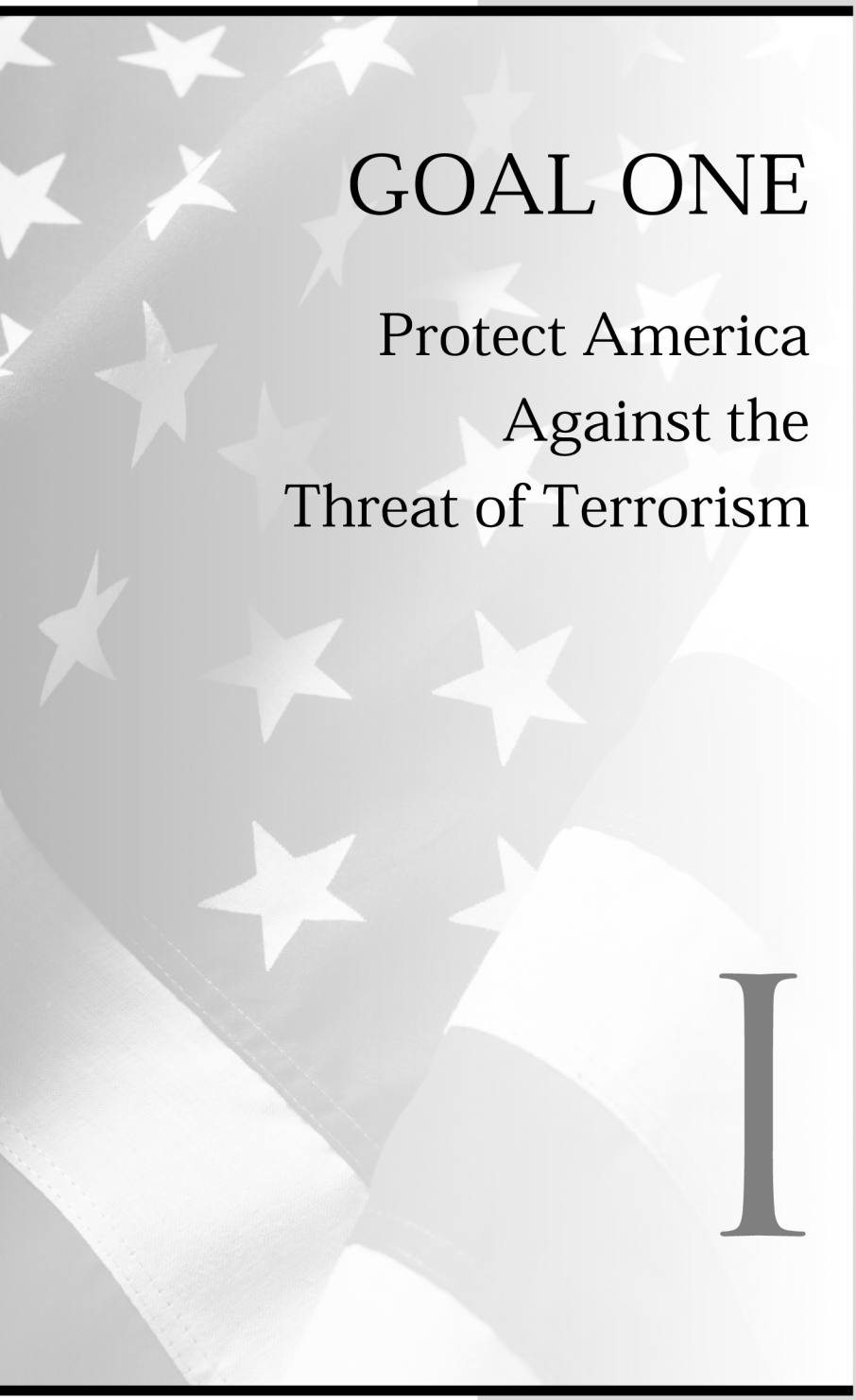

GOAL ONE

Protect America Against the Threat of Terrorism

I

GOAL ONE

Protect America Against the Threat of Terrorism

The orchestrated attacks on the World Trade Center in New York City and on the Pentagon in Washington, D.C., and aborted attacks on other U.S. targets, have brought terrorism dramatically to American soil. With the attacks, terrorism for most citizens shifted from being a distant, occasional threat to a realization of imminent danger to ourselves, our families, and our institutions. The enormous loss of life and property argues forcefully that the homeland must be protected from future terrorist assaults. The Department of Justice will pursue aggressively its challenge to protect Americans from insidious terrorist attacks like those of September 11, 2001.

Dramatic changes in the international and domestic environments have increased the threat of terrorism to levels not realized only a few years earlier. These threats, which include efforts of international as well as domestic terrorists, present the Department with the challenge of protecting America from a growing number of persons willing and able to carry out devastating terrorist attacks.

Domestically and internationally, there are indications that those who would seek to harm America and its citizens are attempting to acquire or develop chemical, biological, or radiological materials for illicit use. Terrorists and other criminals seek to capitalize on the fear generated by the perceived threat of an attack using weapons of mass destruction. As the public's awareness of these weapons has increased, so has the number of threats, including a dramatic increase in threats to use anthrax and other biological and chemical agents.

The rapid technological advancements of the information age have rendered crime-fighting efforts increasingly complex and opened new avenues for global criminal activities. Nearly all critical infrastructures now rely on computers, advanced telecommunications, and, to a great extent, the Internet, for system control and management, interaction with other infrastructures, and communications with suppliers and customers. The increasing interconnectedness of our critical infrastructures through cyberspace and information systems has created new vulnerabilities, as criminals, terrorists, and foreign intelligence services learn to exploit the power of cyber-tools and weapons. Our vulnerability is exacerbated by several factors. Most of our infrastructures rely on commercially available, off-the-shelf technology which means that a vulnerability in hardware or software is not limited to one organization, but is likely to be widespread. Also, infrastructures are increasingly interdependent and interconnected, making it difficult to predict the cascading effects that the disruption of one infrastructure would have on others.

The Department of Justice's approach to protecting the U.S. from terrorism is three-pronged, focusing on the prevention of terrorist acts, the investigation of threats and incidents, and the prosecution of those accused of committing crimes by terrorist means. Prevention is our highest priority, because success in preventing terrorism saves lives and property, and reduces the need to investigate incidents and prosecute individuals. We cannot wait for terrorists to strike to begin investigations and make arrests. The death tolls are too high, the consequences too great.

STRATEGIC OBJECTIVE 1.1
PREVENTION

Prevent, disrupt, and defeat terrorist operations before they occur.

In responding to terrorist threats, the Department seeks to develop a comprehensive understanding of the intentions of terrorist organizations in order to thwart terrorist attacks. This requires effective mechanisms to receive information on a timely basis and to develop program-specific intelligence products that will provide improved evaluation, exploitation, and dissemination of information. A closely coordinated effort among FBI Headquarters, FBI field offices, the Office of Homeland Security, the U.S. Intelligence Community, state and local partners, and the Department's Office of Intelligence Policy and Review (OIPR) in the collection, analysis, and dissemination of information related to specific threats is essential. Once threats are identified, all appropriate investigative actions must be taken, with the goal being the successful prevention of terrorist acts and prosecution of those involved. Every effort will be made to locate those responsible for terrorist acts wherever they are and prevent them from inflicting further harm.

Strategies to Achieve the Objective

Establish Anti-Terrorism Task Forces within each judicial district to coordinate anti-terrorist activities.

At the direction of the Attorney General, each U.S. Attorney's Office identified an experienced prosecutor to serve as the Anti-Terrorism Coordinator for that specific district. Representatives from federal law enforcement agencies, including FBI, INS, DEA, Marshals Service, Customs Service, Secret Service, and the Bureau of Alcohol, Tobacco and Firearms, as well as from primary state and local police forces in that district, will constitute the district's Anti-Terrorism Task Force. The task forces will be part of a national network that will coordinate the dissemination of information and the development of investigative and prosecutive strategy throughout the country. Among their responsibilities, the task forces will serve as coordinating bodies for implementing the operational plan for the prevention of terrorism and as standing organizational structures for coordinated responses to terrorist incidents in their respective districts.

Build and maintain the FBI's fullest capacity to detect, deter, counter, and prevent terrorist activity.

In establishing an objective of deterrence as part of its Counterterrorism Program, the FBI will focus on building and maintaining its utmost capacity to detect, deter, counter, and prevent terrorist activity. By identifying the critical elements of full capacity, the Bureau will be able to assess its current capacity, significant performance gaps, specific risks, and unacceptable vulnerabilities across the United States. Based on this information, the FBI will develop strategies for building its capacity and minimizing the risk of terrorist activity. The elements where capacity will be assessed include investigations, intelligence, communications, liaison, and program management. The last of these includes the mechanism through which senior national program managers articulate and are accountable for programmatic goals, objectives, and anticipated milestones to penetrate and neutralize terrorist

threats and enhance the program s ability to detect, deter, prevent, and swiftly respond to acts of terrorism which threaten U.S. interests at home or abroad.

Develop an intelligence capability that fully supports the Department's counterterrorism efforts.

The DOJ will develop a comprehensive intelligence program that can identify emerging threats and patterns, find relationships among individuals and groups, and provide useful information to investigators in a timely manner. This intelligence and analysis effort will range from tactical to strategic to program intelligence in order to fully support the investigative aspect of the counterterrorism effort throughout all aspects of operation. Finally, the Department will ensure that the information collected and analyzed is disseminated appropriately to ensure that all relevant partners are fully informed and engaged in the counterterrorism effort.

Mitigate threats, especially cyber-threats, to the U.S. national infrastructure.

A key area of focus is preventing and deterring terrorists from infiltrating our complex network of U.S. infrastructures. We must initially identify and strengthen all necessary assets and capabilities (equipment, personnel, training, points of contact, intelligence base) to support and initiate complex operations designed to disrupt or defeat threats to the critical infrastructures. The FBI's National Infrastructure Protection Center (NIPC) will strengthen its intelligence base by developing information resources and working relationships with infrastructure owners and operators and providing a mechanism for information sharing between the public and private sectors. NIPC will develop all necessary assets and capabilities to support operations aimed at disrupting and defeating threats to critical infrastructures. The National Infrastructure Protection and Computer Intrusion Program is working with the National Foreign Intelligence Program on state-sponsored infrastructure threats and with the Criminal Investigative Division on criminal threats to the infrastructure.

Increased dependence on the Internet, computer networks, and computers for e-commerce and critical U.S. infrastructures has raised the stakes and created a significant threat to the economic well-being and national security of the United States from computer intrusions. These infrastructures include banking and financial institutions, the telecommunications industry, oil and gas storage and delivery, transportation, water storage and delivery, electric power, emergency services, and government operations. Hacking tools are easily available, and even unsophisticated users can cause significant harm. In addition, even though computer hacking is a transnational problem, many countries lack criminal statutes, skilled investigators, or the will to investigate computer intrusion matters.

Fully coordinate with federal, state, and local government agencies in a comprehensive effort to develop and maintain adequate domestic preparedness.

Because of the catastrophic consequences posed by a terrorist attack involving weapons of mass destruction, we must increase the preparedness of the Nation by strengthening capabilities at the local, state, and federal levels to respond effectively to terrorist events. At present, there are several international terrorist organizations that have expressed an interest in constructing weapons of mass destruction and appear to have the requisite money, resources, and access to do so. The Department will work with communities throughout the country to ensure that they have the resources and training to respond to incidents of terrorism and to assist U.S. citizens who are the victims of such violence. A comprehensive training program is integral to an effective terrorism response.

In addition to partnerships with federal counterparts, the Department will continue to foster the promulgation and dissemination of cooperative domestic preparedness initiatives in support of state and local emergency responders.

Consistent with the leadership and guidance of the Criminal Division, the U.S. Attorneys have been charged with the responsibility of developing district crisis response plans. The plans will provide a crosswalk to FBI crisis response plans as well as similarly focused state, local, and regional emergency response plans.

Key Crosscutting Programs

Office of Homeland Security. DOJ will work closely with the newly-established Office of Homeland Security as it exercises its responsibility to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks.

FBI Joint Terrorism Task Force (JTTF) System. In the past, the FBI JTTF System has been the principal component for anti-terrorism coordination efforts within the DOJ. With the establishment of the Anti-Terrorism Task Forces coordinated out of U.S. Attorney Offices, described in the first strategy of Objective 1.1, representatives of the JTTFs will participate as members of the newly-established organizations and continue to exercise primary operational authority over most investigative activities.

Critical Incident Response Group (CIRG). The CIRG was created in 1994 to facilitate the FBI's rapid response to, and management of, crisis incidents and to integrate tactical and investigative resource expertise to address terrorist incidents, hostage taking, barricaded subjects, child abductions, serial murders, and other high risk violent crimes requiring an immediate law enforcement response. CIRG's many components interact with most federal, state, and local law enforcement agencies on a daily basis, including the Departments of Defense, Energy, and Treasury, and all state and local law enforcement agencies.

InfraGard. The FBI, in conjunction with the private sector, has developed an initiative called "InfraGard" to expand direct contacts with private and public sector infrastructure stakeholders to share information about cyber-intrusions, exploited vulnerabilities, and physical infrastructure threats.

STRATEGIC OBJECTIVE 1.2
INVESTIGATION

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

Although the Department emphasizes preventing acts of terrorism against Americans and their institutions, many of the same investigative tools and organizational structures developed for prevention can be used to investigate crimes of terrorism once they have been committed. Just as coordinating task forces, intelligence-gathering, and information-sharing are key elements of a prevention program, so too are these the essential elements of an effective investigation of crimes that have been committed.

Strategies to Achieve the Objective

Deploy the Anti-Terrorism Task Forces created within each judicial district to coordinate investigations of terrorist incidents.

These task forces, described earlier under Strategic Objective 1.1, will coordinate post-incident investigative activities by facilitating the dissemination of information and the development of investigative strategy throughout the country. As conduits of information between federal and local authorities, the task forces will provide intelligence regarding suspected terrorists to local authorities who can then aid in their identification and apprehension.

Promote and, when available, use new legislation and authorities to conduct investigations of terrorist incidents.

Because modern terrorism defies conventional crime fighting laws and authorities, the Department will endorse changes that will strengthen the likelihood of criminal terrorists being identified and brought to justice, while at the same time protecting civil liberties. Among these laws are those related to surveillance and wiretapping, ensuring law enforcement's ability to trace the communications of terrorists over cell phones, computer networks, and new technologies that may be developed in the coming years. Under the President's leadership, Congress has amended the laws and authorized new technology-neutral tools to combat and defeat terrorism and to detect and disrupt terrorist plans. The Department will implement these tools and constantly evaluate their efficacy and continued need in the fight against terrorism.

Apply all resources available to develop a comprehensive approach to investigating acts of terrorism.

The Department will expend the full range of its investigative resources to identify and apprehend criminals responsible for terrorist acts. To this end, DOJ will enhance its internal capabilities, such as by hiring investigators and support staff who are fluent speakers in languages used by terrorist organizations. The Department will also seek to complement its internal capacity by developing treaties with foreign powers and agreements with other agencies to share intelligence and collaborate on criminal investigations.

STRATEGIC OBJECTIVE 1.3
PROSECUTION

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

The third prong of the Department of Justice's approach to protecting its citizens from terrorism is the effective prosecution of those who have been charged with criminal violations related to terrorism. A successful prosecution strategy carries

a dual benefit. Not only does it bring criminals to justice and take them off the streets, it also can deter future acts of terrorism by disrupting their organizations by incarcerating their members, or by discouraging potential criminals by dimming their prospects of success.

As with Strategic Objective 1.2, many of the investigative tools and methods developed for preventing terrorism can be applied to build a strong case for prosecuting terrorist crimes. Coordinating task forces, collaborative intelligence-gathering, and cooperative information-sharing have been described above as key elements of prevention and investigation strategies. They are also essential elements of an effective prosecution program.

Strategies to Achieve the Objective

Build strong cases for prosecution through the use of district Anti-Terrorism Task Forces and the evidence they develop.

Because the task forces are coordinated by experienced prosecutors from U.S. Attorney Offices in each district, the Government will be able to build stronger cases, coordinating efforts throughout investigations, so that evidence is solid, properly obtained and developed, and appropriately preserved. With clarified prosecution strategies, federal and local law enforcement authorities will be better guided toward the strongest, most relevant evidence available for a sound prosecution.

Promote and, when available, use new legislation and authorities to prosecute suspected terrorist criminals to the fullest extent of the law.

To now, our laws have made it easier to prosecute members of conventional organized crime than to crack down on terrorists who, as events have shown, can kill thousands of innocent people in an instant. The same is true for drug traffickers and individuals involved in espionage our laws have treated these criminals and those who aid and abet them more seriously than terrorists. Under the President s leadership, Congress has amended the laws to place terrorism on a par with organized crime and drug trafficking. The Department will continue to assess the need for greater legal restrictions on terrorist activities while protecting civil liberties of law-abiding citizens.

MANAGEMENT CHALLENGES

Effectively Managing Counterterrorism. In recent years, the threat of terrorist attacks against the United States has increased. The Presidents budget request for FY 2001 included $11 billion for anti-terrorism programs and activities government-wide, but there may remain potential gaps or duplication of service between state and local governments. Additionally, clear linkages need to be established between DOJ threat analysis and the development of a national anti-terrorism strategy. A recent audit by the Inspector General found that funds disseminated to state, local and non-Department of Justice federal agencies were particularly at risk due to lack of oversight. The Department will meet the management challenge by ensuring accountability in all its programs, especially its counterterrorism efforts.