit. |
| Scope | FDNS will collect disposition data (approved/denied) on 100 percent of all cases. |
| Data Source | The Fraud Detection and National Security Data System (FDNS-DS). This system was designed to provide a central repository of fraud lead/case data available to FDNS staff nationwide. Developed under the guidance and management of the USCIS OCIO, the FDNS-DS is a web-based application that employs the Siebel Public Sector COTS product and resides on an Oracle database platform. |
| Collection Method | Data associated with all validated referrals to FDNS are entered into FDNS DS. Currently, this is done manually. After the Administrative Investigation is conducted, a finding is sent back to the adjudicator to make a final decision. The final decision is then entered into FDNS DS. |
| Reliability | Reliable |
| How Data is Verified | Methods to verify the reliability are being finalized by the program. |

| | |
|---|---|
| Performance Measure | Percent of E-Verify employment eligibility verification queries that required manual review that are later resolved as "Employment Authorized." |
| Program and Organization | Immigration Status Verification - United States Citizenship and Immigration Services |
| Description | Immigration status and employment eligibility verification data is collected in the Verification Information System (VIS) from departmental databases. VIS also has access to the Social Security Administration (SSA) Numident database, which houses Social Security Number (SSN) information. This measure tracks the data completeness of the VIS system by reviewing the percentage of E-Verify Tentative Non-confirmations and DHS Verifications In Process responses that resolve as Employment Authorized, instead of immediately resolving as Employment Authorized through the Automated VIS System, without the need for manual review by an Immigration Status Verifier (ISV). The ISV determines if USCIS has granted employment authorization status. The more complete the VIS |

| | |
|---|---|
| | data, the less likely a query forwarded for manual review will later resolve as Employment Authorized. Data completeness results in more efficient program operation and faster overall response time to employers. |
| Scope | The scope of this measure is all inquiries into the Employment Eligibility Verification Program (EEV), which provides an automated link to federal databases to help employers determine employment eligibility of new hires and the validity of their Social Security numbers. |
| Data Source | Status and employment eligibility verification data is collected in the Verification Information System (VIS). VIS has three components: 1) the Customer Processing System (CPS) - used by Federal, State, and local government agencies to perform electronic immigration status verification for non-citizens applying for benefits/licenses; 2) the Employment Eligibility Verification program - used by employers participating in the EEV program to verify the employment eligibility of all newly hired employees; and 3) the Status Verification System (SVS) - used by ISVs to respond to automated additional verification requests and to log manual G-845 requests and responses. |
| Collection Method | The USCIS Verification Division has developed Verification Information System reports, which are generated monthly to provide data needed to report on these measures. |
| Reliability | Reliable |
| How Data is Verified | The Verification Information System (VIS) keeps an audit trail of all initial and additional verification requests. When an initial verification is performed, VIS keeps a record of who did the query, what date/time the query was done, and what information was provided back to the user agency/employer including the system message. When a user agency/employer submits an additional verification request, VIS keeps a record of who submitted the request, the date/time the request was submitted, the information provided by the user agency, the Immigration Status Verifier who responded to the request, the date/time they responded to the request, and the response provided back to the user agency. The process is automated and the data used to report on the measures is generated from the VIS audit trail records. |

| | |
|---|---|
| Performance Measure | Percent of Systematic Alien Verification for Entitlements (SAVE) queries requiring manual review that are later resolved as lawful status. |
| Program and Organization | Immigration Status Verification - United States Citizenship and Immigration Services |
| Description | Immigration status data is collected in the Verification Information System (VIS) departmental databases. This measure tracks the data completeness of the VIS system by reviewing the percentage of verification queries that are submitted by Federal, State, and local government benefit granting agencies to which the VIS system has responded with "Request for Additional Verification," and the ISV has verified the applicant's lawful status, instead of the status being automatically verified through the VIS system. The more complete the VIS data, the less likely a query forwarded for manual review will later resolve as having lawful status. Data completeness results in more efficient program operation and faster overall response time to benefit and license providers. |
| Scope | The SAVE program enables Federal, State, and local government agencies to obtain immigration status information they need in order to determine an applicant’s eligibility for many public benefits for lawful immigrants. The scope of this measure is all of the inquiries that require manual information to be included in the Verification Information System for determination and response. An Immigration Status Verifier (ISV) manually reviews requests from Federal, State and local government benefit-granting agencies when the VIS system responds to an automated request from such agencies for information on applicants eligibility for public benefits and licenses with Request for Additional Verification. This measure assesses the completeness of the Verification Information System information. |

| | |
|---|---|
| Data Source | Status and employment eligibility verification data is collected in the Verification Information System (VIS). VIS has three components: 1) the Customer Processing System (CPS) - used by Federal, state, and local government agencies to perform electronic immigration status verification for non-citizens applying for benefits/licenses; 2) the Employment Eligibility Verification program - used by employers participating in the EEV program to verify the employment eligibility of all newly hired employees; and 3) the Status Verification System (SVS) - used by ISVs to respond to automated additional verification requests and to log manual G - 845 requests and responses. |
| Collection Method | The USCIS Verification Division has developed Verification Information System reports, which are generated monthly to provide data needed to report on these measures. |
| Reliability | Reliable |
| How Data is Verified | The Verification Information System (VIS) keeps an audit trail of all initial and additional verification requests. When an initial verification is performed, VIS keeps a record of who did the query, what date/time the query was done, and what information was provided back to the user agency/employer including the system message. When a user agency/employer submits an additional verification request, VIS keeps a record of who submitted the request, the date/time the request was submitted, the information provided by the user agency, the Immigration Status Verifier who responded to the request, the date/time they responded to the request, and the response provided back to the user agency. The process is automated and the data used to report on the measures is generated from the VIS audit trail records. |

| | |
|---|---|
| Performance Measure | Customer satisfaction rate with USCIS phone centers. |
| Program and Organization | Information and Customer Service - United States Citizenship and Immigration Services |
| Description | Percentage of people who obtained immigration services and benefits information from United States Citizenship and Immigration Services (USCIS) over the telephone, who have indicated satisfaction with the service they received. On a monthly basis, USCIS selects a random group of customers who have called the phone centers. A contracted company with expertise in conducting phone surveys then calls each customer and conducts a survey to rate their overall experience with the service received from the USCIS phone center. A standardized USCIS and General Accountability Office approved survey tool is used to collect customer responses. This satisfaction rate measures our performance in providing timely, consistent, and accurate information regarding immigration services and benefits to immigrants, U.S. employers, and the American public over the telephone. |
| Scope | This measure is based on a service-wide random sample of customers (approximately 900 each quarter) who have called the USCIS phone centers to obtain immigration services and benefits information. Based on the data collected, the margin of error for the actual results is calculated. |
| Data Source | Responses to phone survey of a random sample of customers. |
| Collection Method | Source data is collected from a telecommunications network that captures telephone numbers of all customers calling the 800-line. Upon contact by contracted employees, responses are input into a database which houses current and historical responses allowing for trending and analysis of data for accuracy. |
| Reliability | Reliable |
| How Data is Verified | The Information and Customer Service Division is responsible for verifying data reliability. Reliability of the data is checked by trending data against previous quarterly data collected. Significant changes in levels of performance may reflect a need to validate responses. |

## United States Coast Guard

| | |
|---|---|
| Performance Measure | Federal aids to navigation availability. (New performance plan measure for FY 2008.) |
| Program and Organization | Aids to Navigation (AtoN) - United States Coast Guard |
| Description | This measure is an indicator of U.S. Coast Guard Waterways Management Program ability to maintain its Aids to Navigation system functionality; which is a key contributor in the prevention of adverse navigation outcomes that can result in disruptions to maritime commerce. |
| Scope | The measure is the hours short range Aids to Navigation were available as a percent of total hours they were expected to be 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), which published *Recommendations on Availability Objectives of Aids to Navigation Services, IALA Recommendation O-130* in December 2004. |
| 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. |
| Collection Method | 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. 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. Temporary changes to the short-range Aids to Navigation System are not considered discrepancies. This was not the case prior to the August 2005 deployment of the I-ATONIS system. |
| Reliability | Reliable |
| How Data is Verified | I-ATONIS discrepancy data entry is generally complete when the database is accessed. To ensure consistency and integrity, data entry is limited to specially trained personnel in each District. The application itself contains embedded Help screens. Additionally, quality control and data review is completed through Coast Guard and National Ocean Service processes of generating local Notices to Mariners, as well as by designated Unit and District personnel. |

| | |
|---|---|
| Performance Measure | Five-year average number of Collisions, Allisions, and Groundings (CAG). |
| Program and Organization | Aids to Navigation (AtoN) - United States Coast Guard |
| Description | The mission of the U.S. Coast Guard's Waterways Management program is to manage, influence, and provide access to a safe, secure, efficient and environmentally sound waterways system. Several statutes clearly link the various components (Navigation Systems, Marine Transportation System services, and Bridge Administration) back to this mission. The program facilitates maritime commerce by minimizing disruptions to the movement of goods and people, while maximizing recreational enjoyment and environmentally sound use of navigable waters, all while maintaining robust waterway restoration capabilities when disruptions do occur. |
| Scope | The measure is the sum of all distinct Collision, Allision, and Grounding (CAG) events involving commercial vessels operating on U.S. navigable waters. A five-year average is used to show the long-term trend. 46 CFR 4.05-10 requires the owner, agent, master, operator or person in charge to notify the U.S. Coast Guard of any occurrence involving a vessel that results in a CAG. Because some reports are delayed in reaching the U.S. Coast Guard, published data is subject to revision. |
| Data Source | Notices of Marine casualties are recorded in the U.S. Coast Guard’s Marine Information for Safety and Law Enforcement (MISLE) database. |
| Collection Method | Only Investigations recorded in the U.S. Coast Guard’s MISLE database of |

| | |
|---|---|
| | reported collision, allision, and grounding incidents in U.S. waters involving commercial vessels are counted. Collision, allision, and grounding incidents not involving a commercial vessel such as a collision between two recreational vessels are excluded. Only distinct events are counted. A collision incident in U.S. waters between two or more vessels, at least one of which is not a recreational boat, is counted as a distinct collision event. An allision incident involving one or more commercial vessels, as might be the case for a tug and several barges in tow, is counted as a distinct allision event. A grounding incident involving one or more commercial vessels, as might be the case for a tug and several barges in tow, is counted as a distinct grounding event. |
| Reliability | Reliable |
| How Data is Verified | 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. 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. |

| | |
|---|---|
| Performance Measure | Defense readiness of patrol boats. (New performance plan measure for FY 2008.) |
| Program and Organization | Defense Readiness - United States Coast Guard |
| Description | This measure is the percent of time that the number of units called for in combatant commander operational plans are ready at SORTS category 2 or better. |
| Scope | In this measure, U.S. Coast Guard patrol boats are measured against the requirements of Department of Defense operational plans. The data includes readiness information about the unit's people (such as training and billet - fill), equipment (physical operating condition), and health of its supplies and logistics - in essence, all pertinent information that could bear on a unit's war-fighting capability. No pertinent data is excluded. Data is always current; the automated collection system is required to be updated immediately upon a change in readiness. There are no limitations (with regard to timeliness, completeness, or accuracy, etc.) to using this data for measurement purposes. |
| Data Source | The measure's data source is the Navy Status of Resources and Training System (SORTS) database, which is populated in the field by carefully-reviewed submissions from each unit's commanding officer. |
| Collection Method | Electronically; the data is uploaded by every applicable U.S. Coast Guard unit via an automated system. |
| Reliability | Reliable |
| How Data is Verified | Data obtained from the Status of Readiness and Training System (SORTS) is maintained by the Department of Defense. The U.S. Coast Guard ensures the accuracy of the data by subjecting it to multiple levels of review. All SORTS reports must be personally approved by each unit's commanding officer; the data is uploaded by a highly structured and automated system which minimizes data entry errors. Furthermore, the U.S. Coast Guard publishes "Credibility and Consistency Criteria", enclosure 9 to COMDTINST 3501.2H, which outlines the procedures by which SORTS data is verified. |

| | |
|---|---|
| Performance Measure | Defense readiness of Port Security Units (PSUs). (New performance plan measure for FY 2008.) |
| Program and Organization | Defense Readiness - United States Coast Guard |
| Description | This measure is the percent of time that the number of units called for in combatant commander operational plans are ready at SORTS category 2 or better. |
| Scope | In this measure, U.S. Coast Guard port security units are measured against the requirements of Department of Defense operational plans. The data includes readiness information about the unit's people (such as training and billet-fill), equipment (physical operating condition), and health of its supplies and logistics - in essence, all pertinent information that could bear on a unit's war-fighting |

| | |
|---|---|
| | capability. No pertinent data is excluded. Data is always current; the automated collection system is required to be updated immediately upon a change in readiness. There are no limitations (with regard to timeliness, completeness, or accuracy, etc.) to using this data for measurement purposes. |
| Data Source | The measure's data source is the Navy Status of Resources and Training System (SORTS) database, which is populated in the field by carefully-reviewed submissions from each unit's commanding officer. |
| Collection Method | Electronically; the data is uploaded by every applicable U.S. Coast Guard unit via an automated system. |
| Reliability | Reliable |
| How Data is Verified | Data obtained from the Status of Readiness and Training System (SORTS) is maintained by the Department of Defense. The U.S. Coast Guard ensures the accuracy of the data by subjecting it to multiple levels of review. All SORTS reports must be personally approved by each unit's commanding officer; the data is uploaded by a highly structured and automated system which minimizes data entry errors. Furthermore, the U.S. Coast Guard publishes "Credibility and Consistency Criteria", enclosure 9 to COMDTINST 3501.2H, which outlines the procedures by which SORTS data is verified. |

| | |
|---|---|
| Performance Measure | Percent of time that Coast Guard assets included in the Combatant Commander Operational Plans are ready at a Status of Resources and Training System (SORTS) rating of 2 or better. |
| Program and Organization | Defense Readiness - United States Coast Guard |
| Description | Through the Defense Readiness program, the U.S. Coast Guard is prepared to provide core competencies such as Maritime Interception Operations; Port Operations Security and Defense; Military Environmental Response Operations; Peacetime Engagement; Coastal Sea Control Operations; and Theater Security Cooperation when requested by the Department of Defense. Selected U.S. Coast Guard forces participate in the Navy Status of Readiness and Training System assessment program and participate in combatant commander operations. |
| Scope | All (100 percent) of U.S. Coast Guard units that are designated by Department of Defense operational plans are measured. The data includes readiness information about the unit's people (such as training and billet-fill), equipment (physical operating condition), and health of its supplies and logistics - in essence, all pertinent information that could bear on a unit's war-fighting capability. No pertinent data is excluded. Data is always current; the automated collection system is required to be updated immediately upon a change in readiness. There are no limitations (with regard to timeliness, completeness, or accuracy, etc.) to using this data for measurement purposes. |
| Data Source | The measure's data source is the Navy Status of Resources and Training System (SORTS) database, which is populated in the field by carefully-reviewed submissions from each unit's commanding officer. |
| Collection Method | Electronically, the data is uploaded by every applicable U.S. Coast Guard unit via the automated SORTS System. The measure is determined by first compiling the individual average SORTS results for High Endurance Cutters, Patrol Boats, and Port Security Units. The three individual SORTS averages for each group are then averaged again (each given equal weight) to complete the measure. |
| Reliability | Reliable |
| How Data is Verified | Data obtained from the Status of Readiness and Training System (SORTS) is maintained by the Department of Defense. The U.S. Coast Guard ensures the accuracy of the data by subjecting it to multiple levels of review. All SORTS reports must be personally approved by each unit's commanding officer; the data is uploaded by a highly structured and automated system which minimizes data entry errors. Furthermore, the U.S. Coast Guard publishes "Credibility and Consistency Criteria", enclosure 9 to COMDTINST 3501.2H, which outlines the procedures by which SORTS data is verified. |

| | |
|---|---|
| Performance Measure | Removal rate for cocaine that is shipped via non-commercial maritime means. |
| Program and Organization | Drug Interdiction - United States Coast Guard |
| Description | The Drug Interdiction program reduces the supply of illegal drugs by denying smugglers the use of air and maritime routes by projecting a U.S. Coast Guard presence in and over the Caribbean Sea, Gulf of Mexico and Eastern Pacific Ocean. |
| Scope | This measure includes the amount of all cocaine physically seized/weighed (and assigned a Federal drug identification number) by the U.S. Coast Guard, as well as drugs intentionally destroyed by smugglers (and not physically recovered by the U.S. Coast Guard) while being pursued. Smugglers increasingly destroy contraband to avoid prosecution; including the total cocaine removed (vice just seizures) more accurately accounts for the program's effectiveness. The amount of cocaine destroyed/jettisoned during a smuggling event is determined externally to the U.S. Coast Guard through the Consolidated Counter - Drug Database (CCDB). CCDB uses intelligence information, video from pursuits, and jettisoned drugs relocated by interdiction units to determine the actual amount of drugs in a given load. Strict rules are employed to avoid inflating non-recoverable drug amounts. U.S. Coast Guard does not include seizures of other drugs (e.g., marijuana) in this measure, as cocaine is the predominant drug interdicted in the maritime transit zone. |
| Data Source | The non-commercial maritime flow component of this measure is provided by the IACM, which has U.S. Coast Guard representation. Since the IACM report is not available until several months after the end of the fiscal year (typically in the Summertime), only estimated performance results are available at the end of the fiscal year. Seizures (not the removal rate) are provided in various reports until the IACM is available later in the year, and can be used to compute the actual removal rate. |
| Collection Method | Both the "physically seized" and the "jettisoned or destroyed" components of this measure are tracked, collected, and analyzed by U.S. Coast Guard Headquarters' Office of Law Enforcement (CG-531). The IACM provides a flow range; the U.S. Coast Guard selects the midpoint of this range for the cocaine flow. For end of year reporting, the U.S. Coast Guard uses prior year flow information as a proxy for current year flow. Reported performance is updated with the latest IACM report. |
| Reliability | Reliable |
| How Data is Verified | Jettison, sunk and otherwise destroyed cocaine data is verified through the consolidated counter-drug data base run by the United States Interdiction Coordinator. U.S. Coast Guard Seizure data continues to be tracked and verified by Federal Drug Identification Numbers. The non-commercial maritime flow data continues to be provided by the annual ICAM report. Data may be reported as estimated because the maritime flow estimates are not available in time to calculate the removal rate for this report. When the flow rate becomes available the removal rate will be calculated and reported in the following years Report. |

| | |
|---|---|
| Performance Measure | Number of days critical waterways are closed due to ice. |
| Program and Organization | Ice Operations - United States Coast Guard |
| Description | This measure is an indicator of U.S. Coast Guard Icebreaking impact on preventing disruptions to maritime commerce due to ice. It is an indicator of the annual number of days critical Great Lakes waterways are closed—with the St. Mary’s River as the reference point. |
| Scope | The measure reports the annual number of days critical Great Lakes waterways are closed due to ice with the St. Mary’s River as the reference point. Closure day targets are performance standards negotiated with Great Lakes Marine Transportation System stakeholders, and are relative to winter severity. Those standards are two days in an average winter, and eight days in a severe winter. |
| Data Source | Data is obtained from U.S. Coast Guard field units, validated at the U.S. Coast Guard District level, and stored in an Excel spread - sheet after end - of - year |

| | |
|---|---|
| | reports are received at U.S. Coast Guard Headquarters |
| Collection Method | Closure days are field observations of the number of non-routine, critical waterway closures during the Winter navigation season. Districts identify which waterways are critical and evaluate classifications as necessary. Non-routine closures are closures other than those that occur every year when icebreaking operations become impractical. A closure is a period of 24 or more hours during which a waterway is closed by a Vessel Traffic Service or Captain of the Port, or blocked by a beset vessel. In keeping with House Joint Resolution 738; Section 112 (P.L. 99-500) of 18 October 1986, the Great Lakes navigation season ends 15 January each year. Results for this measure are closure days with the St. Mary's River as the reference point. |
| Reliability | Reliable |
| How Data is Verified | Data verification and validation is conducted through review of U.S. Coast Guard unit reports by U.S. Coast Guard Districts, and the Mobility and Ice Operations Office in U.S. Coast Guard Headquarters. |

| | |
|---|---|
| Performance Measure | Percent success rate in meeting requests for polar ice breaking. (New performance plan measure for FY 2008.) |
| Program and Organization | Ice Operations - United States Coast Guard |
| Description | Percentage of U.S. Coast Guard provided icebreaking support as requested by the National Science Foundation (NSF). |
| Scope | The performance metric for Polar Ice Operations is the percentage of NSF requests for ice breaking support met by the U.S. Coast Guard. U.S. Coast Guard activity in this mission ensures the mobility needed to achieve the scientific research and logistics replenishment desired by other agencies operating in the polar regions. |
| Data Source | NSF requests for icebreaking are taken from the annual meeting to "consider all national priorities" referred to in the U.S. Coast Guard/NSF Memorandum of Understanding dated August 2005. The amount of the requested icebreaking met is taken directly from the end of mission Summary of Operations Message. |
| Collection Method | NSF requests for icebreaking are taken from the annual meeting to "consider all national priorities" referred to in the U.S. Coast Guard/NSF Memorandum of Understanding dated August 2005. The amount of the requested icebreaking met is taken directly from the end of mission Summary of Operations Message. |
| Reliability | Reliable |
| How Data is Verified | The U.S. Coast Guard is developing an new index metric to better measure its polar ice operations. The U.S. Coast Guard has elected to utilize the historical polar ice mission outcome metric until the new index metric can be completed. Polar Ice operations play an important role in achieving effective control of our borders. |

| | |
|---|---|
| Performance Measure | Percent of fishermen complying with Federal regulations. |
| Program and Organization | Living Marine Resources (LMR) - United States Coast Guard |
| Description | This program's mission is to provide effective and professional at-sea enforcement to advance national goals for the conservation and management of LMR and their environments. The program's primary focus is to compel compliance with Federal fisheries and other LMR regulations on domestic fishing vessels. The program has a maritime stewardship nexus. This goal is accomplished through enforcement of Federal regulations that provide stewardship of living marine resources and their environments. The U.S. Coast Guard is the lead federal agency for at-sea enforcement of U.S. fisheries and marine protected species regulations. |
| Scope | 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 is also collected from the U.S. Coast Guard Law Enforcement Planning and Assessment System. |
| Collection Method | U.S. Coast Guard units enter their enforcement data directly into this database after completion of fisheries enforcement boardings. 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. |
| Reliability | Reliable |
| How Data is Verified | The Program Manager reviews entries into MISLE database monthly and compares to other sources of information (e.g., after-action reports, message traffic, etc.) to assess reliability of the database. Each year a compliance rate is calculated for the data quality. This is determined by dividing the total number of LMR boardings without a significant number of violations by the total number of LMR boardings. |

| | |
|---|---|
| Performance Measure | Five-year average number of chemical discharge incidents per 100 million short tons shipped. (New performance plan measure for FY 2008.) |
| Program and Organization | Marine Environmental Protection (MEP) - United States Coast Guard |
| Description | This measure is a lagging indicator of the U.S. Coast Guard's Marine Environmental Protection Program impact on the long-term trend of chemical discharge incidents. It is a simple moving average of U.S. Coast Guard investigated chemical discharge incidents into navigable waters of the United States for the current and four previous fiscal years, divided by the five-year average annual foreign and domestic short tons (100 million) of Chemical & Chemical Products shipped in U.S. waters. |
| Scope | Chemical spills exceeding reportable quantities in U.S. navigable waters from sources subject to U.S. Coast Guard jurisdiction. A five-year average is used to show the long-term trend. The U.S. Coast Guard has jurisdiction for spills into or upon navigable waters of the U.S, adjoining shorelines, the contiguous zone, Deepwater Ports, the Continental Shelf and other areas. 40 CFR 300 requires Vessel or facility operators to report any discharge any hazardous substance that equals or exceeds reportable quantities listed in 40 CFR 302. Because some reports are delayed in reaching the U.S. Coast Guard, published data is subject to revision. Shipping statistics are from the Army Corps of Engineers, and not generally available until December following the calendar year. Current values are projected from five years of past data. |
| Data Source | Investigations of reportable chemical discharge incidents are recorded in the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database. Shipping data is obtained from the U.S. Army Corps of Engineers, from information they use to compile their annual report of the Waterborne Commerce of the United States. |
| Collection Method | Only investigations recorded in the U.S. Coast Guard's MISLE database of reportable chemical discharge incidents into U.S. waters from maritime sources subject to U.S. Coast Guard jurisdiction are counted. Discharges onto land, into the air, or into enclosed spaces are excluded. Discharges from non-maritime sources such as aircraft, trucks and other vehicles, rail cars and rail equipment; U.S. Navy and other public vessels; fixed platforms and pipelines are excluded. Discharges from unspecified, unclassified, and unknown sources are also excluded. Shipping statistics from the Army Corps of Engineers are not generally available until December following the end of a calendar year. Current values are a forecast, based on a simple least - squares projection of the most recent five years of data. |
| Reliability | Reliable |

| | |
|---|---|
| How data is verified | 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. |

| | |
|---|---|
| Performance Measure | Five-year average number of chemical discharges and oil spills per 100 million short tons shipped. (Retired plan measure.) |
| Program and Organization | Marine Environmental Protection (MEP) - United States Coast Guard |
| Description | This measure is a lagging indicator of U.S. Coast Guard Marine Environmental Protection Program impact on the long-term trend of significant oil and chemical spills relative to their combined foreign and domestic shipping tonnage. It is a simple moving average of U.S. Coast Guard investigated chemical spills and oil spills greater than 100 gallons discharged into navigable waters of the United States for the current and four previous fiscal years, divided by the five-year average annual foreign and domestic short tons (100 million) of Oil & Oil Products and Chemical & Chemical Products shipped in U.S. waters |
| Scope | Chemical discharges exceeding reportable quantities and oil spills exceeding 100 gallons in U.S. navigable waters from sources subject to U.S. Coast Guard jurisdiction relative to tonnage. A five-year average is used to show the long-term trend. The U.S. Coast Guard has jurisdiction for spills into or upon navigable waters of the U.S, adjoining shorelines, the contiguous zone, Deepwater Ports, the Continental Shelf and other areas. 40 CFR 300 requires Vessel or facility operators to report any discharge of oil or oil products that cause a sheen, discoloration, sludge or emulsion; and any hazardous substance that equals or exceeds reportable quantities listed in 40 CFR 302. Because some reports are delayed in reaching the U.S. Coast Guard, published data is subject to revision, the greatest impact on recent quarters. Shipping statistics are from the Army Corps of Engineers, and not generally available until December following the calendar year. Current values are projected from five years of past data. |
| Data Source | Investigations of reportable chemical and oil discharge incidents are recorded in the U.S. Coast Guard’s Marine Information for Safety and Law Enforcement (MISLE) database. Shipping data is obtained from the U.S. Army Corps of Engineers, from information they use to compile their annual report of the Waterborne Commerce of the United States. |
| Collection Method | Only Investigations recorded in the U.S. Coast Guard’s MISLE database of reportable chemical spills and oil discharge incidents into U.S. waters from maritime sources subject to U.S. Coast Guard jurisdiction are counted. Discharges onto land, into the air, or into enclosed spaces are excluded. Discharges from non-maritime sources such as aircraft, trucks and other vehicles, rail cars and rail equipment; U.S. Navy and other public vessels; fixed platforms and pipelines are excluded. Discharges from unspecified, unclassified, and unknown sources are also excluded. Shipping statistics from the Army Corps of Engineers are not generally available until December following the end of a calendar year. Current values are a forecast, based on a simple least - squares projection of the most recent five years of data. |
| Reliability | Reliable |
| How Data is Verified | 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. 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. |

| | |
|---|---|
| Performance Measure | Five-year average number of oil spills per 100 million short tons shipped. (New performance plan measure for FY 2008.) |
| Program and Organization | Marine Environmental Protection (MEP) - United States Coast Guard |
| Description | This measure is a lagging indicator of the U.S. Coast Guard's Marine Environmental Protection Program impact on the long-term trend of significant oil spills. It is a simple moving average of Coast Guard investigated oil spills greater than 100 gallons discharged into navigable waters of the United States for the current and four previous fiscal years, divided by the five-year average annual foreign and domestic short tons (100 million) of Oil & Oil Products shipped in U.S. waters. |
| Scope | Oil spills exceeding 100 gallons in U.S. navigable waters from sources subject to U.S. Coast Guard jurisdiction. A five-year average is used to show the long-term trend. The U.S. Coast Guard has jurisdiction for spills into or upon navigable waters of the U.S, adjoining shorelines, the contiguous zone, Deepwater Ports, the Continental Shelf and other areas. 40 CFR 300 requires Vessel or facility operators to report any discharge of oil or oil products that cause a sheen, discoloration, sludge or emulsion. Because some reports are delayed in reaching the U.S. Coast Guard, published data is subject to revision. Shipping statistics are from the Army Corps of Engineers, and not generally available until December following the calendar year. Current values are projected from five years of past data. |
| Data Source | Investigations of reportable oil discharge incidents are recorded in the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database. Shipping data is obtained from the U.S. Army Corps of Engineers, from information they use to compile their annual report of the Waterborne Commerce of the United States. |
| Collection Method | Only Investigations recorded in the U.S. Coast Guard's MISLE database of reportable oil discharge incidents into U.S. waters from maritime sources subject to U.S. Coast Guard jurisdiction are counted. Discharges onto land, into the air, or into enclosed spaces are excluded. Discharges from non - maritime sources such as aircraft, trucks and other vehicles, rail cars and rail equipment; U.S. Navy and other public vessels; fixed platforms and pipelines are excluded. Discharges from unspecified, unclassified, and unknown sources are also excluded. Shipping statistics from the Army Corps of Engineers are not generally available until December following the end of a calendar year. Current values are a forecast, based on a simple least - squares projection of the most recent five years of data. |
| Reliability | Reliable |
| How data is verified | 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. |

| | |
|---|---|
| Performance Measure | Percent of oil removed or otherwise mitigated as compared to the amount of oil released for reported spills of 100 gallons or more. (New performance plan measure for FY 2008.) |
| Program and Organization | Marine Environmental Protection (MEP) - United States Coast Guard |
| Description | This measure takes into account all methods used to remediate an oil spill from impacting the environment, and thus includes the amount of oil mechanically removed from both the water and shore, dispersed, in situ burned, or evaporated. This is a new metric that will be baselined starting the third quarter of FY 2008 when the mechanisms are in place to properly collect the data. Since collection points for all data sets will not be available until then, the targets for FY 2008 and FY 2009 are estimates only and will be refined once sufficient trend data can be analyzed. |

| | |
|---|---|
| Scope | Oil spills of 100 gallons or more spilled in the U.S. navigable waters is where the U.S. Coast Guard has jurisdiction. The U.S. Coast Guard has jurisdiction for spills into, or upon, navigable waters of the U.S, adjoining shorelines, the contiguous zone, Deepwater Ports, the Continental Shelf and other areas. Data will be collected on all oil spills of 100 gallons or more investigated by the U.S. Coast Guard. |
| Data Source | Investigations of reportable oil discharge incidents are recorded in the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database. |
| Collection Method | Only Investigations recorded in the U.S. Coast Guard's MISLE database of reportable oil discharge incidents into U.S. waters from maritime sources subject to U.S. Coast Guard jurisdiction are counted. Discharges onto land, into the air, or into enclosed spaces are excluded unless the oil reaches a navigable waterway. Policy changes now require Pollution Reports (POREPS) in MISLE for all spills 100 gallons or more. Contained in these POLREPS is the requirement to specify the disposition of the oil spilled by the categories in the measure. |
| Reliability | Reliable |
| How Data is Verified | 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. 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. |

| | |
|---|---|
| Performance Measure | Five-year average number of commercial mariner deaths and injuries. (New performance plan measure for FY 2008.) |
| Program and Organization | Marine Safety - United States Coast Guard |
| Description | This is a measure of the long-term performance trend of the U.S. Coast Guard Marine Safety Program impact on commercial mariner fatalities and injuries. |
| Scope | The sum of all reportable commercial mariner deaths and injuries. A five-year average is used to show the long - term trend. 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. Because some reports are delayed in reaching the U.S. Coast Guard, published data is subject to revision. |
| Data Source | Notices of Mariner casualties are recorded in the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database. |
| Collection Method | For Mariner deaths and injuries, only Investigations recorded in the MISLE database are counted. Mariner deaths and injuries include casualties of crewmembers or employees aboard U.S. commercial vessels in U.S. waters. Casualties aboard foreign flag or government vessels are excluded. Deaths, disappearances or injuries determined to be the result of natural causes or intentional acts such as heart attack, altercation, or the like are excluded. |
| Reliability | Reliable |
| How data is verified | 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. |

| | |
|---|---|
| Performance Measure | Five-year average number of commercial passenger deaths and injuries. (New performance plan measure for FY 2008.) |
| Program and Organization | Marine Safety - United States Coast Guard |
| Description | This is a measure of the long-term performance trend of the U.S. Coast Guard Marine Safety Program impact on commercial passenger fatalities and injuries. |

| | |
|---|---|
| Scope | The sum of all reportable commercial passenger deaths and injuries. A five-year average is used to show the long-term trend. 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. Because some reports are delayed in reaching the U.S. Coast Guard, published data is subject to revision the greatest impact on recent quarters. |
| Data Source | Notices of Passenger casualties are recorded in the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database. |
| Collection Method | For Passenger deaths and injuries, only Investigations recorded in the MISLE database are counted. Passenger deaths and injuries include casualties from passenger vessels operating in U.S. waters. Passenger deaths, disappearances or injuries associated with diving activities are excluded. Deaths, disappearances or injuries determined to be the result of natural causes or intentional acts such as heart attack, altercation, or the like are excluded. |
| Reliability | Reliable |
| How data is verified | 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. |

| | |
|---|---|
| Performance Measure | Five-year average number of recreational boating deaths and injuries. (New performance plan measure for FY 2008.) |
| Program and Organization | Marine Safety - United States Coast Guard |
| Description | This is a measure of the long-term performance trend of the U.S. Coast Guard Marine Safety Program impact on recreational boating fatalities and injuries. |
| Scope | The sum of all reportable recreational boating deaths and injuries. A five-year average is used to show the long-term trend. 33 CFR 173.55 requires the operator of a vessel, that is used by its operator for recreational purposes or is required to be numbered, to file a Boating Accident Report when, as a result of an occurrence that involves the vessel or its equipment, a person dies; or a person is injured and requires medical treatment beyond first aid; or a person disappears from the vessel under circumstances that indicate death or injury. |
| Data Source | Boating Accident Reports are recorded in the U.S. Coast Guard's Boating Accident Report Database (BARD) System. |
| Collection Method | For 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. Also included are casual - ties where a person dies while swimming because of carbon monoxide exposure; a person dies while swimming because a vessel is improperly connected to shore power and resultant stray electrical current causes electrocution; a person dies or is injured after leaving a vessel that is underway to swim for pleasure because the vessel is not anchored, moored or docked and the vessel drifts away from the swimmer and the swimmer is unable to get back to the vessel; and a person is struck by a vessel or its associated equipment where the vessel serves as the instrument striking the person. Deaths, disappearances or injuries determined to be the result of natural causes or intentional acts such as heart attack, altercation, or the like are excluded. |
| Reliability | Reliable |
| How data is verified | 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 | Maritime injury and fatality index.  (Retired plan measure.) |
| Program and Organization | Marine Safety - United States Coast Guard |
| Description | The measure is a five-year average of annual deaths and injuries occurring on both commercial and recreational vessels, and measures the U.S. Coast Guard's success in ensuring the safety of persons embarked on both commercial and recreational vessels. U.S. law requires that any death or injury beyond first aid that occurs on a U.S. vessel (or a foreign vessel in U.S. waters) be reported directly to the U.S. Coast Guard. |
| Scope | This measure is an index of the moving five-year average of mariner, passenger and recreational boating deaths and injuries. This represents a valid outcome measure of the U.S. Coast Guard's success in ensuring the safety of persons embarked on both commercial and recreational vessels. |
| Data Source | Notices of commercial Passenger and Mariner casualties are recorded in the U.S. Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database, while recreational Boating Accident Reports are recorded in the U.S. Coast Guard's Boating Accident Report Database (BARD). |
| Collection Method | Recreational boating casualties are reported to state investigatory bodies who then report their calendar year totals to the U.S. Coast Guard. Under Title 33 CFR, only recreational deaths are required to be reported to the U.S. Coast Guard by the individual states, although all states voluntarily provide data on recreational injuries.  Commercial Passenger deaths and injuries include reportable casualties of commercial passengers on U.S. vessels operating in any waters and commercial passengers on foreign vessels operating in U.S. waters. Commercial Passenger deaths, disappearances or injuries associated with diving activities are excluded. |
| Reliability | Reliable |
| How Data is Verified | Notices of recreational boating casualties recorded in the BARD, and commercial passenger and mariner casualties recorded in the MISLE database, are generally complete when the database is accessed.  Some incidents are never reported, however, and some information is delayed in reaching the U.S. Coast Guard. Previously published data is therefore subject to change; the greatest impact occurring over the most recent five months.  It is also possible that some information is inaccurately reported to the U.S. Coast Guard.  Duplicate information may occasionally be entered or an incident inadvertently omitted or incorrectly coded.  Formal verification procedures strive to rectify any errors, and program logic and comprehensive user guides have been developed to ensure that data is highly reliable. |

| | |
|---|---|
| Performance Measure | Percent of undocumented migrants who attempt to enter the U.S. via maritime routes that are interdicted.  (New performance plan measure for FY 2008.) |
| Program and Organization | Migrant Interdiction - United States Coast Guard |
| Description | The U.S. Coast Guard has been charged through Executive Orders and Presidential Decision Directive to enforce the Immigration and Nationality Act. Performance is measured by the percent of undocumented migrants of all nationalities who are interdicted while attempting to enter the U.S., its possessions, or territories via maritime routes. The measure is computed by dividing the number of successful landings by the number of migrants who attempt illegal immigration. Subtracting this percentage from 100 percent gives the migrant interdiction rate. Migrant interdictions and landings are reported by U.S. Coast Guard units and other law enforcement agencies. |
| Scope | The measure tracks migrants from all nationalities attempting direct entry by maritime means into the United States, its territories, and possessions. |
| Data Source | Data obtained from U.S. Coast Guard and the United States Citizenship and Immigration Services. |
| Collection Method | The interdiction rate compares the number of migrants interdicted at sea by U.S. Coast Guard and other law enforcement agencies, foreign navies/law enforcement interdictions, and deceased migrants recovered from smuggling events, to the number of migrants that landed in the U.S., its territories, or possessions. |

| | |
|---|---|
| | Interdiction information is obtained through the U.S. Coast Guard Marine Information for Safety and Law Enforcement (MISLE) database, and Customs and Immigration Services' records. Migrant landing information is obtained through the analysis of abandoned vessels, other evidence of migrant activity that indicate the number of migrants evading law enforcement successfully landing in the U.S., and self-reporting by migrants (Cuban migrants are allowed to stay once arriving in the U.S. and typically report their arrival). The U.S. Coast Guard Intelligence Coordination Center compiles and analyzed landing information. Data collection is managed by the Migrant Interdiction Program Manager. |
| Reliability | Reliable |
| How Data is Verified | The numbers of illegal migrants entering the U.S. by maritime means, particularly non-Cubans, is subject to estimating error due to migrant efforts to avoid law enforcement. Arrival numbers for Cubans tend to be more reliable than other nationalities as immigration law allows Cubans to stay in the U.S once reaching shore, which encourages self-reporting of arrival. Over the last five years, Cubans have constituted approximately a quarter of all maritime migrant interdictions. Migrant landing information is validated across multiple sources using established intelligence rules that favor conservative estimates. |

| | |
|---|---|
| Performance Measure | Percent of undocumented migrants who attempt to enter the U.S. via maritime routes that are interdicted or deterred. (Retired plan measure.) |
| Program and Organization | Migrant Interdiction - United States Coast Guard |
| Description | The U.S. Coast Guard has been charged through Executive Orders and Presidential Decision Directive to enforce the Immigration and Nationality Act. Performance is measured by the percent of undocumented migrants who are interdicted while, or deterred from, attempting to enter the U.S. via maritime routes. Haitian, Cuban, Dominican & Chinese are tracked, as they constitute the majority of the migrant flow entering the U.S. via maritime means. The measure is computed by dividing the number of successful landings by the migrants who actually attempt illegal immigration or were deterred from making an attempt. Subtracting this percentage from 100 percent gives the total migrants interdicted or deterred. The migrant flow is provided by the U.S. Coast Guard Intelligence Coordination Center; interdictions and landings are reported by U.S. Coast Guard units & other law enforcement agencies. |
| Scope | Political climates, historical flows, and the latest trends figure into the calculations. The potential flows are validated against other flow estimates where available; they are usually found to be more conservative than the other sources. The measure only tracks Cubans, Dominicans, Haitians, and Chinese at this time. A small number of migrants (approximately 10 percent) from various source countries are not included because formal flow estimates of migrants leaving these countries are not available. Using the number of potential migrants in the denominator helps address the deterrence value of U.S. Coast Guard operations, but could lead to confusion of this measure with a simple interdiction rate. |
| Data Source | Data obtained from U.S. Coast Guard and the United States Citizenship and Immigration Services. |
| Collection Method | The success rate is an indicator of the number of migrants entering the U.S. by maritime routes compared against number of migrants that would attempt to enter with no interdiction presence. Flow estimate (provided by the U.S. Coast Guard Intelligence Coordination Center) are compiled with interdiction and arrival information (provided by the U.S. Coast Guard Marine Safety and Law Enforcement Database (MISLE) and the United States Citizenship and Immigration Services, respectively) through Excel and Access databases. These systems are managed by the Program Manager. |
| Reliability | Reliable |
| How Data is Verified | The number of illegal migrants entering the U.S. and the number of potential migrants are derived numbers subject to estimating error. Because of the speculative nature of information used, and the secretive nature of illegal |

| | |
|---|---|
| | migration, particularly where professional smuggling organizations are involved, the estimated potential flow of migrants may contain error. |

| | |
|---|---|
| Performance Measure | Number of incursions into the U.S. Exclusive Economic Zone. |
| Program and Organization | Other LE (law enforcement) - United States Coast Guard |
| Description | This program's mission is to provide effective and professional at-sea enforcement to advance national goals for the conservation and management of living marine resources (LMR) and their environments. The program has both a maritime security and stewardship nexus. The program's primary focus is to prevent illegal encroachment of the U.S. Exclusive Economic Zone (EEZ) by foreign fishing vessels thereby protecting U.S. sovereignty from foreign fishing encroachment. |
| Scope | 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);<br>2) significant financial impact due to volume and value of target fish stocks; or<br>3) significant sovereignty concerns due to uncertainty or disagreement with foreign neighbors over the U.S. EEZ border. Standard rules of evidence (e.g., 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 EEZ. The information is consolidated at U.S. Coast Guard HQ through monthly messages from the Area Commanders. |
| Collection Method | Data obtained from the U.S. Coast Guard Planning and Assessment group. |
| Reliability | Reliable |
| How Data is Verified | The Program Manager reviews entries into MISLE database monthly and compares to other sources of information (e.g., after action reports, message traffic, etc.) to assess reliability of the database. |

| | |
|---|---|
| Performance Measure | Critical infrastructure required visit rate. (New performance plan measure for FY 2008.) |
| Program and Organization | Ports, Waterways and Coastal Security (PWCS) - United States Coast Guard |
| Description | This measure is the accomplishment rate of required visits to maritime critical infrastructure. |
| Scope | These data employ reports of field-level activities and describe percent attainment of Combating Maritime Terrorism standards. The actual standards, which are set by operational order, are classified. |
| Data Source | These data are reported by regional U.S. Coast Guard commands (Sectors). |
| Collection Method | Data is collected using an automated (web based) application. |
| Reliability | Reliable |
| How Data is Verified | Data is collected using an automated application, and is reviewed by all pertinent levels in the organization for accuracy and consistency. That is, U.S. Coast Guard field-level Sectors report their data to their regional U.S. Coast Guard Districts (first review), who in turn report to each of the two U.S. Coast Guard Area Commands (for 3-star review). Final review occurs at the headquarters-level U.S. Coast Guard program office which compares data longitudinally (over time) and across the organization. |

| | |
|---|---|
| Performance Measure | High capacity passenger vessel required escort rate. (New performance plan measure for FY 2008.) |
| Program and Organization | Ports, Waterways and Coastal Security (PWCS) - United States Coast Guard |
| Description | This measure is the accomplishment rate of required escorts of high capacity passenger vessels. |
| Scope | These data employ reports of field-level activities and describe percent attainment of Combating Maritime Terrorism standards. The actual standards, which are set by operational order, are classified. |
| Data Source | These data are reported by regional U.S. Coast Guard commands (Sectors). |
| Collection Method | Data is collected using an automated (web based) application. |
| Reliability | Reliable |
| How Data is Verified | Data is collected using an automated application, and is reviewed by all pertinent levels in the organization for accuracy and consistency. That is, U.S. Coast Guard field-level Sectors report their data to their regional U.S. Coast Guard Districts (first review), who in turn report to each of the two U.S. Coast Guard Area Commands (for 3-star review). Final review occurs at the headquarters-level U.S. Coast Guard program office which compares data longitudinally (over time) and across the organization. |

| | |
|---|---|
| Performance Measure | Number of Transportation Workers Identification Credential (TWIC) spot checks. (New performance plan measure for FY 2008.) |
| Program and Organization | Ports, Waterways and Coastal Security (PWCS) - United States Coast Guard |
| Description | This measure reports the number of TWIC spot checks that occur per year by U.S. Coast Guard officials. It is anticipated that the U.S. Coast Guard will purchase TWIC card readers in FY 2008 and will spot check TWIC cards during vessels and facility inspections. |
| Scope | Data is captured during vessel and facility inspections by TWIC card readers. Data is the count of spot checks or the number of times that a TWIC card was verified/processed by a U.S. Coast Guard member using a hand held card reader. |
| Data Source | Data is collected and reported by regional U.S. Coast Guard commands (Sectors). |
| Collection Method | Data is collected by U.S. Coast Guard members through a hand held automated TWIC card reader. The results from the card reader will then be downloaded into a secure database. |
| Reliability | Reliable |
| How Data is Verified | Currently, the data is low reliability as this is the first year the U.S. Coast Guard will be using TWIC card readers. Confidence in data reliability is expected to improve as the system is implemented and the process is exercised. Data will be collected using an automated application and reviewed at all pertinent levels in the organization for accuracy and consistency. Final review occurs at the headquarters - level U.S. Coast Guard program office. The contractor shall design and implement a system that collects and analyzes performance data to aid in system troubleshooting as well as in quality control measures. |

| | |
|---|---|
| Performance Measure | Percent reduction in the maritime terrorism risk over which the Coast Guard has influence. |
| Program and Organization | Ports, Waterways and Coastal Security (PWCS) - United States Coast Guard |
| Description | This is a risk-based outcome measure that begins with an assessment (by maritime security representatives) of likely high-consequence maritime terrorist attack scenarios. Threat, vulnerability, and consequence levels are estimated for each scenario, which generates a proxy (index) value of "raw risk" that exists in the maritime domain. Next, U.S. Coast Guard interventions (both operational and regulatory regime activities) for the fiscal year are scored against the scenarios with regard to the decreases in threat, vulnerability and consequence that each has been estimated to have afforded. The analysis then focuses on those areas within the U.S. Coast Guard's roles and strategic mandates. The resulting measure is a proxy measure of performance. |
| Scope | Annually, a quantitative self-assessment is conducted by gathering Subject Matter |

| | |
|---|---|
| | Experts from representative U.S. Coast Guard Commands and ports. Normative expert facilitators then solicit the Subject Matter Experts to assess the overall effectiveness of all relevant U.S. Coast Guard activities against a comprehensive set of maritime terror scenarios previously identified through an extensive strategic risk assessment. |
| Data Source | The data source is subject matter expert evaluation of PWCS program stakeholders. |
| Collection Method | The input from several workshops (comprised of subject matter experts) is fed directly into a tightly-controlled excel spreadsheet. Roundtable discussions focus on particular attack scenarios and the type and level of U.S. Coast Guard activities that were brought to bear each to reduce their risk. Discussions are informed by official reports of U.S. Coast Guard activities: both regulatory-regime and operationally oriented. Consensus agreement on the likely percent reduction in risk (by scenario) is recorded and reviewed by the U.S. Coast Guard's leadership. |
| Reliability | Reliable |
| How Data is Verified | The data which comprise this measure are checked for reliability by comparing them to data from similar risk assessments of the maritime domain. Data is verified to ensure consistency in several areas including levels of threat, vulnerability, and consequence. Inconsistencies are noted, and subsequently, resolved or documented. Previously, no external validation and verification was possible. The U.S. Coast Guard has begun the process of identifying external organizations with the competencies to complete an independent validation and verification., DHS Science and Technology has expressed interest in sponsoring this effort, and the U.S. Coast Guard has begun initial talks with representatives from two DHS Centers of Excellence on Risk and Terrorism Behavior (USC CREATE and UMD START) who will work with DHS S&T to complete this task. It is hopeful that this independent validation and verification can be completed during FY 2008. |

| | |
|---|---|
| Performance Measure | Percent risk reduction for the transfer of a terrorist meta-scenario. (New performance plan measure for FY 2008.) |
| Program and Organization | Ports, Waterways and Coastal Security (PWCS) - United States Coast Guard |
| Description | This measure gauges the estimated percent of terrorist-related maritime risk reduction in the transfer of a terrorist(s) through the maritime domain (as a percent of the risk that the U.S. Coast Guard has the ability to impact). This is a risk-based measure that involves the scoring (by maritime security representatives) with respect to threat, vulnerability and consequence of the transfer of a terrorist(s) into the United States with intent and capability to carry out terror attacks where vessels en route from foreign countries are used as a means of conveyance. Such scoring generates an index of "raw risk" that exists in the maritime domain. Next, U.S. Coast Guard incremental interventions (awareness, operational and regulatory -based) that have taken place throughout the fiscal year are scored with regard to the effectiveness that each has been estimated to have afforded. |
| Scope | Annually, a quantitative self-assessment is conducted by gathering Subject Matter Experts from representative U.S. Coast Guard Commands and ports. Normative expert facilitators then solicit the Subject Matter Experts to assess the overall effectiveness of all relevant U.S. Coast Guard activities against a comprehensive set of maritime terror scenarios previously identified through an extensive strategic risk assessment. |
| Data Source | The data source is subject matter expert evaluation of program stakeholders. |
| Collection Method | The input from several workshops (comprised of subject matter experts) is fed directly into a tightly-controlled excel spreadsheet. Roundtable discussions focus on particular attack scenarios and the type and level of U.S. Coast Guard activities that were brought to bear each to reduce their risk. Discussions are informed by official reports of U.S. Coast Guard activities: both regulatory-regime and operationally oriented. Consensus agreement on the likely percent reduction in risk (by scenario) is recorded and reviewed by the U.S. Coast Guard's leadership. |

| | |
|---|---|
| | Targets will be verified and completed during the established U.S. Coast Guard target setting process. |
| Reliability | Reliable |
| How Data is Verified | The data which comprise this measure are checked for reliability by comparing them to data from similar risk assessments of the maritime domain. Data is verified to ensure consistency in several areas including levels of threat, vulnerability, and consequence. Inconsistencies are noted, and subsequently, resolved or documented. Previously, no external validation and verification was possible. The U.S. Coast Guard has begun the process of identifying external organizations with the competencies to complete an independent validation and verification., DHS Science and Technology has expressed interest in sponsoring this effort, and the U.S. Coast Guard has begun initial talks with representatives from two DHS Centers of Excellence on Risk and Terrorism Behavior (USC CREATE and UMD START) who will work with DHS Science and Technology to complete this task. It is hopeful that this independent validation and verification can be completed during FY 2008. |

| | |
|---|---|
| Performance Measure | Percent risk reduction for the transfer of a weapon of mass destruction meta-scenario. (New performance plan measure for FY 2008.) |
| Program and Organization | Ports, Waterways and Coastal Security (PWCS) - United States Coast Guard |
| Description | This measure gauges the estimated percent of terrorist-related maritime risk reduction in the transfer of a Weapon of Mass Destruction (WMD)/ materials into the United States through the maritime domain (as a percent of the risk that the U.S. Coast Guard has the ability to impact). This is a risk-based measure that involves the scoring (by maritime security representatives) with respect to threat, vulnerability and consequence of the transfer of a WMD/materials into the United States to support ongoing terrorist operations where vessels en route from foreign countries are used as a means of conveyance. Such scoring generates an index of "raw risk" that exists in the maritime domain. Next, U.S. Coast Guard incremental interventions (awareness, operational and regulatory -based) that have taken place throughout the fiscal year are scored with regard to the effectiveness that each has been estimated to have afforded. |
| Scope | Annually, a quantitative self-assessment is conducted by gathering Subject Matter Experts from representative U.S. Coast Guard Commands and ports. Normative expert facilitators then solicit the Subject Matter Experts to assess the overall effectiveness of all relevant U.S. Coast Guard activities against a comprehensive set of maritime terror scenarios previously identified through an extensive strategic risk assessment. |
| Data Source | The data source is subject matter expert evaluation of program stakeholders. |
| Collection Method | The input from several workshops (comprised of subject matter experts) is fed directly into a tightly-controlled excel spreadsheet. Roundtable discussions focus on particular attack scenarios and the type and level of U.S. Coast Guard activities that were brought to bear each to reduce their risk. Discussions are informed by official reports of U.S. Coast Guard activities: both regulatory-regime and operationally oriented. Consensus agreement on the likely percent reduction in risk (by scenario) is recorded and reviewed by the U.S. Coast Guard's leadership. Targets will be verified and completed during the established target-setting process. |
| Reliability | Reliable |
| How Data is Verified | The data which comprise this measure are checked for reliability by comparing them to data from similar risk assessments of the maritime domain. Data is verified to ensure consistency in several areas including levels of threat, vulnerability, and consequence. Inconsistencies are noted, and subsequently, resolved or documented. Previously, no external validation and verification was possible. The U.S. Coast Guard has begun the process of identifying external organizations with the competencies to complete an independent validation and verification., DHS Science and Technology has expressed interest in sponsoring |

| | |
|---|---|
| | this effort, and the U.S. Coast Guard has begun initial talks with representatives from two DHS Centers of Excellence on Risk and Terrorism Behavior (USC CREATE and UMD START) who will work with DHS to complete this task. It is hopeful that this independent validation and verification can be completed during FY 2008. |

| | |
|---|---|
| Performance Measure | Risk reduction due to consequence management. (New performance plan measure for FY 2008.) |
| Program and Organization | Ports, Waterways and Coastal Security (PWCS) - United States Coast Guard |
| Description | This measure gauges the estimated percent of terrorist-related maritime risk reduction due to consequence management as a percent of the risk that the U.S. Coast Guard has the ability to impact. This is a risk-based outcome measure that involves the scoring (by maritime security representatives) of likely high-consequence maritime terrorist attack scenarios with respect to threat, vulnerability, and consequence. Such scoring generates an index of "raw risk" that exists in the maritime domain. Next, U.S. Coast Guard incremental interventions (both operational and regulatory -based) that have taken place throughout the fiscal year are scored against the attack scenarios with regard to the percent decrease in threat, vulnerability and consequence that each has been estimated to have afforded. The resultant measure shows the change in "raw risk" (due, in large part, to things outside of the U.S. Coast Guard's ability to control) and the reduction in total risk the U.S. Coast Guard estimates that it has affected. |
| Scope | The data that comprises this measure comes from an annual quantitative self - assessment of the U.S. Coast Guard's activities with regard to risk-reduction. There are no significant limitations to the data except for the fact that it is a self assessment. |
| Data Source | The data source is subject matter expert evaluation of program stakeholders. |
| Collection Method | The input from several workshops (comprised of subject matter experts) is fed directly into a tightly-controlled excel spreadsheet. Round-table discussions focus on particular attack scenarios and the type and level of U.S. Coast Guard activities that were brought to bear each to reduce their risk. Discussions are informed by official reports of U.S. Coast Guard activities: both regulatory-regime and operationally oriented. Consensus agreement on the likely percent reduction in risk (by scenario) is recorded and reviewed by the U.S. Coast Guard's leadership. |
| Reliability | Reliable |
| How Data is Verified | The data which comprise this measure are checked for reliability by comparing them to data from similar risk assessments of the maritime domain. Data is verified to ensure consistency in several areas including levels of threat, vulnerability, and consequence. Inconsistencies are noted, and subsequently, resolved or documented. |

| | |
|---|---|
| Performance Measure | Percent of mariners in imminent danger saved. |
| Program and Organization | Search and Rescue (SAR) - United States Coast Guard |
| Description | This measure reports the percent of mariners who were in imminent danger on our Nation’s oceans and waterways, and whose lives were saved by the 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 conclusion of search operations, are factored into this percentage. Several factors compound the difficulty of successful responses, including untimely notification to the U.S. Coast Guard of distress, incorrect reporting of the distress site location, severe weather conditions at the distress site, and distance to the scene. The number of lives saved is the best outcome measure for search and rescue because it includes lives lost both before and after the U.S. Coast Guard is notified and persons missing, thereby encouraging the U.S. Coast Guard to invest in supporting systems, like awareness or communication systems and safe boater programs, that increase the possibility that a search and rescue mission will end with lives saved. |
| Scope | 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. These case reports are then narrowed to include only cases where there was a positive data element in the field lives saved, lives lost before notification, or lives lost after notification. 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 factors. The first is the rescuers subjective interpretation of the policy criteria for the data point lives saved (For instance, was the life saved or simply assisted? Would the individual have perished if aid had not been rendered?) The second limitation is human error during data entry. |
| Data Source | Search and Rescue Management Information System (SARMIS) I and II and Marine Information for Safety and Law Enforcement (MISLE) |
| Collection Method | Since FY 2003, operational units have input SAR data directly into the MISLE database. Program review and analysis occurs at the District, Area, and Headquarters levels. Cases where over 10 lives are at risk are not counted because they are over-weighted and will mask other trends. |
| Reliability | Reliable |
| How Data is Verified | Data is verified quarterly by the Program Manager via data extraction and checks for anomalies within the data. Checks on data input are also made by individual case owners during case documentation processes prior. The database includes built-in prompts to check questionable data. |

## United States Immigration and Customs Enforcement

| | |
|---|---|
| Performance Measure | Percent increase in ICE investigative and enforcement systems incorporated into ICE Decision Support System consolidated data marts. (New performance plan measure for FY 2008.) |
| Program and Organization | Automation Modernization - United States Immigration and Customs Enforcement |
| Description | Contributes to the Atlas Program goal to enhance security and protection of U.S. citizens by improving investigative and intelligence capabilities to prevent terrorist and other criminal activities both domestically and internationally. Measure helps to ensure that United States Immigration and Customs Enforcement (ICE) law enforcement personnel have access to and can retrieve enforcement information from a single integrated-source of enforcement data. |
| Scope | Provide enterprise data warehousing capabilities for decision support functions as well as interoperability hub to efficiently integrate all related ICE business processes. This effort is called the Enterprise Query sub-project as part of the ICE Mission Information (IMI) Project and will enable ICE to organize information so ICE users can find relevant, timely information from the best sources; improve information search and indexing capabilities; and implement tools for integrating legacy applications with service-oriented techniques. |
| Data Source | Progress on incorporating the systems into ICE Decision Support System (DSS) consolidated data marts is reported to the ICE Chief Information Officer (CIO) by the Atlas IMI Project Manager during Atlas Program Management Review (PMR) meetings. |
| Collection Method | Prior to the Atlas PMR, the Atlas Program Management Office (PMO) issues a data call to Atlas project managers to provide specific data required to calculate progress against established baselines in the Atlas Performance Measures SOPs. The Atlas PMO Performance Measures coordinator gathers and analyzes the data and then processes the data according to each specific Atlas Performance Measure SOP. Each system that has been reported by the Atlas IMI Project Manager as being incorporated into ICE DSS consolidated data marts is included in the performance measure formula to calculate progress towards meeting the performance measure target. |
| Reliability | Reliable |
| How Data is Verified | The Atlas PMO uses the Program Management Review (PMR) meeting held for the ICE CIO as a source to confirm and validate data reliability. In the PMR meeting, the Atlas IMI Project Manager reports project progress towards meeting the performance measure target along with additional status detail. PMR meeting minutes are recorded by the Atlas PMO. |

| | |
|---|---|
| Performance Measure | Removals as a percentage of final orders issued. |
| Program and Organization | Detention and Removal Operations - United States Immigration and Customs Enforcement |
| Description | With certain exceptions, an alien in the United States is "removable" when an immigration judge issues a “final order of removal” or administrative orders are issued per statute. This measure indicates the number of aliens removed in a given year as a fraction of those ordered "removed" during the same year. The aliens removed in a given year are not necessarily the same aliens ordered to be removed in that year. |
| Scope | This measure illustrates the total number of aliens removed compared to the total number of final orders issued in the current fiscal year. |
| Data Source | Data is entered into the Deportable Alien Control System (DACS) by officers at the field offices. |
| Collection Method | The removals are entered in DACS at the field offices. From data retrieved from DACS, this measure is calculated by dividing the number of aliens removed during the fiscal year by the number of new cases entered during the same fiscal |

| | |
|---|---|
| | year. |
| Reliability | Reliable |
| How Data is Verified | The data integrity of DACS falls within acceptable limits of any IT system. Every week through an automated process of normalization or cleaning, the program reviews the data in the system to remove records outside the norm or that are known to be faulty. DACS provides the program with highly reliable data that is used for executive decision-making and Congressional reporting. |

| | |
|---|---|
| Performance Measure | Effectiveness of Federal Protective Service (FPS) operations measured by the Federal Facilities Security Index. |
| Program and Organization | Federal Protective Service - United States Immigration and Customs Enforcement |
| Description | The Federal Facilities Security Index quantifies the overall effectiveness of FPS operations in accomplishing annual performance measurement goals. The index is made up of three components: (1) how effective the FPS is in implementing security threat countermeasures (by comparing actual countermeasure implementation to planned implementation); (2) how well the countermeasures are working (by testing of countermeasures); and (3) how efficient FPS is in responding to incident calls for law enforcement by measuring response time. A security index of one (100 percent) or greater reflects accomplishment of, or exceeding, performance targets. A security index of less than one reflects failure to meet performance goals to protect government employees and the public from acts of terrorism and other illegal activities, and reduce infrastructure vulnerability from acts of terrorism or other criminal activity. |
| Scope | The security countermeasures that will be measured are guard services, x-ray machines, magnetometers, cameras, and other security devices/systems. The FPS Security Tracking System captures planned countermeasure deployment dates thereby eliminating estimated results. Planned countermeasure implementation versus actual implementation is estimated to be met 90 percent of the time. FPS has four Mega Centers that provide a response time report, which indicates the time, location, offense, and status on all incidents. This data will be analyzed to generate measure results. |
| Data Source | Data are collected and entered into the Security Tracking System database by Federal Protective Service regional offices and headquarters. |
| Collection Method | On a quarterly basis, data are collected on the countermeasure implementation, field tests of countermeasure effectiveness, and FPS Law Enforcement response time. Quarterly comparisons of regional performance against established target goals are performed. |
| Reliability | Reliable |
| How Data is Verified | Verification/validation of countermeasures implementation is conducted against implementation records. The countermeasures effectiveness is verified against surveys and quality assurance audits to ensure that the procedures and scoring criteria are accurately applied. |

| | |
|---|---|
| Performance Measure | Number of visa application requests denied due to recommendations from the Visa Security Program. (New performance plan measure for FY 2008.) |
| Program and Organization | International Affairs - United States Immigration and Customs Enforcement |
| Description | The Visa Security Program (VSP) has three primary mission objectives to enhance national security and public safety; 1) by extending the border of the U.S. overseas, Visa Security Officers (VSOs) work proactively to identify and counteract threats before they reach the United States; 2) through proactive law enforcement work, VSOs identify the not-yet-known threats to homeland security; 3) by utilizing all available tools and authorities, VSOs maximize the law enforcement and counterterrorism value of the visa process, taking it beyond the visa decision to address the underlying threat that the visa applicant potentially represents. This measure captures the instances in which a VSO provides input, advice, or information during adjudication that results in a consular officer's decision to deny a visa to an ineligible applicant. |

| | |
|---|---|
| Scope | The metric captures the number of times a VSO recommends refusal of a visa and as a result the visa is denied. This data is collected at all Visa Security Units (VSUs) real- time during the visa vetting process; VSOs manually record their decisions in a tracking system. |
| Data Source | This data is collected at all VSUs real-time during the visa vetting process; VSOs manually record their decisions in a VSP tracking system. The VSP tracking system helps to manage VSO workload, records VSOs significant work efforts, findings, and VSO decision-making. The system also facilitates automated screening functions and reports performance metrics. |
| Collection Method | This data is collected in a tracking system at each VSP office during the visa vetting process. At the end of each month, the VSOs will run a monthly report that queries for this metric and the results are exported to an excel spreadsheet. These spreadsheets are sent electronically to VSP Headquarters to be manually consolidated into a master Excel document with a pivot table for analysis. |
| Reliability | Reliable |
| How Data is Verified | Visa Security Officers review their monthly statistics and conduct quality checks in the tracking system prior to submission to ensure accuracy. Quality checks during consolidated analysis at headquarters also ensure that data is accurate. Data is available monthly after an office becomes fully operational. |

| | |
|---|---|
| Performance Measure | Percent of closed investigations which have an enforcement consequence (arrest, indictment, conviction, seizure, fine or penalty). |
| Program and Organization | Investigations - United States Immigration and Customs Enforcement |
| Description | More effective immigration and trade enforcement will contribute to enhanced homeland security as well as to greater deterrence. One method for measuring this effectiveness is to determine the extent to which criminal investigations are completed successfully, e.g., closed with an enforcement consequence. However, although many criminal cases arise that are worth pursuing, the potential of an investigation is not known at its inception; therefore, it is to be expected that many cases will be closed each year without an enforcement consequence when it is determined that the investigation is no longer viable. In addition to getting criminals off the street, successful investigations also expose and remove, or contribute to the elimination of, vulnerabilities in various aspects of trade and immigration, i.e., the ways in which criminals manage to evade safeguards that are supposed to prevent their illegal activity, and areas in which such safeguards are lax or do not exist. |
| Scope | Percent of closed cases worked by the Office of Investigations in a selected fiscal year that produced an enforcement consequence (e.g., arrest, indictment, conviction, seizure, fine and/or penalty). |
| Data Source | Traveler Enforcement Communications System (TECS). TECS is the official case management system for ICE that directly measures the current status and completion of an investigation. |
| Collection Method | TECS will be used to retrieve and mine the data elements for the number of closed cases and to produce the numbers that have enforcement consequences in relation to the cases worked. |
| Reliability | Reliable |
| How Data is Verified | Ad hoc reports generated through TECS are saved and repeated, as necessary, to ensure consistency of reporting. Results are compared with prior "like" reports to check for anomalies. Any geographic specific information with significant deviation is verified through the entering location. |

## United States Secret Service

| | |
|---|---|
| Performance Measure | Percentage of instances protectees arrive and depart safely. |
| Program and Organization | Campaign Protection - United States Secret Service |
| Description | The security of protectees is the ultimate priority of the Secret Service; therefore, all necessary resources are utilized before and during a protective assignment in order to provide the highest-quality protection the Secret Service demands for all protectees. This measure represents the percentage of travel stops where the protectee safely arrives and departs. The performance target is always 100 percent. Anything under 100 percent is unacceptable. |
| Scope | Performance data capture the activities of major Presidential and Vice Presidential candidates and nominees and their spouses, and President-elect and Vice President-elect and their immediate families. There is no error rate for this measure. |
| Data Source | This program measure originates from every protective event or visit. 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. |
| Collection Method | 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 | Reliable |
| How Data is Verified | Program management and the Management and Organization division continually monitor and review performance, including all instances of arrival and departure. Any breach of Protective Operations would be immediately known and subject to a thorough investigation. |

| | |
|---|---|
| Performance Measure | Percentage of instances protectees arrive and depart safely. |
| Program and Organization | Domestic Protectees (DP) - United States Secret Service |
| Description | The percentage of travel stops where our Nation's leaders and other protectees arrive and depart safely. The security of protectees is the ultimate priority of the Secret Service; therefore, all necessary resources are utilized before and during a protective assignment in order to provide the highest-quality protection the Secret Service demands for all protectees. The performance target is always 100 percent. Anything under 100 percent is unacceptable. |
| Scope | Performance data capture the protection of domestic leaders consisting of the President and Vice President and their families, former Presidents and their spouses, 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 domestic 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. |
| Collection Method | 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 | Reliable |
| How Data is Verified | Program managers and Operations Research Analysts continually monitor and review performance, including all instances of arrival and departure. Any breach of Protective Operations would be immediately known and subject to a thorough investigation. |

| | |
|---|---|
| Performance Measure | Counterfeit passed as a percent of the amount of genuine currency in circulation. (New performance plan measure for FY 2008.) |
| Program and Organization | Financial Investigations (FI) - United States Secret Service |
| 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 | 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 (CCS). This system is used by all Secret Service investigative field offices, and provides a means of record keeping for all case and subject information. |
| Collection Method | The CCS database is comprised of global counterfeit activity on U.S. currency, which is entered by USSS personnel. |
| Reliability | Reliable |
| How Data is Verified | CCS 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 | Counterfeit passed per million dollars of genuine U.S. currency. (Retired plan measure.) |
| Program and Organization | Financial Investigations (FI) - United States Secret Service |
| Description | The dollar value of counterfeit notes passed on the public per million 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, multiplied by one million. 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 | 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 per million 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 (CCS). This system is used by all Secret Service investigative field offices, and provides a means of record keeping for all case and subject information. |
| Collection Method | The CCS database is comprised of global counterfeit activity on U.S. currency, which is entered by USSS personnel. |
| Reliability | Reliable |
| How Data is Verified | CCS 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 | Financial crimes loss prevented through a criminal investigation (in billions). |
| Program and Organization | Financial Investigations (FI) - United States Secret Service |
| 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 | 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. |
| Collection Method | The MCI database is comprised of case and arrest information, which is entered by USSS personnel. |
| Reliability | Reliable |
| How Data is Verified | 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 | Percentage of instances protectees arrive and depart safely - Foreign Dignitaries. |
| Program and Organization | Foreign Protectees and Foreign Missions (FP/FM) - United States Secret Service |
| Description | The percentage of travel stops where visiting world leader protectees safely arrive and depart. The security of protectees is the ultimate priority of the Secret Service; therefore, all necessary resources are utilized before and during a protective assignment in order to provide the highest-quality protection the Secret Service demands for all protectees. The performance target is always 100 percent. Anything under 100 percent is unacceptable. |
| Scope | Performance data captures the protection of visiting heads of state, heads of government, and their spouses and other distinguished visitors to the United States as directed by the President. Data also capture external security to foreign diplomatic embassies and missions in the Washington, D.C., area (and other limited areas, consistent with statute). There is no error rate for this measure. |
| Data Source | This program measure originates from every protective event or visit. 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. |
| Collection Method | 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 | Reliable |
| How Data is Verified | Program managers and Operations Research Analysts continually monitor and review performance, including all instances of arrival and departure. Any breach of Protective Operations would be immediately known and subject to a thorough investigation. |

| | |
|---|---|
| Performance Measure | Financial crimes loss prevented by the Secret Service Electronic Crimes Task Forces (in millions). |
| Program and Organization | Infrastructure Investigations - United States Secret Service |
| Description | An estimate of the direct dollar loss to the public that was prevented due to investigations by Secret Service Electronic Crimes Task Forces throughout the United States, which were established pursuant to the USA PATRIOT Act. This 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. This measure reflects the Secret Service's efforts to reduce financial losses to the public attributable to electronic crimes. |
| Scope | This measure reports an estimate of the direct dollar loss prevented due to the Secret Service's Electronic Crimes Task Forces' investigations. 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. |
| Collection Method | The MCI database is comprised of case and arrest information, which is entered by USSS personnel. |
| Reliability | Reliable |
| How Data is Verified | 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 Protective Intelligence cases completed. |
| Program and Organization | Protective Intelligence (PI) - United States Secret Service |
| Description | The total number of intelligence cases completed by agents assigned to field operations. These cases generally represent an assessment of individuals or groups who have threatened a protectee of the Secret Service. |
| Scope | Performance data capture all Protective Intelligence cases worked by the Secret Service, which are the highest priority cases worked. Because these cases may directly impact the safety of our protectees, all cases are referred for investigation and tracked until completion. Overall error rates are less than one percent. Error is due to lag time in data entry or corrections to historical data. |
| Data Source | The Intelligence Program 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. |
| Collection Method | The MCI database is comprised of case and arrest information, which is entered by USSS personnel. |
| Reliability | Reliable |
| How Data is Verified | 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 application to ensure the accuracy and validity of the data. Only authorized headquarters and field personnel have access to the application, and they are governed by specific procedures to input case and arrest data. |

## Index of Performance Measures

Homeland
Security