FY 2002 PROGRAM PERFORMANCE REPORT

I STRATEGIC GOAL ONE: Protect America Against the Threat of Terrorism

STRATEGIC OBJECTIVE 1.1 & ANNUAL GOAL: PREVENT TERRORISM

Prevent, disrupt, and defeat terrorist operations before they occur

1.1A Prevent Terrorists' Acts

Background/Program Objectives:
The FBI's Counterterrorism (CT) program strategy recognizes that the underlying political/religious/ social movements that drive terrorist acts are beyond the control of any law enforcement organization. The FBI, therefore, cannot prevent all acts of terrorism. To effectively address terrorism, the FBI has developed a comprehensive strategy focused on building maximum feasible capacity in the CT program. Maximum feasible capacity is achieved when the CT program has all necessary elements in place in five areas of competency: investigations, intelligence, communications, liaison, and program management. The effort to achieve maximum feasible capacity involves in-depth assessment of the program's current capacity, identification of performance gaps, and focusing resources and attention on specific initiatives to close these gaps.

By maximizing capacity in all five levels, the FBI can proactively assure that the CT program is in the best possible position to prevent terrorist acts. This strategy enables the FBI to maintain a specific and defined strategy, thorough intelligence gathering, valid and straightforward reporting and tracking mechanisms, effective intra- and interagency liaison and cooperation, and accountable program management.

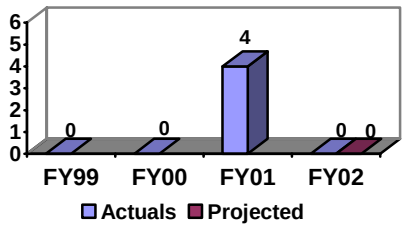
Performance:
***Performance Measure*:** Terrorist Acts Committed by Foreign Nationals Against U.S. Interests (within U.S. Borders) [FBI]

FY 2002 Target: 0

FY 2002 Actual: 0

Discussion: No incidents falling into this category were reported for FY 2002.

Terrorist Acts Committed by Foreign Nationals Against U.S. Interests wtihin U.S. Borders [FBI]



Data Definitions: This measure captures acts that involve the "unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." (28 C.F.R. Section 0.85). For the purposes of this measure, the FBI defines a terrorist act as an attack against a single target (e.g. a building or physical structure, an aircraft, etc.). Acts against single targets are counted as separate acts, even if they are coordinated to have simultaneous impact. For example, each of the 09/11 acts (North Tower of the World Trade Center (WTC), South Tower of the WTC, the Pentagon, and the Pennsylvania crash site) could have occurred independently of each other and still have been a significant terrorist act in and of itself. The FBI uses the term terrorist incident to describe the overall concerted terrorist attack. A terrorist incident may consist of multiple terrorist acts. The 09/11 attacks, therefore, are counted as four terrorist acts and one terrorist incident.

Data Collection and Storage: The reported numbers were compiled through the expert knowledge of FBI CT senior management at headquarters.

Data Validation and Verification: See above.

Data Limitations: The decision to count or discount an incident as a terrorist act, according to the above definition, is subject to change based upon the latest available intelligence information and the opinion of program managers. In addition, acts of terrorism, by their nature, are impossible to reduce to uniform, reliable measures. A single defined act of terrorism could range from a small-scale explosion that causes property damage to the use of a weapon of mass destruction that causes thousands of deaths and massive property damage and has a profound effect on national morale.

1.1B Protect Critical Infrastructure

Background/Program Objectives:
All critical infrastructures now rely on computers, advanced telecommunications, and, to an ever-increasing degree, the Internet. That dependence creates new vulnerabilities, which are exacerbated by several factors. Most infrastructures rely on commercially available technology, which means a vulnerability in hardware or software is not likely to be limited to one company, but to be widespread. Infrastructures are increasingly interdependent and interconnected with one another, making it difficult to predict the cascading effects that the disruption of one infrastructure would have on others. The telecommunications infrastructure is now truly global. Satellite communications, the Internet, and foreign ownership of telecommunication carriers in the U.S. have all combined to undermine the notion of a "National Information Infrastructure." The FBI's National Infrastructure Protection Center's (NIPC) goal is to enhance U.S. national security by preventing infrastructure damage through a multifaceted approach to maximizing its investigative and preventative resources to thwart cyber attacks on the nation's infrastructure.

Performance:
Performance Measure: Computer Intrusions Investigated [FBI]

FY 2002 Target: In accordance with Department guidance, targeted levels of performance are not projected for this indicator.

FY 2002 Actual:
Opened and Pending: 1,956
Closed: 814

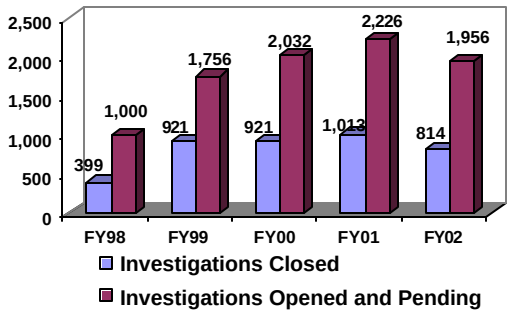
Discussion: Changes in the number of investigations is largely proportional to the number of trained agents in the field who respond to reported intrusions. The number of computer intrusion investigations is also tied to an increase in the intelligence base of the FBI, as well as an increase in violations reported by industry through the InfraGard and Key Asset Programs.

Performance Measure: Computer Intrusion Convictions/Pre-Trial Diversions [FBI]

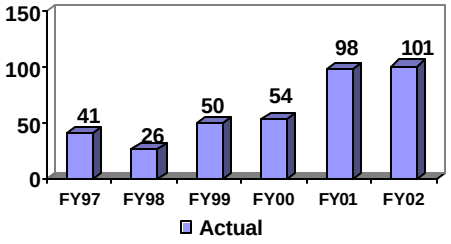
FY 2002 Target: N/A

FY 2002 Actual: 101

Computer Intrusions Investigated [FBI]



Computer Intrusion Convictions/Pre-Trial Diversions [FBI]



Data Definition: Pre-trial Diversion: A pretrial diversion can be claimed when a subject and the USA agree to a pre-trial diversion plan under which the subject must complete a plan of lawful behavior in lieu of prosecution. Generally, a pre-trial diversion plan may be considered for misdemeanor offenses involving first time offenders.

Data Collection and Storage: The data source for the number of intrusions investigated is the FBI's Monthly Administrative Report/Automated Case Support (MAR/ACS) system.

Data Validation and Verification: Computer intrusion data are reviewed and approved by an FBI field manager before they are entered into the system. Data in both systems are subsequently verified through the FBI's inspection process. Inspection occurs on a 2 to 3 year cycle. Using statistical sampling methods data in ISRAA is traced back to source documents contained in FBI files.

Data Limitations: None known at this time.

Discussion: Computer intrusion convictions continue to rise as a result of increased investigations and level of agent expertise.

Performance Measure: NEW MEASURE: Number of Compromised Computer Systems Identified and Notified.

FY 2002 Target: In accordance with Department guidance, targeted levels of performance are not projected for this indicator.

FY 2002 Actual: 2,554

Discussion: Through investigative efforts, additional compromised computer systems are being identified and the owners of these systems are being notified of the compromises and the methods utilized by the intruders to gain access to their computers. This performance measure reflects the complexity of computer intrusion investigative efforts and the success of efforts to identify and target intruders who are breaking into multiple computer networks.

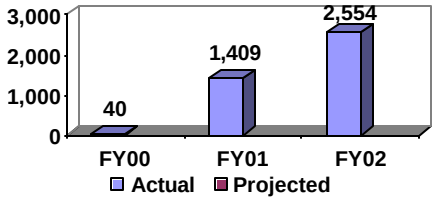
Performance Measure: DISCONTINUED MEASURE: Key Assets Identified [FBI] (NOTE: This indicator is being discontinued - the program has been transferred to the Department of Homeland Security.)

FY 2002 Target: 6,100

FY 2002 Actual: 10,418

Discussion: The number of Key Assets indicates the number of identified organizations, systems, or physical plans, the loss of which would have widespread or dire economic or social impact on a national, regional, or local basis. FBI field agents identify assets in their jurisdiction that may qualify as Key Assets and consult with the owners on their operations and impact on the locality's critical infrastructure. Key Assets are identified and entered into a database from which maps are created that help determine any overlapping or secondary Key Assets that are interlinked.

NEW MEASURE: Number of Compromised Computer Systems Identified and Notified [FBI]



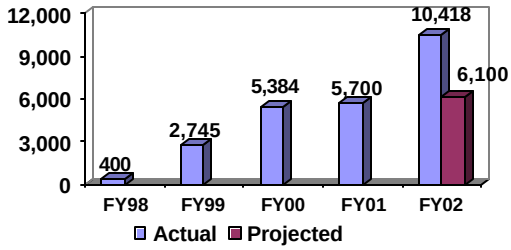
Data Definition: A statistical accomplishment can be claimed when the FBI identifies a computer system/network that has been compromised, through investigative efforts, and notifies the system owners/administrators of this matter. The notification will include the details of the compromise, including the date, item and method of compromise, if known.

Data Collection and Storage: The data source for the number of compromised sites identified and notified is the Integrated Intelligence Information Application (IIIA) system.

Data Validation and Verification: The number of compromised sites identified and notified are reviewed and approved by an FBI field manager before data are entered into the IIIA system. Data in this system are subsequently verified through the FBI's inspection process. Inspection occurs on a 3 year cycle. Using statistical sampling methods data in IIIA is traced back to source documents contained in FBI files.

Data Limitations: None known at this time.

DISCONTINUED MEASURE: Key Assets Identified [FBI]



Data Collection and Storage: Key Assets are identified and entered into a database maintained by the NIPC.

Data Validation and Verification: The mapping process helps to verify that an "asset" is a critical Key Asset. By using the mapping process, the FBI ensures that the information is continually validated. The maps/grids produced from the database are used to plan for various scenarios in the event of a threat or incident.

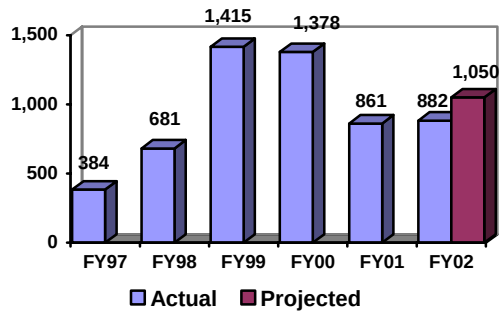
Data Limitations: Although the numbers provided are cumulative, the delta between any two years may not be a true indicator of activity given hat as new assets are identified, other assets may no longer meet the Key Asset criteria and are removed from the database.

1.1C Improve Domestic Preparedness

Background/Program Objectives:
Two key elements of domestic preparedness are expertise in hazardous devices and emergency response capabilities to address threats such as weapons of mass destruction (WMD). The FBI'S Hazardous Devices School (HDS) is the only formal domestic training school for state and local law enforcement to learn safe and effective bomb disposal operations. The HDS prepares bomb technicians to locate, identify, render safe, and dispose of improvised hazardous devices, including those containing explosives, incendiary materials, and materials classified as WMD.

Qualification for bomb technician certification includes graduation from the HDS basic course and the completion of the HDS recertification course every three years. Additionally, a bomb technician must be actively employed by a law enforcement or public safety organization and assigned to bomb squad responsibilities by that organization. Other course offerings include robot courses and executive management courses.

OJP's Office of Domestic Preparedness (ODP) provided grant funding to assist state and local emergency response agencies (law enforcement, fire, hazardous materials, emergency medical services, emergency management, and public health) to enhance their capabilities to respond to the threat posed by terrorist uses of WMD. In addition to the grant funds that may be used to acquire specialized response equipment and design and conduct exercises, ODP developed and delivered emergency responder training, technical assistance, and direct support to plan and conduct exercises tailored to the local jurisdiction. ODP provided training through the delivery of over 30 courses which range in scope from courses to increase awareness of terrorism threats and weapons of mass destruction among public officials, public health and the medical community, public safety and public works personnel, to intensive technician and operations courses that demonstrate the effects of, and response to, live agents, explosives, and radiation.



Data Collection and Storage: Data are maintained in central files and databases located at the HDS.

Data Validation and Verification: The HDS Program Administrator reviews and approves all statistical accomplishment data for dissemination.

Data Limitations: None known at this time.

Performance:
Performance Measure: State and Local Bomb Technicians Trained [FBI]

FY 2002 Target: 1,050 students trained at the Hazardous Devices School (HDS)

FY 2002 Actual: 882

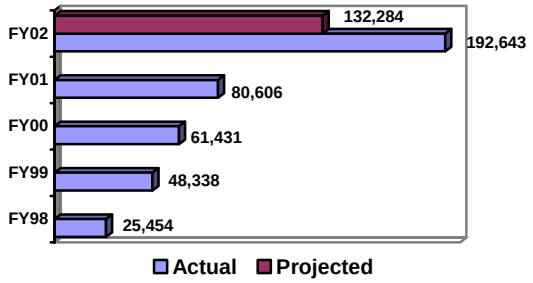
Discussion: The events of September 11, 2001 and the subsequent reallocation of resources had an impact on the performance target for FY 2002, as in many other FBI programs.

Performance Measure: DISCONTINUED MEASURE: Number of First Responders Trained [OJP] (NOTE: This indicator is being discontinued, the program has been transferred to the Department of Homeland Security.)

FY 2002 Target: Cumulative: 132,284

FY 2002 Actual: Cumulative: 192,643

Discussion: ODP exceeded its target by 60,359. ODP achieved this goal by increasing the number of classes offered for existing courses and developing and offering new course deliveries. Additionally, the increased emphasis and desire to receive WMD training by state and local jurisdictions contributed to the vast increase in the number of emergency responders receiving training.



Data Collection and Storage: The data on training participants are reported by the providers of ODP-sponsored training to a central database maintained by one of the providers.

Data Validation and Verification: Beginning January 2002, the database will be maintained by ODP's Central Scheduling Desk and will be verified and analyzed by ODP's evaluation staff.

Data Limitations: None known at this time.

STRATEGIC OBJECTIVE & ANNUAL GOAL 1.2-1.3: INVESTIGATE AND PROSECUTE TERRORIST ACTS

1.2: Develop and implement the full range of resources available to investigate terrorist incidents, bringing their perpetrators to justice

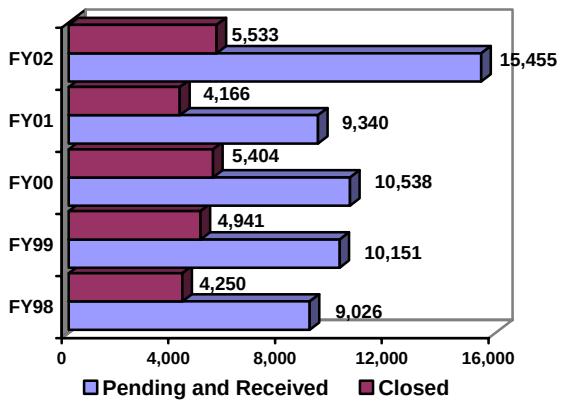
1.3: Vigorously prosecute those who have committed, or intend to commit, terrorist acts against the United States

1.2 – 1.3A Investigate and Prosecute Terrorists' Acts

Background/Program Objectives:
Through criminal and national security investigations, DOJ works to arrest and prosecute or deport terrorists and their supporters and to disrupt financial flows that provide resources to terrorists operations. These investigations enable the Department to gather information, punish terrorists, develop and solidify relationships with critical partners, and maintain a presence visible to both potential terrorists and the American public, all of which are critical pieces of the Department's efforts against terrorism.

The new counterterrorism strategy, implemented by the Department after September 11, 2001, includes the development of Anti-Terrorism Task Forces. Each United States Attorney's office identified one experienced prosecutor to serve as the Anti-Terrorism Coordinator for that district's Anti-Terrorism Task Force. The Coordinator convenes meetings of representatives from the federal law enforcement agencies – including the FBI, INS, DEA, U.S. Customs Service, U.S. Marshals Service, U.S. Secret Service, and Bureau of Alcohol, Tobacco and Firearms (ATF) – and the primary state and local police forces, along with other appropriate state agencies and officials in each district. These task forces are part of a national network that coordinates the dissemination of information throughout the country. The implementation of these task forces coordinated by the United States Attorney in each district and interfacing with the Department through the Criminal Division's Regional Terrorism Coordinators, supports a concerted national assault against terrorism.

In addition, the Department created a Terrorist Financing Task Force, consisting of attorneys from the Criminal and Tax Divisions and the U.S. Attorneys' Offices, to coordinate the nationwide prosecutorial efforts against groups and individuals assisting in financing international terrorism. This task force works closely with the FBI's Financial Review Group, which draws resources from numerous, federal law enforcement agencies and is devoted to the collection and analysis of information concerning terrorist financing.



Data Collection and Storage: The data source for the number of intrusions investigated is the FBI's Monthly Administrative Report/Automated Case Support (MAR/ACS) system.

Data Validation and Verification: Before data are entered into FBI systems, they are reviewed and approved by an FBI field manager. Data are subsequently verified through the FBI's inspection process. Inspections occur on a 2 to 3 year cycle. Using statistical sampling methods, data are traced back to source documents contained in FBI files.

Data Limitations: None known at this time.

Performance:

Performance Measure: Number of Terrorism Cases Investigated [FBI]

FY 2002 Target: N/A

FY 2002 Actual:

Pending and Received: 15,455

Closed: 5,533

Discussion: Each case represents effort towards the investigation and prevention of terrorism. While the number of investigations itself does not fully capture the efforts or effects of the Department's counterterrorism program, measure does show activity towards the ultimate goals of preventing terrorism.

Performance Measure: Terrorism Convictions [EOUSA]

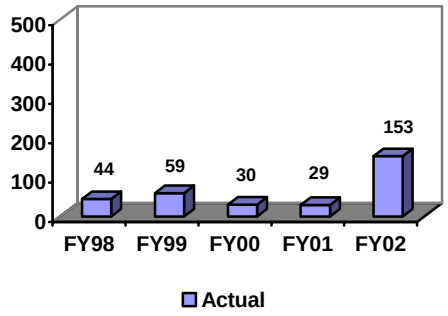
FY 2002 Target: In accordance with Department guidance, targeted levels of performance are not projected for this indicator.

FY 2002 Actual:

Terrorism Convictions: 153

Discussion: Convicted defendants include those defendants who plead guilty or were found guilty in cases classified by the U.S. Attorneys' offices under the Domestic Terrorism or International Terrorism program categories. Those program categories include offenses involving acts (including threats or conspiracies to engage in such acts) that are violent or dangerous to human life and that appear motivated by an intent to coerce, intimidate, or retaliate against a government or civilian population. Examples of offenses that could be classified as international or domestic terrorism include the following: destruction of an aircraft or interference with a flight crew; attack on a mass transit facility or on the means of interstate communication; use of weapons of mass destruction; material support for terrorism; and terrorism. The substantial increase in offenses in these program categories is attributable to the Department's determination, after the terrorist attacks of September 11, 2001, to make the prevention of terrorism its highest priority.

Terrorism Convictions [EOUSA]



Data Definitions: Terrorism convictions are based on our historical data definitions in our original program categories of International Terrorism and Domestic Terrorism.

Data Collection and Storage: Data is collected from the USA-5 monthly Resource Summary Report System, which summarizes the use of personnel resources allocated to USA offices. Data will also be taken from USA central case management system, which contains district information including criminal matters, cases, and appeals.

Data Validation and Verification: The USA offices are required to submit bi-yearly case data certifications to EOUSA. Data are reviewed by knowledgeable personnel (such as supervisory attorneys and legal clerks) in each district.

Data Limitations: As noted above, the USA offices are required to submit bi-yearly case data certifications to EOUSA. Attorneys and support personnel are responsible for ensuring that local procedures are followed for maintaining the integrity of the system data.