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 has responsibility. As dramatically evidenced 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 to 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 identifying and countering threats to the U.S. In addition, the FBI is the designated Lead Agency for terrorism investigations and crisis management. The FBI also provides law enforcement assistance and other specialized support when required.

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 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. It's 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 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 multilateral organizations. In addition, CRM's Computer Crime and Intellectual Property Sections focuses on the development and prosecution of cyberterrorism cases and issues regarding gathering electronic evidence.

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. This office transitions to Federal Emergency Management Agency (FEMA) in FY 2003.

MANAGEMENT CHALLENGES

There are no existing material weaknesses that will hinder the achievement of goals in this area in FY 2003.

However, the DOJ Office of Inspector General's (OIG) December 2001 list of the top ten management challenges facing the Department includes two management challenges in this area:

Counterterrorism: Last year, the OIG restated the General Accounting Office (GAO) finding that governmentwide, anti-terrorism resources were not clearly linked to a threat analysis and a national anti-terrorism strategy (GAO report #T-NSIAD-00-145). According to GAO, this situation creates the potential for gaps or duplication in the United States' anti-terrorism strategy. This year, in light of the September 11, 2001, terrorist attacks on the United States, the OIG has sharpened its focus on this issue. In particular, the OIG refers to the FBI's use of its counterterrorism funds, the mix of cases the FBI chooses to investigate, and the FBI's management of its information technology projects. The OIG also refers to the domestic preparedness grants the OJP awards to state and local entities for training and equipment to respond to acts of terrorism, as well as the amount of funding awarded and whether grants are being used for their intended purpose. Finally, the OIG refers to various INS endeavors, such as the Visa Waiver Program, their efforts to control the northern border, the criteria for sending non-immigrants to secondary inspection at air ports of entry, an automated system to monitor foreign students, and their use of Advance Passenger Information System data to help deter the entry of terrorists or other criminals into the U.S.

Sharing of Intelligence and Law Enforcement Information: The September 11 terrorist attacks also highlighted the critical importance of sharing intelligence and other law enforcement information among federal, state, and local agencies, both for the investigation of terrorist attacks and for the prevention of future attacks. DOJ must ensure that law enforcement agencies at all levels have access to information that could be important in helping detect and deter terrorist attacks. In late October, the President signed the *USA PATRIOT Act of 2001*, which permits greater sharing of intelligence and law enforcement information. The Department faces significant challenges in both ensuring that these new authorities are used appropriately and in ensuring that other federal, state, and local law enforcement agencies have access to information important to their work.

Performance measures related to these management challenges are noted.

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

Annual Goal 1.1: Prevent, disrupt, and defeat terrorist operations before they occur.

STRATEGIES

- Establish Anti-Terrorism Task Forces within each jurisdictional district to coordinate anti-terrorist activities.
- Build and maintain the FBI's fullest capacity to detect, deter, counter, and prevent terrorist activity.
- Develop an intelligence capability that fully supports the Department's counterterrorism efforts.
- Mitigate threats, especially cyber-threats, to the U.S. national infrastructure.
- Fully coordinate with federal, state, and local government agencies in a comprehensive effort to develop and maintain adequate domestic preparedness.

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 criminal 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 Ladin's al Qaeda network, terrorist organizations attempting to obtain a WMD capability, anthrax 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 state, local, and federal 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 our nation's "first responders." 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 addition, the FBI provides training and certification to state and local bomb technicians.

MEANS – Annual Goal 1.1

Dollars/FTE*

Appropriation	FY 2001 Actual		FY 2002 Enacted		FY 2003 Requested	
	FTE	$ mill	FTE	$ mill	FTE	$ mill
Criminal Division	22	4	26	4	31	5
FBI Construction	0	0	0	5	0	0
FBI	4064	595	3834	1063	4392	783
General Admin.	0	0	0	6	7	5
Counterterrorism	0	47	0	5	0	35
OJP (ODP)	48	91	81	646	0	0
U.S. Attorneys	0	0	35	3	55	4
Sep. 11th Fund	[0]	[0]	[0]	[1080]	[0]	[2700]
Subtotal	**4134**	**$737**	**3976**	**$1732**	**4485**	**$832**

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

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.

PERFORMANCE ASSESSMENT – Annual Goal 1.1

1.1A Prevent Terrorists' Acts

Background/Program Objectives:
It is the Department's goal to prevent terrorist acts. In order to achieve that objective, DOJ will build maximum feasible capacity in the counterterrorism program, allowing the Department to identify, assess, and address terrorist threats. Maximum feasible capacity assumes that the political/religious/social movements that drive terrorism are often beyond the control of any one department or government; therefore, it may not be possible to prevent all acts of terrorism. Through this strategy, however, the Department specifically identifies the critical elements of a fully successful counterterrorism program to: 1) assess current capacity, 2) identify performance gaps; and 3) develop strategies to fill these gaps and maximize the government's ability to address terrorist threats.

Performance:
Pilot Performance Measure: Performance Capacity Indicator (PCI)

Status*:* The FBI is finalizing the Performance Capacity Indicator (PCI). The PCI is a statistically valid, numerical measure of the capacity of the FBI CT to accomplish its mission to prevent, disrupt, and defeat terrorist acts before they occur; pursue the arrest and prosecution of those who have conducted, aided, and abetted those engaged in terrorist acts; and to provide crisis management following acts of terrorism against U.S. interests. The indicator works by measuring the interaction between the FBI counterterrorism program's capacity and the external environment. By comparing these factors, the CTD is able to assess its progress in achieving its mission. An increase in the PCI represents an increase in the capacity of the FBI CT to accomplish its mission. This indicator will be completed by March 2002 and will include outyear performance targets. Additionally, the FBI will continue to report other measures in combination with the PCI. Although much of the data used to calculate the index is classified, the equation and the numerical result will be included in the Department's FY 2002 performance report.

Pilot Performance Measure: Performance Capacity Indicator (PCI)

Data Definitions: The PCI is derived from three variables that provide a snapshot of what the FBI Counterterrorism (CT) Program Capacity is, relative to the current environmental conditions and threat. The specific variables used in construction of this index are classified.

Data Collection and Storage: The data source for the PCI is obtained through the FBI CT component of the FBI's automated Annual Field Office Report (AFOR), which is submitted annually by each of the 56 FBI field offices, along with other data sources utilized by the FBI's CT Division. These data sources contain relevant information regarding the overall CT capacity not necessarily exhibited through the AFOR process.

Data Validation and Verification: The data source information is compiled, analyzed, and verified at FBI headquarters. The information is applied to a formula with the result being a numerical indicator, which expresses capacity relative to the prevailing threat level. The FBI will focus efforts on maximizing this score and the capability it represents.

Data Limitations: The data collection method relies upon FBI program managers to audit survey findings to ensure reliability. Although this method relies upon expert knowledge to make the reported information reliable, the survey instrument is still being perfected to provide clear examples of how data responses should reliably report findings.

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

FY 2001 Target: 0

FY 2001 Actual: 6

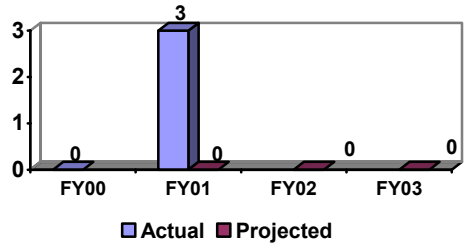
Discussion: Incidents reported for FY 2001 are as follows: September 11, 2001 Suicide airplane bombing of towers One and Two of the World Trade Center (New York, New York), Suicide Airplane bombing of the Pentagon (Washington, DC), and Hijacking/Crash United Airlines flight #93 (Stony Creek, PA).

FY 2002 Performance Plan Evaluation: Regardless of terrorist activity, the target will always remain zero.

FY 2003 Performance Plan: 0 Terrorist Acts

Strategies to Achieve the FY2003 Goal:
A strategy of maximum feasible capacity builds 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. It 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. It requires all elements of crisis and consequence management at the federal, state, and local levels through the country to develop and implement integrated terrorism response plans. It 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, including computer intrusion and infrastructure threats, through early watch and warning capability and preventive measures.

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



Data Definitions: Terrorist Acts Committed by Foreign Nationals counts separate incidents 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 purposes of this measure, a terrorist act can involve one or more perpetrators, but is directed towards a single general target (e.g., a building or physical structure, an aircraft). Although there may be several terrorist acts cited, two or more of these acts may represent a concerted effort to have a widespread, simultaneous impact (e.g., the events of September 11, 2001).

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

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 and the opinion of program managers making the determination. 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 only 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.

Other key components within the Department will also contribute to the deterrence of counterterrorism. DEA will partner with FBI on intelligence analysis and the INS will enhance efforts to obtain tactical and strategic intelligence in source countries and share it with relevant partners. INS will support FBI investigations and conduct investigations of other foreign threats to the national security to disrupt and dismantle terrorism cells and supporters within the U.S. The Department will build on existing liaison mechanisms with foreign governments, intergovernmental organizations, and industry partners. INS intelligence will provide relevant INS offices with a list of terrorist organizations, as identified by the U.S. Intelligence Community that present the most significant threat to U.S. border integrity. Through a collaborative effort, primary organizations/individuals will be targeted. Intelligence gathering activities also include coordination of anti-smuggling/terrorism strategies with the FBI; the completion of a U.S.-Canada bilateral common threat assessment among all concerned agencies on border zones' vulnerabilities; and increased automation in the intelligence collection and analysis process. To improve the effectiveness of efforts to apprehend persons attempting illegal entry, INS will expand international operations to provide consultative services concerning validity of travel documents to airline and immigration officials at airports. Finally, the INS will conduct special, short-term coordinated enforcement operations in source and transit countries, resulting in the apprehension and repatriation of *mala fide* migrants en route to the U.S.

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. Department of Defense (DOD) leads 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. DOJ, 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, 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. 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 (Management Challenge)

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. First, most infrastructures rely on commercially available technology, which means that a vulnerability in hardware or software is not limited to one company, but is likely to be widespread. Second, infrastructures are increasingly interdependent and interconnected with one another, so it is difficult to predict the cascading effects that the disruption of one infrastructure would have on others. Third, 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 maximize its investigative and preventative resources to thwart cyber attacks on the nation's infrastructure.

Performance Measure: Computer Intrusions Investigated

FY 2001 Target: Not Targeted (see below)

FY 2001 Actual: Computer Intrusion Investigations Closed – 1,013, Computer Intrusion Investigations Opened and Pending – 2,226

Discussion: The increase in investigations is directly proportional to the number of trained agents in the field who have the ability to respond to reported intrusions. The number of computer intrusion investigations is also tied to an increase in the intelligence base of the Bureau, as well as an industry partners' increase in violation reporting through the InfraGard and Key Asset programs.

FY 2002/2003 Performance Plan Evaluation: In accordance with Department guidance, targeted levels of performance are not projected for this indicator

Public Benefit: See below.

Performance Measure: Computer Intrusion Convictions Number of Computer Intrusion Convictions/Pre-Trial Diversions

FY 2001 Target: Not Targeted (see below)

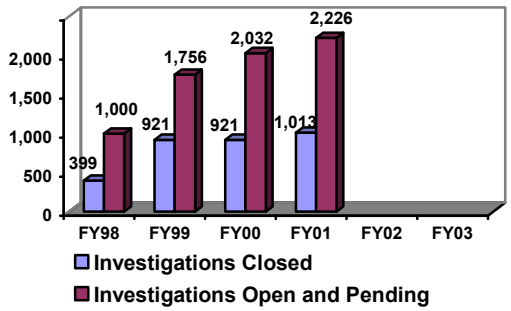
FY 2001 Actual: 91 (84 convictions, 7 pre-trial diversions)

Discussion: Computer intrusions convictions rose as a result of increased investigations and level agent expertise.

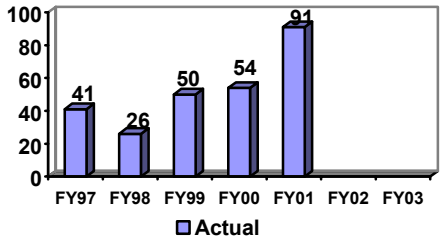
FY 2002/2003 Performance Plan Evaluation: In accordance with Department guidance, targeted levels of performance are not projected for this indicator.

Public Benefit: Through computer intrusion investigations and prosecutions, DOJ works to arrest those who perpetrate computer intrusions that affect the nation's infrastructure. In addition, these investigations enable the Department to gather information, develop and solidify relationships with critical partners, and maintain a presence visible to both potential criminals and the American public, all of which are critical pieces of the Department's efforts against terrorism.

Computer Intrusions Investigated [FBI]



Computer Intrusion Convictions/Pre-Trial Diversions [FBI]



Data Definition: Pretrial Diversion: A pretrial diversion can be claimed when a subject and the USA agree to a pretrial diversion plan under which the subject must complete a plan of lawful behavior in lieu of prosecution. Generally, a pretrial 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: For the computer intrusions, before data is entered into the system, they are reviewed and approved by an FBI field manager. 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: Key Assets Identified

FY 2001 Target: 3,200

FY 2001 Actual: 5,700

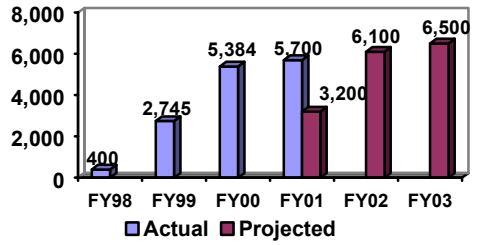
Discussion: The target was exceeded. The number of Key Assets indicates the number of identified organizations, systems, or physical plants, the loss of which would have widespread or dire economic or social impact on a national, regional, or local basis. FBI field agents identify assets in their jurisdiction 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.

FY 2002 Performance Plan Evaluation: Based on program performance in FY 2001, we establishing FY 2002 target to 6,100.

FY 2003 Performance Target: 6,500

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

Key Assets Identified [FBI]



Data Collection and Storage: Key Assets are identified and entered into a database.

Data Validation and Verification: The mapping process helps to verify that an "asset" is a critical Key Asset and any others that have not been identified. This results in a continual process of validating the information. The maps/grids produced from the database are used to plan for various scenarios in the event of a threat or an incident.

Data Limitations: Although the numbers provided are cumulative, the delta between any two 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.

Strategies to Achieve the FY 2003 Goal:

Key Assets continue to be identified. Simultaneously, processes of contingency planning, 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. In FY2003, DOJ will develop all necessary assets and capabilities to support operations aimed at disrupting and defeating threats to critical infrastructures.

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 and infrastructure protection for both FBI personnel and public and private sector partners; 3) continuation of the InfraGard program to ensure that private sector infrastructure owners and operators share information about cyber intrusions, exploited vulnerabilities, and physical infrastructure threats; 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 and infrastructure protection.

In addition, the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) will provide expert legal and technical advice regarding information warfare, infrastructure protection and other topics related to Critical Infrastructure Protection. During FY 2003, CCIPS will focus on: international outreach, in coordination with the Department's Office of International Affairs and the State Department; increasing mechanisms for information sharing between industry and government; legal and policy issues presented by intrusions detection systems, penetration testing and other means of protecting critical networks; devising means to protect network resources while respecting the legitimate privacy rights of persons who use those networks; encouraging the private sector to take sufficient measures to help protect the infrastructure; and develop prevention programs, such as the Cybercitizen Partnership, to increase public awareness and teach responsible/ethical online behavior.

Also, the FBI's National Infrastructure Threat Warning System in the U.S disseminates infrastructure protection alerts, advisories, and vulnerability/threat assessments relative to infrastructure protection to the 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 to 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, etc. 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 (Management Challenge)

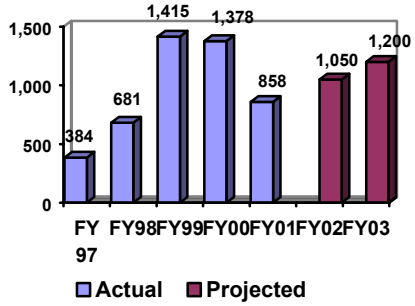
Background/ Program Objectives:
Two key elements of domestic preparedness include expertise in hazardous devices and emergency response capabilities to threats such as weapons of mass destruction. The Hazardous Devices School (HDS) is the only formal domestic training school for state and local law enforcement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

Qualifications for bomb technician certification include graduation from the HDS Basic Course, and the continued successful 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 be assigned to bomb squad responsibilities by that organization. Other course offerings include the Robot and Executive Management Courses.

OJP's Office of Domestic Preparedness (ODP) provides 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 weapons of mass destruction (WMD). ODP provides services to acquire specialized response equipment and emergency responder training, technical assistance, and support to plan and conduct exercises tailored to the circumstances of the jurisdiction. ODP courses are designed 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, as well as provide intensive technician and operations courses that demonstrate the effects of and response to live agents, explosives, and radiation. ODP also established the Center for Exercise Excellence, which will teach state agencies and local jurisdictions how to plan and conduct effective exercises. ODP is transferring to the Federal Emergency Management Agency in FY 2003.

.**Performance:**
Performance Measure: State and Local Bomb Technicians Trained [FBI]
FY 2001 Target: NA – new measure
FY 2001 Actual: 858
Discussion: In FY 2001, HDS trained 858 students from all 50 states, the District of Columbia, and Puerto Rico. Since 1999, the FBI Bomb Data Center has distributed specialized WMD related equipment to state and local bomb squads, and the HDS has integrated this new equipment into its training program. This training has included special bomb suits for WMD events, computerized X-ray, and chemical gas monitoring equipment.
FY 2002 Performance Plan Evaluation: Based on program performance in FY 2002, we expect to meet the corresponding FY 2002 target.
FY 2003 Performance Target: 1,200
Public Benefit: The HDS is providing unique explosives training to all public safety bomb technicians in every state across the country. 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.

NEW MEASURE: State and Local Bomb Technicians Trained[FBI]



Data Collection and Storage: Data is 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 Measure: Number of First Responders Trained (NOTE: This indicator has been refined to include the cumulative total of training offered in this area and prior year actuals have been corrected to reflect the most accurate and current data available.)

FY 2001 Target: 74,431 (adjusted for correction in cumulative totals)

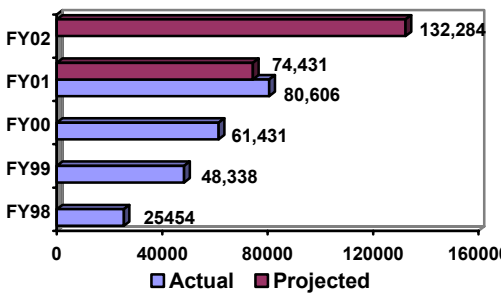
***FY 2001 Actual*:** 80,606

Discussion: In FY 2001, ODP exceeded the target through expanded existing training and new course development. ODP plans to implement an enhanced evaluation program that will provide information to assess enhancements in preparedness at the state and local levels, and to modify and/or enhance program services.

FY 2002 Performance Plan Evaluation: Based on program performance in FY 2001 and an increase in resources, we are increasing the FY 2002 target to 132,284.

FY 2003 Performance Target: NA. ODP will transfer to the Federal Emergency Management Agency.

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. For example, several days into the Arlington County, Virginia response to the September 11, 2001 terrorist attack at the Pentagon, the County Manager indicated that "everything just came together", attributing the successful response to the exercises, training, and planning they participated in, much of which was sponsored by ODP.



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.

Strategies to Achieve the FY 2003 Goal:

As part of the Domestic Terrorism Program, each of the 56 FBI Field Offices has a Weapons of Mass Destruction (WMD) Coordinator, who works to facilitate participation in federal interagency WMD development forums; to develop and deliver training to FBI officials, managers, agents, and field office personnel; and to facilitate and assess field office and FBI Headquarters participation in interagency WMD-related exercises. The FBI also provides a service to the Federal, state and local emergency response community through WMD training and assistance provided by the FBI's Hazardous Materials Response Unit (HMRU) and it's Critical Incident Response Group (CIRG).

The FBI and the U.S. Army will construct a new world-class HDS facility at Redstone Arsenal, Huntsville, Alabama. The current FBI-funded and administered facility at Redstone provides basic, recertification, and other training for approximately 2,300 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 HDS Advanced Course is under development, and will be fully operational as soon as the new HDS facility is completed. A series of pilot courses are anticipated during FY 2002 and FY 2003 to prepare for the full program, which will likely be at the beginning of FY 2004.

States conducted assessments of the threat and vulnerability for terrorism and the capacity and needs of their public health and public safety systems using an assessment tool developed by ODP in cooperation with the FBI and Center for Disease Control and Prevention. The states are using the assessment data, obtained from state agencies and local jurisdictions, to develop State Domestic Preparedness Strategies that will serve as the basis for the allocation of grant funds for the purchase of WMD response equipment and will assist ODP in developing and delivering training and exercise support. To ensure that the grant funds are used to address the greatest needs, states may not apply for FY 2000 and/or 2001 grant funds until they have completed their statewide strategy. All states should have their plans submitted by the second quarter of FY 2002, which will be reviewed and approved by the end of FY 2002.

The FBI is responsible for managing the FBI's National Counterterrorism Threat Warning System in the U.S., which disseminates terrorism alerts, advisories, and threat assessments, to the U.S. counterterrorism community, FBI field offices, and national law enforcement. The FBI maintains contacts with counterparts in international and domestic counterterrorism, law enforcement, and intelligence communities as well as with other relevant entities.

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.

ODP coordinates with the FBI's National Domestic Preparedness Office and will continue such coordination with the newly established Office of National Preparedness in the Federal Emergency Management Agency and, as appropriate, with the newly established White House Office of Homeland Security. In addition ODP coordinates and/or participates in joint activities with the Department of Health and Human Services, the Department of Defense, 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 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.

Annual Goal 1.2 – 1.3: Develop and implement the full range of resources available to investigate terrorist incidents, bringing their perpetrators to justice and vigorously prosecute those who have committed, or intend to commit, terrorist acts against the United States.

STRATEGIES 1.2

- Develop the Anti-Terrorism Task Forces within each jurisdictional district to coordinate investigations of anti-terrorist activities.
- Promote and, when available, use new legislation and authorities to conduct investigations of terrorist incidents.
- Apply all resources available to develop a comprehensive approach to investigating acts of terrorism.

STRATEGIES 1.3

- Build strong cases for prosecution through the use of district Anti- Terrorism Task Forces and the evidence they develop.
- Promote and, when available, use new legislation and authorities to prosecute suspected terrorist criminals to the fullest extent of the law.

The 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 determining responsibility for act of terrorism. In addition, the Department will continue to implement the new tools outlined in the recently passed 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 of district Anti-Terrorism Task Forces and the evidence they develop. Also, the Department will promote, and when available, use new legislation and authorities to prosecute suspected terrorist criminals to the fullest extent of the law.

Another way 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 and other federal agencies, this 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, 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 multilateral organizations. The Terrorism and Violent Crime Section, through its Regional Antiterrorism Coordinators, works closely with the Antiterrorism Coordinators in each U.S. Attorney's office to provide guidance and support on terrorism investigations, prosecutions, and related issues. The Terrorism and Violent

Crime Section is directly involved in the development and prosecution of major terrorism cases, particularly those involving extraterritorial acts of terrorism against Americans and American interests abroad, as well as in multidistrict terrorist fundraising cases. In the aftermath of the events of September 11, the Criminal Division 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 who assist in the financing of international terrorism. The 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. Through these efforts, the Criminal Division pursues the full range of available remedies including criminal prosecution, immigration proceedings, and seizing of financial assets, in conjunction with the U.S. Attorneys and other federal agencies. 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 in crisis preparation and response techniques.

MEANS – Annual Goal 1.2-1.3

Dollars/FTE*

Appropriation	FY 2001 Actual		FY 2002 Enacted		FY 2003 Requested	
	FTE	$ mill	FTE	$ mill	FTE	$ mill
Criminal Division	45	8	50	8	60	9
FBI (see 1.1)	0	0	0	0	0	0
U.S. Attorneys	50	7	366	61	463	63
Subtotal	**95**	**$15**	**416**	**$69**	**523**	**$72**

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

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; and the Automated Case Support System (ACS), a database which captures all information pertaining to the administration of cases

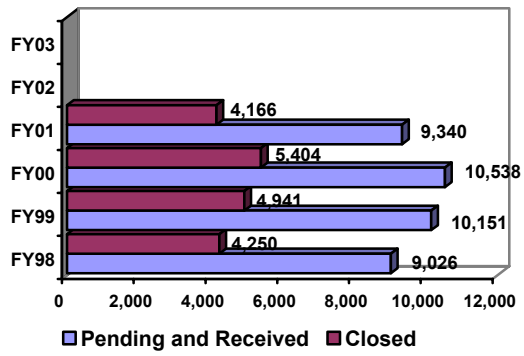
PERFORMANCE ASSESSMENT – Annual Goal 1.2- 1.3

1.2 – 1.3A Investigate and Prosecute Terrorists' Acts

Background/Program Objectives:
Through both 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 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 and the development of an investigation and prosecution strategy throughout the country. The implementation of these task forces coordinated by the United States Attorney in each district provides the operational foundation for a concerted national assault against terrorism.

In addition, the Criminal Division 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 who assist in the financing of 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 investigations convictions Monthly Administrative Report (MAR), which tracks the number of cases opened, pending and closed within any given time period; and ISRAA, a centralized database that tracks statistical accomplishment of cases from inception to closure.

Data Validation and Verification: Before data are entered into the ISRAA system they are reviewed and approved by an FBI field manager. 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:
Performance Measure: Number of Terrorist Cases Investigated

FY 2001 Target: Not Targeted (see below)

FY 2001 Actual: Terrorist cases closed – 4,166
Terrorist cases opened and pending – 9,340

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, in conjunction with the above performance capacity indicator, this measure does show activity towards the ultimate goal of preventing terrorism.

FY 2002/2003 Performance Plan Evaluation: In accordance with Department guidance, targeted levels of performance are not projected for this indicator.

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, and 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: Number of Terrorist Convictions (Former Title: Number of Terrorist and Pre-Trial Diversions was changed as there are no Pre-Trial Diversions in terrorist cases) NOTE: All conviction data including prior year actuals, are now provided from EOUSA instead of FBI to improve accuracy and reliability.

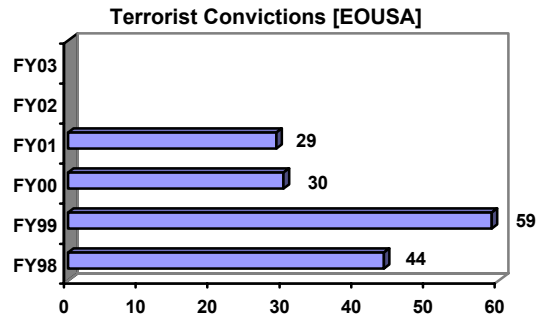
FY 2001 Target: Not Targeted (see below)

FY 2001 Actual:

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 program category or the International Terrorism program category. The data therefore, do not include terrorists convicted through other types of charges. Also, at the inception of an investigation, the original classification by investigative agencies may differ from the designation that occurs at the U.S. Attorney's office.

FY 2002/2003 Performance Plan Evaluation: In accordance with Department guidance, targeted levels of performance are not projected for this indicator.

Public Benefit: The Department's ability to prosecute terrorist cases serves as both a necessary outcome to fruitful investigations and as a deterrent to future acts of terror.



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 United States Attorneys' central case management system, which contains district information including criminal matters, cases, and appeals.

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

Data Limitations: As noted above, the United States Attorneys' 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.

Strategies to Achieve the FY 2003 Goal:

FBI will continue to attack terrorism by investigating those persons and countries that finance terrorist acts. FBI 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.

INS will contribute to the counterterrorism effort by cooperating with other Federal law enforcement and intelligence agencies to conduct investigations of foreign threats to the national security, placing particular emphasis on disrupting and dismantling terrorist cells and supporters in the U.S. INS intelligence personnel will collect, identify, and disseminate investigative leads. The Intelligence Program will provide direct support to anti-terrorism operations through an internal Intelligence Operational Support Unit committed to supporting the National Security Unit.

The U.S. Attorneys, along with the Criminal Division, will utilize the recently enacted USA PATRIOT Act as a new and vital weapon in the war against terrorism. Under the new 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.

In addition, the INS Legal Proceedings Program works in partnership with U.S. Attorney's Offices to increase the number of criminal prosecutions in cases where repeat immigration violators are apprehended. Where feasible, INS will participate in the criminal prosecution process and assist in training federal prosecutors on how to use expedited means of removal such as stipulated judicial removal, administrative removal, smuggling, trafficking, document fraud, and benefits fraud.

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), Federal Emergency Management Agency, 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, the Department of Energy, 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.