

FIVE-YEAR INTERAGENCY COUNTERTERRORISM AND TECHNOLOGY CRIME PLAN



UNCLASSIFIED EDITION

prepared by

THE ATTORNEY GENERAL

SEPTEMBER 1999

**FIVE-YEAR INTERAGENCY
COUNTERTERRORISM
AND TECHNOLOGY CRIME PLAN**

UNCLASSIFIED EDITION

**Prepared by
THE ATTORNEY GENERAL**

September 1999

THE FIVE-YEAR INTERAGENCY COUNTER-TERRORISM AND TECHNOLOGY CRIME PLAN

Unclassified Edition

In response to Congressional direction, on December 30, 1998, the Attorney General submitted to Congress a Five-Year Interagency Counter-Terrorism and Technology Crime Plan.¹ The Five-Year Plan is intended to serve as a baseline strategy for coordination of national policy and operational capabilities to combat terrorism in the United States and against American interests overseas. Although primarily a federal planning document, it has important implications for state and local governments.

As the nation learned from bombings of the World Trade Center in New York City and the Murrah Federal Building in Oklahoma City, a terrorist incident within the U.S. will have its initial and most devastating impact at the local and state levels. In the first critical hours following an attack, it is primarily local public safety and emergency responders, with state back-up support, who must contain the danger; locate, extricate and treat the victims; and take the first steps to restore order. Because of the vital roles that these first responders play, Congress directed that, among other key issues, the Five-Year Plan address strategies to strengthen state and local capabilities to respond to terrorism. In addition, the Plan identifies critical technologies for targeted research and development efforts, many of which have a direct, practical effect on the ability of state and local responders to combat terrorism.

A strong state and local response capability is essential to our national counter-terrorism efforts. Numerous federal programs provide support to state and local responders; however, improvements are needed in the coordination and delivery of federal support. The Five-Year Plan contains several new strategies to assist state and local authorities in accessing federal support.

These strategies reflect significant input from representatives of state and local emergency response agencies. This input was obtained by means of a questionnaire that was distributed to state and local officials and emergency service providers through their national professional associations. The Attorney General also drew upon the results of a state and local domestic preparedness stakeholders forum, convened in Washington, D.C., on August 28 and 29, 1998, by

¹ The Five-Year Interagency Counter-Terrorism and Technology Crime Plan is classified in its entirety. This excerpt is unclassified.

the Department of Justice's Office of Justice Programs, and the Inventory of State and Local Law Enforcement Technology Needs to Combat Terrorism, a 1998 study funded by the National Institute of Justice, Department of Justice.

This excerpt from the Five-Year Plan describes the proposals most directly related to state and local counter-terrorism efforts, including those affecting research and development and technology. It also includes an introduction that describes the purpose of the Plan, the process used to develop it, and the main sources of information, as well as a summary of the responses to the questionnaire circulated to state and local officials and emergency responders.

BACKGROUND

The Conference Committee Report accompanying the 1998 Appropriations Act for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies required the Attorney General, in consultation with the Secretary of Defense, the Secretary of State, the Secretary of the Treasury, the Director of the Federal Bureau of Investigation, and the Director of Central Intelligence, to develop a Five-Year Interagency Counter-Terrorism and Technology Crime Plan to serve as a baseline strategy for coordination of national policy and operational capabilities to combat terrorism in the United States and against American interests overseas. The Attorney General was charged with creating a Plan that would be representative of all participating agencies involved in the government's counter-terrorism effort, drawing upon the expertise of academia, the private sector, and state and local law enforcement. The Conference Committee directed that the Plan contain concrete proposals for implementation over the next five years relating to a broad range of topics encompassing our efforts to prevent and deter terrorist attacks, manage a crisis created by a terrorist incident, and handle the consequences of such an incident, including issues of cyber-terrorism, the use of conventional and unconventional weapons by terrorists, and research and development projects designed to combat the terrorist threat.

The specific goals which the Attorney General was directed to address in the Plan are:

- (1) to identify critical technologies for targeted research and development efforts;
- (2) to outline strategies for preventing, deterring, and reducing vulnerabilities to terrorism and improving law enforcement agency capabilities to respond to terrorist acts while ensuring interagency cooperation;
- (3) to outline strategies for integrating crisis and consequence management;
- (4) to outline strategies to protect our National Information Infrastructure; and
- (5) to outline strategies to improve state and local capabilities for responding to terrorist acts involving bombs, improvised explosive devices, chemical and biological agents, and

cyber attacks.

The final Plan, which is classified, was submitted on December 30, 1998, and is to be updated annually.

The Process

In order to foster the interagency aspect of the Plan, senior representatives of 24 federal agencies designated as the Core Agency Group (CAG) were called together periodically to help create the Plan and to keep participating agencies fully informed about input to the Plan from other sources. The CAG members supervised completion by their respective agencies of an extensive survey that was designed to obtain specific information concerning current and proposed programs, activities and initiatives, as well as research and development projects in the area of counter-terrorism. The CAG representatives also nominated experts from within their agencies who served on seven working groups established to consider specific issues to be addressed in the Five-Year Plan.

In order to obtain input from state and local law enforcement, a questionnaire was created for distribution to associations representing state and local officials, including governors, mayors, state attorneys general and district attorneys; law enforcement; first responders; and emergency medical personnel. These associations distributed the questionnaire to a cross-section of their constituencies, including major urban areas as well as mid-size and smaller suburban and rural jurisdictions; those with experience responding to a terrorist incident as well as those who have not had such an experience; those who have a key asset or special event site and those who do not; and those who have had the opportunity for counter-terrorism training and those who have not. The questionnaire addressed many of the same issues as those presented to the working groups: preventing and deterring terrorist acts in the U.S.; crisis and consequence planning and management; preventing and responding to terrorist attacks against the national information infrastructure; research, development and technology. A summary of the responses to this questionnaire is included as an appendix to this excerpt.

Additional input to the Five-Year Plan from the state and local law enforcement and emergency response communities was gathered through various efforts of the Department of Justice's Office of Justice Programs (OJP), including a Stakeholders Forum for assisting state and local jurisdictions to respond to incidents of domestic terrorism held on August 28 and 29, 1998, in Washington, D.C., and the Inventory of State and Local Law Enforcement Technology Needs to Combat Terrorism, a 1998 study funded by the National Institute of Justice, Department of Justice.

In order to obtain input from academia, a one-day colloquium was held on July 10, 1998, with the Universities Study Group on Catastrophic Terrorism at the Kennedy School of Government at Harvard University to address critical issues in counter-terrorism. The specific issues addressed included: organizational restructuring to address non-conventional threats such

as chemical, biological, radiological and nuclear (CBRN) weapons and agents; collection of intelligence information and dissemination of warnings; the role of the Department of Defense in responding to catastrophic attacks; crisis and consequence management; and budget and acquisition innovations to meet extraordinary needs. The Deputy Attorney General, the Deputy Secretary of Defense, and the Deputy Director of the FBI attended, along with senior officials of other agencies centrally involved in counter-terrorism, i.e., the Departments of State, the Treasury, Energy, Health and Human Services, and the Federal Emergency Management Agency.

Outreach efforts to the private sector were deferred to prevent duplication and overlap with the extensive network of federal agency-private sector interaction mandated by Presidential Decision Directive (PDD) 63. The first annual review of this Plan will include as one of its tasks an evaluation of whether additional outreach to the private sector is necessary in order to supplement and update the Plan.

An effort was made to coordinate the priorities and specific actions identified in the interagency development of this Plan with cross-cutting reviews of counter-terrorism resource requirements by the National Coordinator for Security, Infrastructure Protection and Counter-terrorism and the Office of Management and Budget. It is anticipated that annual updates of the Plan will improve upon this coordination, will adjust the time frame for updating the Plan to correspond more closely with the budget process and, in so doing, will enhance our ability to identify deficiencies and duplications in government-wide counter-terrorism efforts.

The Five-Year Interagency Counter-Terrorism and Technology Crime Plan does not purport to be a compendium of all efforts government-wide arguably related to terrorism. Many of the agencies which participated in the Core Agency Group have a number of programs and initiatives integrally tied to their individual missions which also share a counter-terrorism aspect. It is beyond the scope of this Plan to catalogue all of these efforts. Rather, this is a strategic plan which sets forth present and projected efforts by the Attorney General in partnership with other federal agencies and with state and local entities to improve our readiness to address the threat of terrorism. It is a strategic plan which considers where we are now and where we want to be in five years in our national preparedness to prevent and respond to terrorism, and sets out specific steps outlining how to reach these goals. In doing so, the Plan builds on past successes as well as on-going counter-terrorism efforts.

Since the issuance of Presidential Decision Directive 39 in 1995, which sought to organize more systematically the federal government's counter-terrorism activities, responsibility for coordination has been held by the interagency Coordinating Sub-Group (CSG) of the Deputies Committee. This National Security Council-chaired group has included the Departments of State, Defense, Justice, FBI, CIA, Treasury and, when appropriate, Transportation, the Federal Aviation Administration (FAA), Federal Emergency Management Agency (FEMA) and Health and Human Services (HHS). Under the leadership of this group, significant strides were made in counter-terrorism measures, including the rendition of an unprecedented number of foreign terrorists both to the United States and to other countries. The

CSG has also coordinated defensive efforts against terrorism, including coordination of security arrangements for the Atlanta Olympics, which was judged to be an attractive target for attack by terrorists using unconventional weapons. The CSG also coordinated initial implementation of a nationwide effort to build state and local first response and consequence management capabilities, while sponsoring an unprecedented series of complex exercises to test our national capacity for responding to simultaneous unconventional threats. Because the threat of a terrorist attack involving unconventional weapons has grown, and the vulnerability of our critical infrastructure has emerged, President Clinton decided to expand and elaborate the system developed by PDD 39 and the CSG and did so by issuing PDD 62 and PDD 63. These new PDDs created interagency working groups to deal with these new issues: the Weapons of Mass Destruction Preparedness Group (WMDPG) and the Critical Infrastructure Coordination Group (CICG). In addition, the CSG was renamed the Counter-Terrorism Security Group to reflect more accurately its new mandate.

Scope of the Plan

The Five-Year Interagency Counter-Terrorism and Technology Crime Plan seeks to outline the steps necessary to achieve nationwide readiness to address the full range of terrorist threats. The Plan describes emerging terrorist threats which present new challenges and lays out a number of strategies to begin to meet those challenges. As national policy on combating terrorism continues to evolve, our nation extends its focus beyond the acts of terrorism which we have experienced both at home and abroad through the use of conventional weapons to the threat of catastrophic terrorism and the use of weapons of mass destruction (WMD).² The Five-Year Plan outlines specific steps we can take to work internationally, on the federal level, and with state and local authorities to improve our counter-terrorism capabilities.

Over the past decade, our diplomatic and law enforcement efforts have sensitized the international community to the need to treat terrorism as criminal conduct and have resulted in increased international cooperation in our efforts to investigate and prosecute those responsible for terrorist incidents. As part of our message equating terrorism with criminal conduct, we have maintained that sanctuaries for terrorists must be eliminated, that countries that sponsor terrorism must be penalized, that criminal acts committed by terrorists should be punished, and that states victimized by terrorism, as well as states that help bring terrorists to justice, should receive assistance from the United States. We must continue to build international cooperation

² The Plan uses the term "weapons of mass destruction" to include conventional and non-conventional weapons capable of causing mass casualties and damage. Although more expansive than the definition used in some federal training programs, this definition is consistent with the federal law prohibiting the use of weapons of mass destruction, 18 U.S.C. § 2332a, and reflects the fact that, in addition to non-conventional chemical, biological, radiological or nuclear weapons, conventional devices such as truck bombs can cause large scale harm that would severely strain or overwhelm our existing response capabilities. Our national goal must be to prepare to meet the full range of threats.

in counter-terrorism efforts.

Federal, state and local agencies have developed crisis and consequence management plans to respond to a variety of emergency situations. State and local governments continue to modify their existing emergency response plans to address terrorist incidents. This process should be completed as soon as possible, and federal, state and local plans should be integrated so that in the event of a terrorist incident, all jurisdictions and individuals involved in the response and mitigation can work together in a jointly planned, fully integrated effort. By educating themselves as to the scope and provisions of each agency's and jurisdiction's plan, and by exercising and training together, these entities can learn to work effectively together and enhance our overall readiness. The Department of Justice is proposing to establish a National Domestic Preparedness Office (NDPO) to serve as a single point of contact for federal efforts and resources available to state and local authorities for these purposes.

The NDPO would serve as the cornerstone of federal efforts and resources to assist state and local authorities in regard to planning, training, and providing equipment to enhance our readiness to respond to WMD. We must make every effort to prepare to identify and respond to the consequences of a WMD attack, should one occur. To do so, we must continue to assist state and local authorities to train and equip first responders and emergency workers. These efforts should include a concentrated effort to train and equip medical and public health personnel and to strengthen the existing public health infrastructure, particularly the surveillance system, so that we are more likely to detect a surreptitious biological attack.

The Five-Year Plan outlines specific steps we can take to safeguard public safety by improving state and local capabilities. These steps include increased communication and intelligence sharing among federal, state and local law enforcement agencies; increased training, planning and equipping of first responders and emergency personnel to address terrorist acts involving WMDs; enhancement of strategically placed resources to enable local medical providers to quickly and safely treat victims of WMD attack and protect others at risk; and enhancement of public health systems and resources to detect and respond to WMD attacks. Working in partnership with state and local officials and emergency responders, we will continue to refine and augment these objectives through the annual updating process.

The NDPO would also serve as a mechanism to provide input from state and local authorities to the annual updates of the Plan. This will afford us an assessment of what actions outlined in this Plan we have accomplished, what objectives we have achieved, and what new efforts and programmatic adjustments are required in future years.

Our counter-terrorism efforts must also include protection of our critical infrastructures, those vital networks of independent, interdependent, mostly privately-owned, systems and processes that work together to produce and distribute a continuous flow of essential goods and services. According to The President's Commission on Critical Infrastructure Protection, these infrastructures are deemed critical because they are "so vital that their incapacity or destruction

would have a debilitating impact on our defense and economic security” The Commission identified eight critical infrastructures: transportation; oil and gas production and storage; water supply; emergency services (police, fire, medical); government services; banking and finance; electrical power; and telecommunications. Most of our nation’s critical physical infrastructure is privately owned, making partnerships between the public and private sectors vital to its maintenance and protection. PDD 63 outlines comprehensive steps to be taken nationwide to achieve and maintain the ability to protect our nation’s critical infrastructures from intentional acts, including terrorist acts, to disrupt their operations.

The Plan focuses on cyber terrorist threats to our National Information Infrastructure; it does not address all threats to our critical information systems, nor does it consider the much broader range of vulnerabilities and needs of the entire spectrum of critical infrastructures. The latter is comprehensively addressed in Presidential Decision Directive 63 and is the focus of ongoing interagency activity coordinated by the National Coordinator for Security, Infrastructure Protection and Counter-terrorism. In the annual reviews of this Plan, we will monitor this progress as it relates to counter-terrorism and suggest course corrections consistent with this Plan.

Technological development has a significant role to play in protecting U.S. citizens and assets from the terrorist threat. Technology is a vital tool to be used in conjunction with intelligence gathering, law enforcement and other activities to safeguard U.S. persons and interests both within the U.S. and abroad. While there is no technological “fix” for terrorism, many terrorist acts, particularly against fixed targets, can be deterred, prevented or mitigated by judicious use of technical tools.

A number of agencies are engaged in independent research and development efforts, consistent with their individual agency missions, which relate to our nation’s overall counter-terrorism strategy. In addition, agencies pursue joint research and development projects to develop technologies which further their individual agency goals; these joint efforts allow them to leverage their resources for greater gains than they might achieve independently. Some of these joint efforts impact on our overall counterterrorism R & D goals. There are a number of working groups and other mechanisms in place which enable agencies involved in research and development to exchange ideas, keep abreast of each other’s progress, and minimize duplication. We suggest some improvements to more efficiently manage these various research and development efforts and to spur progress toward targeted areas of need identified by federal, state and local officials and by the responder community which are reflected by the goals and strategies of this Plan. The proposed National Domestic Preparedness Office would provide an avenue for continuing input from state and local authorities to federal agencies concerning their terrorism-related technology needs. Further, the NDPO would provide a forum for the coordination and sharing of R&D and ensure that emerging technologies are integrated into current and future first responder training, planning and equipment efforts.

The Plan identifies high-level goals and sets forth a number of objectives to achieve and specific actions to take in order to reach these goals. These goals, which closely track the specific focus areas identified in the Conference Report, are summarized below:

GOALS OF STRATEGIC PLAN

- GOAL 1: PREVENT AND DETER TERRORISM WITHIN THE U.S. AND AGAINST U.S. INTERESTS ABROAD**

- GOAL 2: MAXIMIZE INTERNATIONAL COOPERATION TO COMBAT TERRORISM**

- GOAL 3: IMPROVE DOMESTIC CRISIS AND CONSEQUENCE PLANNING AND MANAGEMENT**

- GOAL 4: SAFEGUARD PUBLIC SAFETY BY IMPROVING STATE AND LOCAL CAPABILITIES**

- GOAL 5: SAFEGUARD OUR NATIONAL INFORMATION INFRASTRUCTURE**

- GOAL 6: SPEARHEAD RESEARCH AND DEVELOPMENT TO ENHANCE COUNTER-TERRORISM CAPABILITIES**

This unclassified edition of the Five-Year Plan includes pertinent portions of Goals 1, 3, 4, 5 and 6 which are of particular relevance to state and local authorities.

NATURE OF THE THREAT

As national policy on combating terrorism continues to evolve, our nation extends its focus beyond the acts of terrorism which we have experienced both at home and abroad through the use of conventional weapons to the threat of catastrophic terrorism and the use of weapons of mass destruction. As PDD 62 states, "because of our military superiority, potential enemies, be they nations, terrorist groups, or criminal organizations, are increasingly likely to attack the U.S. in unconventional ways." Given this environment, we must build on past successes in

preventing, detecting, and responding to conventional terrorism. In addition, we must move forward to improve still further our preparedness to address conventional terrorism which we will continue to face in the years ahead, and we must also meet the challenge of emerging threats concerning the use of chemical, biological, radiological, nuclear (CBRN) and other non-conventional weapons, as well as possible attacks on the national and global information infrastructure. Such attacks could come from either domestic or foreign terrorists and are increasingly likely to occur within our own borders. The tremendous damage and psychological impact that such an attack would have compels us to prepare for this possibility. In order to adequately address these emerging threats, we must increase our preparedness at the federal, state, and local levels to prevent and deter such attacks and to respond to the consequences of such an attack, should one occur.

The Five-Year Plan is formulated to address these new dimensions of the terrorist threat building on our current technical capabilities. This Five-Year Plan outlines specific steps we can take to enhance federal resources and to work with state and local authorities to improve our counter-terrorism capabilities, particularly in these emerging threat areas where the most work remains to be done.

In describing and evaluating the terrorist threat facing our nation, we must answer three basic sets of questions:

- Who are the terrorists? Individuals? Small groups? Movements?
- How will they likely strike? What weapons will they use and what are the potential effects of those weapons?
- Where will they strike? What are the likely targets?

Who Represents a Terrorist Threat?

The Threat from Domestic Terrorists

Domestic terrorists are generally extremists, sometimes affiliated with an extremist group, who use or threaten to use force, violence or intimidation against an individual, group or government in order to further social or political ends. Their inspiration tends to spring from issues related to American political and social concerns. The threat from domestic extremist groups and individuals ranges from specific instances of individual violence to well-organized criminal activities, and includes such acts as strings of bank robberies in the Midwest and Northwest and high-casualty incidents such as the bombing of the Murrah Federal Building in Oklahoma City.

Right-wing extremist groups currently constitute the primary domestic threat to our security. These groups espouse the themes of conspiracy, such as a United Nations takeover of

the U.S., the coming of a New World Order, or a movement by the government to take away citizens' weapons. Many extremists on the right articulate anti-government, anti-taxation, and white supremacy sentiments, and many adherents to these philosophies engage in paramilitary and survivalist training. The most ominous aspect of some extremists advancing these views is their belief that there is an impending conflict with the federal government that necessitates the stockpiling of weapons. Some militia members, for example, assert that the federal government is enacting gun control laws in order to make it impossible for the people to resist the imposition of a "tyrannical regime" or a "one-world dictatorship."

Some right-wing extremists have shown an interest in obtaining chemical, biological, or radiological weapons. For example, in 1995, four persons associated with a group known as the Patriot Council were convicted in Minnesota on charges of manufacturing ricin, a highly toxic biological substance made from castor beans. Their intended targets were a Deputy U.S. Marshal and a sheriff.

The threat from such groups may well increase in the near future due to the following factors:

- The beliefs of certain groups encourage violent action. For example, the coming of the millennium requires Christian Identity adherents to prepare for the Second Coming of Christ by taking violent action against their enemies. The increasingly popular Phineas Priesthood philosophy, which demands violent action of followers, also provides religious justification for acts of terrorism.
- The structure of certain groups favors violent action. Some groups have adopted the principle of "Leaderless Resistance," which calls for a secretive, decentralized cell-structure. Not only does this structure make it difficult for law enforcement to investigate them, but it removes the restraining influence of a larger group, thereby increasing the potential of violence from small units of isolated, like-minded individuals.
- The need to maintain credibility and recruit new members favors violent action. In order to preserve and build upon the conspiratorial, anti-government momentum generated by events at Waco and Ruby Ridge, some groups seek a martyr to rally the movement. This may escalate confrontations with law enforcement.
- Advances in communications technology have allowed these groups to cooperate with each other and spread their ideas. Extremists have become adept at the use of the Internet, computer bulletin boards, and fax networks. The well-established support network among members of extremist groups allows for easier access to training information, intelligence and weaponry. This, in turn, may support increased levels of violence.

In addition, religious/apocalyptic sects which are unaffiliated with far right extremists may pose an increasing threat. Thus far, these groups have inflicted damage primarily on

themselves. With the coming of the millennium, some may turn to violence as they seek to achieve dramatic effect to fulfill their prophecies. The possibility of an indigenous group, such as Aum Supreme Truth, cannot be excluded.

The threat posed by extremist groups on the left has greatly diminished in recent years. The end of the Cold War and subsequent fall of the Soviet Union have drastically reduced the political underpinnings of left-wing organizations. Puerto Rican terrorist groups, such as the Fuerzas Armadas de Liberacion Nacional Puertorriquena (FALNP) and the Ejercito Popular Boricua Macheteros (EPB-Macheteros), are an exception and represent an on-going threat. They have previously used violence in an attempt to achieve independence for Puerto Rico. In an eleven-year span, Puerto Rican terrorists were responsible for more than 100 bombings and arsons, in both Puerto Rico and on the U.S. mainland. Factors which increase the present threat from these groups include renewed activity by a small minority advocating Puerto Rican statehood, the 100-year anniversary of the U.S. presence in Puerto Rico, and the impending release from prison of members of these groups jailed for prior violence.

A third source of the domestic threat comes from certain special interest extremists who seek to influence specific social issue, rather than effect widespread political change. These extremists seek to force segments of society, including the general public, to change attitudes about issues considered important to their causes. These groups occupy the extremist fringes of animal rights, anti-abortion, environmental, anti-nuclear, and other movements. As recent events in Atlanta and Birmingham graphically demonstrate, some persons with extremist views are willing and able to cause harm to both property and persons. Extremist animal rights groups and environmental groups have repeatedly demonstrated the ability and willingness to engage in acts of sabotage and property destruction to achieve significant commercial impact. Some of these acts, such as throwing firebombs at logging trucks, threaten the safety of people, though most members of these groups would disclaim intent to cause such harm. Although it is possible that these groups could resort to violence against individuals, it is not anticipated that this will constitute a major threat in the near future.

A fourth category of terrorist threat of concern to law enforcement is the lone offender. Such persons may hold views resembling those of left or right-wing extremists but they act on their own and not as part of any group. Because they are not part of a group, they are not bounded by or controlled by group structure and may resort to violent acts that a group would deem too risky or otherwise reject. Further, it is much more difficult for law enforcement to track the activities of such persons, since they have little or no contact with larger groups that are monitored. Lone offenders represent an unsettling and, to a significant degree, unknown threat to U.S. security.

The Threat from International Terrorists

The current international terrorist threat confronting the United States both at home and abroad can be divided into four general categories: 1) state sponsors, 2) formalized terrorist

organizations, 3) loosely affiliated extremists or rogue terrorists, and 4) religious/apocalyptic groups.

Nations designated as state sponsors of terrorism provide support to terrorists and their activities. State sponsors, as currently designated by the State Department, are Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria. The threat posed by several of these nations has diminished during the past several years. However, three of these nations -- Iran, Iraq, and Sudan -- pose a serious and continuing threat.³

Formalized terrorist organizations are generally transnational groups that have their own infrastructures, personnel, financial arrangements and training facilities. They are able to plan and mount terrorist campaigns on an international basis, and many actively support terrorist activities in the United States.⁴ On October 8, 1997, Secretary of State Albright formally designated 30 foreign terrorist organizations⁵ under the Antiterrorism and Effective Death Penalty Act of 1996, P.L. 104-132, 110 Stat. 1312 (1996), which makes it illegal for anyone subject to the jurisdiction of the U.S. to provide material support to such groups. These designations are subject to biannual review. Additional organizations can be designated at any time that the standards for designations are met.

Loosely affiliated extremists and rogue terrorists may pose the most urgent threat to the United States because they may remain relatively unknown to law enforcement. Characterized by the rogue band assembled by Ramzi Yousef for the 1993 bombing of the World Trade Center, loosely affiliated groups may form on an ad hoc basis and then disband after their operational objectives have been met. These terrorists pose an especially urgent challenge because they seek to perpetuate violence and destruction as a way of life.

³ See Patterns of Global Terrorism 1997, Department of State, at 29-35.

⁴ See Patterns of Global Terrorism 1997, Department of State, at Appendix B.

⁵ These 30 designated organizations are Abu Nidal (ANO), Abu Sayyaf Group (ASG), Armed Islamic Group (GIA), Aum Supreme Truth (Aum), Basque Fatherland and Liberty (ETA), Democratic Front for the Liberation of Palestine (DFLP), al-Gama'at al-Islamiyya (Islamic Group, IG), HAMAS (Islamic Resistance Movement), the Harakat ul-Ansar (HUA), Hizballah (Party of God), Japanese Red Army (JRA), al-Jihad, Kach, Kahane Chai, Kurdistan Workers' Party (PKK), the Liberation Tigers of Tamil Eelam (LTTE), Manuel Rodriguez Patriotic Front (FPMR), Mujahedin-e Khalq Organization (MEK), National Liberation Army-Colombia (ELN), the Palestine Islamic Jihad (PIJ), Palestine Liberation Front (PLF), the Party of Democratic Kampuchea (Khmer Rouge), Popular Front for the Liberation of Palestine (PFLP), Popular Front for the Liberation of Palestine-General Command (PFLP-GC), Revolutionary Armed Forces of Colombia (FARC), Revolutionary Organization 17 November (17 November), Revolutionary People's Liberation Party/Front (DHKP/C), Revolutionary People's Struggle (ELA), Sendero Luminoso (Shining Path, SL), and Tupac Amaru Revolutionary Movement (MRTA).

Usama bin Muhammad bin Awad Bin Laden is an example of a rogue terrorist who sponsors and supports loosely affiliated extremists. Bin Laden founded an organization whose goals include driving U.S. forces from the Arabian Peninsula, overthrowing the Government of Saudi Arabia, "liberating" Muslim holy sites from perceived occupation by Western forces, and supporting Islamic revolutionary groups around the world. In February 1998, Bin Laden issued a *fatwa* (religious edict) threatening violence against American civilians and military personnel worldwide. He has funded terrorist training around the world and has provided safe haven and financial support to other leaders of formalized terrorist groups with whom he has close associations. He and persons affiliated with him have been charged with crimes connected to the bombings of the embassies in East Africa in August 1998 and for his role in the attacks on U.S. troops in Somalia in October 1993. In addition, on August 20, 1998, Bin Laden and three others were designated as terrorists who threaten to disrupt the Middle East Peace Process pursuant to Executive Order 13099.

Religious/apocalyptic groups based abroad, such as Aum Supreme Truth, present an additional threat. The closed nature of their groups and the bizarre nature of their beliefs contribute to the danger they pose. The monetary resources and technical expertise of such groups require that we not underestimate their potential to exploit conventional and unconventional weapons.

There is some concern that the demarcation between domestic and international terrorists may be bridged in the near future. Communication or other links between international and domestic extremists may substantially increase the threat each sector poses separately.

How Will the Terrorists Likely Strike?

The nature of the weapons and the means that terrorists may use to strike range from conventional weapons, including mail and vehicle bombs, to CBRN weapons and cyber attacks. Factors such as availability, effectiveness, and ease of use, lead us to conclude that conventional weapons and methods, i.e., bombings, use of firearms and kidnappings, will likely continue to be favored by most terrorists, particularly those with specific political objectives. Consequently, we must continue to enhance our readiness to withstand and respond to terrorist attacks at home and abroad which rely on conventional weapons and methods. At the same time, we must prepare to meet new threats, as there is increasing intelligence of interest by terrorists in the use of chemical and biological weapons and cyber attacks both in the United States and abroad. Because the threat of use of CBRN agents and cyber attacks is relatively new, they require additional focus.

CBRN

Our greatest present concern is that adequate steps be taken to achieve a greater degree of readiness so that we can effectively respond in the event of an attack using CBRN weapons. Intelligence and investigations reveal that lone offenders and, to a lesser extent, extremist

elements of right-wing groups have surfaced as those most likely to be involved with such weapons. The number of investigations involving CBRN agents, though small, is increasing. This disturbing trend is expected to continue, although it should be noted that the majority of the CBRN investigations initiated by the FBI last year were determined to be "non-credible," i.e., hoaxes.

The use by terrorists or extremists of biological weapons in the U.S. is threatened more often than use of chemical, radiological or nuclear materials, perhaps because materials and information on how to produce biological weapons are more widely available. A terrorist attack using a biological weapon may not be immediately apparent, and the resulting spread to and impact on additional victims, as well as first responders and emergency health personnel, could be far reaching. The depth of information pertaining to the development and utilization of chemical and biological agents easily obtainable via the Internet heightens the risk that these materials may be used by terrorists. Many dangerous substances have legitimate dual uses and are thus readily available. Unprotected exposure to these hazardous substances can cause breathing difficulties, burns, or other health problems to the general public.

Less likely is the use of radiological weapons, in the form of either a radiological dispersal device or an improvised nuclear device. Recent cases do not demonstrate a significant increase by terrorists in interest in radiological devices. However, as with all WMD scenarios, the mere threat of any of these options can cause concern and disruption. The FBI shares information with the Department of Energy (DOE) and the Nuclear Regulatory Commission (NRC) on the always present threat of the use of an improvised nuclear or radiological device, the theft of nuclear or radiological material and the sabotage of a nuclear facility.

Cyber

The cyber threat from individuals or organized group attacks on U.S. computer systems has grown substantially in recent years. For example, in early 1998, hackers located in both the United States and abroad gained access to a number of government computer systems.⁶ Although this incident did not involve terrorists, it demonstrated that the tools for a cyber attack - a computer, modem, telephone, and user-friendly hacker software - are widely available. Domestic and international terrorists have easy access to these capabilities if they should desire to develop them. Software tools for cyber-attack include computer viruses, Trojan Horses,

⁶ Currently, there are very loosely organized groups of hackers, who share techniques and boast among themselves about their exploits. These groups do not seem to target particular entities; indeed, private sector networks are targeted as often as federal government networks. Choice of targets is based upon what will receive the most publicity, rather than on ideology or political goal.

worms, logic bombs and eavesdropping sniffers.⁷ Cyber attacks can impair data confidentiality (through the unauthorized access to or interception of data), data integrity (by unauthorized alteration), and system availability (through denial of service attacks).⁸ Unlike most physical attacks, a cyber attack may not be immediately apparent. Damage assessment can take significant amounts of time.

Because of the widespread availability and low acquisition costs of tools and techniques to conduct cyber-attacks, some international terrorist groups have developed a capability to conduct such attacks. For example, the Liberation Tigers of Tamil Eelam (LTTE), a Sri Lankan separatist group, conducted a successful "denial-of-service" attack on the Sri Lankan government, and the Zapatistas, a Mexican separatist group, successfully hacked into the Mexican government's computers and modified them to broadcast Zapatista propaganda. A group sympathetic to the Zapatistas has called for worldwide "electronic disobedience," targeting selected Internet websites for disruption. In addition, hacking techniques and use of computer viruses are widely promoted over the Internet. There are numerous home pages on the World Wide Web that contain an index of hacking techniques and computer viruses, and include step-by-step instructions to break into specific U.S. government computer networks, such as "milnet," the DOD unclassified network.

Many nation-states are trying to develop information warfare capabilities. Cyber access to the United States and to critical U.S. infrastructures is much easier to obtain than physical access, making this an attractive, low-cost method to launch terrorist attacks against the United States.

The most worrisome cyber threat comes from the insider--someone with legitimate access to a system or network. Terrorists or others may make use of a witting or unwitting insider to gain access to a computer or network. Because we are increasingly reliant upon interdependent cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may significantly harm our military power and our economy.

As we focus on scientific and technological advances which terrorists may seek to harness for their own purposes, we must not overlook the wide availability of benign source

⁷ A "Trojan Horse" is a software program that has an apparently useful function and additional hidden, usually harmful, functions. A "worm" is a sometimes malicious program that can self-propagate to other computers via networks. A "logic bomb" is a program that triggers an unauthorized action when a certain event occurs (i.e., a specific date). A "sniffer" is a program that intercepts key strokes as they are entered, allowing someone to eavesdrop on an electronic communication.

⁸ A "denial of service attack" is a cyber attack on the availability of a computer system. In such an attack, the victim computer's processing capability is so completely devoted to processing the attack program that it cannot perform any other function.

materials, knowledge and technology, which can be used to create a weapon of mass destruction or cyber weapon. Even innocuous materials can be used for terrorist purposes, and the more sophisticated individuals and groups may have access to and be trained in the use of more deadly materials.

Where Will They Strike?

The threat of terrorist attacks in the U.S. is increasing. There are more identified followers of international terrorist groups and a greater number of loosely affiliated extremists in the United States than there were ten years ago. In the past, formalized terrorist groups limited their violent terrorist activities on U.S. soil because they viewed the United States as a lucrative source for fundraising and fertile ground for recruitment of new members. Loosely affiliated extremists are not bound by controls established by formalized terrorist groups. These loosely affiliated extremists pose the greatest threat of attack against U.S. citizens and U.S. interests both at home and abroad.

U.S. Persons and Property Overseas

Numerous state sponsors of terrorism and international terrorist groups pose a threat to U.S. persons and property overseas. The extensive U.S. cultural, political, economic and military presence abroad, in conjunction with opposition by certain foreign groups and governments to American values, policies and actions, continues to make U.S. citizens and interests targets for terrorists. A confluence of recent events, including Usama bin Laden's February 1998 *fatwa* (reaffirmed in May, 1998), the embassy bombings in Africa, the U.S. missile strikes on Afghanistan and Sudan, the indictments of Usama bin Laden and others in the Al Qaeda; the formal designation of 30 foreign terrorist organizations by the Department of State; the U.S. convictions and sentencing of Shayk Omar Abdel Rahman, Mir Aimal Kasi and Ramzi Ahmed Yousef; simmering Arab frustration over the stalled Middle East peace process; and the ongoing threat of United States tensions with Iraq increases the risk that individuals or groups will attack U.S. individuals and interests. The United States deployment of military forces in Bosnia and Saudi Arabia, as well as our growing commercial infrastructure overseas, also increase our presence and exposure abroad.

While U.S. persons and property overseas are often direct terrorist targets,⁹ at other times, U.S. persons are incidentally injured or killed in terrorist attacks not specifically directed against them. Terrorists are mounting more lethal attacks focusing on civilian targets as governments harden official installations.

In addition to established terrorist groups, such as Hizballah, the Egyptian al-Gamalat al-Islamiyya (IG) and the Islamic Resistance Movement (HAMAS), the United States faces an

⁹ The two lethal bombings committed on August 7, 1998 against the U.S. Embassies in Kenya and Tanzania are sobering reminders of this fact.

increased threat from such groups as the organization of terrorist financier Usama bin Laden and small terrorist cells that have no known backing but which form to commit a single, specific terrorist attack. The cells organized by Ramzi Yousef exemplify this type of group. The threat from Islamic extremist groups has grown in recent years as they have developed infrastructures and undertaken operations worldwide.

Palestinian groups such as the Palestine Islamic Jihad (PIJ) and HAMAS pose a threat to U.S. interests in that they continue to oppose the Middle East peace process by violent means, including the use of suicide bombers. Such activities pose dangers to Americans in the Middle East.

Similarly, ethno-nationalist terrorist groups pose a threat to Americans by their use of indiscriminate attacks on commercial areas that occasionally contain Americans. There is also an increased threat to information infrastructures.

State sponsors of terrorism remain a moderate to significant threat to U.S. persons and property overseas. While formally disavowing terrorism, these nations support and harbor terrorists who threaten U.S. persons and facilities overseas.

The most significant terrorist attacks overseas will likely continue to occur in urban areas. While U.S. government personnel and facilities will be the preferred targets, security precautions will limit the number of attacks in these areas but may prompt more violence against private U.S. citizens and their commercial interests.

Domestic Targets

Past targets of terrorist attacks in the U.S. have included government facilities and employees, special events and infrastructure targets. As visible symbols of government control and authority, national, state and local government facilities present inviting targets to terrorists. Special events -- ranging from large sports competitions to political meetings -- have high visibility and can command world-wide media attention. As a recent FBI report stated, "Heads of state and foreign ministers, presidential candidates and distinguished political officials, decorated athletes and enthusiastic fans from all over the world present a powerful motivating force for individual zealots or terrorist extremists to use these events as staging areas for their causes."¹⁰

National lands, parks, federal facilities and monuments constitute attractive targets, both because of their federal character and because of the large crowds they attract. As terrorists increasingly focus on maximizing the damage they inflict in terms of physical destruction and lives lost, these potential targets are increasingly at risk. The belief that the federal government is an enemy of the people allows many right-wing extremists to rationalize violence against

¹⁰ Federal Bureau of Investigation, Terrorism in the United States, 1996, p. 23.

government facilities and workers. While this poses a danger to all federal employees, some employees are particularly vulnerable. For example, employees of the Intelligence Community are at increased risk because their headquarters' facilities are viewed as symbolic targets. Law enforcement officers, such as FBI and Bureau of Alcohol, Tobacco and Firearms (ATF) agents, are obvious targets of anti-government violence, as are Internal Revenue Service (IRS) agents, who may be targets of tax protesters, and federal officers who manage and patrol national forests, parks or other federal lands which some government extremists claim are not the lawful property of the U.S. The easy accessibility and expansiveness of federal lands puts the law enforcement personnel who police these areas at increased risk, particularly where they patrol as single units in isolated areas. Improved communications and updating security can, in part, address these vulnerabilities.

Our crops and livestock are vulnerable as well, particularly to bioterrorism, although current threat assessments and intelligence do not indicate a significant risk of such an attack. We must maintain vigilant for any information which indicates increased risk, since our agricultural products feed not only our own population but a significant portion of the world. A comprehensive plan which details the roles and responsibilities of the various public and private sector participants involved in the food supply production, marketing and distribution system is a necessary component of our overall preparedness. Current resources available to address naturally occurring outbreaks of disease in our crops and livestock are the logical starting point of such a coordinated plan.

There is increasing concern about the possibility of a terrorist attack on our critical national infrastructures. As the President's Commission on Critical Infrastructure Protection found in 1997, the interconnectedness of the infrastructures has created a new level of vulnerability to attack, so that an outage in one node of one infrastructure could impair the functioning of other nodes of other infrastructures. For example, an attack (either physical or cyber) on an electrical power generating station could impact the water distribution, banking and finance activities, and communications of that area. Similarly, an attack on an area's water supply will impact that area's agriculture, industry, business, emergency and government services, as well as disrupt the personal lives of the area residents. Transportation mechanisms, such as tank cars and pipelines, could constitute targets of opportunity for the release of dangerous quantities of hazardous materials within close proximity to large population centers where various infrastructures are centered. In short, what makes an attack on the infrastructure so serious is the possibility of massive disruption due to increasing interconnectedness.

Certain key National Information Infrastructure (NII) assets may be particularly vulnerable (or at least attractive) as terrorist targets. The Internet Domain Name Server (DNS) system, which currently consists of 13 servers that are responsible for directing the routing of Internet traffic is one example. The primary or "A" server, which is responsible for distributing the master copy of the domain name database to the other root servers, is currently operated by a private company in Herndon, Virginia under a cooperative agreement recently transferred from the National Science Foundation to the Department of Commerce. Nine of the other 12 root

servers are located in various locations around the U.S., including several at U.S. government facilities. The remaining 3 are located in foreign countries. The Commerce Department is currently undertaking a process to transition certain DNS technical management functions to a private sector, not-for-profit corporation.¹¹ Although the distributed nature of the system was designed to preserve DNS functions in the event of a successful attack against one or more of the DNS root servers, it is essential that this system be protected against both physical and cyber attacks. This is true regardless of whether the servers are in government or private hands. Accordingly, as part of the transition process, a review of the Internet Root Server System will be conducted with a view toward increasing the security and professional management of the system.

Next generation telecommunication switches represent another class of key cyberassets at risk. These machines are dedicated computers designed to perform the increasingly complex tasks involved in setting up, routing and processing telephone calls. Many of these computers are dependent on massive software programs, often containing millions of lines of source code. Such machines have long been favorite targets of the hacker community, and they will undoubtedly present even more attractive targets for cyberterrorists as more of our "real world" assets are computerized and connected to the NII.

Attacks on banking and other financial networks, particularly as on-line payment options and on-line securities trading become more prevalent, may prove to be an effective means not only of direct terrorist attack but also of fundraising by terrorist groups who may seek to use the Internet to circumvent the fundraising restrictions of Executive Order 12947 and the Terrorism Sanctions Regulations, 31 CFR Part 595, implementing that Order. Such attacks will require far less risk and investment than traditional fundraising activities and could potentially prove more financially rewarding.¹²

Virtually all of our critical infrastructures are reliant on the NII at some level and could, therefore, be subjected to a terrorist cyberattack. Both electrical power and water are distributed over transport systems that rely on the NII for command and control functions. Virtually all segments of the transportation industry depend on reliable telecommunications, and these sectors are increasingly reliant on Internet-based tracking and routing systems. Emergency services are

¹¹ See Department of Commerce Statement of Policy entitled Management of Internet Names and Addresses, June 5, 1998. See also the National Telecommunications and Information Administration's (NTIA) proposed rule entitled A Proposal to Improve the Technical Management of Internet Names and Addresses, January 30, 1998.

¹² Although not instigated by a terrorist organization, the Russian hacker penetration of Citibank is an example of the type of attack that might be attempted by a terrorist organization. In this case, a group of hackers working in concert managed to transfer some \$10 million from Citibank accounts to various financial institutions around the world. Fortunately, all but \$360,000 was recovered.

significantly dependent on telecommunications. A successful attack on the phone system in a sufficiently large region could potentially impact all of these infrastructures simultaneously. For example, when a hacker recently disabled a Bell Atlantic digital switch in the Boston area, telecommunication services were cut off for everyone for over six hours, including the Worcester Airport, which was closed as a result. Ultimately, it is important to recognize that *any* network system is a vulnerable target for terrorist attacks.

In summary, the greatest terrorist threat today emanates from domestic right-wing extremists and lone offenders and from loosely affiliated international extremists and rogue terrorists. Both domestically and internationally, terrorists have relied upon conventional weapons and large scale truck bombs. However, given the increasing amount of information indicating terrorist interest in and acquisition of chemical and biological agents, there is growing concern that terrorists may turn toward the use of these weapons as well as the use of cyber attacks. The U.S. needs to develop effective and comprehensive means to prevent, deter, and respond to these new methods of attacks.

We cannot know with certainty where terrorists will strike. Domestically, there is continued concern about terrorist attacks at high profile special events and on critical infrastructures.

The timing of terrorist acts is inherently unpredictable but such acts are likely to continue and turn deadlier. Further, given the interest by extremists in acquiring chemical and biological weapons both in the United States and abroad, we may see the use of such weapons of mass destruction by terrorists. Finally, given the growth of the Internet, demonstrated terrorist interest in using the Internet as a weapon, and increasing global dependence on critical infrastructures, we will likely see an increase in terrorist attacks using cyber means.

GOAL 3: IMPROVE DOMESTIC CRISIS AND CONSEQUENCE PLANNING AND MANAGEMENT

The Presidential Decision Directives sets forth lead agency responsibilities for combating terrorism, including responding to terrorist incidents. The Department of Justice, in particular, the FBI, has lead responsibility for responding to terrorist threats and incidents occurring within the United States. The federal response to terrorism includes two components: crisis management (led by the FBI) and consequence management (led by FEMA, in support of state and local government). Crisis management includes measures to identify, acquire and plan the use of resources needed to anticipate, prevent and resolve a threat or act of terrorism. It is primarily a law enforcement response. Consequence management includes measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of an act of terrorism. It is primarily a public health and safety response.

Numerous federal, state and local agencies¹³ have devoted significant resources in recent years to the development of crisis and consequence management plans. Significant work remains, however, to successfully integrate those plans so that in the event of a terrorist incident, all those involved in the response and mitigation aspects can work together as if under a common plan rather than as separate players whose efforts may, at times, be at cross purposes with the efforts of others. By educating themselves as to the scope and provisions of each agency's and jurisdiction's plan, and by exercising and training together, these entities can learn to work effectively together.

**OBJECTIVE: Enhance Integration And Coordination Of Crisis And
Consequence Management, Planning, Training, Command
And Transition Among Federal Agencies**

Experience has taught us that there is often no clear point in time when resolution of a terrorist incident moves from the crisis to the consequence management stage. Indeed, these phases may occur simultaneously or, in some instances, the consequence phase may actually precede the identification of a terrorist event. This is particularly true in regard to a biological terrorism event; we may have to address emergency management, victim treatment and other services before we determine that these effects were caused by an intentional terrorist act.

Under Presidential Decision Directives, the FBI is the lead federal agency for operational response to any domestic terrorist incident. As the on-scene commander, the FBI is responsible for implementing crisis management efforts to resolve a terrorist threat or incident. PDD 39 designated FEMA as the lead federal agency for consequence management and directed that FEMA ensure that the Federal Response Plan¹⁴ is adequate to respond to the consequences of a terrorist incident. As a result of this mandate, FEMA developed a Terrorism Incident Annex to the Federal Response Plan. The Terrorism Incident Annex details procedures for FEMA and other agencies to provide consequence management support to the FBI during a terrorist incident. This plan also details the procedures that FEMA and other federal agencies would use to provide federal assistance to state and local authorities in dealing with the consequences of a terrorist act.

¹³ Approximately two-thirds of responders to the State and Local Questionnaire reported that they had crisis and consequence management plans in place for terrorist incidents. See Appendix B: State and Local Questionnaire, responses to question 17.

¹⁴ The Federal Response Plan describes the strategy for responding to any incident or situation requiring federal emergency or disaster assistance. This Plan is supported by 27 federal departments and agencies and the American Red Cross.

**Action: Finalize, Adopt And Conduct Exercises Of The CONPLAN
And The Domestic Guidelines**

To ensure that agency crisis and consequence management roles are clarified and coordinated, numerous other contingency plans have been developed. These plans have been vetted through an interagency process designed to ensure that they are coordinated at all levels and that they will provide for seamless transition between crisis and consequence activities at all stages of a terrorist incident. The FBI, in concert with DOD, FEMA, HHS, DOE, and EPA, is developing a Concept of Operations Plan (CONPLAN) to ensure that the counter-terrorism strategy established in PDD 39¹⁵ is fully implemented in a coordinated manner. The CONPLAN is designed to provide overall guidance to federal, state and local agencies concerning how the federal government will respond to a potential and actual terrorist threat or incident that occurs in the United States. It includes procedures for assessing the credibility of the threat, notifying appropriate federal agencies of the nature of the threat, and deploying the requisite advisory and technical resources to assist the lead federal agency in executing a crisis and consequence management response to a domestic terrorist incident. It also defines procedures by which the federal government would marshal resources to augment and support local and state governments in restoring public safety and services. This plan will facilitate interagency coordination of crisis and consequence management functions to ensure proper direction and guidance to other agencies and to provide the framework for the integration of the federal response with that of the state and local incident command system.

The Guidelines for the Mobilization, Deployment, and Employment of U.S. Government Agencies in Response to a Domestic Terrorist Threat or Incident, also known as the PDD 39 Domestic Guidelines, or simply the Domestic Guidelines, have also been developed. The Domestic Guidelines describe specific procedures and responsibilities for deploying federal resources comprising a specialized interagency team known as the Domestic Emergency Support Team (DEST). The Domestic Guidelines enumerate the responsibilities of the various agencies in the case of a chemical, biological, nuclear or radiological dispersal incident and specifically address the use of specialized military assets. The Domestic Guidelines await the signature of the Attorney General and the Secretary of Defense and the approval of the President. They are expected to be approved and become effective this fiscal year.¹⁶

¹⁵ PDD 39 set forth a strategy, interagency coordination mechanism and a management structure to combat terrorism occurring both domestically and abroad. The strategy, reiterated in PDD 62, specifically requires development of a robust capability to combat and manage the consequences of incidents involving WMD.

¹⁶ In addition to interagency plans, individual agencies are developing plans to address the threat posed by the terrorist use of a WMD. For example, the FBI has finalized a revised contingency plan for internal FBI response to terrorist acts that involve the use of a WMD. This plan details the sequence of actions required to appropriately guide, oversee, and support

In essence, the CONPLAN forms an overarching framework for the federal response, while the Domestic Guidelines provide specific information on the response capabilities and responsibilities of each federal agency listed in PDD 39 as well as the procedures required for notification, authorization, and deployment of federal assets.

To ensure that there is effective coordination of crisis and consequence management, planning, training, command and transition, current contingency plans, including the CONPLAN, the Terrorism Incident Annex of the Federal Response Plan, and the Domestic Guidelines, need to be exercised on a regular and continuing basis. A significant number of these exercises need to involve all elements of the federal, state, and local community that could be called upon to respond to a terrorist act, including one involving use of a WMD. Because acts of terrorism committed in the United States are federal crimes, the U.S. Attorneys' Offices (USAOs) will play a critical legal advisory and prosecutive role in responding to domestic terrorism. In order to perform that role successfully, these offices must be informed of crisis response plans in their districts and be regularly involved in exercises with FBI field offices. Since the FBI is the lead agency for crisis response, its field offices should establish procedures for informing the USAO of relevant federal, state and local crisis response plans and for including the USAO in all crisis/consequence response exercises in which the field office is involved. The involvement of the full spectrum of federal, state, and local agencies in regular exercises would help to assure that all participants are fully cognizant of current contingency plans, implementation and deployment procedures, and roles and responsibilities of the various agencies in the event of a terrorist act.

The federal government conducts a considerable number of training exercises each year to test the preparedness of federal, state and local authorities to handle a terrorist incident through coordinated efforts. Interagency exercises are conducted annually. Individual agencies also conduct interagency exercises to test the crisis and consequence management response of the participating agencies.¹⁷ Additional exercises designed to ensure the preparedness of an individual agency's components also occur regularly.

successful execution of the FBI-directed United States response to a WMD terrorist threat or incident. This plan is being shared with federal, state, and local emergency responders to ensure a unified approach to the on-scene management of the crisis.

¹⁷ FEMA ensures, through training and exercises, that the Federal Response Plan is adequate to respond to the consequences of terrorism in the United States, including terrorism involving the use of a WMD. Crisis and consequence management planning coincide during a credible chemical, biological, or radiological/nuclear incident and run on parallel tracks. Within the FBI, the Critical Incident Response Group (CIRG) manages the FBI's national level crisis management training and exercise program. On an ongoing, rotational basis, CIRG conducts standardized crisis management training and exercises throughout the FBI.

Federal interagency exercises have enhanced communication among participating agencies and helped to identify shortfalls in response capabilities. While these are important first steps, the federal interagency exercise process needs to be strengthened. Domestic exercises currently tend to focus on tactical response capabilities, with less attention to interagency and intergovernmental command and management issues. The FBI especially should increase the number of its field exercises that practice its interagency leadership role in a crisis. FEMA, which leads consequence management exercises, should encourage more field exercises to test actual response capabilities.

In addition, federal exercises should continue to include the active participation of state and local authorities, including the state emergency structure with which FEMA regularly deals. Some exercises should be conducted exclusively at the national level, and some at the state and community levels, in order to promote communication and coordination within these respective levels of government. However, state and local authorities will most likely be the first responders to a crisis site, and they will take the lead in dealing with the consequences of a terrorist act. They cannot use federal resources available to them under the Federal Response Plan or contribute to crisis management effectively unless they have been included in federal response planning and exercises. Although state and local emergency responders can obtain information about federal resources from sources such as the Rapid Response Information System (RRIS),¹⁸ participation in appropriate federal interagency field exercises is needed to test the coordination and effectiveness of these various resources in a more realistic environment.

The National Domestic Preparedness Office (NDPO) within the Department of Justice will become the focal point for federal efforts to support state and local needs for equipment, training and participation in exercises related to WMD preparedness. The NDPO, under the management of the FBI, will include representatives from those federal agencies which have, in the past, conducted such programs, including DOD, HHS, DOE, EPA, and FEMA. The NDPO will be the single point of contact that state and local authorities have requested. The NDPO will examine funding options for those state and local agencies with insufficient budgets to participate in counter-terrorism training exercises.

In addition, interagency communication and notification of planned exercises must improve. The exercise schedule should be disseminated to all of the approximately 41 government agencies with counter-terrorism responsibilities, perhaps via a secure website.

¹⁸ RRIS is a congressionally mandated planning and training resource for use by planners and responders at all levels of government. It contains databases on characteristics and precautions for chemical, biological, radiological and nuclear (CBRN) agents; federal response capabilities; surplus federal equipment; CBRN help and hotline phone numbers; and other reference materials.

**Action: Clarify The Interrelationships Among The Numerous Existing
Emergency And Consequence Management Plans**

The current consequence response framework includes an array of emergency plans, capabilities and resources of local, state and federal governments, and of private and voluntary organizations. At the federal level, emergency plans deriving from statutory authorities, executive orders, and national security guidance are used by departments and agencies to carry out their emergency response missions. Under this response framework, federal resources and capabilities are provided to augment those of state and local responders.

Although there are a substantial number of interagency plans that have been and are being developed to meet the challenges of managing a terrorist crisis and its consequences, several problems exist in the planning area: (1) federal operational plans and guidance are not fully understood by all responding agencies; consequently, additional coordination is required to facilitate the most efficient federal response; (2) the relationship between and among operational response and technical guidance documents such as the Federal Response Plan, Terrorism Incident Annex to the Federal Response Plan, Federal Radiological Emergency Response Plan (FRERP), National Oil and Hazardous Substances Pollution Contingency Plan (NCP) and the Domestic Guidelines is not clear or fully understood by various agencies;¹⁹ and (3) the concept of lead federal agency and the attendant responsibilities of that designation are not fully understood by all emergency response organizations.

The development of terrorism-specific plans and emergency operating procedures by federal, state and local governments needs to be consistent and compatible to the maximum extent possible to ensure interoperability among all responders during a WMD incident. Planning also must build on existing local, state and federal emergency systems, capabilities and coordination mechanisms.

FEMA has the lead for federal terrorism-related consequence management planning, using the structures of the Federal Response Plan. FEMA coordinates this activity through several interagency forums. These include the Emergency Support Function Leaders Group and the Catastrophic Disaster Response Group at the national level, and the Regional Interagency Steering Committees in each FEMA Regional Office composed of regional representatives of the key response agencies with crisis and consequence management responsibilities.

These groups focus on developing terrorism-specific plans and procedures to support Federal Response Plan implementation, including supplementing Regional Response Plans (RRPs) and development of regional specific procedures and checklists to support consequence management activity at the regional level. This includes the development of Memoranda of

¹⁹ For example, the NRC has lead agency responsibilities in the FRERP, yet the NRC is not among the federal agencies given specific roles by PDD 39 or the Terrorism Incident Annex to the Federal Response Plan.

Understanding (MOU) between each state and its FEMA Regional Office to supplement the RRP. These MOUs form the basis for operational relationships, such as defining expectations regarding notification and deployment of liaisons in response to terrorism incidents.

FEMA also provides assistance to support state and local government terrorism-related emergency response planning. This includes providing grants to the states to support the development of terrorism-specific annexes to existing state and local emergency operations plans; disseminating guidance for use by local and state emergency management planners and officials in developing emergency operations plans; support for the Rapid Response Information System (RRIS) as a planning tool to aid federal, state, and local emergency responders in preparing for and responding to a terrorism incident involving WMD; and support for states regarding development of mutual aid agreements, such as the Emergency Management Assistance Compact (EMAC).

The FBI and FEMA, working through the NDPO and in cooperation with other federal agencies with state and local response planning roles,²⁰ should perform outreach at the state and local level to assess and increase the understanding by state and local authorities of federal plans and command systems. This process will also increase the understanding that federal agencies have of local plans and resources. Toward the same end, the FBI should incorporate into its field office training programs information about the kinds of incident command and crisis/consequence response systems that are being used by state and local responders. This will facilitate the FBI's ability to lead and coordinate federal response efforts in the event of a domestic terrorism incident.

Action: Ensure That The Vulnerabilities And Recommendations Identified In Exercise And Terrorism Incident After-Action Analyses Are Shared With Participating Agencies

After-Action Reports (AARs) are normally generated as a result of inter-agency exercises and terrorism incidents. These reports contain a description of problems and issues that arose during the exercise or incident as well as recommendations for addressing identified deficiencies. Although a number of agencies have their own systems, until recently there was no system to track the after-action items (AAIs) that are generated in these reports, to ensure that identified weaknesses or suggested improvements were shared with all affected agencies. Consistent with the decision made by the Weapons of Mass Destruction Preparedness' Interagency Working Group for Exercise and Contingency Planning, the FBI has begun to address this shortfall. The FBI is pursuing efforts to obtain DOD's Windows Joint Instructional Input Program (WinJIIP)

²⁰ For example, EPA provides technical assistance and advice to state and local planning entities responsible for developing plans to address the environmental consequences of a hazardous materials release. EPA is encouraging the addition of WMD response annexes to existing HAZMAT plans.

database²¹ so that it can be distributed to FBI field offices and to other federal agencies for use in tracking AARs, AAls, and lessons learned.

Government-wide, federal responsiveness and coordination in crisis and consequence management will be streamlined and improved as the National Defense Preparedness Office (NDPO) develops procedures to record and disseminate lessons learned that affect operations and interagency coordination and cooperation. All participating agencies will be encouraged to submit relevant after-action analyses to the NDPO for dissemination to other affected federal agencies, as well as to state, local, and other WMD responders across the country. As this system is developed, it will assist in determining whether exercise goals and objectives were achieved. It will also provide a means to identify vulnerabilities and make recommendations to address such vulnerabilities. Further, it will help in identifying WMD equipment procurement needs or modifications, improve training and planning initiatives and, ultimately, improve the capability of WMD responders in actual incidents. A mechanism will also have to be established to track and ensure that all corrective actions have been implemented in response to earlier lessons learned from exercises and actual incidents.²²

Distribution of the WinJIIP database should be completed by June 30, 1999, and development and implementation of the lessons learned distribution system, and the system for tracking corrective action, should be completed by December 31, 1999.

**Action: Achieve A Unified Communications Capability And Protocols
 To Enhance Coordination Among Federal, State And Local
 Response Agencies And The Public**

In the event of a terrorist incident, federal, state and local response agencies must be able to communicate quickly among themselves and with the general public. Despite the importance of this function, there are gaps in our technology and policies that impair effective communications among these entities.

Currently there is no common, comprehensive communications capability among the numerous federal, state, and local agencies that could be called upon in the event of a terrorist incident. Existing communications systems often are not technically interoperable. The result is that one set of responders may be able to communicate among themselves but not with responders in other jurisdictions. Where common capability does exist, the systems tend to be

²¹ WinJIIP is the Windows 95 version of DOD's Joint Uniform Lessons Learned System (JULLS) and should be more user-friendly and accessible than earlier versions.

²² During the pendency of a criminal investigation and prosecution, it may not be possible to divulge information about the operation. After these proceedings are complete, however, the operation should be subject to the same analysis as exercises, and lessons learned should be shared with appropriate audiences.

overwhelmed in times of crisis. In the event of an incident, communication between federal agencies and among federal, state, and local entities, occurs in the FBI's Joint Operations Center or on-site, often face-to-face. Then each agency, using its own equipment and frequency, communicates with its responders. Consideration should be given to use of FEMA's Mobile Emergency Response Support (MERS) Detachments as an additional asset for use in and around the site of a terrorist incident. MERS is strategically located in five different regions and has quick response and deployment capabilities.

A study should be conducted to determine the best technical approach to resolving this critical communication problem. As a result of the OJP Stakeholders Forum held in August 1998, a group consisting of FBI, FEMA and representatives from other interested agencies will study the issue of a unified communications capability and the requirements of such a system. Existing regional capabilities, as well as potential new technologies should be considered in order to develop alternatives for use by all affected agencies. The Technical Support Working Group (TSWG) should consider including this issue as a priority area for research and development in FY 2000, consistent with concerns voiced by state and local authorities. Any efforts along this line should be coordinated with the Public Safety Wireless Network (PSWN) program coordinated by DOJ and Treasury. PSWN has been directed, by the Vice President's National Performance Review, to develop a plan for the implementation of a nationwide public safety radio network to ensure interoperability among state, local and federal law enforcement, public safety agencies.

There is also a need for improved communications capability in general, aside from the issue of compatibility. If an incident occurs in a remote area, agencies will have a difficult time establishing secure communications back to their regional and national headquarters command centers. One approach to this problem will be to develop a mobile command system for use in crises. A prototype communications/surveillance support trailer was built for the 1996 Olympics in Atlanta to coordinate the response to incidents in the outlying venues hosting the Olympic events. This system was used successfully in establishing communication links and served as a command post for consolidated tracking and monitoring equipment. These units could provide the quickest communications support in response to incidents in remote areas where current communications do not exist.

Another area that requires increased attention is the coordination and release of emergency information to the general public and the media during the response to a terrorist incident, particularly one involving a WMD. Timely, accurate information will be a critical component of efforts to preserve order, reduce panic and save lives. At the same time, the proper balance must be struck between the need to inform the public and the need to protect sensitive law enforcement information, particularly as it might affect our ability to preclude any further incidents from taking place, or to apprehend those responsible for the terrorist attack. The lack of agreed-upon protocols and procedures among federal, state and local officials hampers our ability to meet this important need. Accordingly, we recommend that the appropriate interagency working group working closely with agencies' public affairs representatives, and including state

and local officials, develop the methodology and plans to implement emergency public information activities in response to a terrorist incident.

SAFEGUARD PUBLIC SAFETY BY IMPROVING STATE AND LOCAL CAPABILITIES

Terrorist acts have their initial devastating impact at the state and local level. It is the first responder and emergency worker who must literally begin to pick up the pieces; locate, extricate, and treat the victims; put out the fires; take the first steps to begin to make order out of chaos. We owe it to these vital personnel and to ourselves to make sure that they are adequately trained and equipped for these tasks. We cannot measure our preparedness to deal with terrorist acts without measuring the degree to which we have prepared first responders.²³

Yet state and local first responders and emergency personnel consistently report inadequacies in their preparation for these tasks. While their training and equipment to respond to attacks by conventional weapons is sufficient more frequently than not, this is not the case in regard to chemical, biological, radiological or nuclear (CBRN) weapons. The response to the state and local questionnaire was consistent and alarming: 80% or more responders reported that they are ill prepared for CBRN events and 75% or more reported that they are not trained or equipped to preserve or recover evidence from such events. See Appendix: State and Local Questionnaire, responses to questions 26 and 28.

If we were to experience an attack using chemical or biological weapons, the results would be severely disruptive, both psychologically and physically, to the affected areas and

²³ This section deals primarily with the first responders employed by state and local governments. There are other categories of individuals with public safety responsibilities who could be the first responders on scene at a terrorist incident. Some, such as transit system employees or private security officers, may be private sector employees. Others, such as public safety and security officers who are responsible for U.S. facilities and lands, may be federal employees. All federal agencies with law enforcement, emergency response or public safety duties as part of their mission should ensure that they conduct appropriate planning for, and are properly trained, equipped and practiced in dealing with a terrorist incident, particularly one involving unconventional weapons. As states and localities incorporate counter-terrorism measures into their public safety and emergency response plans, they should address the need for training, equipment and other preparedness programs for private sector responders. Federal agencies with private sector constituencies should also be pro-active in developing and promoting appropriate counter-terrorism planning and training. In particular, agencies with lead responsibilities for critical infrastructure protection under Presidential Decision Directive 63 should ensure that their vulnerability assessments consider their sector's readiness to deal with the effects of a physical attack, particularly one using unconventional weapons such as chemical, biological, radiological or nuclear materials.

populations. In the case of biological weapons, an attack might not be immediately apparent, and the resulting spread to and impact on additional victims, as well as first responders and emergency health personnel could be far-reaching. Determining the extent of an attack and apprehending the perpetrators would be difficult. For these reasons, we must make every effort to prepare to identify and respond to the consequences of an attack, should one occur. To do so, we must properly and thoroughly train and equip first responders and emergency workers.

Improving state and local capabilities begins with information and intelligence sharing. In order to prepare for a terrorist event, we must know as much as we can about the potential threat. One way to accomplish this on the state and local level is to increase the participation of state and local authorities in task forces and working groups with their federal counterparts to facilitate the sharing of information. In addition, regular, periodic sharing of information concerning terrorist groups active in a particular locale -- not just threat warnings tied to a specific incident -- would be helpful to local officials.

A significant aspect of increasing state and local capabilities to respond to terrorist acts involves proper training, equipment and planning. We must address these needs in terms of conventional weapons as well as chemical, biological, radiological and nuclear weapons. In addition, because of the unique challenges posed by bioterrorism, we must look at specific remedies to boost medical and public health resources at the state and local level and to enhance back-up capabilities at the federal level.

Finally, we should make available the protection of federal laws to state and local government employees who are the targets of obstructive and threatening actions by anti-government extremists.

Intelligence Collection and Local Capabilities

OBJECTIVE: Increase State And Local Awareness And Intelligence-Gathering Capabilities Regarding Terrorist Activity

While the ability of state and local agencies to acquire information about terrorist activity in their regions has increased as a result of recent federal outreach efforts, challenges remain. As indicated by the responses to the State and Local Questionnaire, state and local law enforcement and non-law enforcement agencies, such as emergency responders, agree that they would benefit from more training and information about terrorism, particularly information that is regional in focus, or that addresses emerging issues such as cyber-terrorism, or the use of chemical or biological weapons. Such training and information sharing would help local agencies focus their own counter-terrorism law enforcement and intelligence efforts. It would be especially beneficial to those agencies that do not have strong intelligence gathering capabilities. Particularly in rural areas, local law enforcement agencies may not have sufficient personnel to support their own intelligence unit or even to participate in federal intelligence-sharing task forces. Similarly, state and local law enforcement agencies may not have the equipment or training to take advantage of

existing electronic systems for communicating intelligence information. Another obstacle to effective communication is that intelligence gathered by federal agencies is often classified and, therefore, federal agencies must either facilitate the necessary security clearances or sanitize the information of its classified details.

Action: Expand Joint Terrorism Task Forces And Related Federal Efforts To Improve Communications Among Federal, State And Local Law Enforcement Agencies

For most state and local agencies, the primary federal source of information and intelligence about terrorist activities is the Federal Bureau of Investigation (FBI).²⁴ The FBI obtains intelligence from a variety of sources including intelligence agencies such as the Central Intelligence Agency (CIA); the FBI's own intelligence gathering and law enforcement operations, as well as the operations of other agencies such as the Bureau of Alcohol, Tobacco and Firearms (ATF) and the Customs Service; and, to a lesser extent, from state and local law enforcement agencies.

The FBI uses several means of communicating terrorism information to state and local agencies. When intelligence information reveals a potential terrorist threat, the FBI relies on the Terrorist Threat Warning System (TTWS) to get vital information to the U.S. counter-terrorism and law enforcement community. If the threat information warrants broad dissemination, the FBI can quickly transmit unclassified messages to state and local law enforcement agencies nationwide over the National Law Enforcement Telecommunications System (NLETS).²⁵ For information that is less urgent, the FBI can communicate through the Law Enforcement On-Line (LEO) system. These systems are a critical link in the federal/state/local counter-terrorism partnership. They should be continued at robust levels.

While state and local law enforcement authorities appreciate receiving such vital information in a timely fashion,²⁶ many identify a need for regular periodic intelligence analysis and reports, particularly concerning groups operating in their jurisdiction. FBI field offices routinely share information through their ongoing working relationships with state and local law enforcement agencies. To strengthen these existing relationships and improve communication about terrorism issues, the FBI created Joint Terrorism Task Forces (JTTFs) as a mechanism for interaction between federal agencies and their state and local level counterparts in specific

²⁴ See Appendix: State and Local Questionnaire, responses to question 5.

²⁵ Similarly, warnings can be sent using the Awareness of National Security Issues and Response (ANSIR) program, which utilizes the Law Enforcement On-Line (LEO) system and is designed to provide unclassified national security threat and warning information to U.S. corporate security directors and executives, law enforcement, and other government agencies.

²⁶ See Appendix: State and Local Questionnaire, responses to questions 4-9.

jurisdictions. The JTTFs, which exist in 18 major metropolitan areas, are composed of state and local officials, and local representatives from the FBI and other federal agencies, such as ATF, the Customs Service, the Secret Service and the Immigration and Naturalization Service (INS). Participants work together, usually on a full-time basis, to gather, analyze and disseminate intelligence, and to jointly investigate terrorist activity. The FBI also recently established a regional terrorism task force to serve several rural states with common terrorism concerns. In addition to ongoing intelligence sharing, these task forces sponsor regional terrorism conferences to train local law enforcement agencies about the terrorism threat in their region. These face-to-face working arrangements not only improve the flow of information from federal intelligence agencies to localities, but they allow federal agencies to obtain intelligence from local sources.

The existing 18 JTTFs involve participation by approximately 260 full- and part-time federal, state and local personnel plus 420 FBI agents. State and local law enforcement personnel endorse such federal, state and local joint efforts. Many report that they would participate in JTTFs if they were available to them.²⁷ Based on local interest and an assessment of terrorist activity, creation of a dozen additional JTTFs over the next three years may warrant consideration.

Where appropriate, over the next five years, the FBI also will establish domestic terrorism working groups in field offices. Such working groups would provide a supplemental means of increasing cooperation and intelligence-sharing among federal, state, and local law enforcement officials. They would be particularly important in those parts of the country where there are not enough state and local resources to support full-time JTTFs. No additional funding is required for this initiative.

Action: Assist Local Law Enforcement Agencies To Identify And Gain Access To State And Federal Intelligence Systems

Many local law enforcement agencies report that the lack of resources to support their own intelligence infrastructure is a real barrier to effective counter-terrorism efforts. Often the problem is as basic as the inability to spare officers to perform intelligence activities. To some extent, participation in JTTFs can address this need because the FBI makes overtime money available to compensate state and local participants. However, this cannot redress the problems faced by many small town or county law enforcement agencies, which may have only a handful of officers to perform all duties. Ideally, at a minimum, a local law enforcement office unable to perform its own intelligence activities should have access to a state or regional electronic information system that provides real-time, accurate intelligence, a system that should include timely federal information on criminal and terrorist activity. However, even this solution often is out of reach for local police or sheriffs offices because of the lack of resources to procure computers, appropriate software or the training needed to acquire access to electronic

²⁷ In the State and Local Questionnaire, 69% responded yes to this question. See Appendix, responses to question 3.

information systems, or because of the unavailability of a reliable, centralized repository of information.

Within the next fiscal year, the FBI, in cooperation with associations representing state and local law enforcement agencies and with the advice of the Intelligence and Assistance to State and Local Authorities working groups of the NSC's WMDP Group, should determine the extent to which local law enforcement agencies do not have access to such systems; identify existing successful methods of bridging such gaps; and develop concrete proposals to strengthen these vital state and local capabilities.²⁸

**Action: Develop More Effective Means Of Sharing Classified
Information With State And Local Law Enforcement And
Emergency Response Agencies**

Even where mechanisms for developing and sharing terrorist information exist, state and local officials express frustration because of their belief that critical information is often denied or delayed because it has been classified. This problem is greatly diminished in areas with JTTFs because all federal, state and local law enforcement participants must obtain Top Secret clearances before joining a task force. Law enforcement agencies in general are likely to have personnel with necessary security clearances, which means that this perceived problem may be alleviated through better working relationships between FBI field offices and their state and local counterparts. Thus, expansion of JTTFs and similar cooperative arrangements may go a long way toward solving this problem. Nonetheless, other solutions may be needed. The FBI should assess the degree to which security restrictions on dissemination of information have impeded its work with local law enforcement agencies and whether the FBI needs to pursue additional remedies, such as greater efforts to sanitize classified information and report such information on a more regular basis.

Lack of access to classified information may be an obstacle to non-law enforcement agencies as well. Many emergency responders believe that security restrictions on information possessed by the federal government have prevented dissemination of sufficiently detailed

²⁸ An example of an existing federal program that has improved state and local intelligence gathering capabilities is a cooperative arrangement between the FBI and the Alaska Department of Public Safety, Division of State Troopers. Since 1995, the FBI and the state have operated, under FBI auspices, a Statewide Law Enforcement Information Center (SLEIC). The SLEIC combines analysts from the Alaska State Troopers under FBI management at an FBI-supported site. It gathers intelligence from multiple sources in a centralized database with full text query capability in order to give state law enforcement agencies efficient access to current and historical information. One of its specific goals is to provide immediate on-scene information management support for administrative and operational activities during a critical incident, such as a terrorist threat.

information to allow them to plan or react appropriately in an emergency.²⁹ On the other hand, many members of the intelligence community believe that much intelligence information is not relevant to planning or response needs, and that there are mechanisms for sharing essential information.

The need to protect national security information from unnecessary disclosure must be carefully balanced against the need to ensure timely and adequate dissemination of relevant intelligence to state and local first responder officials who are ultimately responsible for the safety of their communities. Emergency responders ordinarily cannot participate in JTTFs because the JTTFs actively investigate terrorist crimes and, accordingly, their membership must be restricted to law enforcement personnel. To increase confidence among the emergency response community that federal agencies are sharing necessary intelligence, and thereby increase intergovernmental coordination, new approaches are needed. The appropriate working groups within the NSC's WMDP Group, drawing on the expertise of national security and public safety specialists from the federal, state and local government levels, should study the feasibility of establishing a system for granting the necessary security clearances to a small number of senior public safety personnel so that they can have access to classified information relating to terrorist threats as needed.³⁰ At a minimum, each state and the nation's most heavily populated urban areas should be assured access. This assessment should have no budget implications.

A closely related issue is the extent, if any, to which restricted information needs to be shared with security officers in certain critical private sectors, such as the nuclear power industry. The National Infrastructure Protection Center (NIPC) and the critical infrastructure private sector

²⁹ In response to the State and Local Questionnaire, a substantial number of law enforcement, emergency response and medical personnel identified issues of inadequate information sharing and the lack of security clearances as factors that limit the usefulness of information or threat assessments obtained from the federal government. These state and local personnel seek more timely dissemination of more localized and specific information. See Appendix, responses to questions 6 and 9.

³⁰ One such proposal has been advanced by the Competency Panel on Civil Integration and Response of the Defense Science Board. See Report of the Competency Panel on Civil Integration and Response at page 16. This Panel proposes that an average of three to five public safety personnel who are responsible for planning and directing the public safety effort in the community, rather than political leaders, be provided with security clearances for the purpose of receiving this classified information. Under this proposal, access to classified documents would be restricted to reviewing the material at cleared facilities maintained by the federal government (such as an FBI field office, Secret Service office, U.S. Marshal's Service office or military installation). The cleared public safety personnel could be notified of the need to review a classified threat analysis either by personal visits from locally based federal agents or by unclassified messages instructing them to report to a secure facility to access the particular material.

liaisons developed under PDD 63 are required to establish effective threat warning and security information systems to serve key infrastructures.³¹ As these systems are established, the NSC's Critical Infrastructure Coordination Group should assess the need for dissemination of classified information to security personnel in these sensitive areas. The National Coordinator and the Critical Infrastructure Assurance Office will also play key roles in assessing the need for dissemination of classified information.

Another hindrance to intelligence dissemination is uncertainty about which organizations have equipment and storage capability for classified information. Many local law enforcement and most emergency response agencies lack secure communications equipment and secure storage for sensitive or classified information. As part of its assessment of other barriers to intelligence sharing, the FBI will assess whether lack of equipment is a significant barrier to effective exchange of intelligence. If so, the FBI should recommend appropriate remedial actions which can be coordinated through the NDPO.

OBJECTIVE: Increase Capabilities Of State And Local Emergency Responders To Address Terrorist Acts Involving Weapons Of Mass Destruction

Although combating terrorism is primarily a federal responsibility, state and local emergency responders (police, fire and emergency medical personnel) are almost certain to be the first to respond to the use of a weapon of mass destruction (WMD), whether a conventional

³¹ Our nation is rapidly augmenting its capabilities to safeguard both the physical and cyber aspects of critical infrastructures through the National Infrastructure Protection Center (NIPC), which was created by the Department of Justice during FY98. The NIPC is an interagency center hosted by the FBI, that will deter, assess, warn, investigate, and respond to attacks, threats and unlawful acts targeting the critical infrastructure of the United States, including illegal intrusions into government computer networks and protected computers. An important feature of the NIPC is an analytical capability designed for all the information that will flow through the NIPC, including intelligence, criminal investigative, and infrastructure information, tied to a watch and warning unit set up to disseminate analytical product and warnings to a variety of audiences. The watch and warning unit will be linked electronically to other federal agencies, including other warning and operations centers, and will be a focal point for the collection and dissemination of information on cyber intrusions and other infrastructure related information from open sources, intelligence sources and, to the extent agreed upon, by other federal agencies and private sector organizations that gather and analyze information about cyber intrusions. The mission of the watch and warning unit will include providing timely warnings of intentional threats and comprehensive analyses. NIPC warnings may also include guidance regarding additional protection measures to be taken by owners and operators. In providing this guidance, the NIPC will coordinate closely with the PDD 63 critical infrastructure Sector Liaisons and Sector Coordinators, and other relevant federal and private sector entities, that are responsible for developing sector based plans for protecting their critical infrastructures.

explosive or incendiary device, or an unconventional weapon containing chemical, biological, radiological or nuclear (CBRN) matter. They also may be the first to discover a WMD before it is activated and, thus, will be responsible for disarming or containing it. Their initial actions will be critical to the success of the overall response and, hence, to public health and safety.

Our capability to prevent or respond to a terrorist incident varies according to the type of weapon used and the magnitude of harm caused, although there is room for improvement in all areas. In general, state and local emergency responders are best prepared to deal with incidents involving conventional explosive or incendiary devices. Of the CBRN weapons, our ability as a nation to deal with nuclear or radiological weapons is the strongest because of military programs developed during the Cold War and regulatory programs developed in response to the use of nuclear energy. State and local capabilities are adequate in areas hosting nuclear facilities. Similarly, many states and local communities have some basic chemical detection and response capabilities because of the pervasive risk posed by routine transportation of hazardous materials and the presence of chemical storage and manufacturing facilities or chemical weapons stockpile disposal sites. By far, our greatest deficiency in regard to WMD lies in our limited capability to detect, prevent and respond to the use of biological agents. Moreover, if terrorist use of a conventional or unconventional WMD were to cause mass casualties, even those localities with some degree of response capability would quickly be overwhelmed.³²

A comprehensive federal effort to enhance and support state and local capabilities to respond in WMD incidents should:

- promote the addition of WMD response plans to every state emergency response plan and the development of WMD response plans in every significant jurisdiction of a state;
- develop national standards for CBRN and conventional terrorism response capabilities and promote their adoption by national and state professional accreditation systems;
- identify, develop and make available, through existing national, state and local training systems, courses to enable emergency responders (including, but not limited to, firefighters, police officers, emergency medical and other medical and public health professionals, and specialists such as bomb squad and HAZMAT technicians) to meet the terrorism response capability standards in their respective fields;
- develop recommended standards for CBRN civilian response equipment and provide financial support to enable first responders to acquire equipment that meets recommended standards;

³² These assumptions are supported by the results of various studies and surveys of state and local agencies. See, e.g., Appendix: State and Local Questionnaire, responses to questions 26-28.

- encourage federal agencies to include state and local responders in federal interagency terrorism response exercises and encourage states and localities to conduct terrorism-focused exercises as part of their ongoing emergency preparedness efforts; and
- provide readily accessible information and technical assistance to first responders and emergency planners on the full range of WMD issues, from the use of conventional explosives to the use of chemical, biological or radiological material.

Conventional Explosives

Although first responders must be properly trained to deal with the unique character of CBRN weapons, they are more likely to encounter conventional explosives which are more available and familiar to terrorists. States and localities must be prepared to deal with weapons ranging from pipe bombs to large truck bombs. Such weapons may be directed at first responders as the primary or secondary target. Although we have experience and existing training programs to deal with more conventional explosive weapons, there are still gaps which we can and should address. There is also concern that terrorists may combine deadly CBRN materials or matter with conventional explosive devices, thereby creating dual hazards for which first responders are largely unprepared.

**Action: Increase Availability Of Federal Pre-Blast And Post-Blast
Bomb Technician Training For First Responders**

Primary responsibility for pre-blast response to a suspicious package or recognized explosive device rests with local bomb squads. There are approximately 630 bomb squads associated with police and fire departments throughout the United States. Federal law enforcement agencies play a significant role in training these state and local first responders. Through an interdepartmental support agreement with DOD, the FBI manages the Hazardous Devices School (HDS) at Redstone Arsenal in Huntsville, Alabama. Since 1981, when Congress assigned this responsibility to the FBI, HDS has been the only school in the United States that trains public safety officials as bomb technicians. To date, over 5,000 technicians have graduated from the four-week-long basic HDS course and 4,000 have received the one-week refresher training course. In FY 97, 192 technicians received the basic course; the same number participated in refresher training. An additional 240 bomb technicians, who were graduates of the HDS basic course, received additional training through a series of one week regional training seminars conducted by the Bomb Data Center. There was a lengthy waiting list for attendance at the HDS basic course. All Regional Technician Seminars were filled.

To address the backlog in requests for training at the HDS, Congress appropriated \$5.2 million in FY 98 under the Attorney General's Counter-terrorism Fund. This allowed the FBI to train 1,270 students at the HDS. The Administration's 1998 Chemical/Biological Preparedness budget amendment proposed \$5.2 million for FY 99 and subsequent years to continue the increased level of training started in 1998. With this funding, the FBI has implemented a WMD

Emergency Actions course and has begun a Robotic Training Course and an Executive Management Course. An Advanced Diagnostics and Disablement course is being designed to meet training needs identified by the bomb technician community. This enhanced level of training should be maintained.

To support expanded training capacities and certification programs for bomb technicians, the FBI proposes to upgrade HDS facilities. Current facilities -- which consist primarily of three aging metal buildings and small test ranges located an inefficient distance from other facilities -- limit the quantity and quality of personnel trained. Because of the increased number of students, classrooms, practical problems training rooms and equipment storage space are over-capacity. In addition, there is no practical problems training course that allows students to practice techniques in a realistic setting and under instructor supervision. The Administration is currently considering upgrades to the facility in a number of areas.

Federal post-blast investigative training for civilian first responders comes primarily from two agencies: the FBI and the Treasury Department's Bureau of Alcohol, Tobacco and Firearms (ATF). The FBI's Explosives Unit and Bomb Data Center conducts a Post Blast Investigators school that offers instruction in bomb evidence collection, preservation, and evaluation. Only public safety personnel with investigative responsibilities in bombing cases are eligible for this training. In FY 97, approximately 365 investigators received post blast training conducted by the FBI either regionally or at the FBI Academy at Quantico, VA. ATF conducts similar training through the Federal Law Enforcement Training Center (FLETC) and, on request, offers the training to state or local agencies. In FY 97, ATF taught Bomb Threat Management, Post-blast and Explosives Recognition courses to approximately 30,000 state, local and federal officers as well as members of civic groups. Other post-blast training was provided to 7,000 state and local responders; that number is expected to be even larger in FY 98. In addition, 95 state and local investigators participated in the FLETC Advanced Explosives Investigative Techniques in FY 97. Both the FBI and ATF report that the demand for these courses exceeds their availability.

To maximize the effect of federal post-blast investigative training, the FBI and ATF will assess, through an existing interagency working group, whether they are providing compatible post-blast investigative training to state and local agencies. If incompatibilities are found, FBI and ATF will propose modifications to ensure that training is consistent. No additional funding is required for this assessment.

Action: Prepare Bomb Technicians To Address Incidents Involving A Combination Of Explosives And Chemical, Biological Or Radiological Agents

Even though bomb technicians may be among the first emergency responders to encounter a terrorist device, they are relatively unprepared to address incidents involving the combined use of explosives and a chemical, biological or radiological substance.³³ To meet these unique needs, we need to expand related training and equipment programs for these first responders.

In FY 98, the FBI's HDS at Redstone Arsenal created a one-week specialized Weapons of Mass Destruction Bomb Technician Emergency Actions course, which it expects to provide to approximately 340 students within the fiscal year. With enhanced funding in 1999, the WMD course will be integrated into an expanded and revised recertification course.

To support and protect bomb technicians, the Department of Justice will administer a three-year program to outfit the approximately 630 bomb squads throughout the United States with equipment to allow them to detect and react to a chemical or biological agent. Each year of the program, approximately 210 squads will be able to procure detection equipment, including mass spectrometers and polymer-chain reaction (PCR) devices capable of detecting and identifying chemical and biological agents/toxins; robots; portable x-ray machines; chemical/biological suits; percussion automated non-electric (PAN) disrupters; digital probes and other tools; technical and reference manuals; and training materials for state and local bomb squads. Additional support to retrofit 200 total containment vehicles currently in use by state and local bomb technician squads to accommodate improvised explosive devices suspected of having chemical or biological agents or toxins is also being considered.

In addition to these training and equipment programs, state and local bomb squads need protocols for working with HAZMAT units in situations that involve packages that do not contain an explosive device but may contain a chemical or biological substance. The FBI will be working with the HAZMAT community and federal agencies such as the Environmental Protection Agency (EPA) and Federal Emergency Management Agency (FEMA) to develop and promote such protocols.

The proposed National Domestic Preparedness Office, in consultation with the WMDP Group, would assess whether bomb squads need radiological monitors and personal protective equipment as well as chemical and biological devices and equipment. If so, the office would develop specific proposals for ensuring the availability of this equipment.

³³ See Appendix: State and Local Questionnaire, responses to questions 26 and 27.

CBRN Agents

Since 1996, the federal government has made first responder preparedness for terrorist incidents involving CBRN agents, particularly chemical or biological agents, a high priority. Primarily through the Nunn-Lugar-Domenici (NLD) Domestic Preparedness program,³⁴ CBRN training, equipment and related field exercises have been made available to first responders in the nation's largest cities. If carried to completion, in five years this program will create a basic emergency response capability in the most heavily populated areas of the country. It has raised awareness of terrorism issues among first responders and fostered closer working relationships among federal, state, and local emergency response agencies.³⁵ Thus, the NLD program represents an important step in the development of a long-term strategy for building and maintaining first responder capability nationwide.

Nonetheless, many observers believe that corrections are needed in the initial course set by the NLD program and in the federal approach to domestic preparedness generally. The most frequently identified shortfalls in the current approach are: 1) the lack of coordination among, and focal point for, federal domestic preparedness efforts;³⁶ 2) insufficient coordination of federal efforts with the pre-existing state and local emergency response systems;³⁷ 3) inattention to the

³⁴ This program was authorized in the National Defense Authorization Act for Fiscal Year 1997. The popular name refers to the program's three primary Senate sponsors.

³⁵ See U.S. General Accounting Office, Combating Terrorism: Opportunities to Improve Domestic Preparedness Program Focus and Efficiency (GAO/NSIAD-99-3, November 12, 1998) (hereafter "Domestic Preparedness Report"), at p. 4.

³⁶ On August 27-28, 1998, DOJ convened a state and local "stakeholders" forum in Washington, D.C., to solicit first responder input on domestic preparedness issues. More than 200 state and local emergency response planners and practitioners attended this forum. One of the recommendations from this group was that a single point of contact should be designated for coordination of the various federal initiatives that provide training, equipment and other domestic preparedness assistance. See also Domestic Preparedness Report, *supra* footnote 15, at p. 20 ("Some local officials viewed the growing number of WMD consequence management programs. . . ., as evidence of a fragmented and possibly wasteful federal approach toward combating terrorism.")

³⁷ See Domestic Preparedness Report, *supra* footnote 15, at p. 8 (noting that current NLD focus on large cities does not leverage existing state emergency management structures, mutual aid agreements among local jurisdictions or other collaborative arrangements for emergency response).

training and equipment needs of states and localities not served by the targeted cities;³⁶ and 4) the absence of a plan to maintain responder skills and equipment once the initial training is completed. As explained below, future efforts should focus on correcting these shortfalls.

**Action: Coordinate Emergency Responder CBRN Training, Exercise
 And Equipment Initiatives And Expand To All Jurisdictions**

Training

A brief review of the major federal first responder training and equipment programs illustrates why states and localities call for better coordination and a single federal point of contact.

Nunn-Lugar-Domenici Training Program: In the NLD Domestic Preparedness program, Congress authorized the Department of Defense (DOD) to develop and conduct first responder training focusing on terrorist incidents involving nuclear, chemical or biological weapons. DOD targeted the 120 most populated U.S. cities to receive this training. The NLD program has offered two medical and six non-medical courses aimed at educating experienced city trainers so that they can train law enforcement officers, firefighters, HAZMAT technicians, emergency medical personnel, and emergency managers in general subjects such as awareness and incident command, as well as in more specialized courses in specific operational areas (e.g., HAZMAT, emergency medical, hospital provider). Through courses developed by FEMA, DOD has also provided some direct training in basic awareness and a workshop for senior officials, such as mayors and their cabinets. In addition to classroom instruction, the NLD program includes a table-top and a field exercise to test participants' ability to apply the information taught. Once DOD identifies a city for training, it is left up to mayors and city managers to decide which and how many trainers to send through this program. DOD has now stated its intention to transfer this entire program to the Department of Justice.

By the end of FY 98, DOD had trained approximately 10,000 trainers in 32 cities and conducted 10 follow-up field exercises. DOD had planned to introduce its program in all 120 cities by the end of fiscal year 2000.

The Office of Justice Programs Chem/Bio Training Program: Congress also authorized, through the Antiterrorism and Effective Death Penalty Act of 1996, a second terrorism training program for firefighters and emergency medical personnel. This program has been administered by the Office of Justice Programs (OJP) within the Department of Justice. The OJP courses are based on materials developed by FEMA's National Fire Academy (NFA). They cover explosive, incendiary, chemical and biological, but not nuclear or radiological, incidents. OJP has provided

³⁶ See Domestic Preparedness Report, *supra* footnote 15, at p. 6 (120 cities represent about 22 percent of the U.S. population; 12 states and the U.S. territories have no cities in the program and 25% of the NLD cities are in California and Texas).

a two-part basic concepts "train-the-trainer" course and a direct course in incident management and tactical decision-making to responders in the 120 largest urban jurisdictions (cities and counties). OJP's target audience overlaps but is not identical to the DOD target audience. Combined, the "train-the-trainer" classes offered by DOD and OJP encompass 157 separate urban jurisdictions in 38 states. OJP has also made its "train-the-trainer" course available to instructors from all state fire training academies, and has offered a self-study terrorism awareness course to all firefighters and emergency medical teams. OJP estimates that by the end of calendar year 1998, 75,000 firefighters and EMS personnel and 420 trainers will have been trained (including through self-study) in its 120 targeted urban jurisdictions.

In addition, in FY 98 and FY 99, OJP will receive up to \$10 million to establish a Center for Domestic Preparedness at Fort McClellan, Alabama. This center will provide advanced hands-on training for law enforcement officers, firefighters, emergency medical and emergency management personnel in responding to terrorist incidents involving CBRN weapons, including some courses involving actual chemical agents. OJP estimates that 1,800 first responders will receive training by the end of FY 99; 450 of them will participate in courses involving actual chemical agents.³⁹

FEMA Course Materials and Grants: FEMA, through its National Fire Academy (NFA) and Emergency Management Institute (EMI), issues basic course materials concerning emergency response to terrorism for emergency responders generally, including firefighters, emergency medical service providers, and HAZMAT technicians. FEMA also issues course materials aimed at preparing elected officials and managers to deal with the consequences and management of terrorism and other events resulting in mass fatalities. Both DOD and OJP have used FEMA materials as the basis for some or all of their first responder training courses.

In FY 98, FEMA also provided grants totaling \$110 million to the states for planning, training and exercises to improve disaster preparedness and support development of a risk-based all hazard emergency management capability. Of these grants, \$1.2 million was earmarked for terrorism-related training and for assessing and improving plans and systems to enhance the capability for dealing with the consequences of terrorism. Also in FY 98, FEMA provided \$2.0 million in grants to state fire training centers to support training and enhance the capability of fire departments to respond to terrorist attacks.

³⁹ In response to Congressional direction, OJP has established a consortium of facilities for training development and delivery. In addition to the Center for Domestic Preparedness, the consortium includes the Energetic Materials Research and Testing Center at the New Mexico Institute of Mining and Technology; the National Center for Bio-Medical Research and Training at Louisiana State University; the Nevada Test Site; and the National Emergency Response and Rescue Training Center at Texas A&M University. These centers will be used to promote advanced training and curriculum development for first responders.

Other Federal Training Programs: the Environmental Protection Agency's (EPA) Environmental Response Team provides training to federal, state and local HAZMAT technicians (responders and planners) which addresses radiological, biological and chemical hazards. EPA is adding training dealing with weapons of mass destruction to its existing five-day training course. The Department of Energy (DOE) also sponsors training in how to respond to incidents involving the release of nuclear or radiological substances. This training is made available primarily to communities in which nuclear facilities are located. The Department of Transportation (DOT), in consultation with FEMA, administers the Hazardous Materials Emergency Preparedness (HMEP) Grant Program, which makes grants to states, territories and Indian Tribes for training of public sector employees who respond to emergencies and for the development of improved hazardous materials emergency response plans. Approximately \$6.75 million per year is expected to be made available for this program over the next five fiscal years. Depending on the needs perceived by each state, this grant money can support training programs with a terrorism focus.⁴⁰

In order to provide state and local responders with a single point of contact for the multitude of federal domestic preparedness efforts, the Attorney General will be proposing to establish a National Domestic Preparedness Office (NDPO) within the Department of Justice. The primary mission of the NDPO is to coordinate Department of Justice programs with those of other federal agencies to enable state and local first responders to establish and maintain a robust crisis and consequence management infrastructure within the United States capable of responding to a conventional or nonconventional terrorist attack. To facilitate this coordination, DOD proposes to transfer responsibility for the NLD city training program and related equipment, exercise and most technical assistance initiatives to the Department of Justice by the end of FY 00.⁴¹ The NDPO, under the leadership of the FBI, would address planning, training, equipment, exercises, research and development, intelligence and information sharing, and health and medical service needs at the federal, state and local levels.

The NDPO would coordinate the overall state and local training effort, and fully integrate the various domestic preparedness training programs now conducted by DOD, OJP, FEMA, and

⁴⁰ This is only a partial illustration of the federal programs that might be used by states and localities to acquire or improve their WMD response capabilities. As part of its domestic preparedness program, DOD compiled a directory of federal courses relating primarily to CBRN response. That directory lists over 80 courses sponsored by 11 different agencies that could be used by first responders. Most of the courses address preparedness to deal with the use of a CBRN weapon, although some courses relating to incident command issues would apply to all WMD incidents. These are in addition to the federal programs that train bomb technicians how to address the use of bombs or improvised explosive devices by terrorists.

⁴¹ The National Defense Authorization Act of FY 97 allows the President to transfer lead agency responsibility for the domestic preparedness program from DOD to another federal agency on or after October 1, 1999.

other departments and agencies into the broader national training initiative. Training development will be done in consultation with participating federal agencies, state and local government officials, and first responders. An interagency training development group would be established. Its participants would include training and curriculum development expert staff from the FBI, OJP, FEMA, DOD, Health and Human Services (HHS), EPA, and DOE. As required, additional expert staff from other relevant federal, state and local agencies would supplement the core interagency training development group. The curriculum would include response training tailored to meet the needs of first responders in a variety of WMD crisis scenarios. This program will be based on the capabilities and needs assessment developed by NDPO and conducted by each community.⁴² To the greatest extent possible, existing FEMA programs, networks and facilities, such as the National Fire Academy and the Emergency Management Institute, and other federal, state and local training systems should be used to deliver training to state and local responders.

As part of its coordination effort, and in response to questions raised about the efficiency of the current NLD focus on the 120 largest cities, the NDPO could assess whether the NLD delivery model results in the best use of federal resources. This method by-passes the well-established emergency response training and planning systems in most states, which are the key means by which states establish their own priorities, based on existing resources, and coordinate their emergency response efforts. The General Accounting Office (GAO) has challenged the NLD 120 cities approach on several grounds, including that it results in duplicative training efforts in neighboring cities while at the same time offering no training in several states and across large regions of the country. Domestic Preparedness Report, *supra* footnote 15, at pp. 6-17.

Reorienting federal domestic preparedness programs so that they serve the entire nation, reflect priorities established by the individual states and are delivered through existing state training systems would address the problems identified by the GAO. Nonetheless, many cities have already built the expectation of NLD training into their emergency response planning. It may be too disruptive, and result in too many countervailing inefficiencies, to abruptly change the NLD program focus now. An alternative would be to complete the NLD cities program as initially conceived, while assessing the opportunity to provide support that will allow states, in compliance with federal standards, to provide training, equipment and related domestic

⁴² Congress has amended the Defense Against Weapons of Mass Destruction Act to include a new subsection which requires the Attorney General, in consultation with the FBI and appropriate federal, state and local agencies, to develop and test a methodology for assessing the threat and risk of chemical, biological or radiological weapons being used against cities or other local areas. Congress also provided that such assessments could be used to determine the training and equipment to be provided under federal domestic preparedness programs focusing on chemical, biological or radiological weapons. The FBI will conduct a pilot project to develop and test such a methodology.

preparedness planning for the balance of the nation.⁴³ Once the NLD cities training is done, the tasks of maintaining and enhancing capabilities in those cities could revert to the states, again with the continuing guidance and technical assistance of the NDPO. This would allow state and local emergency response managers, who are most familiar with all state and local resources and needs, to better allocate training and resources. At the same time, federal agencies with experience in CBRN preparedness would need to continue to update and maintain training, courses, and equipment standards and test and develop innovative or enhanced preparedness initiatives to supplement state efforts. The NDPO should address this issue promptly, with substantial input from the state and local first responder and emergency planning communities and advice from the NSC's WMDP Group.

Coordination of initial first responder training is just the first step in a sounder domestic preparedness strategy. Training programs must ensure that the proficiency of responders trained is maintained, follow-on training is provided as refresher instruction, and responders are informed of new equipment, techniques, and threats as they appear. Regular exercise and planning cycles should be developed in order for plans and skills to remain up to date.

Exercise Programs

Current federal terrorism response exercise efforts focus almost exclusively on the participation of federal agency personnel and assets. Yet field exercises are a crucial means by which participants evaluate and validate their planning, training and equipment. As more state and local responders complete terrorism preparedness programs, it will be necessary to involve them in more field exercises to test the effectiveness of the training and to refresh capabilities. The proposed NDPO would undertake an initiative to support the planning, scheduling and implementation of coordinated exercises involving state and local responders. These exercises should be closely integrated with the federally-supported training programs and be realistic, hands-on, multi-team, multi-agency events based on threat-driven scenarios, and designed to evaluate performance, reinforce training and provide positive feedback. Ideally, exercises will range from simple local events to complex multi-jurisdictional national level episodes -- from local and regional exercises, to state and multi-state exercises, as well as national-level exercises. At the same time, development of these exercises should reflect that first responders already participate in non-terrorism-related exercises as part of their continuing professional certification

⁴³ One grant program that offers a useful model for how such a program could be administered is the Hazardous Materials Emergency Preparedness (HMEP) Grant Program administered by DOT. Although HMEP grants are made to states, so that planning and training can be coordinated with each state's unique emergency response system, the majority of grant money must be spent directly on programs that reach first responders and the money must be used to achieve national objectives. In connection with this grant program, FEMA has developed for DOT required and recommended training and planning guidelines so that states can select courses that ensure that their public sector employees can safely and efficiently respond to hazardous materials emergencies.

or state and local emergency planning obligations. The domestic preparedness initiatives should be closely integrated with existing exercise obligations in order to reduce unnecessary demands on emergency response professionals.

Equipment Programs

State and local first responders are not adequately equipped to respond to a CBRN terrorist incident.⁴⁴ In most cases there is only marginal awareness of overall capability, requirements, shortfalls, and the potential for mutual support. Deficiencies in CBRN specialized equipment are compounded by uncoordinated procurement and maintenance programs. The result is a lack of sufficient equipment, standardization, and inter-operability necessary to respond to a CBRN terrorism incident in a safe, timely and effective manner. Provision of CBRN training is fruitless unless first responders have access to the proper equipment.

To support NLD training, Congress authorized DOD to lend CBRN equipment to first responders for training purposes. DOD makes up to \$300,000 available to each NLD city for training equipment and materials under a five-year loan agreement that requires the cities to repair, maintain, and replace the equipment. Equipment that may be loaned includes personal protection equipment, detection equipment, decontamination and containment equipment, and training aids. Many cities are dissatisfied with this arrangement because they view the maintenance provisions as an expensive unfunded federal mandate. *See Domestic Preparedness Report, supra* footnote 14 at p. 18. Cities also express frustration that they are not supposed to use the loaned equipment for anything but training. *Id.* However, despite this restriction in the authorizing statute, DOD reports that it will allow the cities to keep the "loaned" equipment and use it for operational purposes as well as training. *Id.* In addition, some cities also report frustration that they must comply with two separate application processes in order to obtain training-related equipment for the core NLD training program and the related Metropolitan Medical Response System program, discussed *infra* at pp. 32-33, which was also authorized by the FY 97 Defense Authorization Act. *Id.*

Recognizing that equipment loans were not sufficient, in FY 98 and 99, Congress appropriated \$103.5 million to make chemical/biological equipment permanently available to first responders through grant programs that will be administered by DOJ's Office of Justice Programs. OJP estimates that this money would support two to three HAZMAT response teams per locality with individual and team equipment consisting of personal protective clothing and equipment with self-contained communication, air supply, and metering, monitoring and detection systems; antidote delivery systems; and mass decontamination systems and equipment. Equipment grants programs should be continued. The proposed NDPO could offer useful guidance. In addition, the WMDP Group should assess whether there is a comparable need for nuclear/radiological equipment.

⁴⁴ *See* Appendix: State and Local Questionnaire, responses to questions 26 and 27.

The proposed NDPO also could coordinate the creation and promotion of national equipment standards to enable states and local agencies to procure reliable, compatible CBRN response equipment. These standards should be developed in consultation with representatives of state and local responders, and conform to National Institute for Occupational Safety and Health, National Fire Protection Association and other recognized standards. All equipment procured through the federal grants program should conform to the promulgated standards and be in compliance with state and applicable federal emergency response plans.

**Action: Ensure That Emergency Response Training Programs Address
Crime Scene Issues of Personal Safety And Evidence
Preservation**

The majority of fire, EMS and emergency management personnel have received insufficient training in the special issues that may arise when they respond to a WMD/terrorist crime scene. Two specific crime scene issues must be addressed in WMD emergency response training programs: the targeting of first responders and emergency personnel for terrorist attack and evidence preservation. First responders who understand that they are increasingly the primary or secondary targets of terrorist acts can better protect themselves. Equally important, if properly trained, first responders will be better able to notice and preserve evidence.

Existing NLD and OJP basic awareness courses educate first responders in the target urban areas in dangers they may encounter as potential targets of terrorist attack. These courses also need to promote new protocols for securing the scene and conducting operations to protect the responder and the public from deliberate secondary attacks. Priority should be given to providing first responders throughout the country with similar basic terrorism awareness/personal safety courses. FEMA should coordinate this effort, in consultation with the federal agencies and professional associations that traditionally work with or represent first responder constituencies, and with organizations representing state and local governments. The proposed NDPO could assist in this effort. To speed delivery, these materials should be distributed through existing training delivery mechanisms such as state training academies, long distance learning centers (e.g., the long distance learning system supported by the National Guard), and self-study programs using traditional and innovative methods such as interactive CD-ROMs. The goal should be to guarantee by the end of FY 00 that every first responder in the country has access to these basic awareness materials, either through group courses or self-study.

Some emergency response training materials already introduce first responders to evidence collection and preservation issues. For example, FEMA's Emergency Management Institute offers a six to eight hour course entitled "Emergency Response to Criminal/Terrorist Incidents," that is aimed at firefighters, emergency medical services, law enforcement, public works and emergency managers. Among other goals, the course is designed to enhance evidence preservation and foster cooperative working relationships among responders by clarifying roles and responsibilities, particularly between law enforcement and emergency responders. In a similar effort, FEMA's National Fire Academy, with support from OJP and in coordination with

the FBI, is developing advanced courses in incident management and operations that will include a unit on evidence preservation. EPA also includes training in evidence preservation through its National Enforcement Investigations Center. Courses under development should be completed as soon as possible and evidence preservation instruction made a required component of any federally-supported WMD/terrorism training or grants program for first responders.

Action: Encourage States And Localities To Develop Terrorism Response Plans

Most states and many localities, particularly urban areas, have emergency response plans to enable them to deploy and coordinate necessary resources during a natural disaster. These plans reflect the unique combination of resources present in each community and often incorporate mutual aid agreements among jurisdictions in the state or even across state lines. Although these plans are not specifically designed to deal with terrorist-caused disasters, there are common elements among the resources needed to respond to any kind of disaster, and first responders are accustomed to working within the existing disaster response systems. To promote efficient use and coordination of resources, terrorism response plans need to build upon these existing emergency response systems.

The FBI and FEMA will share responsibility for coordinating federal, state and local planning, with the goal of promoting the adoption of terrorism crisis and consequence response plans at the federal, state and local government levels nationwide. FEMA already has a limited grants program in place to encourage development of terrorism-specific annexes to existing state emergency response plans and for other terrorism response activities. FEMA should assess the number of states that have successfully incorporated terrorism response plans into their existing emergency response systems and determine what, if any, additional incentives are needed to achieve adoption of terrorism response plans by all states by the end of the calendar year 2000. In addition, FEMA should examine whether its current program successfully promotes the inclusion of desirable planning elements such as inventories of specialized terrorism response resources within that state (e.g., specially trained WMD response teams); mutual aid agreements; and coordination with federal terrorism response agencies. Although care should be taken not to impose unnecessary or overly restrictive requirements on state planners, it is appropriate to condition receipt of federal assistance on the attainment of reasonable national objectives.

Promoting terrorism response plans at the local level presents the greatest challenges. Many communities simply do not have the resources or the necessary governmental infrastructure to develop all-purpose emergency response plans, much less specialized plans to deal with WMD incidents. Through the proposed NDPO and in consultation with national associations representing the affected state and local governments and planning agencies and the Contingency Planning and Exercises Working Group of the WMDP Group, the FBI and FEMA should develop by the end of FY 99 specific proposals for stimulating the development of WMD crisis and consequence response plans, respectively, at the local level. These proposals should include performance measures, such as the proportion of localities to adopt such plans in a given

period of time. Again, if financial incentives are proposed, then they should be tied to the inclusion of necessary planning components. Linkages with federal, state and other local plans would be especially important.

Particular attention should be paid to leveraging complementary local planning processes. For example, states and localities have State Emergency Response Commissions and Local Emergency Response Committees (LEPCs) to address the environmental consequences of a hazardous materials release, which would include releases caused by a terrorist act. LEPCs are responsible for developing hazardous materials response plans for their communities; where the community also has a more general emergency operations plan, the HAZMAT plans must be incorporated into it. The EPA, which provides technical assistance and advice to LEPCs, has set an administrative goal that, by the calendar year 2005, fifty percent of the LEPCs will incorporate WMD preparedness into local HAZMAT response plans. While this is an important step, communities with broader response capabilities should not limit their terrorism response plans to HAZMAT response activities. Localities that intend to add WMD preparedness plans to their local HAZMAT plans should be encouraged to expand the focus to WMD preparedness for all emergency responders. Similarly, HHS promotes local planning through the Metropolitan Medical Response Systems program, which provides funds and encouragement for municipal officials to develop plans for use of medical resources in conjunction with police, fire and emergency response systems.

As illustrated above, states and localities may develop emergency response plans for different purposes in order to comply with different federal mandates. While it may be useful for various plans to include terrorism-specific components, the federal agencies that oversee the different planning processes should not impose or encourage inconsistent terrorism planning requirements. To avoid conflicting requirements, the NDPO, in consultation with the WMDP Group, could ensure that federal agencies with state or local emergency planning roles adopt complementary terrorism-related planning requirements for states or localities. The same forum could be used to ensure that technical assistance to state or local planners is not conflicting or unnecessarily duplicative.

**Action: Establish And Maintain Reliable, Immediately Accessible
Expert Assistance To First Responders On CBRN Terrorism
Matters**

In the FY 1997 National Defense Authorization Act, DOD was directed to establish a "helpline" and a "hotline" to provide relevant data and expert advice for the use of state and local officials responding to emergencies involving CBRN weapons or related materials.⁴⁵ The

⁴⁵ Although the National Defense Authorization Act uses the term "weapons of mass destruction" to describe its preparedness initiatives, the Act does not include explosive or incendiary devices within the definition of WMD, as we do in this Plan. Accordingly, we do not use the term to describe DOD's programs.

Helpline was opened on August 1, 1997, to provide access to information about chemical and biological agents on a routine, non-emergency basis; it is staffed weekdays from 9:00 a.m. to 6:00 p.m. Operators have the capability to access and retrieve information quickly and distribute it by a variety of means, including fax and e-mail.

A 24-hour Hotline was activated in January 1998 through an agreement with the U.S. Coast Guard's existing and successful National Response Center. All incoming calls detailing the release of a chemical or biological agent will be connected with the relevant expert DOD agency as well as with the appropriate FBI Field Office. In the event a call involves a threatened or pre-release scenario, the call will be forwarded to the FBI for further threat assessment. Access to expertise in a nuclear or radiological incident is available through the Department of Energy's 24-hour emergency operations center.

A related effort involves FEMA's development of the Rapid Response Information System (RRIS) to aid federal, state and local emergency responders in preparing for and responding to a terrorism incident involving CBRN agents. The RRIS provides information on federal response capabilities that could be made available to support state and local government response efforts; information on surplus federal equipment available from the General Services Administration; databases of the characteristics and safety precautions for chemical and biological warfare agents and radiological materials; information on physical descriptions, characteristics and safety precautions for chemical and biological munitions; information on the advantages and limitations of current CBRN equipment used by the federal government; CBRN Hotlines and Helplines; and a reference library of internet-related resources dealing with CBRN topics.

These systems should be maintained on a permanent basis. In addition, the appropriate working group of the WMDP Group, in coordination with the proposed NDPO, should formally survey the extent to which state and local emergency responders and planners find these resources useful and, in particular, whether they know how to and expect to access the emergency hotlines in the event of an emergency.⁴⁶ FEMA has already made an electronic survey form available to RRIS users to supply informal feedback on the system. The WMDP Group should develop specific proposals to address any deficiencies revealed by formal assessments.

⁴⁶ A number of city and state officials interviewed by the GAO had limited knowledge of the hotline or the RRIS and expressed skepticism of their value during a crisis. Domestic Preparedness Report, *supra* footnote 15, at p. 5.

Medical and Public Health Response

The emergency responder training and equipment programs described above are designed to prepare local governments to respond rapidly, safely and effectively to a WMD terrorist attack, whether it involves conventional explosives or the use of CBRN materials. They are directed at existing police, fire, and emergency medical community response capabilities. While these programs enhance essential public safety functions, additional measures are needed to prepare medical and public health systems to deal with the consequences of a mass casualty WMD incident, especially one involving a biological weapon. This is particularly important because the release of a biological agent may not be discovered until health care providers recognize and correctly diagnose the symptoms in victims who have been exposed. Even if a release is known to have occurred, the medical and public health communities will play a critical role in correctly identifying and treating victims, and protecting the unexposed public and emergency personnel from harm.

We must pursue a two-pronged strategy in this area: 1) enhance our existing emergency and disaster medical response systems to include the ability to address the unique requirements of CBRN incidents; and 2) support a public health surveillance and response system capable of identifying and countering surreptitious CBRN incidents, with a special focus on incidents involving biological agents. This will require enhancing or, in some cases, building state and local capabilities and federal support systems to supplement local efforts.

Providing appropriate care for the affected population and obtaining critical health system assets, including health professionals, pharmaceuticals, equipment and facilities, are crucial to a successful response. Health response requirements are driven by the type of WMD incident encountered. A chemical incident generally results in immediate effects at a known incident site and requires the on-scene determination of the causative agent. Short term goals in such an incident include keeping people alive, providing immediate care, and accessing more definitive care. The longer term goals include maximizing patient recovery, which could take days to months.

Radiological incidents involve fewer treatment options. Nuclear incidents would result in severe traumatic and thermal injuries similar to those experienced in a conventional mass casualty event, but on a larger scale. There would also be considerable radiation injuries. Both radiological and nuclear incidents would incur significant long term medical and environmental consequences.

Unlike a chemical or nuclear attack, an intentional silent release of a biological weapon may not be apparent for days until it is detected and identified by the public health surveillance system. A biological incident can be characterized by its stealth, including delayed effects from exposure to an unknown pathogen. When the release occurred, where it occurred, and what was released may be unknown. The health response would include mass prophylaxis, mass patient care, and mass fatality management. Environmental cleanup might be larger in scope and more

complex than in a localized chemical incident.

If intelligence and law enforcement measures are unsuccessful in preventing a bioterrorist attack, communities must rely on the public health surveillance system to detect signs of a possible bioterrorist event. This means that public health providers, such as family physicians, school nurses, infectious disease specialists and emergency room personnel, must be able to recognize as early as possible that an anomalous situation exists and transmit these concerns immediately to state and national health authorities for rapid diagnosis.

Much of the burden and responsibility for providing an appropriate health system response to a terrorist attack of any kind rests on state and local governments. The local public health system will be called on to provide appropriate protective and responsive measures for the affected population. However, depending on the scope and magnitude of the event, appropriate urgent support must be provided by federal agencies. Surveillance, epidemiologic capabilities and medical response systems are activities where the federal government can work in partnership with states and localities, providing leadership and funding early in this multi-year effort, but where states and localities should be expected to assume more responsibility for their share of partnership expenses over time. The nature of terrorist attacks requires that assistance be provided in a well integrated manner to support local public health and medical needs.

OBJECTIVE: Enable Local Medical Providers To Quickly And Safely Treat Victims Of A CBRN Attack And Protect Others At Risk

As a result of PDD 39, HHS reviewed the adequacy of the nation's medical systems in responding to terrorist incidents. That review concluded that "[t]raining for [medical] response operations in an NBC⁴⁷ environment is almost totally lacking at this time." HHS also found a compelling need to train non-EMS medical personnel, such as physicians, nurses and hospital staff, in triage and treatment of CBRN victims.⁴⁸

Among the potential terrorist weapons, biological agents present special challenges that require unique preparation. Whereas explosives as well as most chemical weapons cause immediate casualties, an intentional, silent release of a biological agent can take days or even weeks before it is detected. Therefore, the traditional first responder (police, firefighters, paramedics) scenario is not likely to occur as a result of a bioterrorist attack. Suspicions about such an attack will develop only when unexplained clusters of illness and/or death begin to

⁴⁷ In its review, HHS used the term "nuclear, biological, chemical (NBC)" to refer to the kinds of agents that this Plan refers to as "chemical, biological, radiological and nuclear (CBRN)" agents.

⁴⁸ No more than 20% of the medical system personnel who responded to the Plan's State and Local Questionnaire believed that first responders and emergency personnel were adequately equipped and trained to respond to a terrorist attack involving CBRN weapons.

emerge. If the biological agent used is contagious or if travelers have been exposed, then the adverse health effects could be felt well beyond the site(s) of the actual terrorist incident. Management of the medical consequences, therefore, is much more demanding than in the case of a localized attack involving explosives or chemicals.⁴⁹

An attack using biological weapons could produce an unprecedented health and medical emergency, generating a demand for medical services that could overwhelm the existing health care system at the local level. It could require the delivery of medical services to a potentially large symptomatic population, providing preventive care to an even larger number of those who are at risk, and ensuring safe disposition of those who have died. A concerted and integrated effort must be mounted by federal, state and local governments to ensure that the array of services required for medical and public health consequence management will be available when needed.

A number of steps have been taken to address this compelling need. First, EMS and some non-EMS medical personnel are now receiving training in CBRN incident response through the DOD Domestic Preparedness and the OJP emergency responder programs. This capability will be advanced and maintained through the training strategies outlined above.

In addition, HHS has begun a two-part program to assist local governments to develop Metropolitan Medical Response Systems (MMRS), as well as to add CBRN capability to the existing National Disaster Medical System (NDMS),⁵⁰ which supplements state and local systems. Also, HHS is developing a national vaccine and pharmaceutical stockpile and delivery

⁴⁹ Similar problems could occur in the event of a surreptitious use of a radiological substance. We are better prepared to respond to such an event. For example, the Department of Energy, in executing its responsibilities for handling radiological emergencies, has trained over 3000 physicians and medical responders in triage, identification of overexposure to radioactive substances, and the use of pharmacologies through the Radiation Assistance Center and Training Site (REAC/TS). Some of this training might also be used in handling overexposures to biological and chemical agents.

⁵⁰ The NDMS is a cooperative interagency program that combines the assets of HHS, DOD, the Department of Veterans Affairs (VA), FEMA, state and local governments and the private sector. Since 1984, it has provided a nationwide medical response system to supplement state and local medical resources during disasters and emergencies; back-up medical support to the military and VA health care systems during an overseas conventional conflict; and development of community-based disaster medical service systems. NDMS is composed of over 5,000 private sector medical and support personnel organized into teams that can be deployed in a national emergency to provide immediate medical attention to the sick and injured when local emergency response systems become overloaded. The NDMS also includes a back-up system of patient beds in almost 2,000 civilian hospitals. These beds are managed by Federal Coordinating Centers run by DOD and the VA.

system. As described below, each of these initiatives is an important component in the nation's counter-terrorism policy.

Action: Support And Increase Metropolitan Medical Response System Capabilities In Strategically Identified Locations

The Office of Emergency Preparedness (OEP) at the Department of Health and Human Services has contracted with local governments of 27 major cities to develop Metropolitan Medical Response Systems (MMRS), [formerly called Metropolitan Medical Strike Team (MMST) Systems].⁵¹ Through teams of specially trained and equipped local emergency medical, HAZMAT, fire and law enforcement professionals, the MMRS enhances local HAZMAT and emergency response systems by providing capabilities for on-site victim extraction, antidote administration, decontamination, primary care, emergency medical transportation and definitive, hospital-based medical care and crisis counseling, primarily in the event of a chemical attack. Success in reducing morbidity and mortality depends on the local response capability for the first day -- until supplemental state and federal assets arrive. MMRS capabilities need to be expanded to include an appropriate response to known sudden releases of biological or radiological agents.

By the end of FY 1999, HHS anticipates assistance to a total of 35 local areas in developing MMRS. Collectively, these systems represent less than one-half of the metropolitan areas targeted for CBRN training in DOD's Domestic Preparedness Program. MMRS should be developed in as many of the targeted areas as possible.

Action: Enhance The National Disaster Medical System's Ability To Respond To CBRN Incidents

The nature of CBRN agents makes it likely that there will be mass casualties, possibly reaching catastrophic numbers, which could quickly overwhelm ordinary local response capabilities. HHS should expand the existing National Disaster Medical System (NDMS) to provide limited supplemental federal assistance to state and local resources as needed, particularly in areas unable to support their own specialized WMD response systems.

The NDMS relies on specialized teams of state and local health professionals who can be deputized for federal service and deployed nationwide to assist communities when their

⁵¹ Eligible cities are drawn primarily from the list of most-heavily populated cities that is used by DOD in targeting its Domestic Preparedness program. To receive HHS support and to enhance their existing systems to include CBRN response capability, cities must present detailed proposals that are subject to interagency review and HHS approval. The 27 cities now participating in the program are: New York, Los Angeles, Chicago, Houston, Philadelphia, San Diego, Detroit, Dallas, Phoenix, San Antonio, San Jose, Baltimore, Indianapolis, San Francisco, Jacksonville, Columbus, Milwaukee, Memphis, Boston, Seattle, Denver, Kansas City, Honolulu, Miami, Atlanta, Washington, D.C., and Anchorage.

emergency response systems are overwhelmed. Disaster Medical Assistance Teams (DMATs) provide in-field medical triage and patient stabilization for transport to medical facilities. There are 24 fully deployable DMATs nationwide, and four enhanced teams that have been specially trained and equipped to respond to CBRN incidents. These teams have been named National Medical Response Teams-Weapons of Mass Destruction (NMRTs). NMRTs are capable of providing victim decontamination, medical triage, and initial treatment and have a limited extraction capability. Three of the NMRTs can be deployed anywhere in the United States.⁵² An additional NMRT is dedicated to service in the National Capital area.

In addition, NDMS Disaster Mortuary Teams (DMORTs) would be needed to assist local medical examiners and coroners deal with the potentially large number of casualties. Decisions must be made on how to safely manage these remains for proper burial or cremation after appropriate steps have been taken to preserve evidence, and how to provide appropriate family support and assistance.

The Office of Emergency Preparedness will also be investing in activities to strengthen and maintain the national health and medical infrastructure that will be called upon in the event of a bioterrorist incident. NMRTs will be enhanced by increasing the number of deployable members, providing additional equipment, and pharmaceuticals. NMRTs train and participate in coordinated exercises with local response systems, DMATs and teams from other agencies, including the Departments of Defense, Energy, State, Justice, and the Environmental Protection Agency.⁵³

Action: Expand Capability To Access And Rapidly Distribute Medical Supplies And Pharmaceuticals

A biological weapon would create a public health crisis in the United States requiring extraordinarily large amounts of antibiotics, antivirals and/or vaccines for treating those who become ill or for protecting those who may have been exposed. To establish the national requirements for critical pharmaceutical supplies to be available to these victims in less than 24 hours, one must identify the biological or chemical agents that present the greatest threats, estimate the potential size of the population that may be affected, determine the best prophylaxis or treatment options, and then decide how best to assure immediate access to sufficient quantities. The term "stockpile" has been applied to this ready supply.

⁵² These teams are based in Los Angeles, California; Denver, Colorado; and Winston-Salem, North Carolina.

⁵³ In addition, DOD is adding significant capabilities in this area. Reserve components are developing new capabilities to support first responders in each of the following specialty areas: Triage, Trauma, Stress Management, NBC Medical, Preservation Medicine, Mass Care and Mortuary Affairs. These capabilities are accessed through existing procedures established by the Federal Response Plan and the Governors' state authorities.

The federal government is working with the private sector to develop such a stockpile of pharmaceuticals because the kinds of pharmaceutical products which would be required during a biological or chemical weapon attack are not normally found in the marketplace in adequate quantities to meet mass casualty demands, and production lead times are too long to meet urgent needs. This national domestic stockpile of critical pharmaceuticals and biologics (e.g., antibiotics, vaccines) that the federal government would make available to local and state jurisdictions can substantially enhance our readiness to respond to bioterrorism. However, a stockpile in and of itself is not sufficient to provide an adequate medical response. Related objectives must also be met: (1) establishment of an infrastructure to assure the rapid delivery and distribution of the products to the needed geographic location(s), the exposed population(s) and the health care professionals who must to administer them, and (2) development of an adequate monitoring and record-keeping system, especially for continuity of care, compensation, assessment of risks, and evaluation of the efficacy of the therapeutics/vaccines that would be administered in response to a bioterrorist attack.

Traditionally, with respect to natural epidemics or other outbreaks of disease, local and state governments have been responsible for developing plans to identify the affected population; establish distribution systems; organize mass immunization or prophylactic treatment centers with trained, professional staffing; maintain appropriate health records; make referrals to treatment centers; and keep the public informed regarding critical health information. These responsibilities will not change in the event of a biological attack. However, local and state governments will need guidance from HHS on how to meet the unique challenges of a deliberately caused outbreak, which is likely to involve relatively unknown diseases. HHS already provides such technical assistance to the cities that participate in the MMRS program and requires inclusion of procedures for mass immunization and prophylaxis in MMRS plans. As it is developing a national network of readily accessible pharmaceutical supplies, HHS also should develop and promote related planning guidelines and treatment protocols for use by all local and state governments.

**OBJECTIVE: Assist State And Local Public Health Systems To Recognize
 And Respond To CBRN Terrorist Attacks**

Unless announced by the terrorist, the deliberate release of biological, radiological, and some chemical substances into a community will not be discovered until victims begin to exhibit the effects of their exposure. Discovery will depend on the ability of medical providers and public health authorities to diagnose individual cases of diseases that are highly unlikely to have been acquired naturally, or to recognize suspicious disease outbreaks that are difficult to explain in any other way, and report their incidence to a system capable of correlating and analyzing suspicious patterns of illness. This is particularly true in the case of bioterrorism because of the delayed onset of signs and symptoms in exposed victims.

The first line of response against bioterrorism rests with the public health and medical infrastructure. It must be capable of detecting unusual patterns of morbidity or death,

determining their cause (whether natural, accidental or intentional) and, in the case of disorders caused by microbes, detecting and identifying the organism(s) involved. To do so, this infrastructure must have the following:

Increased local and state capacity for public health surveillance;

Expanded epidemiologic capability to investigate and control potential threats;

Strengthened public health laboratories to identify and diagnose suspected biological or chemical agents; and

Coordinated communications among the various components of the public health system, between public health agencies and other government organizations, and between public health officials and the public.

Recognizing the interdependent roles of federal, state and local governments in preparing for and combating bioterrorism, efforts to strengthen the public health infrastructure must be carried out in conjunction with authorities at all three levels. Because health departments vary in size and organization, type of population served and level of support, the capacity to mount an appropriate response to a terrorist event varies from locale to locale. Consequently, there are deficiencies that impede the ability to detect problems, investigate and control potential threats, identify suspected agents and coordinate communications.⁵⁴

HHS proposes expanding the local and state as well as federal laboratory, clinical and epidemiological capacity required to respond to bioterrorist attacks/outbreaks of infectious disease. These investments would include providing local and state health departments with resources and staff to develop methods of active public health surveillance; strengthening sentinel networks of health care providers (e.g., emergency rooms, medical examiners, travel clinics, infectious disease specialists) to serve as front-line sources of information on unusual health events; buttressing this surveillance with adequate laboratory capacity to rapidly characterize and identify biological/chemical agents; and ensuring that pertinent information and data are shared electronically with all relevant authorities and health care providers as quickly as possible.

⁵⁴ For example, more than half of the medical systems personnel who answered the State and Local Questionnaire responded that they did not have a database or help line to assist them in recognizing symptoms that may include exposure to a chemical or biological agent.

Action: Train Public Health Providers To Detect, Investigate And Control Incidents Involving The Release Of Dangerous Chemical, Biological And Radiological Agents

Local and state health departments need assistance in recruiting and training staff who are skilled in detecting, investigating, and diagnosing potential acts of terrorism. At both levels, epidemiologists are needed to analyze surveillance data and investigate any unusual clusters of unexplained death or unusual illness that may signal a bioterrorist event. It will be important to create and support a sufficient number of provider-based sentinel networks that could identify and report unusual health events, e.g., encounters with early victims of what could turn out to be a bioterrorist attack; early cases among perpetrators who mishandled the weapons; or bystanders affected by small intentional releases made to test the efficacy of CBRN weapons. Development of these resources should be reinforced with simulations and exercises involving local, state and federal officials. The federal government will provide leadership and funding in the early years of this multi-year effort, with states assuming a larger share of expenses over time.

Action: Improve Federal, State And Local Electronic Information Systems For Reporting And Responding To Health Threats

To respond effectively to a terrorist threat or event, public health officials must coordinate their communications with one another; with other local, state and federal officials; and with the general public. Electronic communications need to be enhanced to enable rapid analysis and reporting of emerging infectious diseases potentially caused by biological weapons. States will need staff and resources to expand their telecommunications systems to include regional laboratories and local health departments, thus facilitating the rapid recognition of unusual clusters of illnesses and changing mortality patterns. Key information -- including clinical guidelines, recommended antibiotics and vaccines, protective measures and policy decisions -- must be quickly and accurately disseminated to health care providers, health agencies, the media and the public. The federal government will provide leadership and funding in the early years of this multi-year effort, with states assuming a larger share of expenses over time.

Action: Expand Laboratory Capacity To Identify And Diagnose Suspected Agents

In the event of a terrorist attack involving chemical or biological weapons, rapid detection and diagnosis will be critical so that appropriate prophylaxis and treatment can begin promptly. Adequate laboratory capacity must be available to identify and characterize suspected agents. This calls for making rapid diagnostic tests and reagents available for testing potential biological and chemical agents; making new-generation diagnostic methods widely available to state and selected metropolitan health laboratories; establishing and implementing protocols for the safe collection, handling and shipping of specimens to reference diagnostic laboratories; and developing a plan to identify and expand, on an incremental basis, a network of regional

laboratories located throughout the U.S. that would provide rapid and accurate diagnostic and reference support for biological and chemical agents. This network of laboratories should rely as much as practicable on existing federal or federally-supported laboratories with experience in these areas, such as DOD's USAMRIID, the Centers for Disease Control's (CDC's) intramural laboratories, and EPA's in-house and contract laboratories. The federal government will provide leadership and funding in the early years of this multi-year effort, with states assuming a larger share of expenses over time.

OBJECTIVE: Protect Government Employees From Terrorist Attack And Intimidation

Because they symbolize government authority, federal, state and local facilities and employees are frequently the targets of foreign and domestic terrorists. Acts against government targets range from devastating violence to intense harassment and intimidation; from the bombing of the Murrah Federal Building in Oklahoma City to the filing of fraudulent court actions against federal, state, and local law enforcement and judicial employees. To discourage such assaults, we must strengthen our physical and legal defenses.

Action: Pursue Legislation To Deter Threats Against And Intimidation Of Federal, State And Local Government Employees

Persons disaffected with government within the United States are increasingly manifesting their discontent by undertaking obstructive and threatening actions against federal, state and local government employees. Although most of these actions are nonviolent attempts to obstruct or impede the performance of official duties, some have involved explicit threats or violence. Further, even non-violent actions may be disruptive, inconvenient and intimidating. They adversely affect both official performance and the personal well-being of the targeted employees.

Federal law contains effective provisions to address violence, and threats of violence, directed against federal officers or employees. See, e.g., 18 U.S.C. § § 111 and 115. In addition, 26 U.S.C. § 7212 prohibits non-violent actions undertaken to intimidate, obstruct or impede Treasury Department employees. Because other federal employees are increasingly subject to non-violent but intimidating actions, a proposal to extend the protections of Section 7212 to all federal employees is being considered. This would provide protection against a wide range of harassing actions, including the filing of frivolous encumbrances against the property of federal officers or employees in retaliation for the performance of their public duties.

While the protection of state and local government officials is primarily the responsibility of the states, these officials are frequently the subject of threatening or harassing actions by advocates of so-called common law courts, and state and local law enforcement authorities in many states have experienced difficulties in addressing the problem effectively. This is especially the case where the offending conduct is initiated totally or partially from outside the

state of the victim employee. Further, the victims are often local employees in relatively rural areas which lack sufficient law enforcement resources to address the problem.

After consultation with organizations representing state and local government officials, DOJ has developed federal legislation to prohibit the initiation of groundless actions against state or local officials or public employees with the intent to obstruct or impede, or retaliate because of, the employees' performance of their official duties. Consistent with Constitutional limits, such prohibitions would apply only if the actions were taken in circumstances that have traditionally been recognized as providing an appropriate basis for federal involvement. No additional funding is required for this initiative.

GOAL 5: SAFEGUARD OUR NATIONAL INFORMATION INFRASTRUCTURE

Our national policy on infrastructure protection is still evolving. Following large scale terrorist attacks in New York City and Oklahoma City in 1993 and 1995, respectively, PDD 39 set forth our nation's policy on terrorism. Pursuant to PDD 39, the Attorney General chaired a Cabinet Committee to assess the vulnerability of the nation's critical infrastructures and recommend measures to protect them. Based on this committee's recommendations, the President's Commission on Critical Infrastructure Protection (PCCIP), also known as the Marsh Commission, working under the direction of a Steering Group chaired by the Attorney General, addressed this issue. As a result of the Marsh Commission Report, the President issued PDD 63, which outlined comprehensive steps to be taken government-wide to achieve and maintain the ability to protect our nation's critical infrastructures from intentional acts to disrupt their operations.⁵⁵

PDD 63 directs the National Coordinator for Security, Infrastructure Protection and Counter-terrorism to: implement the directives of the PDD; ensure interagency coordination on critical infrastructure issues; review crisis activities concerning infrastructure events with significant international involvement; provide advice during the budget process in regard to agency budgets for critical infrastructure protection, and chair the Critical Infrastructure Coordination Group (CICG). Much of the work concerning infrastructure protection is on-going under the PDD 63 implementation process. PDD 63 set as a national goal achievement of a baseline capability by the year 2000, and full operational capability by the year 2003, to protect our nation's critical infrastructures from physical and cyber attacks. In the annual reviews of PDD 63 and this Plan, the National Coordinator will monitor this progress as it relates to counter-terrorism and suggest course corrections consistent with this Plan as necessary. This plan is consistent with the goals of PDD 63 and is intended to contribute to achieving and maintaining the protection our nation's information infrastructure through a partnership of appropriate federal, state, and local authorities as well as private sector infrastructure owners and

⁵⁵ As stated in the Introduction to this Plan, we do not attempt to duplicate here the comprehensive national approach of PDD 63. Instead, we focus on selected counter-terrorism related aspects of infrastructure protection, to be pursued in conjunction with PDD 63 activities.

operators.

The PCCIP defined infrastructure as “a network of independent, interdependent, mostly privately-owned, man-made systems and processes that function collaboratively, interdependently and synergistically to produce and distribute a continuous flow of essential goods and services.” Those infrastructures that are “so vital that their incapacity or destruction would have a debilitating impact on our defense and economic security are deemed critical.” The PCCIP identified eight critical infrastructures: transportation; oil and gas production and storage; water supply; emergency services (police, fire, medical); government services; banking and finance; electrical power; and telecommunications.⁵⁶ Most of our nation’s critical infrastructure is privately owned, and PDD 63 states that market forces are the first choice to ensure infrastructure protection. Therefore, true partnerships between the public and private sectors are essential to the maintenance and protection of the infrastructure.

In order to protect infrastructure assets, we must know both where they are, how vulnerable they are, and how to reconstitute them after attack. PDD 63 assigns lead federal agencies to work with their private sector counterparts to:

- assess the vulnerabilities of each sector to cyber and physical attacks;
- recommend a plan to eliminate significant vulnerabilities;
- propose a system for identifying and preventing attempted major attacks;
- develop a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

Federal agencies are currently drafting their timetables for completion of these sector plans. These assessments and plans constitute individual sectoral plans which, when integrated together, will yield a National Infrastructure Assurance Plan. This overall plan will provide for coordination, integration, and interdependencies. A draft National Plan for Critical Infrastructure is currently under consideration by the National Coordinator for Security, Infrastructure Protection and Counter-terrorism.

PDD 63 calls for a National Plan that will:

- Protect our nation’s critical infrastructures from intentional acts from whatever source that would significantly degrade the ability of those infrastructures to perform essential services;

⁵⁶ The PCCIP specifically declined to address the food supply as a critical infrastructure.

- Ensure that any interruptions or manipulations of critical functions are infrequent, manageable, quarantined, and minimally detrimental to the welfare of the United States; and
- Achieve an overall end state of "assured capability" of our nation's infrastructures, defined as achieving a condition that is hardened against attack and capable of being quickly reconstituted after any disruption in function. Four broad objectives are integrally linked to achieving this end state: assess and prioritize, prepare and prevent, detect and respond, and monitor and improve.

In developing the National Plan, the CICG is examining many issues, including several with a cyber focus:

- **Qualified Computer Specialists:** the number of computer specialists trained in safeguarding computer systems and networks is inadequate. The CICG is examining the use of existing, and perhaps new, authorities — including educational incentives — to ensure that the government has a cadre of well-trained computer security specialists;
- **Intrusion Detection Networks:** The CICG is examining three interlocking systems - - one for the Department of Defense (DOD), one for the other federal agencies, and a system that may be offered to the private sector. The exact specifications of each system are still being developed. Two important and sensitive problems must be addressed in setting up intrusion detection networks: (a) we must avoid the perception that we are creating a system that will to any degree compromise the privacy, integrity and civil liberties of U.S. citizens; and (b) we must avoid creating a centralized, highly lucrative target for attack or deception;
- **Private Sector Centers:** The Information Sharing and Assessment Centers (ISACs) encouraged by PDD 63 could serve as a private industry component that links up to U.S. government entities such as the National Infrastructure Protection Center. The exact design of these ISACs will be left to the private sector. ISACs can also provide one useful and effective conduit for threat assessments and warnings generated by the NIPC. In addition, they could perform other functions such as outreach, education and awareness, and the creation of standards for best practices;
- **Reconstitution:** The ability to reconstitute minimum essential infrastructure following a cyber attack is an explicit requirement of PDD 63. Efforts to build a reconstitution capability and to develop redundant systems in many critical infrastructures are being evaluated. The Year 2000 will also require significant reconstitution capabilities; therefore, the National Coordinator has initiated contingency planning efforts with the Y2K Commission; and
- **Research and Development:** The Office of Science and Technology Policy (OSTP) chairs a subgroup of the CICG in order to identify potentially promising research and

development projects not present in any departmental program. Appropriate recommendations of this sub-group will be reflected in the President's FY 2000 budget.

As regards cyber terrorism, much work has already been accomplished by the federal government in identifying assets that may be at risk to terrorists attacks. For example, the PCCIP report, Critical Foundations: Protecting America's Infrastructures, includes an analysis of existing physical and cyber vulnerabilities. Special attention has been given to our vulnerability to cyber attacks. The FBI, in cooperation with the Computer Security Institute, publishes an annual report based on their "Computer Crime and Security Survey," which describes existing vulnerabilities and attempts to identify vulnerability trends across various industry sectors.⁵⁷ Review of these broad-scope threat assessments makes clear that virtually all of the United States' critical infrastructures rely on the public switched telephone network and, to a lesser extent, on the Internet -- both key elements of the National Information Infrastructure.

As directed by the Conference Committee Report, our focus here is on terrorist threats to the National Information Infrastructure (NII). The definition of the NII used in this Plan is the computer and telecommunications networks that support our critical infrastructures. These systems consist of the following main classes of components: transmission media such as wires and fiber optic cables, switching equipment, processing equipment and software, all subject to physical attack; as well as wireless and satellite systems subject to disruption through the air waves. Vulnerability to attack is essentially determined by the level of physical protection available for the physical asset. Thus, in the physical realm, telecommunication wires are highly vulnerable because they are spread across wide ranges of insecure space, whereas telecommunication switches are generally more secure based on their typical placement in unidentified, locked and guarded locations.

In stark contrast, cyber attacks on the NII generally do not depend on physical access to the targeted asset (although such access can make the attacker's job far easier). Because the networks that make up the NII were designed to facilitate information sharing and ease of use, it is often just as easy to launch a cyber attack from half-way around the world as it is from right next door. Moreover, it may be extremely difficult to determine the source of an attack in real time, especially if the attacker is skilled and knowledgeable about the victims' systems. Indeed, domestic cyber attacks can be intentionally woven through a series of remote foreign locations in an attempt to obscure the actual source of the intrusions.

Because cyber attacks are not dependent upon physical access, vulnerabilities generally cannot be determined or addressed by traditional means. For example, telecommunication wires

⁵⁷ See Richard Power, Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare (1998).

which are highly vulnerable to physical attacks are usually not the subject of pure cyber attacks.⁵⁸ On the other hand, Internet and telecommunication switches, which are often endowed with considerable processing intelligence, can be subjected to a variety of cyber attacks notwithstanding the fact that they are often well protected from physical tampering and destruction. In other words, conventional methods of guarding against terrorist attacks may be wholly ineffective against cyber attacks on the NII.

Virtually all infrastructures are at risk to some level of cyberattack; some level of risk is acceptable; some is not. The amount of risk associated with a given asset relates to a wide variety of factors, including, but not limited to: the physical security surrounding the asset; the type of hardware used; the operating system employed; the security software installed on the asset; the skill, reliability and diligence of the person(s) authorized to maintain and use the asset; and the number and type of connections available between the asset and the outside world. Because these factors vary widely even among relatively similar networks, it is difficult to generalize about the risks presented by a given system unless that system and its operators have been individually analyzed.⁵⁹

Pursuant to PDD 63, a comprehensive, government-wide plan for an assessment of infrastructure vulnerabilities is being prepared. These assessments will provide information about cyber-asset vulnerabilities and protections on a sector-by-sector basis for the private sector and on an agency-by-agency basis for the public sector. As part of the Critical Infrastructure Coordination Group (CICG) process, the National Security Agency and the National Institute of

⁵⁸ Certain types of attacks, however, are hard to characterize as purely "physical" or purely "cyber." For example, it is possible to attach a physical device to wires on a computer network and capture logon and password combinations for that system, thereby gaining illegal access to user accounts. Such an attack combines both cyber and physical world techniques. Moreover, prevention, detection and response to such an attack can and should involve both physical and cyber security measures.

⁵⁹ Several system specific studies have been conducted to test the vulnerability of government and private networks. The General Accounting Office (GAO) has analyzed and reported on the vulnerabilities of various non-classified computer systems at the State Department and the Department of Defense. GAO also reported on vulnerabilities of banking industry networks associated with on-line banking in a report entitled Electronic Banking: Experiences Reported by Banks in Implementing On-Line Banking, November 1997. Other similar studies include: National Security Telecommunications Advisory Committee, Information Assurance Task Force, Electric Power Information Assurance Risk Assessment (1996), and An Assessment of the Risk to the Security of the Public Network (1995); and Information Infrastructure Task Force (IITF) Security Issues Forum, NII Security: The Federal Role (1996), and IITF's NII Risk Assessment: A Nation's Information at Risk (1996). The Office of Science and Technology Policy report, Cybernation: The American Infrastructure in the Information Age, provides a technical primer on issues associated with infrastructure protection.

Standards and Technology are assessing opportunities to work with industry to develop best practice standards and accreditation regimes for improving information systems security. These best practice standards would be adopted or adapted as appropriate across federal agencies.

OBJECTIVE: Establish A National Capability For Analysis, Warning And Response

When fully implemented, the National Infrastructure Protection Center (NIPC) is intended to function as the focal point for response to any cyber-based attack on U.S. critical infrastructures. It will either integrate or have seamless connectivity with the National Coordinator and with all of the relevant operations response components (law enforcement, counter-terrorism, intelligence community, national defense and emergency responders). Voluntary links with the owners of the infrastructures (whether government or private sector) and the intelligence community will also ensure that the maximum amount of information about any ongoing cyber-attack is concentrated in the NIPC. In the event of a significant cyber attack, the NIPC will initiate several simultaneous response activities:

- The NIPC will correlate information from available sources (government and private sector) in order to determine the true scope and likely consequences of the ongoing attack.
- The NIPC's Computer Investigations and Operations Section will begin active collection of information aimed at supporting a preliminary attribution for the attack. The process will involve coordination and joint efforts with other relevant agencies (e.g., DOD investigative or counterintelligence components, intelligence community components, Secret Service, federal agency inspectors general, state and local law enforcement). The attribution process will generally use criminal legal authorities within the United States (when such authorities are required to obtain data), unless and until the predicates for national security authorities are present. The NIPC will incorporate the intelligence community in the flow of information, consistent with applicable legal restrictions so that the community can initiate overseas collection pursuant to foreign intelligence authorities and can provide such assistance to the criminal investigation as is legally permitted.
- The analytical components of the NIPC, in addition to supporting the activities just described, will compile and disseminate product about the ongoing attack. The NIPC, in conjunction with the National Coordinator, will also assess the need for, prepare, and issue warnings to the government, the critical infrastructure operators, and/or the public, as appropriate under the circumstances.

As these activities continue, the NIPC will reach out to other operations response components. If, for example, the process begins to reveal a possible link to an international terrorist group, the NIPC will involve and coordinate with the international terrorism components of the FBI (and through them, the "traditional" counter-terrorism network). On a larger scale, if

something other than an investigative response is deemed appropriate (i.e., a military, covert, or intelligence response) the NIPC would function in a support role to the relevant agency responsible for the response. The NIPC thus will not duplicate the investigative functions of counter-terrorism components, or the functions of the intelligence community or military. Rather, the operations arm of the NIPC will maintain an investigative expertise in computer intrusions which can be deployed as part of an attribution effort and then either conduct or support further investigative response.

This vision rests on the ability of the NIPC to integrate representatives of counter-terrorism, intelligence, and defense communities. If these representatives are integrated (through detailees or close connectivity), then the movement from the attribution phase of the response to whichever community will conduct the active response will not be a cold "hand off" between unrelated operations. Rather, it will be a coordinated effort between the NIPC and an already knowledgeable component that can bring its own expertise and resources to bear on the needed response.

**Action: Develop The Full Operational Capability Of The National
 Infrastructure Protection Center**

Our nation is rapidly augmenting its capabilities to safeguard both the physical and cyber aspects of critical infrastructures through the National Infrastructure Protection Center (NIPC), which was created by the Department of Justice during FY98. The NIPC is an interagency center hosted by the FBI, that will deter, assess, warn, investigate, and respond to attacks, threats and unlawful acts targeting the critical infrastructure of the United States, including illegal intrusions into government computer networks and protected computers. An important feature of the NIPC is an analytical capability designed for all the information that will flow through the NIPC, including intelligence, criminal investigative, and infrastructure information, tied to a watch and warning unit set up to disseminate analytical product and warnings to a variety of audiences. The watch and warning unit will be linked electronically to other federal agencies, including other warning and operations centers, and will be a focal point for the collection and dissemination of information on cyber intrusions and other infrastructure related information from open sources, intelligence sources and, to the extent agreed upon, by such federal agencies as the Defense Information Systems Agency, NSA, the Joint Task Force for Computer Network Defense (JTF-CND), Secret Service, DIA, CIA, as well as such private sector organizations as the Computer Emergency Response Team (CERT)⁶⁰ and the National Security Telecommunications Advisory

⁶⁰ The Computer Emergency Response Team (CERT) is run by Carnegie Mellon University and funded by the government. Through voluntary reporting by systems administrators in the private and public sectors, CERT collects information on computer intrusions, viruses, and other vulnerabilities, works with hardware and software manufacturers to develop a solution to the problem, publishes public advisories describing in general terms the vulnerability, and directs users to the appropriate point of contact to obtain the solution. This organization has been a highly successful model of private-public cooperation. Industry

Council (NSTAC).⁶¹ The mission of the watch and warning unit will include providing timely warnings of intentional threats and comprehensive analyses. NIPC warnings may also include guidance regarding additional protection measures to be taken by owners and operators. In providing this guidance, the NIPC will coordinate closely with the Sector Liaisons and Sector Coordinators, and other relevant federal and private sector entities, that are responsible for developing sector based plans for protecting their critical infrastructures.

In addition, the NIPC includes a crisis management capability that will address interagency and government/private sector coordination, response capabilities, and integrated management for cyber-emergencies. NIPC will have personnel on site who possess extensive computer and information security skills and knowledge, criminal and national security investigative experience, and will work closely with those in the Laboratory Division. A primary infrastructure protection goal of the NIPC is to be able to respond quickly in the initial stages of a crisis situation, and to continue to pursue the appropriate law enforcement or national security strategies, depending on the nature of the incident. The NIPC structure will be supported by an interagency team of analysts and investigators from the FBI, Secret Service, DOD, the intelligence community, and other federal agencies specializing in infrastructure issues, including representatives from all the lead agencies designated in PDD 63. The NIPC is also seeking representatives from the private sector representing the critical infrastructures identified in PDD 63.

particularly likes this model because industry representatives report vulnerabilities in a discreet manner, receive technical assistance in developing a solution, and have access to a communications system to make the solution available.

⁶¹ The National Security Telecommunications Advisory Committee (NSTAC) was created by the President in 1982 by Executive Order 12382, to advise him on matters concerning national security and emergency preparedness telecommunications. NSTAC is composed of up to 30 presidentially appointed industry leaders (usually chief executive officers) representing various elements of the telecommunications industry. NSTAC meets approximately every nine months to report on its activities and provide recommendations to the President on issues related to national security and emergency preparedness (NS/EP) telecommunications. The National Communications System (NCS), consisting of 23 federal member departments and agencies, is responsible for ensuring the availability of a viable NS/EP telecommunications infrastructure. The NCS also runs the National Coordinating Center for Telecommunications (NCC), which is staffed by selected government agencies and several of the largest telecommunications carriers. The NCC assists in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services and facilities, and serves as the operational focal point for all the National Telecommunications Management Structure (NTMS) all-hazards response levels. A number of government agencies and NSTAC members participate in the government and industry Network Security Information Exchanges (NSIE), respectively, the joint meetings of which provide a unique forum to exchange information on electronic intrusion threats, vulnerabilities, incidents and countermeasures. These public-private information sharing partnerships are often cited as models for other sectors.

The NIPC incorporates both an infrastructure protection and an investigative response component. The protection function (which includes analytical work on infrastructure risk assessment, indications and warnings) spans all of the critical infrastructures, and addresses both the "physical" and the "cyber" aspect of the threat. The NIPC's investigative component is limited to addressing "cyber" based attacks. In the event of physical attacks on key infrastructures, the investigative response will be handled by FBI criminal investigative or counter-terrorism components as appropriate. The NIPC would then serve in a supporting role, providing relevant information about the victim infrastructure and other focused analytical or intelligence products. Close communication between the NIPC and the FBI's counter-terrorism components is critical and will be enhanced whenever possible. Physical co-location of the NIPC and the International Terrorism and Domestic Terrorism Sections adjacent to the expanded FBI Strategic Information and Operations Center will promote this enhanced communication.⁶²

The NIPC is currently operating with approximately 75 people at FBI headquarters, but is aggressively recruiting within the FBI, at other agencies, among state and local law enforcement, and in the private sector and universities to swiftly obtain highly qualified personnel to fully staff the Center at its initial operating capacity of 125 people (85 FBI personnel and approximately 40 representatives from other government agencies and the private sector). Hiring staff for which funding has already been authorized is the most significant problem currently facing the NIPC. The Cyber Emergency Support Team, the Analysis and Information Sharing Unit, and the Watch and Warning Unit will not be fully functional until the NIPC is fully staffed. The NIPC is attempting to fill the gap in the interim by using other FBI headquarters staff and contractor personnel. Additionally, NIPC is working with DOD, the intelligence community, and other government agencies to quickly identify and obtain representatives to serve in the NIPC.

Action: Collect, Analyze And Disseminate Threat Information

The NIPC is tasked with collection and dissemination of threat information. Information is collected from numerous sources: from the Watch and Warning Unit (WWU), which monitors open source reporting and serves as a collection point for information moving in intelligence channels (such as Intelink, discussed *supra*, footnote 32); from investigative files of the FBI and other law enforcement agencies through the Computer Investigations Unit; from the private sector through links established by NIPC direct outreach or as a result of sector plans (e.g., information sharing and analysis centers (ISACs)), and from other government agencies, especially those with sector responsibilities. The NIPC, working with the National Coordinator, Sector Coordinators, Sector Liaisons Officials, and the National Economic Council, will consult with private industry in regard to the creation of private sector information sharing and analysis centers.

⁶² Within the FBI, the NIPC's functions were designed as a formal FBI program, analogous to the National Foreign Intelligence Program. This new program is called the National Infrastructure Protection and Computer Investigations Program and is located within the National Security Division of FBI.

All of this information will be directed into the Analysis and Information Sharing Unit (AISU), where it will be analyzed. Infrastructure analysis (e.g., assessments done by the various sectors pursuant to PDD 63), threat analysis (e.g., country or terrorist group threat analysis from the Intelligence Community), and current intelligence (derived from investigative, operational, or private sector reporting), will all be combined to produce infrastructure risk assessments. These assessments will form the basis for a variety of products, including a monthly or quarterly intelligence digest, a weekly watch report, and topical electronic reports. These products will be designed for tiered distribution to both government and private sector entities consistent with applicable law through the Watch and Warning Unit.

The analysis conducted at the NIPC will not occur in isolation, but rather will form a component of the U.S. government's overall analytical effort. To this end, the AISU has already established liaison with the CIA's CTC and with NSA components. The goal of these connections is to allow a cross-pollination of analytical work and to provide a forum for the exchange of relevant data. The AISU also produces case specific product in support of NIPC responses to cyber intrusion incidents. Here again, the connection to the Intelligence Community enables those resources to directly support the NIPC response, as permitted by law.

Ongoing analysis of threats and vulnerabilities must be supplemented by a robust capability for a real-time indications and warnings system for cyber attacks. This need will require not only the establishment of the technical capacity for indicator collection, but also the determination, through analysis of current intrusion data, of what constitutes an indication of a foreign power or terrorist cyber attack. Current efforts focus on the technical aspects of establishing secure connectivity between existing points of collection in the federal government. This connectivity has already been established between the NIPC and key NSA and DOD components.

Threat analysis requires a coordinated approach, which is now under way. The National Intelligence Council continues to sponsor discussions among the National Indications and Warning System, the Defense Indications and Warnings System, the NIPC, representatives of the Joint Chiefs of Staff, and the National Coordinating Center of the National Communications System. The goal of this process is to produce an indications and warning system that is consistent and that meets the requirements of the national defense, law enforcement and intelligence communities. As the process develops, the emphasis will be on achieving near real-time operation of the system and on increasing the sophistication of the indicators. Given the private ownership of most of the critical infrastructures, the system will have to integrate real-time warnings to the private sector through the NIPC.

The establishment of a secure, government-wide network for dissemination of information directly to network security personnel on a real-time basis would greatly enhance system security. NIPC will coordinate the establishment of such a network. All federal agencies will need to allocate some technology resources to link with this system. In order to be truly useful to system administrators, traffic on this network must be limited to dissemination of

serious threat risks, notifications of actual attacks and specific information on exploited vulnerabilities. Ideally, distribution of such information would be targeted only to operators of affected systems so that activation of the system would itself serve as a red flag for security specialists. Archives of past warning notices could be maintained as a reference for past security breaches and possible future threats.

The NIPC is working on this connectivity. Currently it relies on existing communications channels to disseminate information and to communicate with state and local law enforcement. These channels will continue to be used while a comprehensive warning system is established. The NIPC is also relying on existing systems to gather information about threats and intrusions. Some sectors have existing mechanisms and those are being exploited. In sectors with no existing reporting mechanisms, NIPC is working with the Sector Lead Agencies as defined in PDD 63 and through other channels to develop reporting protocols and to encourage reporting of incidents.

In building the partnership between the federal government and infrastructure providers envisioned by PDD 63, the NIPC will involve interested representatives of identified assets in a threat warning system through its Watch and Warning Unit (WWU) and expansion of InfraGard.⁶³ The WWU will be the focal point for the collection and dissemination of cyber intrusion and infrastructure-related information from open sources, intelligence sources, and other agencies, as well as various Computer Emergency Response Teams (CERTs) and any private sector Information Sharing and Analysis Centers (ISACs) whether or not they are direct

⁶³ InfraGard is a pilot project initiated by the FBI's Cleveland Field Office. This program is a cooperative effort to exchange information among the business community, academic institutions, the FBI and other government agencies to protect the information infrastructure. InfraGard features an alert network that members can use to report intrusions. Reports are sent to the FBI via encrypted e-mail in two forms: a detailed description and a sanitized description. The FBI uses the detailed description to analyze the incident, identify trends, and open an investigation if warranted. Only the sanitized version, which removes company-identifying and proprietary information, is shared with other InfraGard members. The NIPC plans to expand InfraGard nation-wide in FY 99. This expansion includes the development of a secure website for InfraGard members and annual conferences.

The FBI also reaches appropriate private sector security personnel through its Awareness of National Security Issues and Response (ANSIR) program, through which information is disseminated nationwide via the ANSIR-E-mail and ANSIR-FAX networks. The ANSIR Program will require the periodic upgrading of communications equipment in order to stay current with developments in new communications technology. In addition, new security measures will be necessary as cyberterrorists and foreign intelligence services develop new means to attack the computer infrastructure. (U)

partners with the WWU.⁶⁴ The WWU will draft and disseminate warnings and advisories involving cyber and infrastructure-related incidents and information to federal, state, and local law enforcement and the private sector in coordination with the FBI's Terrorist Threat Warning System. One of the goals of the WWU will be to ensure that all critical infrastructure assets are notified in a timely manner of terrorist threat warnings, alerts and advisories.

As the NIPC matures, the WWU will continue to identify additional appropriate recipients of advisories and warnings, as well as produce a weekly report highlighting the most important information collected. NIPC staff is developing protocols for the sharing of information among the various categories of NIPC participants to achieve the maximum dissemination of relevant information and analysis consistent with applicable law and the protection of investigative equities and intelligence sources and methods.⁶⁵ Under any scenario, the NIPC will assure alerts and warnings are broadcast as widely as practicable to both government and industry, including to those organizations that are not direct WWU partners. The NIPC plan includes the relocation of the WWU adjacent to the FBI's expanded Strategic Information and Operations Center, the integration of DOD and intelligence community analysts into the NIPC, and the acquisition of additional technical resources.

The NIPC, as well as the National Coordinator and the CICG, is formulating a comprehensive outreach plan, with subsidiary plans for each infrastructure sector, that will address this task as well as the specific outreach tasking in PDD 63. This plan builds on the work of the PCCIP, starting with key individuals and organizations identified by the Commission. The plan contains a variety of outreach activities, including the use of pre-existing FBI contacts in the private sector, new outreach to corporate leaders and industry associations, and cooperation with other government or quasi-government entities that have established relationships with the private sector. The goal of the plan is to connect the NIPC with existing mechanisms for government/private sector interaction and, where no such mechanisms now exist, focus outreach resources to create them in order to establish an efficient flow of information between the NIPC and each infrastructure.

⁶⁴ PDD 63 encourages the private sector to create information sharing and analysis centers (ISACs) in consultation with the federal government. These centers could serve as a mechanism for gathering, analyzing, sanitizing, and disseminating private sector information regarding vulnerabilities, threats, intrusions, and anomalies to industry. The ISACs should not interfere with direct information exchanges between industry and the government.

⁶⁵ Some laws related to information sharing may need to be amended to permit sharing of information relating to infrastructure protection. See *infra*, pp. 162-164 for proposed changes to existing laws.

**Action: Develop And Promote Integrated Federal, State And Local
Crisis, Consequence Management And Continuity Of Service
Plans**

The NIPC will provide the principal means of facilitating and coordinating the federal government's response to a cyber incident, mitigating attacks and monitoring reconstitution of the government's cyber assets, including the telecommunications and computer networks on which the government relies. PDD 63 directs the Chief Information Officer and the Chief Infrastructure Assurance Officer of each agency to develop a plan for protecting its own critical infrastructure. These plans, together with the Industry Sector plans, will become part of the National Infrastructure Assurance Plan to be drafted pursuant to PDD 63. The NIPC is the lead government component for coordinating crisis management in response to cyber attacks.

Crisis management plans must include methods to: detect cyber attacks on government networks; establish thresholds for reporting attacks to the NIPC; retain electronically all information related to attacks; provide that information to the NIPC in a useable format; provide for a unified, secure communications capability with the NIPC, other federal agencies and departments, and the private sector, as necessary; and continue to perform the agency's essential functions during the crisis. Consequence management plans must provide for reconstitution of computer and telecommunication networks, including restoration of any data lost in the crisis. Plans should include some guidelines for transition from crisis management to consequence management. Both plans should also emphasize the importance of thorough criminal and intelligence investigations coordinated by the NIPC.

The mission of the NIPC includes leading a coordinated response to an attack on the national infrastructure, along with other government agencies, FBI field offices and headquarters components, the state and local response efforts, and the private sector. Consistent with PDD 63, the NIPC along with FEMA and the sector liaisons and coordinators, will work with the state and local levels to ensure that their response plans adequately account for security, recovery, and maintenance of continuity of services in the event of a terrorist attack against a critical infrastructure asset.⁶⁶ Under PDD 63, FEMA has a principal role in promoting plans to maintain the continuity of essential government services.

The NIPC is developing a "Key Asset Program" whereby it will build and maintain a database of specific "key assets" within each infrastructure sector (such as particular power grids, telecommunications switching nodes, and the like) and points-of-contact at each asset. Eventually, when resources permit, the Program could include exercises to test response plans within each jurisdiction and modeling to determine the effects of an attack on particular assets.

⁶⁶ The need for this assistance is clear from the responses to the State and Local Questionnaire. Fewer than 50% of the respondents stated that their crisis and consequence plans identified key infrastructure assets or had procedures for responding to terrorist incidents targeting those sites. See Appendix B: State and Local Questionnaire, responses to question 19.

FBI Field Offices will be responsible for developing a list of the assets within their respective jurisdictions, while the NIPC will maintain the national database. This program will be developed in coordination with DOD and other agencies. Because these assets are vulnerable to both physical and cyber attack, the Key Asset Program, and related response plans, will address both types of vulnerabilities and attacks.

As part of its crisis management capabilities, NIPC can respond to significant incidents involving possible violations of criminal law, threats to national security or threats to the national infrastructure. NIPC will have personnel who possess the requisite computer and information security skills and knowledge, and criminal and national security investigative experience. The goal of the NIPC is to respond quickly in the initial stages of a crisis, and to pursue the appropriate law enforcement or national security strategies, depending on the nature of the incident. In order to facilitate this, the NIPC is moving forward with plans for a Cyber Emergency Support Team (CEST) which will be capable of rapid deployment once full staffing is achieved.

Crisis and consequence management plans can be tested and evaluated in simulated attacks or exercises that can focus on crisis management and demonstrate how the government would recognize and respond to an information warfare attack, and reveal some of the existing coordination difficulties, both within the government and with the private sector. Additional useful information was developed about the vulnerability of government networks through "red team attacks"⁶⁷ on DOD systems. PDD 63 requires that the government regularly perform vulnerability testing of its cyber-assets. The government should conduct exercises focused on cyberattacks on at least an annual basis to determine whether existing crisis and consequence management plans are effective.

To this end, the NIPC is planning a range of exercises to test infrastructure crisis management plans. DOD wishes to conduct exercises three to four times per year to assist in developing consequence management plans for infrastructure attacks. Because the government infrastructure is almost entirely dependent upon the private sector infrastructure, the private sector must be invited and encouraged to participate in these exercises.

**Action: Ensure Domestic Substantive And Procedural Laws Facilitate
Computer Crime Investigations And Prosecutions**

Several existing statutes should be reviewed to determine if amendments would facilitate investigation and prosecution of infrastructure attacks while not violating Constitutional and statutory protections. Currently, a federal grand jury subpoena has effect and can be served anywhere in the United States, so that a grand jury sitting in one district has the power to compel evidence that is located in another district, without going to another grand jury. Similarly, an

⁶⁷ "Red team attacks" are penetration testing exercises developed by the NSA (see *infra* p. 172), and performed upon request with available resources for a limited number of agencies.

order under Title 18, section 2703(d) seeking transactional records of a subscriber of a telecommunications or network service provider can be issued by any federal district court judge, and can be executed anywhere in the United States. This facilitates investigations in which the target of the investigation and the service provider are located in different districts.

The appropriateness of a similar nationwide statute for orders relating to requests for trap-and-trace/pen registers should be explored. Under current law, a trap-and-trace order⁶⁸ can only compel the production of data from providers in the district in which the order was issued. It is important for law enforcement to have the ability to go to one court and obtain one order that will be effective anywhere in the United States. Seeking multiple orders wastes precious time in computer intrusion cases, where time is of the essence because the evidence is ephemeral. However, the impact on privacy protections needs to be carefully considered.

Additionally, the desirability of amending Rule 41 of the Federal Rules of Criminal Procedure governing search warrants, at least with respect to infrastructure attacks, should be explored. Currently, Rule 41 only authorizes courts to issue search warrants for property that is within their district or was within the district at the time the warrant was issued. "Geography" is not a particularly meaningful concept in cyberspace, where information and data freely cross jurisdictional lines. The ability to execute one search warrant within the United States, and obtain all the evidence on the designated computer network, regardless of its actual physical location, would aid investigations. We may also need to develop transborder search authority, allowing an agent in one country to remotely search a computer located in another country. Trans-border search principles are under development by the G-8 and the Council of Europe. Again, however, the impact on privacy protections needs to be carefully considered.

Amendments to the Computer Fraud and Abuse Act, 18 U.S.C. section to more clearly protect certain types of computers and/or information may be desirable. Specifically, all intrusions into DOD computers, postal computers, and computers used in the administration of justice (including courts, prisons, and parole boards) could be designated a violation of section 1030(a)(5) regardless of the dollar amount of damage. Currently, the statute requires at least \$5,000 in damage before section 1030(a)(5) applies, but there are computer intrusion cases which involve extremely serious infractions that do not amount to \$5,000 in damage.

The juvenile jurisdictional statute, 18 U.S.C. section 5032, could also be amended to permit federal jurisdiction in appropriate cases in which the defendant is a minor. Currently, the federal government must defer to the state authorities, and obtain a certification from the state

⁶⁸ A trap and trace order, which can be served on any telecommunications service provider, is used to learn the originating address of all incoming communications (telephone numbers if the order is for a telephone, Internet Protocol (IP) addresses and ports if the order is for a computer). A pen register order is used to learn the intended destination for all outgoing communications. Requests to obtain information about all incoming and outgoing communications can be combined into one order.

that it declines to prosecute. Yet, many serious computer crimes are committed by juveniles each year. In addition, terrorist groups or foreign intelligence services might be able to co-opt juveniles, either knowingly or unknowingly, to conduct infrastructure attacks on their behalf, and the involved juveniles would be outside the reach of the federal criminal code.

There are a number of other possible amendments to existing statutes that would facilitate information sharing with the private sector. These changes include:

- creation of a limited antitrust exception to allow private sector entities to share information for purposes of infrastructure protection without violating antitrust laws;
- protection from disclosure under the Freedom of Information Act of sensitive information (even information that does not rise to the level of a trade secret) that relates to threats and vulnerabilities of computer networks; and
- immunity from civil liability for the private sector in sharing sensitive personnel information related to security concerns.

Such changes would be controversial, and would require extensive study and evaluation before legislation is proposed.

OBJECTIVE: Enhance Computer-Related Capabilities

Action: Expand Forensics Capability, Including Cryptanalysis Capability

Law enforcement is increasingly encountering encrypted information in investigations. Because of the perceived lack of security of computer data in storage and transmission, there is a developing market for encryption. The low cost of software and decreasing cost of hardware encryption, combined with this market demand, assure that encryption will become common in the near future for both stored data and communications. In order to fulfill its critical mission, law enforcement must be able to obtain plaintext under proper legal authority when it encounters encryption in this new environment and, therefore, must develop the technical ability to create and deploy appropriate tools for its own use.

In the Antiterrorism and Effective Death Penalty Act of 1996 Congress directed the Attorney General to "provide support and enhance the technical support center and tactical operations of the Federal Bureau of Investigation[.]" The FBI is currently enhancing its staffing and equipment to augment its technical support capability. The FBI will develop law enforcement technical requirements for obtaining plaintext which support operational strategies; serve as the center of strategic partnership among federal, state and local law enforcement entities with regard to obtaining plaintext; act as the law enforcement liaison to industry on

access-to-plaintext issues;⁶⁹ develop access-to-plaintext and processing tools for use in cases in which encryption is used and traditional methods are ineffective; and support, through on-site expertise and training, the operational use of plaintext access tools. The Secret Service has determined that the need for some baseline decryption capability is urgent and is, therefore, enhancing its own capability, which it plans to make available as a resource to state and local investigators. The government will retain control of sensitive information and technology.

Given the nature of the threat to the cyber infrastructure, industry participation in this issue is critical. We recommend that the FBI encourage industry to provide assistance on a long-term basis through detailees. We must look to create and maintain economic incentives that support cooperation over the long term. In addition, in conjunction with relevant community examiners, the government should develop a computer forensics examiners certification program to ensure that computer forensics examiners and technicians undergo regular professional training and stay abreast of current technology.

The Department of the Treasury has begun its third year of a combined enforcement initiative to provide training and equipment in the area of computer forensics to agents assigned to the IRS, ATF, Customs, and the Secret Service. The initiative was designed to integrate the expertise and experience of the existing programs at all of the bureaus into a training exercise that leads to forensic standards needed in the examination of computer evidence. Over 200 agents from all four bureaus have taken part in the program to date, with the plan to double that figure by the year 2000. This initiative effectively provides for the individual bureaus to place agents trained in the examination of computer evidence in all of the respective field offices.

Action: Develop Better Software Engineering Processes

The federal government's efforts to rapidly repair Year 2000 software problems has led to the outsourcing to foreign companies of large source-code rewriting projects. This has prompted concerns that malicious code could be written into widely used software or government operating systems by terrorists or others. There is no question that this possibility exists and that it could result in considerable threats to the NII. At the same time, no readily viable solution to the problem currently exists. It is not practical to attempt to monitor all code placed on government systems - - let alone private sector infrastructure networks. Furthermore, any restrictions on code written by foreign nationals might face discrimination challenges and industry opposition. The Justice Department therefore intends to study this issue further, consistent with on-going examination of this issue by the CICG.

To the extent that the government is developing software for itself, or having custom software written for its own use, building in security should be, and generally is, a mandatory

⁶⁹ A separate private sector entity could also serve as an advisory board for the government on access to plaintext issues, as well as acting as the primary liaison for exchange of relevant information between government and industry.

requirement. For example, DOD's Critical Asset Assurance Program is designed to ensure that infrastructures critical to DOD's mission requirements are secure. Assuring security in software or services purchased "over the counter" from private industry is significantly more difficult.

The development of technical tools to address and respond to new developments in the commercial marketplace is an on-going and difficult process. The federal government works with industry to understand how new products work and uses this knowledge to develop effective investigative tools to detect and combat intrusions.

At present, government involvement in software engineering is concentrated on the telecommunications side of the NII. Pursuant to the Communications Assistance for Law Enforcement Act of 1994 (CALEA), 47 U.S.C. § 1001, *et seq.*, U.S. law enforcement and intelligence gathering entities cooperate with telecommunication providers to ensure that law enforcement's ability to legally intercept communications is maintained as the industry shifts from analog to digital signal processing. The National Security Telecommunications Advisory Committee further serves to ensure that the federal government and the telecommunications industry are coordinating on a variety of issues including software engineering. These activities should be continued and supported.

On the non-telecom side of the NII, the government funds the Software Engineering Institute (SEI) at Carnegie Mellon University.⁷⁰ In addition, many federal agencies participate in various software and telecommunication industry groups in an effort to encourage the introduction of security features at all levels of software and network development.⁷¹ We should

⁷⁰ The SEI was established in 1984 as a response to the risk presented by automated and human driven attacks on the Internet. The Institute concentrates on the development and implementation of improved software engineering practices by operating a 24-hour point of contact to respond to security emergencies on the Internet; facilitating communications among experts working to solve security problems; providing a central point for identifying vulnerabilities in computer systems and for working with technology producers to resolve those vulnerabilities; serving as a model for, and facilitating the creation of other computer security incident response teams (CERTS); taking steps to increase awareness of information security and computer security issues; maintaining close ties to the research community and conducting research and development to produce methods and tools that improve the security of networked computer systems. See Testimony of Richard Pythia, Manager, Trustworthy Systems Program and CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, before the Permanent Subcommittee on Investigations, U.S. Senate Committee on Government Affairs, June 5, 1996.

⁷¹ The Critical Infrastructure Coordination Group's sub-group on Research and Development coordinates research and development on a variety of programs and technologies associated with infrastructure protection. Similarly, GSA is involved with the implementation and development of Internet/internet security mechanisms including firewalls and other access-

continue to participate in industry groups working on software development in an effort to share intrusion experiences and suggest software improvements to assist law enforcement's anti-terrorism activities. Most such suggestions will also enhance general security and will, therefore, assist in further development of the economic benefits of electronic commerce. We should also invest in research and development of cyber tools that assist our counter-terrorism efforts, as discussed at page 183 of this Plan. We do not recommend that any additional regulatory or statutory requirements be placed on the software industry with respect to security engineering.

Action: Develop Investigative Expertise By Recruiting, Training And Equipping Computer-Literate Agents And Analysts

PDD 63 specifically directed the FBI and the Secret Service to vigorously recruit undergraduate and graduate students with relevant computer related technical skills and facilitate the hiring and retention of qualified personnel for technical analysis and investigation of cyber attacks. The FBI and the Secret Service have developed plans to fulfill this directive.

One of the difficulties that the FBI, the Secret Service, and other federal law enforcement agencies have in recruiting and retaining personnel with technical backgrounds is that the starting salaries for new agents and non-agent personnel are not competitive with the private sector market. Methods for attracting computer-savvy personnel are currently under study in the Justice Department's the Technology Talent Task Force. One of the options being explored that would be open to all federal law enforcement agencies is more aggressive use of recruitment bonuses to attract highly skilled, technically trained individuals.⁷²

The FBI plans to expand the number of technically trained investigators at the headquarters level in the NIPC and in the field offices. The NIPC has undertaken an initiative to train 200 FBI agents in computer investigative skills this year and plans to train up to 500 agents per year by the year 2000. Additional training opportunities include specialized courses in information security developed by the private sector. The FBI will have National Infrastructure Protection and Computer Intrusion (NIPCI) squads in 10 large metropolitan field offices in FY 99. In addition, every field division includes a NIPCI Team. The FBI is also expanding its computer forensics program to have at least one full-time computer forensics examiner in each field office.

control devices. The White House Office of Science Technology and Policy (OSTP) works with the NSTAC and various other industry groups.

⁷² Currently, federal agencies are permitted under Title 5 of the United States Code to pay recruitment bonuses to employees in occupations in which the government has or anticipates a shortage of qualified personnel, especially in occupations involving critical skills. The Department of Justice anticipates using this authority to attract highly qualified persons.

The NIPC is seeking to train investigators and at least one trainer from state level investigative agencies in each of the fifty states and the District of Columbia. The NIPC is also seeking to train investigators from the municipalities represented in the Major Cities Chiefs and the Major Sheriff's Associations and has been consulting on this with the International Association of Chiefs of Police and the National Sheriffs Association. A larger effort to include the training of 500 state and local law enforcement personnel at a one week hands-on course will be launched in FY 99. Funding permitting, an additional effort will also be undertaken to provide a three-day overview course to 2000 state and local officials.

The Secret Service has an Electronic Crimes Special Agent program designed to support field operations in digital technology, satellite communications, advance paging systems, and telecommunications tracking, and to provide forensic analysis of computer equipment. The Secret Service proposes to provide high-tech training in the area of network intrusion and telecommunications compromise activity to federal, state, and local law enforcement, as well as to private industry.

In order to enhance coordination and prevent duplication, computer related training of investigators and prosecutors is offered through the National Cybercrime Training Partnership (NCTP), a strategic alliance among federal, state, and local investigative and prosecuting agencies which have as its mission the creation of a national network of high-tech law enforcement personnel who can serve as trainers. The NCTP seeks to develop the skills and knowledge required to investigate and prosecute high-tech crime through actively designing, developing, and delivering detailed technical training courses for investigators, forensic examiners, and prosecutors. The NCTP serves as a forum to notify federal, state, and local law enforcement of training and technical assistance programs, and is establishing a secure communication system to facilitate this notification. The NCTP will develop instructors through its training program, and will also provide academic institutions with developed courses for use in colleges, universities and professional-technical schools.

Over the next 12 months the NCTP will complete development of curricula, other training materials, a national database of trainers, and a database of points of contact for technical and legal issues. Thereafter, the NCTP will develop materials to conduct training needs assessments, training program evaluations, and a "best practices" guide for investigators and prosecutors. The NCTP will serve as a clearinghouse for high-tech issues, including information on available tools for computer investigations.

**ACTION: Develop Prosecutive Expertise By Recruiting, Training And
 Equipping Computer-Literate Prosecutors**

Over the next five years, the Justice Department plans to increase significantly the number of federal prosecutors with technical training and expertise, so that we will be able to competently assist investigations on infrastructure attacks and bring prosecutions to deter these attacks. Toward this end, the Department will expand the core group of highly trained,

specialized prosecutors in the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division.⁷³

To increase prosecutive expertise in the field, in 1995 the Department created the Computer and Telecommunications Coordinator program in the U.S. Attorneys' Offices. Each of the 94 U.S. Attorneys' Offices has designated at least one Assistant U.S. Attorney to serve as the coordinator for that office, with three specific responsibilities: (1) serve as resident consultant on high-tech issues; (2) be part of a nationwide network of high-tech prosecutors available to serve on a nationwide high-tech prosecutive team for multi-district computer cases; and (3) serve as a leader and legal consultant to federal, state and local agents and those technical experts working high-tech cases in their districts in order to share information about developing technologies, and strengthen local technical expertise. As part of this program, the coordinators receive specialized training in computer crime and infrastructure protection annually through the National Advocacy Center in Columbia, South Carolina. The Executive Office for U.S. Attorneys should continue to make computer crimes a priority, and should consider a program to detail Assistant U.S. Attorneys to CCIPS for up to 12 months so that they can receive additional training and develop technical expertise in more complex cases.

The Department of Justice also seeks to expand the Computer and Telecommunications Coordinator program to state prosecutors, who are often the first line of defense in infrastructure attacks. In addition, the Department would like to expand the CCIPS detail program to include more state and local prosecutors. The first detailee in this program, from the New Jersey Attorney General's Office, just completed a 9-month detail (funded by a grant to the state) and now heads the Computer Crime Section for the New Jersey Attorney General's Office.

A formal program should also be developed to educate judges, who may not grasp the technical aspects of these cases and may underestimate the seriousness of a computer crime or infrastructure attacks. This program could be facilitated through the Federal Judicial Conference.

Action: Encourage And Facilitate Implementation Of Good Computer Security Practices

It is not good enough to know which targets are vulnerable and to have ways of protecting

⁷³ CCIPS prosecutors have, and will continue to develop through additional technical training, specialized expertise in infrastructure protection, including experience in investigating infrastructure attacks. CCIPS prosecutors will provide legal advice, and help obtain needed court orders for investigators from federal law enforcement agencies. CCIPS prosecutors will also provide advice to state and local investigators on computer search and seizure issues and compliance with federal laws applicable to state agents. In addition, CCIPS prosecutors will continue to assist U.S. Attorneys with the technical aspects of investigations into infrastructure attacks that take place in their districts.

those assets from attack. The inconsistent application of known security fixes can lead to significant security risks. In numerous cases involving attacks against U.S. government computers, attackers have exploited known vulnerabilities for which solutions had previously been made available to the public.⁷⁴ Attackers are quickly attracted to weak links in a chain of networked systems and will use a vulnerable network as a launching point for attacks on more secure systems. If a system with weak security serves as the home system for an individual with access to more secure networks, a hacker may be able to breach the weak system and use the individual accounts to bootstrap his or her way into the more secure systems. In this way, access to a single node can lead to access to a huge number of related systems. Moreover, because hackers often brag about their exploits over the Internet, often disclosing in detail precisely how to access a compromised system, a single probing by hackers can potentially expose a system to far more serious terrorist attacks.

It is, therefore, extremely important that both government and private sector system operators be encouraged and enabled to implement good computer and telecommunications security practices. There are several ongoing efforts to encourage the adoption and implementation of such practices at federal agencies including training missions, internal system upgrades, secure communication channels and simulated attack exercises.

One of the greatest challenges to enhancing information security programs and developing a workable infrastructure protection program is to ensure that protection efforts are "owned" by the program and business managers at federal agencies who are accountable for the success of their entire program, including security. The Information Technology Management Reform Act of 1996 (Clinger-Cohen) went a long way to addressing that issue by establishing agency chief information officers, who were given responsibility over the security of agency systems, and the OMB co-chaired CIO Council. The mission of the CIO Council's Security Committee is to ensure implementation of security practices within the federal government that gain public confidence and protect government services, privacy, and sensitive and national security information. Among the particular efforts that are ongoing by the CIO Council Security Committee to address this priority area:

- Promoting security awareness and training with the Federal Computer Security Program

⁷⁴ For example, in the recent "Solar Sunrise" case, an Israeli hacker and two California minors were able to exploit a known vulnerability to acquire root access on dozens of U.S. government and private computers systems using the Sun Solaris operating system. Once the hackers gained root access to the systems, they left "sniffer" programs behind and applied security patches available on the Internet to seal the hole through which they had entered. (A "sniffer" is a software program that captures keystrokes as they are entered, and can be used to capture users' account names and passwords.) They then proceeded to advertise the success of their exploits over the Internet through the "Anti-on-line" hacker web site. Had the security patches used by the hackers been employed by the system administrators before the attacks, the hackers would not have had such an easy route to complete control of these systems.

Managers' Forum and publishing a training plan;

- Reviewing the appropriate qualifications and attributes of computer system administrators -- the first line of defense for secure systems;
- Partnering with others, such as GAO and the President's Council on Integrity and Efficiency, to identify best security practices in industry and government, conduct an awareness program and publish a report to promote these practices; and
- Developing an interagency security assistance team to conduct independent and confidential reviews of agency security programs.

The CIO Council Security Committee is also working with the NSC to coordinate PDD 63's new requirements with the existing requirements of OMB Circular A-130, the Computer Security Act, Paperwork Reduction Act, and the Clinger-Cohen Act. The objective is to establish the government as a model for security and develop and promote a process by which government agencies can: 1) identify and assess their existing security posture; 2) implement security best practices to assure program improvement and effectiveness; and, 3) set in motion a process of continued maintenance.

The Federal Computer Incident Response Center (FedCIRC),⁷⁵ conducts security training seminars for federal system administrators. Attorneys from the Justice Department speak regularly at FedCIRC conferences and before a variety of other gatherings of government and private sector computer and telecommunication system operators in order to both encourage good security practices and disseminate information gained from prior system intrusions. The Secret Service, the FBI, and other government agencies participate in the Network Security Information Exchange (NSIE) to provide information and training on past intrusion activity and current threats. The NIPC will also be conducting outreach to the private sector on intrusions and threats.

Many federal departments and agencies also have ongoing programs to assess specific existing networks and increase security where necessary.⁷⁶ Some federal agencies have also

⁷⁵ FedCIRC, currently operated by GSA, collects information related to computer intrusions into government computers and issues warnings about known vulnerabilities.

⁷⁶ For example, the IRS is currently in the second year of a program to review and increase the security of its internal computer systems. It is developing capabilities through its Office of Security Standards and Evaluation to identify and respond to potential cyberattacks from both internal and external sources. Similarly, DOD's Critical Asset Assurance Program (CAAP) provides an integrated asset and infrastructure vulnerability assessment and assurance program that identifies dependencies, vulnerabilities and the effects of system disruptions on DOD plans and operations.

established special secure communication channels that can be used to facilitate system security operations. NSA's penetration testing ("red team") exercises simulate actual attacks against DOD and other government networks generating vulnerability information that can be used to improve system security and prevent actual attacks. The results of these exercises will be used to develop the vulnerability assessments and infrastructure assurance plans required under PDD 63.

Action: Promote The Training And Development Of System Administrators And Network Security Specialists

As mentioned previously, the CIO Council Security Committee is reviewing the appropriate qualifications and attributes of computer system administrators -- the first line of defense for secure systems. These efforts are important because several obstacles currently stand in the way of consistent, widespread implementation of good security practices, including personnel security and training issues, lack of security standards and certifications, and insufficient information sharing.

In the past ten years the enormous increase in the demand for telecommunication and computer network administrators has significantly outstripped the education system's capacity to produce qualified candidates to fill available slots. Moreover, both the government and the private sector have failed to comprehend the complexity of modern networks and the demands and importance of network administration. We must recognize the value of skilled technical personnel and invest sufficient resources in their development. The U.S. government must hire, train and retain sufficient numbers of skilled information security specialist and system administrators to protect its networked systems.

Virtually all federal government components are negatively affected by the insufficient numbers of computer security system specialists available in the work force to perform necessary security functions. Many system administrators have multiple responsibilities of which security issues make up only a small part. Moreover, even when security concerns are used as a justification for adding personnel, the additional resources are rarely designated as full time security managers, and are often diverted to other, more immediate concerns.

We should explore dedicated line-item budgeted security resources to be assigned to critical government computer and telecommunication systems. Moreover, in order to be competitive with private sector employment, such positions must carry sufficient salary and benefits to attract and retain qualified candidates. In light of the current salary differential between private sector and government sector Information Technology (IT) positions, it may be necessary to create a separate or supplemental pay scale for IT professionals using existing statutory authority. Ideally, any "IT-Scale" would permit technical employees to rise to the top of the pay-scale without being forced out of technical tasks and into management positions.

The Critical Infrastructure Coordination Group IWG on personnel and training issues is considering ways to recruit, retain, and provide advanced training for government IT

professionals, and is assessing such options as creation of a "cyber-corps," funding undergraduate or graduate education for IT professionals in return for government service, providing fellowships for private sector IT professionals, and a number of other initiatives. Similarly, the Department is also looking at existing incentives to recruit and retain highly qualified personnel.

The lack of uniform training standards for computer security administration (either within government or at the university level) makes hiring decisions difficult. Non-technical supervisors lack the expertise to assess the security of computer systems without the benefit of clear standards against which to judge system performance, nor do they have the expertise to evaluate applicants to perform these tasks. NSA, the National Institute of Standards and Technology (NIST),⁷⁷ and the Defense Advanced Research Project Agency should therefore set standards for networks that include recommendations: (1) for the number of dedicated security personnel necessary for operation of various systems; (2) for the necessary skill levels of each security administrator; and (3) for training and certification programs for computer/telecommunication security experts. In addition to ensuring adequate security for government systems, a comprehensive and intensive certification program, available only through a set period of government service, could enable the government to retain such personnel and compete with private enterprise for qualified security candidates while simultaneously providing the public sector with a model for security procedures.

The CIO Council Security Committee should consider whether the lack of routine background checks on government employees who serve in positions of trust as systems administrators or programmers for sensitive government computer systems is a valid concern. The shortage of qualified applicants for system administrator positions increases the pressure to fill positions without proper regard for security concerns. Even when these systems do not themselves contain classified or sensitive information, they often have privileged access connections to other systems that do contain such information. The utility of a formalized system of background checks for all applicants for these positions should be explored. Moreover, security clearances for such positions should be standardized across federal agencies to ease and expedite the movement of employees among government agencies.

⁷⁷ NIST currently works with industry and government to establish secure information technology systems and develop methods for protecting the integrity, confidentiality, reliability and availability of information resources. NIST also works to enable the measurement and improvement of the security of information technology systems and networks while addressing technical issues such as cryptographic techniques, advanced authentication systems, communications security, public key certificate management, firewall policy and design, incident response, vulnerability analysis, security architectures and security criteria and metrics. NIST is also engaged in the production of standards, guidelines, prototypes, conformance tests, assurance metrics and reference implementations. NIST and NSA co-chair the Critical Infrastructure Coordination Group's sub-group on standards.

SPEARHEAD RESEARCH AND DEVELOPMENT TO ENHANCE COUNTER-TERRORISM CAPABILITIES

Technological development has a significant role to play in protecting U.S. citizens and assets from the terrorist threat.⁷⁸ Technology is a vital tool to be used in conjunction with intelligence gathering, law enforcement, and other activities to safeguard U.S. persons and interests within the U.S. and abroad. While there is no technological "fix" for terrorism, many terrorist acts, particularly against fixed targets, can be deterred, prevented, or mitigated by judicious use of technical tools.

The U.S. is a world leader in developing new technology to enhance counter-terrorism capabilities. In order to sustain the technological advantage within the U.S. counter-terrorism community, there must be a comprehensive research and development strategy which includes: defining near and longer term technology needs, meeting specific requirements defined by end-users of technology in the emergency responder community, supporting fundamental research in targeted technical sectors, and supporting both competitive and centralized research programs to promote technological breakthroughs. Our efforts should not be limited to the off-the-shelf technical solutions for today's technical shortfalls, but should also encourage new concepts based on a national strategic policy which supports long term technical requirements.

Research and development efforts to enhance our counter-terrorism capabilities must be consistent with and complementary to our nation's overall technology goals. The National Security Council's Critical Infrastructure Coordination Group's R & D Interagency Working Group (IWG) has drafted a comprehensive R & D strategy which addresses the full spectrum of critical infrastructures. Similarly, the NSC's Weapons of Mass Destruction Preparedness R & D IWG is overseeing our R & D efforts to respond to WMD terrorist attacks and is addressing broad national technology goals in this area. As these efforts continue through the interagency process, the White House Office of Science and Technology Policy, which chairs these two IWGs, should continue to assure that programs to develop the specific critical technologies identified below to increase our capabilities to prevent, deter and respond to terrorism are well coordinated and in harmony with these national technology goals.

A number of federal agencies are engaged in independent research and development efforts, consistent with their individual agency missions, which relate to our nation's overall counter-terrorism strategy. In addition, agencies pursue joint research and development projects to develop technologies which further their individual agency goals. These joint efforts allow them to leverage their resources for greater gains than they might achieve independently. Some of these joint efforts impact on our overall counter-terrorism R & D goals. There are a number of working groups and other mechanisms in place which enable agencies involved in research and development to exchange ideas, keep abreast of each other's progress, and minimize duplication.

⁷⁸ Office of Technology Assessment, U.S. Congress, Technology Against Terrorism: The Federal Effort (July 1991).

We suggest some improvements to more efficiently manage these various research and development efforts and to spur progress toward targeted areas of need highlighted by the goals and strategies of this Plan.

**OBJECTIVE: Improve Management, Coordination And Development Of
Critical Technologies**

There is a need for a comprehensive clearinghouse and coordinator of interagency counter-terrorism research and development to provide overall structure and focus to interagency activities. This entity would highlight research programs with leading technical strengths; pinpoint duplication, overlaps and gaps; identify outstanding technical needs; provide a forum for improved inter-agency communication and exchange of ideas; and promote greater efficiency. It could coordinate as well as synthesize our counter-terrorism technology program and serve as a center for strategic thinking and planning on related research and development.

**Action: Designate Lead Interagency Mechanism To Provide
Broader R & D Coordination Authority**

Uncoordinated counter-terrorism R & D efforts dilute the focus of and return on research dollars and may promote unwanted duplication of effort. Various federal agencies have memoranda of understanding to jointly fund specific types of projects to augment their individual agency expertise and to provide greater return on their research dollars. For example, pursuant to the recently signed Memorandum of Understanding for Science and Technology between the Department of Energy and the Federal Bureau of Investigation, eight National Laboratories will initiate 27 projects to provide enhancements to the FBI Laboratory's capabilities for conducting forensic and other analyses and for responding to events involving hazardous chemical, biological, and radiological materials.

One highly successful interagency model is the Technical Support Working Group, known as TSWG, jointly funded and managed by the Departments of Defense, State, and Energy, and the FBI.⁷⁹ TSWG provides an interagency forum to address multi-agency needs and requirements through funding of specific projects. Its focus is on rapid research, development and prototyping to meet specific user requirements. Through multi-agency subgroups chaired by agency experts, TSWG identifies R & D requirements and how to meet them in the following eight areas: explosives detection and defeat; infrastructure protection; investigative support and forensics; personnel protection; physical security, surveillance collection and operations support; tactical operations support; and chemical, biological, radiological, and nuclear countermeasures.

⁷⁹ Department of State provides policy oversight; the Departments of Defense and Energy and the FBI co-chair the technical oversight; DOD provides the management staff and facilities; and State, DOD, Energy, and FBI provide the research funding, with the majority of research funding contributed by DOD. FBI is seeking significant funding in FY 2000 for TSWG related R&D activities.

The ability of TSWG to reach down into its well-established and functioning subgroups, where much strategic thinking and peer review takes place, is a significant advantage. TSWG's current focus is on chemical and biological threats in urban areas, large vehicle bomb countermeasures, stand-off detection of explosives, infrastructure protection, and structural blast mitigation. The more than 40 federal agencies and components which participate in TSWG⁸⁰ endorse its successful approach, which includes assessments of threats, capabilities, and requirements; setting priorities; issuing announcements to federal agencies, the private sector and academia for proposals which meet these requirements; evaluating responses to these announcements; awarding contracts for specific proposals; and monitoring progress on these projects to completion. TSWG is highly successful in developing solutions by leveraging resources of the federal government, state and local representatives, the National Laboratories, academia, the private sector, and its three contributing foreign partners.⁸¹

These efforts, and others like them, are useful and necessary. We should build on them to maximize our R & D efforts. Nevertheless, what is needed is a comprehensive mechanism which sets national (as differentiated from agency, mission-dependent) counter-terrorism priorities; tracks on-going projects consistent with these counter-terrorism priorities; provides a forum for agencies to meet, discuss, and share results of agency counter-terrorism R&D efforts; and promotes strategic thinking concerning long range basic research. Through the R & D IWGs of the Critical Infrastructure Coordination Group and the Weapons of Mass Destruction Preparedness Group, the National Coordinator has created such a mechanism. These IWG's, chaired by the Office of Science and Technology Policy (OSTP), are developing and coordinating broad national technology goals and priorities. Provision must also be made for additional avenues of input and designated points of contact to provide state and local authorities with a means to voice their terrorism related technology needs.⁸² The Justice Department's proposed National Domestic Preparedness Office could help fill this liaison role by serving to inform federal R&D programs about the needs of state and local first responders, coordinating and sharing development priorities and results within the federal community, and ensuring that emerging technologies are integrated into current and future first responder training, planning, and equipment efforts.

⁸⁰ Since 1995, TSWG has also had agreements in place for joint R & D projects with three other nations: Canada, Great Britain, and Israel.

⁸¹ TSWG is credited with having greatly increased communication among scientists of various agencies working similar problems. Technology Against Terrorism: The Federal Effort, *supra*, footnote 35, at 4. TSWG's interagency role in identifying needs, seeking common approaches, and coordinating the development of new technologies was recognized in the 1995 President's National Security Science and Technology Strategy.

⁸² Two-thirds of the responses to the State and Local Questionnaire indicated the need for such a point of contact. See Appendix: State and Local Questionnaire, responses to question 46.

Broader R & D coordination is not intended to adversely impact individual agency R&D efforts. In addition to supporting counter-terrorism research through the TSWG forum and interagency memoranda of understanding, the National Coordinator should support those principal agencies engaged in terrorism-related research, such as DOD, FBI, HHS, CIA, EPA, Department of Agriculture (USDA), DOE, and FDA, to pursue projects specific to their responsibilities. These projects, which may be of use to only a single agency, contribute significantly to the overall technology development effort in counter-terrorism. Although these projects may be pursued by a single agency, they should be coordinated through the CICG and WMDPG so that the counter-terrorism community is kept fully informed.

Action: Require Responses To Government Announcements Which Solicit Proposals For Research And Development Projects To Identify Pending Similar Submissions

Numerous agencies issue announcements seeking proposals from diverse sources for specific research and development projects. Responders to these announcements are not required to state whether they have a current application to fund essentially the same proposal pending at another agency. Research and development announcements issued by federal agencies which seek project proposals should require responders to disclose this information. This would mitigate against duplicate funding for essentially the same project; it would not preclude funding of a more efficient or alternative approach. In addition, disclosure of this information in the response to the announcement would provide agencies with sufficient information to confer among themselves as to similarity of requirements and the feasibility of joint efforts. This recommendation does not require budgetary enhancements.

Action: Develop Critical Technologies That Increase Our Capabilities To Prevent, Deter And Respond To Terrorism

There appears to be considerable agreement on the areas to target for counter-terrorism research investment. On-going research and development projects are addressing many of these needs. This Plan does not attempt to catalogue these on-going efforts. It is clear, however, that presently funded projects will not meet all outstanding requirements to develop prototypes to satisfy all presently identified needs or for next-generation technologies. Highlighted below are specific areas in need of additional research and development focus.

Communication

State and local law enforcement authorities as well as federal officials identify command, control, and communication needs as significant. The ability to communicate information quickly and accurately and to direct and coordinate the activities of diverse individuals and organizations to resolve successfully a terrorist incident is important regardless of the character of the terrorist incident. Development and acquisition of interoperable, secure, mobile, compact, and affordable communications systems which connect first responders and other emergency

personnel to the on-site command structure are a high priority.

WMD Detection

Another high priority area is improved means for detecting and identifying chemical, biological, radiological, nuclear, and explosive agents. Law enforcement and other responders express urgent need for portable (handheld or wearable), low-cost equipment responsive to a wide range of hazards, but particularly chemical and biological agents. First responders' primary need is not for highly sophisticated devices which distinguish among a broad range of agents and identify precisely which specific agent is present. Rather, they urgently need a lightweight inexpensive alerting device which alarms when a CBRN agent -- of whatever variety -- is present. At the request of the Weapons of Mass Destruction Preparedness's R&D subgroup, TSWG has recently completed a detailed assessment of non-medical R & D needs relative to chemical and biological agents and countermeasures.

There is also a need to develop a flexible deployable area monitoring system for CBRN agents, both pre- and post release. Such a system would allow authorities to know where a safe perimeter could be established in the event of an attack. The system could also be useful at special events to protect against a terrorist incident.

Cyber Tools

Certain critical needs relate to the unique nature of particular threats and the rapidly evolving nature of technology. For example, cyber-terrorism poses unique challenges in terms of detecting an incident, defending against and recovering from such an event, and tracing it back to its point of origin so that the perpetrators can be identified and prosecuted. A related need exists for tools to aid in critical infrastructure protection, vulnerability assessment, penetration testing, and recovery, and there is an urgent need for a portable methodology for vulnerability assessments/penetration testing ("red team" attacks). In 1995, TSWG formed an infrastructure protection subgroup, which has identified requirements for information infrastructure security, electrical power distribution, and control and data acquisition systems. TSWG has also completed a road map that identifies deficiencies and is intended to serve as a guideline for future infrastructure protection activities in specific technical areas.

Protecting our nation's critical infrastructures will require new tools, techniques, technologies, standards, and practices. PDD 63 directs OSTP to coordinate research and development agendas for the government related to critical infrastructure protection through the National Science and Technology Council (NSTC). Accordingly, OSTP established the Critical Infrastructure Protection R&D Interagency Working Group under the NSTC in March 1998. This group, in coordination with the Critical Infrastructure Assurance Office, has developed a comprehensive list of infrastructure protection R&D needs.

Medical Response Technologies

Improving our medical therapeutics, including antidotes, vaccines, supportive therapy, and alternative treatment approaches, is a high priority. Research and development targeted to produce new diagnostics, vaccines, and antidotes, including broad spectrum therapeutics not limited to specifically identified biological agents, are urgently needed, as is underlying biological research on the genetic make-up of disease-causing bacteria and viruses and on the mechanisms by which bacteria and viruses cause disease.

Preparedness for and response to an attack involving biological agents are complicated by the large number of potential agents (most of which are rarely encountered naturally), their sometimes long incubation periods and consequent delayed onsets of disease, and their potential for secondary transmission. In addition to naturally occurring pathogens, agents used by bioterrorists may be genetically engineered to resist current therapies and evade vaccine-induced immunity. Initial research emphasis should be placed on microbes such as smallpox and anthrax which have the greatest potential for use as a weapon of mass destruction. For the longer term, research must target agents and diseases such as Ebola virus, brucellosis, plague, tularemia, viral encephalitides, viral hemorrhagic fevers, and botulism.

A research program to produce vaccines and therapeutics for biological weapons faces the challenge of not being able to proceed with Phase III efficacy clinical trials involving human subjects. Given ethical and safety concerns, infecting human subjects with a deadly organism in order to test a vaccine or therapeutic cannot be undertaken. Therefore, the regulatory process for approval of treatments must be modified to permit the emergency use of antibiotics/antivirals and vaccines that have been shown to be safe and efficacious in animal models.

Since it is likely that an intentional release of a bioweapon will become apparent in the form of a disease outbreak, emphasis must be placed on the development, evaluation and approval of rapid diagnostics. The ability to rapidly identify and characterize a suspected biological agent will permit speedy treatment and/or prophylaxis. The rapid diagnostic technologies to be developed should be capable of detecting known biological agents as well as genetically engineered organisms.

Diagnostics. The areas to be emphasized include the design, development and approval of methods for rapid detection and identification of the biological agent itself; development and approval of technology to rapidly identify components of a bioengineered microorganism; rapid identification of virulence factors in bioengineered microorganisms; rapid determination of the microbe's drug sensitivity; development of sensitive and specific assays to identify a serological response to the microbe or virulence factor or to a unique pathology caused by the microbe; and development of antibody-detection-based diagnostics to assist in epidemiologic studies.

Antimicrobial Drug Design, Development, and Testing. Research needs in this area will focus on the development of therapies for known agents with significant potential for use as

bioweapons (e.g., anthrax, smallpox); therapies active against drug-resistant microbes; multiple therapies encompassing three or more therapeutic agents, aimed at different gene functions, for each targeted microbe to enable treatment of drug resistant microbes; and broad-spectrum therapies active against microbial families. In the development of these therapeutics, it is important to focus on those with favorable pharmacokinetic properties which result in drugs which can be taken by mouth and require fewer doses to facilitate treatment of civilians in an emergency situation.

New Vaccine Development and Testing. Vaccines are the most effective method of providing primary prevention against a broad array of infectious diseases. Research to develop safe, effective vaccines that can be administered to the general population or specific groups at highest risk is critical to protect the U.S. population from bioterrorist attacks. Although the priorities and timeframes for the military vaccine development program do not coincide with civilian needs, it would be worthwhile to explore the feasibility of leveraging existing military programs to develop vaccines for civilian use as well, recognizing that some military-produced vaccines may not be suitable for the civilian population which has a much wider range of age and health status.

Basic Research and Behavioral Studies. The successful development of strategies for dealing with biological weapons depends on the availability of a foundation of knowledge about these organisms and the diseases they cause. Because the numbers and types of microbes that can be used as bioterrorist weapons are many and diverse, it is critical to develop more fundamental knowledge of the molecular, cellular, and genetic mechanisms involved in microbial pathogenesis and host immune defense mechanisms. Furthermore, bioweapons may be delivered by non-traditional routes (e.g., water-borne, inhalation) and at higher-than-normal concentrations (such as that achievable by aerosolization). Increased knowledge of factors that play a decisive role in determining virulence and invasiveness, as well as those events or processes critical to initiating infection or influencing the severity of disease, are crucial to the development and approval of therapeutic strategies. Behavioral study and analysis are needed to assess personal and public health risk, determine the effects of public information, and identify the immediate behavioral responses to the unique characteristics of a biological attack, as well as the longer term impact on individuals and communities.

Expedited Regulatory Review and Approval. Notwithstanding the fact that efficacy clinical trials of therapeutics and vaccines against the most likely biological weapons are not possible, the Food and Drug Administration (FDA) is committed to assisting and expediting the development of, and access to, important new products for serious and life-threatening illnesses and conditions, including products that could be used to treat outbreaks caused by bioterrorist agents. To meet this objective, the FDA is considering changes to regulations to allow approval of such drugs and biological products based on evidence of effectiveness derived from appropriate studies in animals, forgoing efficacy studies in humans. The changes would allow FDA to rely on evidence from animal studies where (1) the mechanism by which biological, chemical, radiological, or nuclear substance causes disease and illness and its treatment or prevention by the product is reasonably well understood; (2) the effect is reproducible in multiple animal

species; (3) the study endpoint is clearly related to the desired benefit in humans; and (4) it is therefore reasonable to expect the effect of the product in animals to be a reliable indicator of its efficacy in humans.

Conventional Weapon Technologies

Research must continue and be enhanced regarding the strengthening of existing physical structures against the threat of explosive attack. As we have seen with the recent events in East Africa, our physical structures continue to be vulnerable to terrorist attacks by conventional means.

Improved tools to defeat, mitigate, decontaminate, transport and dispose of weapons are also needed. Stand-off detection and disruption of large vehicle bombs are another critical requirement in the fight against terrorism. Large vehicle access tools and diagnostics, as well as large bomb and tanker truck bomb disrupters, are important technologies in the fight against frequently used terrorist weapons. Technologies also need to be improved for rendering safe improvised explosive devices (IEDs). Low cost robotics to support bomb squads and evidence response teams would also be useful.

Non-Lethal Apprehension Tools

Past experience with hostage and barricade situations indicates a need for development of non-lethal apprehension tools and techniques. Effective tools which enable law enforcement to stun and temporarily incapacitate terrorists and other perpetrators who put themselves and others at risk of serious bodily injury or death might well provide law enforcement with alternatives to the use of deadly force in some situations. This would give us additional capability to defuse highly charged threat situations.

Casualty Management

An area of significant need where new technologies would be helpful is mass casualty management. Regardless of the weapon used, if a catastrophic event occurs, we will need every available resource to facilitate response and recovery. Management of these resources and prioritization of utilization will be essential. Technology to control utilization of resources and facilitate difficult decisions, to help plan responses to catastrophic events, and to provide training for simulation and decision making, will increase our preparedness for such incidents.

Technologies to Counter Agricultural Bioweapons

USDA continues to explore and pursue a comprehensive, long-term research and development program aimed at safeguarding our agricultural sector. Consistent with national technology goals to be established by the WMDPG and the CICG, it should coordinate these efforts with TSWG and OSTP on projects which overlap into the counter-terrorism arena. Such projects may include research programs to provide tools to detect, trace, and respond to a terrorist attack on agriculture or the food production, processing, and marketing system that involve biological agents or pests, some of which can also infect humans. USDA should cooperate with other federal agencies in preventing and controlling zoonotic (transmittable from animals to humans) microorganisms and pests and insect vectors (i.e., transmitters) of animal and human diseases, including bioweapons agents.

The broad-based long term research program proposed by USDA includes:

- Research to expand identification capabilities;
- Research to develop quick response diagnostic tests which do not incorporate infectious materials for use on site by non-professionals;
- Epidemiologic mapping of pathogens and pests to pinpoint their worldwide geographical origins for use in determining the source of a pathogen or pest;
- Research on genetically-engineered vaccines that can be manufactured in the U.S. and which are effective against all the highly infectious animal and zoonotic disease agents of biological warfare concern;
- Research to support U.S. licensing of disinfectants, acaricides and other foreign pest or pathogen control chemicals;
- Research on alternatives to widespread aerial chemical control of mosquitoes, midges, and other insect vectors of human, animal, and zoonotic disease;
- Research to prevent and control pathogens that are potential anti-crop biological warfare weapons;
- Research to identify resistance genes that can enhance genetic resistance of major crops to pathogens that are potential biological warfare weapons;
- Research to create biological weapons Hazard Analysis Critical Control Points (HACCP)

programs⁸³ for targeted animal and plant commodities and their potential biological warfare pathogens;

- Research on rapid and humane animal euthanasia methods and economically and environmentally sound carcass disposal;

As USDA continues to develop a targeted approach to this broad-based, long-term research agenda, the National Coordinator and relevant agencies should work with USDA to support and pursue counter-terrorism related research consistent with the Five-Year Plan.

Forensics and Epidemiological Investigation

Additional areas of need for research and development include tools for forensic and epidemiological investigation, technology for protection from and detection of conventional weapons, tools for data mining and information searching, and technology and supporting databases for biometric personal identification. While these technologies may be less pressing and more discrete in their application than other technologies discussed herein, they are still necessary to a well balanced counter-terrorism R & D program. However, they may be more appropriate for individual agency pursuit or for joint efforts pursuant to existing memoranda of understanding.

One such example is the Mobile Analytical Platform that EPA seeks to build to provide forensic evidence collection and analysis support to the FBI evidence response teams and the Hazardous Materials Response Unit (HMRU). To provide proper support, EPA needs to design, construct, operate, and maintain a fully equipped mobile laboratory capable of sophisticated and accurate analysis for the identification of unknown chemical substances during on-scene criminal investigations. This is an enhancement of ongoing support to the FBI which EPA has been coordinating with FBI's HMRU. EPA and FBI are currently drafting a memorandum of understanding on this issue.

Additional work is required to develop database technologies that can link existing federal government forensic and other databases. This effort will result in an increased ability regarding source attribution, a critical factor in successfully identifying and prosecuting terrorists. TSWG is currently working on three projects in this area. The first deals with identifying ink sources on fraudulent passports. The second is identifying international soils and dust samples, as well as air quality and pollen. The third deals with fiber identification, particularly from carpets and microcontaminants in dyes.

⁸³ USDA maintains emergency operational plans to guide eradication programs triggered by the discovery of dangerous pests and pathogens. These plans should be extended to all recognized bioweapons risks for targeted commodities in cooperation with other federal agencies, the states and private industry.

Action: Provide For Coordinated Acquisition Of Technology

Our overall strategy on meeting technology needs arising out of this counter-terrorism plan must encompass various aspects, including development of new technologies, production and testing of prototypes, establishing standards and specifications, broader production of affordable technologies, acquisition, distribution, and training for effective use. At present, each agency functions largely on its own. A central acquisition mechanism could reduce costs and promote efficiency without interfering with mission specific procurements and established time lines.

In our consultations with academia,⁸⁴ they shared this view and recommended a coordinated, broadly focused budget program to plan, coordinate, and track all R & D and acquisition projects to improve all counter-terrorism capabilities -- conventional and unconventional, defensive and offensive, domestic and foreign.⁸⁵ They propose drawing on Defense Department expertise in rapid, large-scale procurement.

On a limited scale, the Department of Justice is putting in place the necessary procedures to provide for acquisition of equipment which meets uniform standards to facilitate operations relative to terrorist acts within the U.S. which may involve numerous agencies and jurisdictions. The proposed National Domestic Preparedness Office (NDPO) within the Department of Justice, discussed supra, at pp. 22-23, would be one means by which to coordinate such an effort and to encourage state and local authorities to purchase equipment which meets such standards. In addition, in coordination with other agencies which have statutory authorities and programs for preparing for and responding to terrorist incidents involving weapons of mass destruction, including DOD, HHS, DOE, FBI, EPA and FEMA, the Department of Justice is establishing an acquisition mechanism through its Office for State and Local Domestic Preparedness Support, which will provide grants to state and local authorities to purchase equipment through the Department of Defense from an approved list of standardized items best suited for WMD response. These acquisitions must meet defined needs consistent with preparedness plans to be drafted locally. It is anticipated that this acquisition mechanism will begin functioning during FY99. Consideration should be given to an overarching acquisition mechanism which applies to counter-terrorism acquisitions which fall outside the scope of equipment needs of first responders and emergency personnel involved in state and local domestic preparedness.

⁸⁴ This approach was discussed at the Colloquium on Counter-terrorism at the Kennedy School of Government, Harvard University, July 10, 1998.

⁸⁵ We recognize that cyber R&D development and acquisition needs to be coordinated. However, development and acquisition of cyber technology is somewhat unique. Significant private sector infrastructure issues are but one aspect of cyber R&D which impact on whether an overall central mechanism should include cyber technology or whether the cyber area should be handled separately. This issue requires further study within the R&D and cyber communities.

In the Attorney General's April 1998 statement to Congress concerning the threat of chemical and biological weapons,⁸⁶ the Attorney General described the extraordinary acquisition requirements that could be created by a significant or catastrophic chemical or biological terrorist event. "We may need to develop an approach which will permit the government to accelerate the normal procurement procedures to quickly identify and deploy new technologies and substances needed to thwart terrorist threats and respond to terrorist acts. These procedures would be used not only to purchase medications and other needed tools, but also, in some instances, to borrow medications or tools from, or to enter into effective partnerships with both academia and industry." Such extraordinary acquisition needs could also arise in the context of a broad based conventional weapon terrorist attack or as the result of a cyber attack.

Congress responded to this need in the 1999 Appropriations Act for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies by providing expedited acquisition procedures under extraordinary circumstances. Section 115 of that Act provides that the Attorney General may use any appropriated counter-terrorism funds for the purchase or lease of equipment or services in the event of an exigent need for such equipment or services to support an ongoing counter-terrorism, national security, or computer crime investigation or prosecution which need cannot otherwise be timely met. This provision, which allows the Attorney General to by-pass normal acquisition rules and regulations, provides a mechanism to facilitate quick response in appropriate circumstances.

The Office of the National Coordinator, through the interagency Weapons of Mass Destruction Preparedness and Critical Infrastructure Coordination Groups, is exploring new ways of doing business in order to more expeditiously respond to new types of terrorist threat. With the provision of state and local input, these working groups - - or subgroups thereof - - could be charged to fully explore this concept and to develop a suggested approach or approaches. State and local input is important because two-thirds of the responders to the state and local questionnaire indicated a need for a point of contact on counter-terrorism technology issues, and because state and local personnel will be the end users of much of the tools, equipment, and other technology related to counter-terrorism.

CONCLUSION

The Conference Committee Report which called for the preparation of this strategic Plan directed that the Plan be updated annually to institutionalize coordination of national policy and operational capabilities in regard to counter-terrorism. These same aims are also at the core of PDDs 62 and 63, which provide for specific, progressive, and coordinated agency actions over the next several years to continue to strengthen our national counter-terrorism program and fortify our National Information Infrastructure. Our present assessment indicates that many of

⁸⁶ Statement of Attorney General Janet Reno, Hearings of the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information and the Select Committee on Intelligence, "The Threat of Chemical and Biological Weapons," April 22, 1998.

the specific proposals and recommendations in the Five-Year Plan correspond directly to requirements outlined in the PDDs. Thus, the PDDs and the Five-Year Plan should be viewed as complementary efforts to further our goal of increased readiness and capability to deal with terrorism and its consequences.

The Plan suggests a number of issues to be studied during the coming year. Although a few of these studies are mission-specific to certain agencies, many of them fall within the purview of the Weapons of Mass Destruction Preparedness Group, the Critical Infrastructure Coordination Group, and the numerous subordinate interagency working groups established to implement PDDs 62 and 63. The first annual review of the Plan should evaluate progress made in these studies and report any additional recommendations or other steps to be taken as a result of these studies. In addition, the first annual review should reassess whether feedback from the private sector through the network established pursuant to PDD 63 is sufficient and how this feedback ought to be incorporated into updates to the Plan.

The Plan is broad in scope and ambitious in its goals. It attempts to address comprehensively the mandate of the Conference Committee Report, particularly in the areas of emerging threats from chemical and biological agents and from cyber-attacks on computer systems as emphasized in the Report. It is hoped that the Five-Year Interagency Counter-Terrorism and Technology Crime Plan will serve as a baseline strategy for coordination of national policy and operational capabilities in this vital national security area.