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

Terrorism, both international and domestic, poses the most complex threat of any, for which the Department of Justice (DOJ) has responsibility. This was dramatically demonstrated by the attacks on September 11, 2001 and the subsequent anthrax attacks. International radical extremists and ad hoc coalitions of loosely affiliated individuals motivated by perceived injustices, as well as domestic groups and disgruntled individual American citizens – have attacked U.S. interests at home and abroad. They have increasingly chosen nontraditional targets and have employed unconventional weapons. In addition, the technological advancements of the information age have rendered crime-fighting efforts increasingly complex and have opened new avenues for global criminal activities. The increasing interconnectedness of critical infrastructures has created new vulnerabilities as criminals, terrorists, and hostile foreign intelligence services exploit the power of cyber tools and weapons.

To effectively address international and domestic terrorism, DOJ must concentrate on both prevention and response. The Department utilizes a multifaceted approach to detect, assess, deter, prevent, investigate, and respond to terrorist operations. On November 8, 2001, the Attorney General outlined a wartime reorganization and mobilization of the nation's justice and law enforcement resources to meet the counterterrorism mission of DOJ. To fulfill the critical mission of protecting the U.S. from the threat of terrorism, the DOJ will devote all resources necessary to disrupt, weaken, and eliminate terrorist networks, to prevent or thwart terrorist operations, and to bring to justice the perpetrators of terrorist acts. DOJ recognizes that success in counterterrorism efforts will require not only the coordinated efforts of all Department components, but also productive and cooperative efforts with other critical state, local, and federal partners.

Several of the Department's major components are heavily involved in the fight against terrorism:

- The *Federal Bureau of Investigation (FBI)* plays a critical role in identifying and countering threats to the U.S. In addition, the FBI is the designated Lead Agency for terrorism investigations and crisis management of terrorist acts that occur within the U.S. The FBI also provides specialized support in connection with terrorist acts against U.S. interests abroad and appropriate law enforcement assistance to foreign governments upon request.

- The *Immigration and Naturalization Service (INS)* and the Criminal Division work together to prevent the entry of terrorists into the U.S. through effective border control and through measures targeting smuggling organizations that may be used by potential terrorists. INS also works with the FBI in select counterterrorism investigations and exercises administrative removal authority against persons who finance or provide material support to terrorists or designated terrorists organizations.

- The *Drug Enforcement Administration (DEA)* provides intelligence support to the FBI and agencies conducting counterterrorism activities. Their Special Operations Division (SOD) serves as a point of contact for electronic surveillance assistance for terrorism-related requests.

- The *United States Attorneys* offices, through their Anti-Terrorism Task Force Coordinators, 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 and officials in each district throughout the country.

- The *Criminal Division (CRM)*, through the Terrorism and Violent Crime Section, focuses on the development and prosecution of terrorism cases, preparation for and response to acts of terrorism, and coordination of counterterrorism issues with the U.S. Attorneys' offices, other pertinent

Executive Branch agencies, and foreign governments. CRM's Computer Crime and Intellectual Property Section focuses on the development and prosecution of cyberterrorism cases and issues regarding gathering electronic evidence. In addition, CRM's Alien Smuggling Task Force coordinates investigations and prosecutions of alien smuggling organizations that may be used by potential terrorists.

- The *Office of Justice Program's (OJP)* Office of Domestic Preparedness (ODP) provides state and local agencies with grant funding and needed services to acquire specialized response equipment, training, and technical assistance. In an effort to consolidate the terrorism mission, in FY 2003, the ODP will transition to the Department of Homeland Security.

**STRATEGIC OBJECTIVE 1.1 & ANNUAL GOAL: PREVENT TERRORISM**
Prevent, disrupt, and defeat terrorist operations before they occur.

Dramatic changes in the international and domestic environments have produced credible and serious terrorist threats. Each of these threats, which include the efforts of international terrorists, the growing threat of use of weapons of mass destruction (WMD), and criminal acts perpetrated by domestic terrorists, present the Department with a clear, but difficult challenge.

The wide range of terrorist threats include: Osama bin Laden's Al Qaeda network, terrorist organizations attempting to obtain WMD capability, anthrax threats, attacks and hoaxes, radical animal rights and environmental groups, violent anti-government groups and white supremacists, and threats against the information infrastructure. Due to the diversity of the terrorist threat and the complicated nature of terrorist investigation and response, the Department focuses on developing the capacity to respond to any terrorist issue, whether it is domestic or international. While the Department cannot prevent all terrorism, by developing a structure to build and maintain maximum feasible capability, the Department is in a position to prevent and deter terrorism to the maximum extent possible.

To fulfill the critical mission of protecting the U.S. from the threat of terrorism, DOJ will devote all resources necessary to disrupt, weaken, and eliminate terrorist networks, to prevent or thwart terrorist operations, and to bring to justice the perpetrators of terrorist acts. DOJ recognizes that success in counterterrorism efforts will require not only the coordinated efforts of all Department components, but also productive and cooperative efforts with other critical federal, state, and local partners. DOJ is fully committed to breaking down the bureaucratic and cultural barriers that prevent meaningful coordination and cooperation between criminal law enforcement and counterintelligence operations, both within the Department and between the Department and other entities, while respecting legitimate legal restrictions.

While the federal government plays a major role in preventing and responding to terrorist incidents, the state and local public safety community serve as the nation's "first responders." The FBI provides both training and certification to state and local bomb technicians. Additionally, OJP's Office of Domestic Preparedness (ODP) provides state and local agencies with grant funding services to acquire specialized response equipment, emergency responder training and technical assistance, and support to plan and conduct exercises tailored to the circumstances of the jurisdiction. In FY 2003, ODP's functions will be transferred to the newly created Department of Homeland Security; however, OJP's National Institute of Justice (NIJ) will continue to support the development of technologies that enhance the ability of federal, state and local public safety agencies to prevent and respond to terrorist attacks and other critical incidents.

**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.

DOJ focuses on the criminal prosecution of terrorists to bring perpetrators to justice, disrupt terrorist operations, and disrupt financing of terrorism. The Department will pursue investigations based on various criminal violations, including material support to terrorists, espionage, money laundering, fraud, smuggling, immigration charges, and any other charge that may be applicable in order to fully utilize all tools available to investigators. Terrorism investigations will emphasize source development and intelligence gathering, as well as deterring and determining responsibility for acts of terrorism. In addition, the Department will continue to implement the new tools outlined in the USA PATRIOT Act, which will significantly aid law enforcement and intelligence partners in information sharing, coordination, and cooperation.

The Department will build strong cases for prosecution through the use the Joint Terrorism Task Forces headed by each FBI field office, and with the support of the district Anti-Terrorism Task Forces. Also, the Department will promote, and when available, use new legislation and authorities to prosecute suspected terrorists to the fullest extent of the law.

One of the Department's strategies to prevent and deter terrorist acts is to cut off the lifeblood of terrorism – its funding and other means of support. DOJ, in consultation with the State Department and the Department of the Treasury, exploits all available avenues to designate individuals and entities as terrorists, thereby freezing their financial assets and other means of support, excluding their members and associates from entering the U.S., and providing a basis for prosecuting those who offer material support to these individuals and entities. The Criminal Division plays a critical role in coordinating the focus on the financial underpinnings of terrorism through the Terrorism Financing Task Force. With the U.S. Attorneys, the FBI's Financial Review Group, and other federal agencies, the Task Force pursues the full range of available remedies: criminal prosecution, immigration proceedings, and seizing all financial assets.

The Criminal Division, through the Terrorism and Violent Crime Section, and the U.S. Attorneys' offices, are directly involved in the development and prosecution of major terrorism cases – particularly those involving extraterritorial acts of terrorism against Americans and American interest abroad, as well as in multidistrict terrorist fundraising cases, preparation for and response to acts of terrorism, and coordination of counterterrorism issues with other pertinent Executive Branch agencies, and multilateral organizations. Working closely with the Anti-Terrorism Coordinators in each U.S. Attorney's Office, the Terrorism and Violent Crime Section provides guidance and support to strengthen terrorism investigations and prosecutions. In the area of preparation for and response to acts of terrorism, the Terrorism and Violent Crime Section is responsible for administering the Department's Attorney Critical Incident Response Group and its Crisis Management Coordinators program, which involves the development of a crisis response plan for each federal judicial district and the training of specially selected federal prosecutors from the U.S. Attorneys' offices and the DOJ litigating divisions in crisis preparation and response techniques.

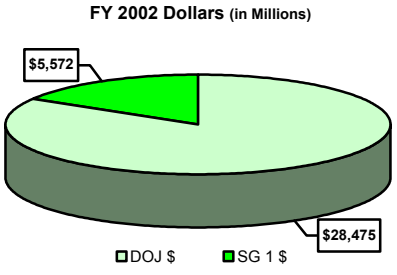
## PERFORMANCE SUMMARY

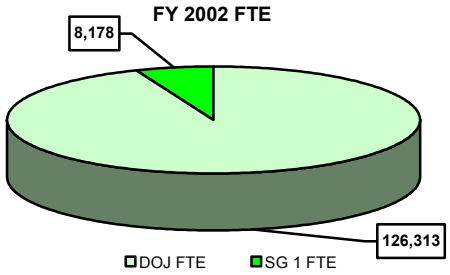
| Strategic Objective, Page # | | Performance Measure/ Indicator | Was the Target Achieved | | | FY 2002 Performance | | |
|---|---|---|---|---|---|---|---|---|
| | | | Yes | No | N/A | Target | Actual | Performance Improvement From FY 2001 |
| 1.1 | 6 | Terrorist Acts Committed by Foreign Nationals Against U.S. Interests within U.S. Borders | ■ | | | 0 | 0 | |
| 1.1 | 8 | Computer Intrusions Investigated<br>• Closed<br>• Open/Pending | | | ■<br>■ | N/A<br>N/A | 814<br>1,956 | |
| 1.1 | 8 | Computer Intrusions/ Convictions, Pretrial Diversions | | | ■ | N/A | 101 | |
| 1.1 | 9 | NEW MEASURE: Number of Compromised Computer Systems Identified and Notified | | | ■ | New for FY 2002 | 2,554 | |
| 1.1 | 9 | DISCONTINED MEASURE: Key Assets Identified | ■ | | | 6,100 | 10,418 | |
| 1.1 | 11 | State/Local Bomb Techs Trained | | ■ | | 1,050 | 882 | Reallocation of resources to CT mission |
| 1.1 | 12 | DISCONTINED MEASURE: Total # State/Local First Responders Trained | ■ | | | 132,284 | 192,643 | |
| 1.2/ 1.3 | 13 | Terrorist Cases Investigated<br>• Pending & Received<br>• Closed | | | ■<br>■ | N/A<br>N/A | 15,455<br>5,533 | |
| 1.2/ 1.3 | 14 | MEASURE REFINED: Terrorism Activities<br>• Terrorist Convictions<br>• Terrorism Related Convictions | | | ■<br>■ | N/A<br>N/A | 153<br>251 | |

## RESOURCES

| | Appropriation | FY 2002 FTE | FY 2002 Actual $ (millions) | FY 2003 FTE | FY 2003 Request $ (millions) | FY 2004 FTE | FY 2004 Request $ (millions) |
|---|---|---|---|---|---|---|---|
| 1.1 | Criminal Division | 46 | 8 | 56 | 9 | 57 | 9 |
| 1.1 | FBI | 7,672 | 1,502 | 5,810 | 1,152 | 6,681 | 1,406 |
| 1.1 | General Administration | 0 | 6 | 7 | 5 | 7 | 2 |
| 1.1 | Office of Justice Programs | 78 | 1,109 | 3 | 67 | 6 | 48 |
| 1.1 | US Attorneys | 15 | 2 | 55 | 7 | 55 | 7 |
| | *Subtotal 1.1* | *7,811* | *$2,627* | *5,931* | *$1,240* | *6,806* | *$1,472* |
| 1.2/1.3 | Criminal Division | 86 | 15 | 107 | 16 | 110 | 17 |
| 1.2/1.3 | FBI (see 1.1) | -- | -- | -- | -- | -- | -- |
| 1.2/1.3 | US Attorneys | 281 | 63 | 463 | 61 | 463 | 61 |
| | *Subtotal 1.2/1.3* | *367* | *$78* | *570* | *$77* | *573* | *$78* |
| | ***TOTAL SG 1*** | ***8,178*** | ***$2,705*** | ***6,501*** | ***$1,317*** | ***7,379*** | ***$1,550*** |

### RESOURCE COMPARISON: Strategic Goal to Total DOJ $ and FTE




| | |
|---|---|
| ***Required Skills*** | The Department requires skilled agents, attorneys, analysts, and linguists. Linguists are critical to supporting criminal and national security investigations and intelligence success. This goal requires the skills and abilities of experienced attorneys, law enforcement professionals, and intelligence analysts. |
| ***Information Technology Utilized*** | FBI programs in this area are supported by: the Integrated Statistical Reporting and Analysis Application (ISRAA), a centralized database which tracks statistical case accomplishment from inception to closure; the Automated Case Support System (ACS), a database which captures all information pertaining to the administration of cases; and internal databases that support the National Infrastructure Protection Center. |

## PROGRAM EVALUATIONS

There are no program evaluations planned for FY 2003.

## 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

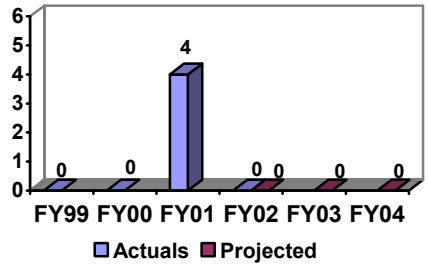
***FY 2002 Actual:*** 0

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

***FY 2003 Performance Plan Evaluation:*** Regardless of terrorist activity, the target will always remain zero terrorist acts.

***FY 2004 Performance Target:*** 0 terrorist acts.

**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.

***Public Benefit:*** The FBI's focus on building CT capacity ensures that all the elements are in place to prevent terrorism. The FBI works to build maximum feasible capacity, enabling investigators and analysts to pursue specific operational strategies against priority targets. The FBI is able to monitor progress towards achieving maximum capacity and to move resources to address gaps in the foundation that supports investigative efforts.

**Strategies to Achieve the FY2003/FY 2004 Goal:**
The FBI will continue to build maximum feasible capacity to ensure that the FBI has the capability to restrain all types of groups and individuals engaged in acts of terrorism and to deter and respond to threats *before* attacks occur. This strategy builds the capacity to safely and effectively respond to the challenges of unconventional terrorist methods such as the use of chemical, biological, nuclear, and radiological materials. A strategy of maximum feasible capacity requires all elements of crisis and consequence management at the federal, state, and local levels throughout the country to develop and implement integrated terrorism response plans. The strategy also builds the capacity to rapidly identify, locate, apprehend, and prosecute those responsible for terrorist attacks when they do occur; and to prevent, disrupt, and defeat terrorist elements and plans.

Specific strategies to build maximum feasible capacity include the complete implementation of the Counterterrorism Division (CTD) reorganization; full establishment of the Information Sharing Initiative currently in development with law enforcement partners; the integration of personnel (especially analytical personnel) into the CT program; and the full expansion of the Joint Terrorism Task Force (JTTF) program to all FBI Field Offices.

**Crosscutting Activities:**
Crosscutting functions include deterring and responding to terrorist acts; improving capabilities through training, planning, exercises, and research and development; and improving coordination domestically and internationally. The FBI has the lead in deterring and responding to terrorists acts which occur in the U.S., while the Department of State has the lead in regard to acts abroad which impact U.S. citizens or U.S. interests. The Department of Defense (DOD) assists with tactical and logistical support through well-established protocols. Extensive interagency and inter-jurisdictional training and exercising efforts focus on the goal of seamless counterterrorism response. The Criminal Division, in coordination with the Departments of State, the Treasury and others, works closely with our allies in the G-8, in the Council of Europe, in the Financial Action Task Force, in the United Nations, and in other multinational fora, to pursue common counterterrorism efforts.

Crosscutting efforts to establish comprehensive border enforcement include cooperation with local communities and industries, as well as Canadian and Mexican authorities. The Criminal Division's Alien Smuggling Task Force and INS meet regularly with Canadian and Mexican counterparts to identify and implement measures to improve border security. INS agents in offices worldwide will continue to work closely with the Department of State, DEA, the U.S. Customs Service, the FBI, the U.S. Coast Guard, the Department of Agriculture, and foreign governments in order to exchange information with foreign immigration counterparts and to better identify and disrupt terrorist activities. The Border Coordination Initiative (BCI) is a crosscutting effort to increase shared information and intelligence along the U.S.-Mexico border. Through the establishment of joint performance measures, BCI has proven successful and is considering priority areas for expansion such as the Northern Border. This will further bolster the borders against terrorism threats. Other cooperative intelligence/investigative efforts include the INS Law Enforcement Support Center, which provides a link between federal, state, and local law enforcement officers and the database accessed by INS, and the El Paso Intelligence Center, which is a DEA-led, multi-agency tactical intelligence center.

## 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 goal of FBI's National Infrastructure Protection Center (NIPC) is to enhance U.S. national security by preventing infrastructure damage through a multifaceted approach to maximize its investigative and preventative resources in order to thwart cyber attacks on the nation's infrastructure.

**Performance:**
***Performance Measure*:** Computer Intrusions Investigated [FBI]

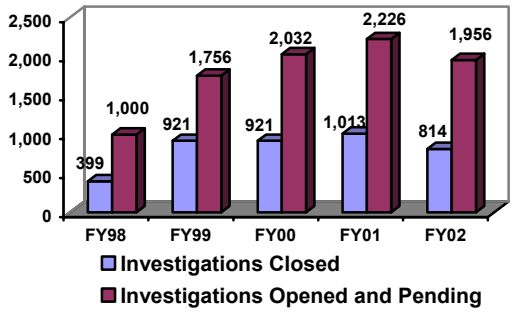
***FY 2002 Target:*** In accordance with Department guidance, targeted levels of performance are not projected for this indicator.

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

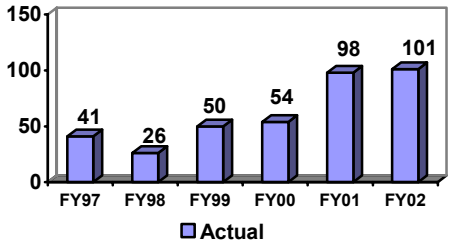
***Discussion:*** Changes in the number of investigations is largely proportional to the number of trained agents in the field who respond to reported intrusions. The number of computer intrusion investigations is also tied to an increase in the intelligence base of the FBI, as well as an increase in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

***FY 2003 Performance Target:*** N/A
***FY 2004 Performance Target:*** N/A
***Public Benefit:*** See below.

**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.

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

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

***FY 2002 Actual:*** 101

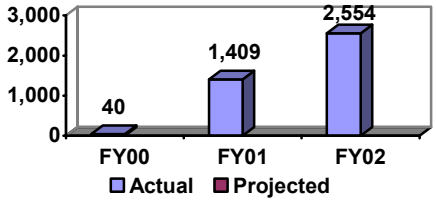
***Discussion:*** Computer intrusion convictions continue to rise as a result of increased investigations and level of agent expertise.

***FY 2003 Performance Target:*** N/A

***FY 2004 Performance Target:*** N/A

***Public Benefit:*** See below.

**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 (IIA) 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:*** NEW MEASURE: Number of Compromised Computer Systems Identified and Notified [FBI]

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

***FY 2002 Actual*:** 2,554

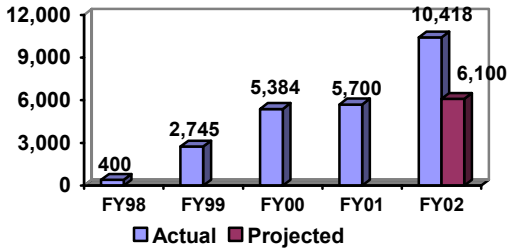
***Discussion:*** Through investigative efforts, additional compromised computer systems are being identified and the owners of these systems are being notified of the compromises and the methods utilized by the intruders to gain access to their computers. This performance measure reflects the complexity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

***FY 2003 Performance Target:*** N/A

***FY 2004 Performance Target:*** N/A

***Public Benefit:*** Through computer intrusion investigations and prosecutions, the FBI works to arrest those who perpetrate computer intrusions that affect the nation's infrastructure. In addition, these investigations enable the FBI to gather information, develop and solidify relationships with critical partners, and maintain a visible presence to both potential criminals and the American public.

**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 2 years may not be a true indicator of activity given that as new assets are identified, other assets may no longer meet the Key Asset criteria and are removed from the database.

***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.

***Public Benefit:*** The FBI's NIPC works closely with the private sector, law enforcement, industry, and government at all levels. The core of the NIPC approach is prevention, detection, and response.

**Strategies to Achieve the FY2003/FY 2004 Goal:**
Processes of contingency planning and determining cascading effects and interdependencies have already begun for some key assets. NIPC will continue to work to assess vulnerabilities and develop proactive techniques and countermeasures. NIPC will also work closely with the private sector and promote a close working relationship between law enforcement, industry, and government at all levels.

Specifically, NIPC will work to assess vulnerabilities and develop proactive techniques and countermeasures. Other strategies within NIPC include: 1) the recruitment of agents and analysts with specialized computer expertise; 2) training and education on computer incident investigations for both FBI personnel and public and private sector partners; 3) continuation of the InfraGard program to ensure that private sector infrastructure owner and operators share information about cyber intrusions, exploited vulnerabilities, 4) the development of an indications and warning network for federal computer systems; 5) the continuation of research and development; and 6) the provision of state of the art tools, technologies, and intellectual capital related to computer intrusions.

Also, the FBI's National Infrastructure Threat Warning System disseminates, advisories and vulnerability/threat assessments to public and private sector stakeholders and the law enforcement community. The FBI ensures the development and implementation of contingency plans designed to protect infrastructure assets, maintain maximum feasible capacity for deterrence, and facilitate the rapid response to threats, compromise, or attack.

**Crosscutting Activities:**
The NIPC staff includes detailees from federal and state agencies as well as two international partners. These agencies include: Department of Energy (DOE), Central Intelligence Agency (CIA), DOD, United States Air Force (USAF), Defense Central Intelligence Service, NSA, Postal Service, Navy, GSA, and others. NIPC staff ensures coordination with FBI field offices, other government agencies and foreign police and security. Rapid response to intrusions is often required, placing a premium on cooperation.

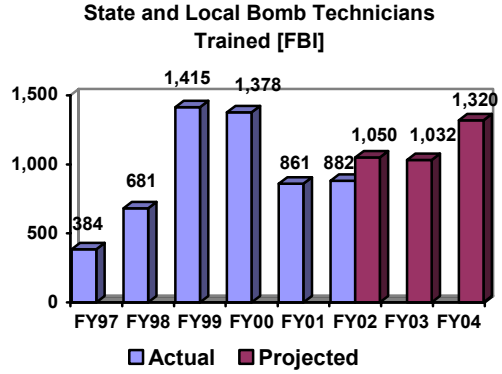
The InfraGard initiative encourages the exchange of information by government and private sector members through the formation of local InfraGard chapters within the jurisdiction of each FBI Field Office. Chapter membership includes representatives from the FBI, private industry, other government agencies, state and local law enforcement, and the academic community. The initiative provides four basic services to its members: an intrusion alert network using encrypted e-mail, a secure website for communications about suspicious activity or intrusions, local chapter activities, and a help desk for questions.

## 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 3 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)

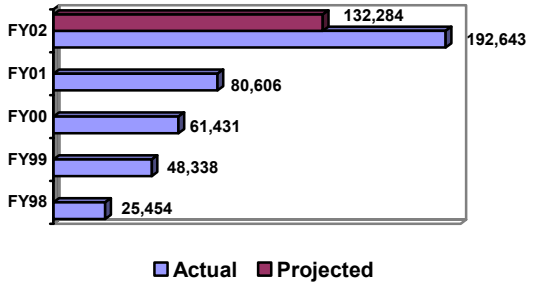
***FY 2002 Actual:*** 882

***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.

***FY 2003 Performance Plan Evaluation:*** Based on performance in FY 2002, we have revised our FY 2003 target downward. The revised target is 1,032.

***FY 2004 Performance Target:*** 1,320 students

***Public Benefit:*** The HDS is providing unique explosives training to all public safety bomb technicians in every state. Recent terrorist events and the increased availability of sophisticated and advanced technologies makes it essential that the FBI provide the best possible training for state and local bomb technicians. Training in new instruments and methods is critical to core competency and future operational and investigative successes.




**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.

***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.

***Public Benefit:*** First responders, emergency response agencies, and jurisdictions that have participated in ODP-sponsored training courses and exercises are better prepared to prevent or respond to a WMD terrorism incident resulting in enhanced safety for the first responders and the public, as well as more effective use of available resources.

**Strategies to Achieve the FY2003/FY 2004 Goal:**
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. A pilot course is anticipated during FY 2003. Any necessary revisions to the course will be made in FY 2004, with six courses planned for FY 2005.

**Crosscutting Activities:**
The HDS represents a partnership between the FBI and the U.S. Army to provide state and local law enforcement agencies with state of the art explosives training to improve domestic preparedness. Recent terrorist events and the increased availability of sophisticated and advanced technologies makes it essential that the FBI provide the best possible equipment and training for state and local bomb technicians. Training in new instruments and methods is critical to core competency and future operational and investigative successes**.**

ODP coordinates with and/or participates in joint activities with the Department of Health and Human Services, FEMA, the State Department, DOD, the National Security Council, and the Department of Energy. These working relationships are demonstrated through the joint participation in the planning and conducting of national exercises, such as the ODP-sponsored Top-Off exercises, the Training Resources and Data Exchange Group, the Interagency Board for Equipment Standardization and Interoperability, and the Domestic Preparedness Support Helpline.

**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

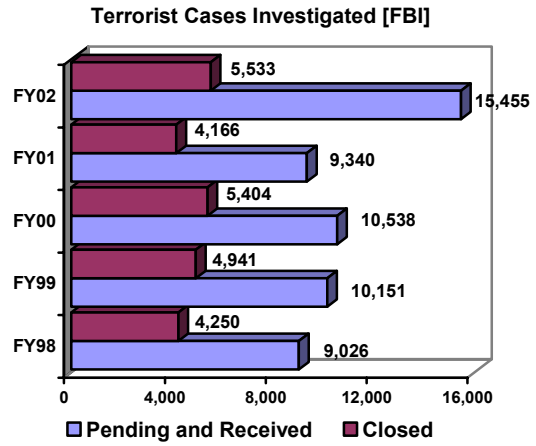
## 1.2 – 1.3A Investigate and Prosecute Terrorists' Acts

**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, Firearms, and Explosives (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 Terrorist Cases Investigated [FBI]

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

***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, this measure does show activity towards the ultimate goals of preventing terrorism.

***FY 2003 Performance Target:*** N/A

***FY 2004 Performance Target:*** N/A

***Public Benefit:*** The Department's multi-faceted effort seeks to prevent future terrorist attacks, investigate acts of terror, and prosecute those who intend to commit or have committed terrorist acts against the United States. Law enforcement officials at all levels of government – federal, state, local – must work together, sharing information and resources needed to arrest and prosecute individuals responsible. The preventive and investigative efforts culminate with the prosecution of terrorist acts.

***Performance Measure:*** MEASURE REFINED: Terrorism Related Convictions (*Formerly:* Number of Terrorist Convictions) [EOUSA]

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

***FY 2002 Actual:***

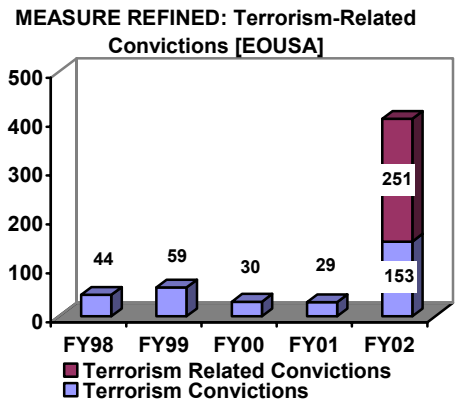
Terrorism Convictions: 153

Terrorism-Related Convictions: 251

***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. As of August 2002, the United States Attorneys began a review of their terrorism caseload data to classify these cases based on a new set of terrorism codes.

***FY 2003 Performance Target:*** N/A

***FY 2004 Performance Target:*** N/A




**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 and allow us to capture more terrorism-related work.

**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.

***Public Benefit:*** The public benefit from the prosecution of terrorists, associates of terrorists, and supporters of terrorists is the prevention and deterrence of terrorism. In the last year, the Department has successfully prosecuted a number of person's accused of terrorist acts, such as the American Taliban, John Walker Lindh and the airplane shoe bomber, Richard Reid. The Department has also successfully prosecuted several persons accused of materially supporting terrorism or suspected of transferring funds to terrorists abroad.

**Strategies to Achieve the FY2003/FY 2004 Goal:**
FBI will continue to attack terrorism by investigating those persons and countries that finance terrorist acts. The Department will aggressively use the money laundering and asset forfeiture statutes to locate and disrupt the financial sources of terrorist organizations. FBI will also work to effectively and efficiently utilize the tools authorized by Congress in the USA PATRIOT Act of 2001. While the ultimate goal is to prevent a terrorist act before it occurs, the FBI must be able to respond should an act occur. FBI's efforts in this area include improved information gathering and sharing, improved analytical capabilities, and enhanced training and liaison.

The U.S. Attorneys, along with the Criminal Division, will continue utilizing the USA PATRIOT Act as a vital weapon in the war against terrorism. Under the law, prosecutors and law enforcement officers may now share grand jury and wiretap information regarding foreign intelligence with a wide range of federal personnel, including State Department officials, including those responsible for issuing visas, and members of the intelligence and national defense communities. In addition, we will target and prosecute cases developed by the Terrorist Financing Task Force and the Financial Review Group.

**Crosscutting Activities:**
DOJ coordinates with other Executive Branch partners. These include the Central Intelligence Agency (CIA), DOD, the Departments of State and the Treasury, Department of Transportation (DOT), FEMA, National Security Agency (NSA), the Department of Energy (DOE), Environmental Protection Agency (EPA), the Department of Commerce, and the Department of Agriculture. The National Defense Authorization Act of 1996 provided funding and a training mandate to assist state and local authorities in the proper response to a terrorist incident. The DOJ participates with DOD, DOE, and EPA in the development and delivery of this training.

INS cooperates with federal, state, and local law enforcement organizations, to create a secure and seamless border management system. The crosscutting activities required for this effort are extensive and are discussed in detail in Strategic Goal 5.1 Secure America's borders.

This page intentionally blank.