1 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

The Department's Federal Bureau of Investigation (FBI) is committed to stopping terrorism at any stage of development, from the positioning of those who would conduct an act, to the financiers of the operations. All investigations are nationally managed by FBI Headquarters and applied to a broader national perspective, which focuses on the strategy of creating an inhospitable terrorist environment.

Preventing terrorists from entry into the country, enhancing intelligence to monitor terrorist subsistence, and increasing awareness of terrorist surveillance on potential targets are methods that the FBI employs to disrupt the terrorist presence to conduct an attack.

The FBI protects the U.S. from terrorist attack by disrupting the terrorists' ability to conduct an act. Training, finances, recruiting, logistical support, pre-attack planning, and preparation are all required components of terrorist operations. These dependencies create vulnerabilities and the FBI focuses on creating a comprehensive intelligence base to exploit these vulnerabilities.

In order to develop a comprehensive intelligence base, the FBI employs its new Model Counterterrorism Investigative Strategy, which primarily focuses each terrorist case on intelligence. A terrorist disruption (i.e., a criminal prosecution or non-prosecutorial sanction) is be administered only after all intelligence is gathered. This intelligence focuses on identification of terrorist training, fund raising, recruiting, logistical support, and pre-attack planning activity.

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

- **FY 2003 Target:** 0
- **FY 2003 Actual:** 0
- **Discussion:** No incidents falling into this category were reported for FY 2003.

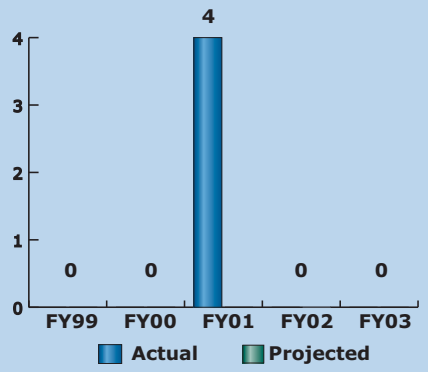
Data Definitions: This measure captures acts that involve the "unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." (28 C.F.R. Section 0.85). For the purposes 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 September 11, 2001 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.

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



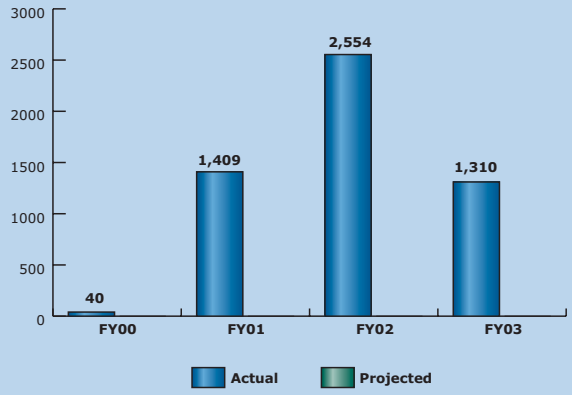
1.1B Protect Critical Infrastructure

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."

Certain functions performed by the National Infrastructure Protection Center (NIPC), previously housed at the FBI, were transferred to the new Department of Homeland Security (DHS). This involved the transfer of approximately 185 positions (131 FBI, 54 detailees from other agencies) to the DHS. The newly established FBI Cyber Division consolidated the FBI's investigative role in addressing cyber threats received from individuals or groups who intend to attack or exploit computers or computer networks for illegal purposes. The FBI will continue to investigate these cyber threats. The NIPC will continue to focus on vulnerabilities or weaknesses in computer systems and on networks that are subject to attack. These entities will perform separate functions, and close coordination will be necessary to achieve successful outcomes in each one.

Performance Measure: Number of Compromised Computer Systems Identified and Notified [FBI]

- **FY 2003 Target:** In accordance with Departmental policy, targeted levels of performance are not projected for this indicator.
- **FY 2003 Actual:** 1,310
- **Discussion:** Through investigative efforts, additional compromised computer systems are being identified and the owners of those 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. The comparative drop in this statistical accomplishment for FY 2003 is due to the fact that FY 2002 data included an extraordinary case that resulted in the identification of over 1,000 compromised computer systems.



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.

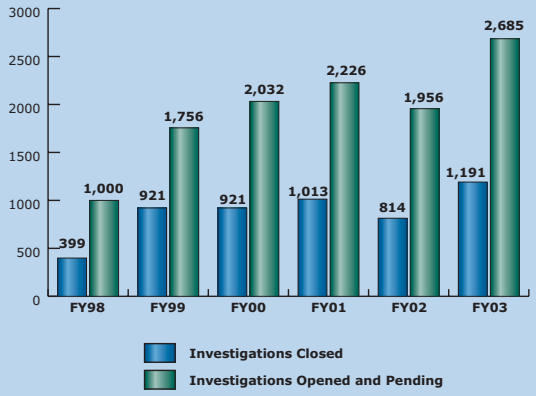
Data Limitations: None known at this time.

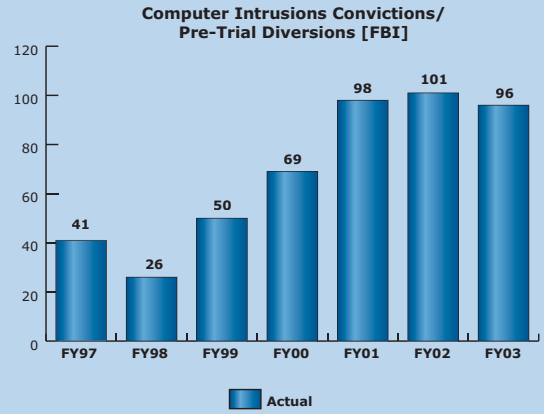
Performance Measure: Computer Intrusions Investigated [FBI]

- **FY 2003 Target:** In accordance with Departmental policy, targeted levels of performance are not projected for this indicator.
- **FY 2003 Actual:**
  Open and Pending: 2,685
  Closed: 1,191
- **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.

Performance Measure: Computer Intrusion Convictions/Pre-Trial Diversions [FBI] (**NOTE:** Review of FY 2000 data revealed additional convictions/pre-trial diversions; therefore, data have been updated to reflect these findings.)

- **FY 2003 Target:** In accordance with Departmental policy, targeted levels of performance are not projected for this indicator.
- **FY 2003 Actual:** 96
- **Discussion:** Computer intrusion convictions continue to rise as a result of increased investigations and level of agent expertise.





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.

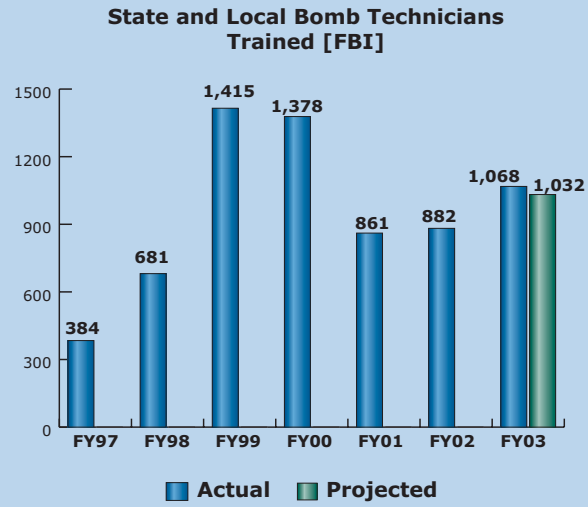
1.1C Improve Domestic Preparedness

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.

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

- **FY 2003 Target:** 1,032 students trained
- **FY 2003 Actual:** 1,068 students trained
- **Discussion:** The FBI and the U.S. Army will construct a new HDS facility at Redstone Arsenal, Huntsville, Alabama. The existing FBI-funded and administered facility at Redstone provides basic, recertification, and other training for public safety bomb technicians in the United States. The new site, four administrative and classroom buildings and 14 practical exercise-training villages, is scheduled for completion in FY 2004. An Advanced Diagnostics and Disablement Course in under development, and should be fully operational as soon as the new HDS facility is completed.



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.

Dta 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

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 Joint Terrorism Task Forces (JTTFs), located in each of the FBI's 56 field divisions and in larger resident agencies, consist of regional investigative experts to include the Intelligence Community, other federal agencies, state and local law enforcement, and FBI Special Agents. The collective knowledge of task force members enhances the investigative capacity of each FBI field division. Additionally, the participating agencies in a JTTF allow for enhanced cooperation and coordination in sharing information and pursuing investigations. JTTFs bring the resources of multiple counterterrorism partners under one roof to investigate potential terrorist activities and create an inhospitable terrorist environment for their respective divisions.

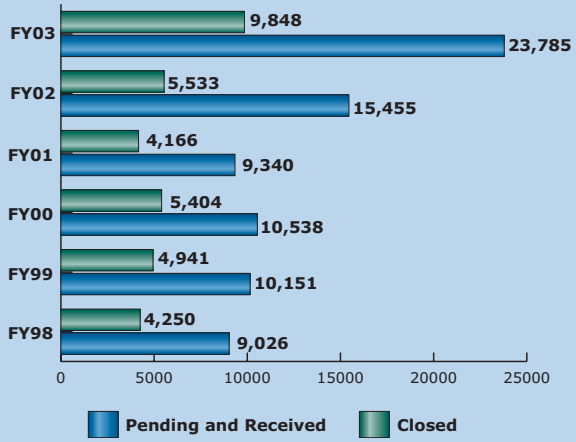
While the FBI plays a lead role in the investigation process, both the Criminal Division and the United States Attorneys are heavily involved in the DOJ's counterterrorism mission. The Criminal Division and the U.S Attorneys' offices focus on the development and prosecution of terrorism and cyberterrorism cases, as well as the preparation for and response to acts of terrorism. The Criminal Division also coordinates counterterrorism issues with the U.S. Attorneys' offices, other Executive Branch agencies, and multilateral organizations. The 94 United States Attorneys' offices are part of a national network that coordinates the dissemination of information and the development of a preventive, investigative and prosecutorial strategy among federal law enforcement agencies, primary state and local police forces, and other appropriate state agencies in each of the 94 federal judicial districts.

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.

Performance Measure: Number of Terrorist Cases Investigated [FBI]

- **FY 2003 Target:** In accordance with Departmental policy, targeted levels of performance are not projected for this indicator.
- **FY 2003 Actual:**
  Pending and Received: 23,785
  Closed: 9,848
- **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 FBI's counterterrorism program, this measure does show activity towards the ultimate goal of preventing terrorism.

Terrorist Cases Investigated [FBI]



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 Measure: Terrorism Related Convictions [EOUSA] (**NOTE:** 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.)

- **FY 2003 Target:** In accordance with Departmental policy, targeted levels of performance are not projected for this indicator.
- **FY 2003 Actual:** 661 defendants convicted (Terrorism Convictions: 103; Terrorism-Related Convictions: 558)
- **Discussion:** The substantial increase in convictions 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.

In the last year, the Department successfully prosecuted a number of persons accused of terrorist acts. Some of the notable achievements include charging six men in Buffalo, New York, allegedly trained at al Qaeda camps in Afghanistan, with providing material support to terrorists. Four individuals indicted in Detroit, Michigan, were charged with conspiracy to engage in fraud, misuse of visas and identification documents, and material support to terrorists. Also, six individuals in Portland, Oregon, were charged with engaging in a conspiracy to join al Qaeda and Taliban forces fighting against United States and allied soldiers in Afghanistan. The Department has also successfully prosecuted several persons accused of materially supporting terrorism or suspected of transferring funds to terrorists abroad.

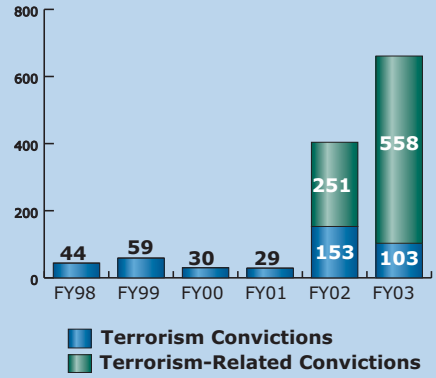
Data Definitions: Terrorism convictions are based on our historical data definitions in our original program categories of International Terrorism and Domestic Terrorism. Terrorism-related convictions include program categories for Terrorism-Related Hoaxes, Terrorist Financing, and Anti-Terrorism. These categories were implemented after September 11, 2001, and allow us to capture more terrorism-related work. **NOTE:** Not every case opened leads to an arrest or conviction.

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 the 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.

Terrorism-Related Convictions [EOUSA]



This page intentionally left blank.