S. HRG. 105–711

COUNTERTERRORISM—EVALUATING THE 5-YEAR PLAN

HEARING

BEFORE A

SUBCOMMITTEE OF THE

COMMITTEE ON APPROPRIATIONS

UNITED STATES SENATE

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

SPECIAL HEARING

Printed for the use of the Committee on Appropriations

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE

51–901 cc WASHINGTON : 1998

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0–16–057751–9

COMMITTEE ON APPROPRIATIONS

TED STEVENS, Alaska, *Chairman*

THAD COCHRAN, Mississippi
ARLEN SPECTER, Pennsylvania
PETE V. DOMENICI, New Mexico
CHRISTOPHER S. BOND, Missouri
SLADE GORTON, Washington
MITCH McCONNELL, Kentucky
CONRAD BURNS, Montana
RICHARD C. SHELBY, Alabama
JUDD GREGG, New Hampshire
ROBERT F. BENNETT, Utah
BEN NIGHTHORSE CAMPBELL, Colorado
LARRY CRAIG, Idaho
LAUCH FAIRCLOTH, North Carolina
KAY BAILEY HUTCHISON, Texas
ROBERT C. BYRD, West Virginia
DANIEL K. INOUYE, Hawaii
ERNEST F. HOLLINGS, South Carolina
PATRICK J. LEAHY, Vermont
DALE BUMPERS, Arkansas
FRANK R. LAUTENBERG, New Jersey
TOM HARKIN, Iowa
BARBARA A. MIKULSKI, Maryland
HARRY REID, Nevada
HERB KOHL, Wisconsin
PATTY MURRAY, Washington
BYRON DORGAN, North Dakota
BARBARA BOXER, California

STEVEN J. CORTESE, *Staff Director*
LISA SUTHERLAND, *Deputy Staff Director*
JAMES H. ENGLISH, *Minority Staff Director*

SUBCOMMITTEE ON COMMERCE, JUSTICE, AND STATE, THE JUDICIARY, AND RELATED AGENCIES

JUDD GREGG, New Hampshire, *Chairman*

TED STEVENS, Alaska
PETE V. DOMENICI, New Mexico
MITCH McCONNELL, Kentucky
KAY BAILEY HUTCHISON, Texas
BEN NIGHTHORSE CAMPBELL, Colorado
ERNEST F. HOLLINGS, South Carolina
DANIEL K. INOUYE, Hawaii
DALE BUMPERS, Arkansas
FRANK R. LAUTENBERG, New Jersey
BARBARA A. MIKULSKI, Maryland
ROBERT C. BYRD, West Virginia
(ex officio)

Subcommittee Staff
JIM MORHARD
KEVIN LINSKEY
PADDY LINK
DANA QUAM

SCOTT GUDES *(Minority)*
EMELIE EAST

Detailees
CARL TRUSCOTT
DEREK ORR

CONTENTS

DEPARTMENT OF JUSTICE

COUNTERTERRORISM—EVALUATING THE 5-YEAR PLAN

TUESDAY, MARCH 31, 1998

U.S. SENATE,
SUBCOMMITTEE ON COMMERCE, JUSTICE, AND
STATE, THE JUDICIARY, AND RELATED AGENCIES,
COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 9:57 a.m., in room S–146, the Capitol, Hon. Judd Gregg (chairman) presiding.

Present: Senator Gregg.

Also present: Senator Shelby.

DEPARTMENT OF JUSTICE

STATEMENTS OF:

HON. JANET RENO, U.S. ATTORNEY GENERAL

HON. LOUIS J. FREEH, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Senator GREGG. It is a little early, and I certainly appreciate the Attorney General and the Director being here early. But I suspect there are other Senators that are going to come, so I will make my statement and take it up to 10 o'clock, and, hopefully, the other members will be here.

We do have a vote at 10:30, and I would hope that we could get the opening statements of the Attorney General and the Director in before that, and then come back and do questions right after the vote.

The purpose of this hearing is to review the efforts of the agencies, of the Justice Department, specifically, but the agencies generally within the Government that are charged with the question of counterterrorism and protecting our country from terrorist acts.

A couple of years ago this committee became very focused on this issue, and initiated the first major expansion of funding in the area of counterterrorism. The purpose of that was to assist the FBI, specifically, and other agencies throughout the Government in being able to pursue an effective counterterrorism strategy. That has been very successful in the sense that it has brought about an expediting of planning and an expediting of the efforts of coordination. As chairman, I have had a chance to visit almost all the major agencies involved in counterterrorism, not only those that are under the jurisdiction of this committee, but also agencies outside the jurisdiction of this committee.

This committee does have a large jurisdiction, because it has both the FBI and the Justice Department, which have the domestic responsibility, and it has the State Department, which has the international responsibility. And in visiting these agencies, I must say I have been impressed with the energy, the enthusiasm, and the commitment and the sincerity of the commitment in trying to develop a coordinated counterterrorism strategy for the country.

But we are clearly in the infancy stage. We are not, by any stretch of the imagination, at a point where we have a mature program that is effectively functioning and that really is not the failure of the Government agencies involved. It is simply the factor of the threats changing so radically as we move into this part of the history of man—especially the expansion of weapons of mass destruction—something that had not really been anticipated at the level it is today, even just a few years ago. We did not know the effects that terrorist action can have on the infrastructure, which has now become so electronically dominated.

Those two factors, which really were not a high visibility threat just 5 years ago, are today not only a high visibility threat, but a legitimate threat, and something that we have to address. So tooling up to address those factors, those two areas, has been and will continue to be an intense and complex effort. I certainly respect and congratulate the various agencies that have been involved in this.

The primary concern of this committee is the jurisdiction of the Justice Department and the State Department, but we have attempted, as a committee, to try to push a coordinated strategy. As part of that we asked for a report which the Attorney General is going to talk about today, which would develop a core around which we could develop a strategy. I look forward to hearing about that report.

In addition, we have as a committee made a commitment of resources which is considerable. We want to make sure those are not being duplicated in other departments, but are going toward the specific needs that we have assessed as necessary in order to address this threat.

In sort of a declining level of threat, the first threat is weapons of mass destruction, exercised either by individuals or by other nations. The second threat is the threat to our infrastructure, especially the technology threat to our infrastructure. The third threat is an individual acting as a free lancer, or an individual group acting as a free lance group, which commits a terrorist act. Each one of these threats take different response structures and fairly complex response structures.

The question is, are we putting together a process which adequately anticipates the threat, and, hopefully, gives us the opportunity to cut it off before it occurs, not only domestically, but internationally? Second, if we have an event occur, are we adequately equipped to respond to it both from a standpoint of taking care of the damage and the injuries which may occur and also pursuing the perpetrators. Those are the elements that need to be addressed in any comprehensive counterterrorism strategy.

The problem is that we have, by my count, something like 15 different agencies which are charged at some level with counter-

terrorism responsibility. They are across the Government, and the coordination of those agencies is what the first step has to be—making sure that they are talking to each other and that there is a central, coordinated approach to the issue.

PREPARED STATEMENT OF SENATOR GREGG

And so that is what the committee asked the Attorney General and the FBI to develop, and we are going to hear today as to how that is proceeding. There have been press reports relative to, regrettably, some turf issues, which, hopefully, we can address today. We can talk a little bit about where we need to go from here, as we go from the process of developing a strategy to the process of implementing one.

[The statement follows:]

PREPARED STATEMENT OF SENATOR JUDD GREGG

I want to thank the Attorney General and the FBI Director for coming here today. Terrorism is both a threat to our national security as well as a criminal act. We must use all appropriate means to deter, defeat, and respond to terrorist attacks.

That is why last year, this subcommittee directed the Attorney General to prepare a plan that would lead us to being pro-active to the threat and also be able to respond to a terrorist event.

While the number of terrorist incidents has declined in recent years, the level of violence and lethality of attacks has increased. There is a continuing trend toward more ruthless attacks on civilian targets. Also, the capability of hostile nations and terrorists groups to acquire weapons of mass destruction is greater than ever before.

Until this decade, biological and chemical weapons were the province of superpowers or renegade states like Iraq and North Korea. All that changed with the Aum Supreme Truth sect in Japan. The cult's scientists produced anthrax, botulin toxins and sarin.

We talk of weapons of mass destruction and you immediately think of nuclear weapons. A nuclear incident is actually a less likely scenario than biological or chemical weapons attacks.

Also, we must begin to educate people on the risks involved with computer systems that make up much of our critical infrastructure. It is now reported that six out of ten businesses, government offices, and universities are reporting computer security breaches. Many incidents continue to be adolescent pranks, but security experts universally agree that the political and financial risks of break-ins will rise.

The plan we directed the Attorney General to do is in its first phase. The working groups have been assembled. They will address prevention, deterrence, crises management, consequence management, cyber-terrorism, critical technologies and R&D. These working groups are made up of DOJ, FBI, DOD, Treasury, CIA, NSA, DOE, EPA, FEMA, PHS, FAA, Commerce, and DOT.

I commend the Attorney General for her effort on this important issue. None is more important to this Nation. And no one wants to look back and say we could have done more.

ATTORNEY GENERAL'S OPENING STATEMENT

Senator GREGG. I thank the Attorney General and the Director for being here, and since it is 10 o'clock we shall proceed. So, Madam Attorney General.

Ms. RENO. Thank you, Mr. Chairman.

Mr. Chairman, I think I speak for Director Freeh, as well. We both appreciate the leadership that you have shown in this area. The great time and effort that you have put into visiting the agencies, understanding the issues, and prodding all of the Government to come together to develop cohesive plans that can effectively address modern day terrorism.

FIVE-YEAR COUNTERTERRORISM PLAN

One of the points that you have raised is your desire as spelled out in the appropriations bill for a 5-year interagency counterterrorism and technology plan.

As you know, we have submitted to you an outline of issues for a 5-year interagency counterterrorism and technology crime plan, and have gone over it with you and will continue to keep you apprised as we prepare this plan. It is my expectation that the final plan will constitute a road map of counterterrorism efforts for the next 5 years, which will demonstrate both the existing strength and future enhancement of these interagency efforts.

It will be tied in with the spending plan that you again have taken the leadership to mandate, which I think has already proven to be a useful tool in making sure that we use our limited dollars as wisely as possible, building on appropriations efforts in the various agencies.

CURRENT RESPONSE TO TERRORIST ATTACKS

Our primary objective is to prevent terrorist attacks before they occur. I think we spelled that out clearly in the strategy. The life blood of prevention, however, is foreign intelligence information from the intelligence community about the identity, the plans and the movement of international terrorists, and information developed by the FBI about the activities of terrorist groups in this country.

The FBI vigorously and appropriately develops information from a variety of sources, consistent with the Attorney General guidelines, on general crimes, racketeering enterprise, and domestic security terrorism investigations. Information about terrorist threats is shared with appropriate agencies in a threat assessment conference which analyses the threat, determines whether it is plausible, and how the threat might be carried out; then prepares and positions the appropriate resources to respond to the threat.

The procedures for responding to threatened or actual terrorist events represent more than just abstract plans. They have been developed based on lessons learned in responding to past terrorist events.

I would like to publicly commend Director Freeh for the leadership that he has shown in a number of arenas with respect to the prevention of terrorist attacks in the United States, with the thoughtful way that he has approached it, in terms of gathering the information, consistent with the guidelines, working with State and local agencies across the country, and, I think, taking very effective action.

Many of these plans have been the subject of tabletop and field training exercises which facilitate the development of important coordinative relationships and the identification of those procedures which require modification of refinement.

When we are confronted with a major terrorist act within the United States, it is almost always local authorities who are the initial responders. It is their efforts in the minutes following a terrorist act that we rely on to save lives, contain the scope of the crisis, and apprehend terrorists who may be fleeing the scene. It is for

this reason that programs that provide training and support for local authorities such as those provided by the Defense Against Weapons of Mass Destruction Act of 1996 are so important.

As a matter of established practice, local authorities quickly notify the local FBI office of the event. Bureau field offices are trained to initiate immediately and simultaneously a number of responsive actions when confronted with a major terrorist act. Those actions, which are undertaken in coordination with the other agencies, include the initiation of a site survey of the crime scene to assess the potential of continuing danger and to evaluate preliminarily the relevant forensic aspects of the crime; coordinate with local emergency responders in an effort to insure optimal efforts to save lives while preserving evidence important to a later prosecution; notification of headquarters and the local U.S. attorney's office.

They form a joint operation center in proximity to the crime scene to bring together representatives of all pertinent Federal, State, and local agencies; they identify and coordinate with the U.S. attorney and local authorities a central point of contact for the dissemination of information to the public. And I think under Director Freeh's leadership what was done in Oklahoma City, with Oklahoma City police, with so many people working together was a classic example of how it should be done.

INVOLVEMENT OF STRATEGIC INFORMATION OPERATIONS CENTER

While these activities are underway in the field, the headquarters in Washington immediately act to bring together the pertinent headquarters support staff. The Strategic Information Operations Center [SIOC] is immediately activated and staffed on a 24-hour basis. It combines the resources and expertise of representatives of 19 Federal agencies, which support this effort, and the representatives of the pertinent agencies are integrated into the SIOC operation.

Additionally, officials at headquarters coordinate through the SIOC, and evaluate with the Bureau's on scene commander and the local U.S. attorney the deployment of additional specialized resources to the scene. These resources include experts in explosives, bomb scene reconstruction, and evidence preservation; specialized units such as evidence response teams, hazardous materials response unit, and a rapid start computer data base team.

This has been fascinating to watch, the use of the rapid start system, and the ability of the Bureau to assimilate in very rapid fashion pieces of data from so many different parts of the investigation into an inclusive whole that can be used so effectively, both to identify the perpetrator and to prepare the case. And this early ability to respond in that fashion, I think, has proven essential in some of our successes.

Agents with pertinent skills from surrounding Federal investigative field offices are made available. FBI SAC's with specialized training in crisis response are available on a 24-hour basis. Where multiple SAC's are sent in to augment the local SAC, one is selected as the overall on scene commander.

In addition, we have attorneys who are trained in critical incident response available to advise and assist the local U.S. attorney.

DOMESTIC EMERGENCY SUPPORT TEAM

When appropriate, the FBI can activate the domestic emergency support team [DEST], which is an interagency team that can be tailored to the needs of the specific terrorist event, and is available to be air lifted to the scene within a matter of hours.

Its function is to provide the expert guidance that is necessary, especially to address chemical, biological, and nuclear incidents. The chem-bio module combines the expertise of representatives from the FBI, DOD, the Public Health Service, EPA, and FEMA. The nuclear radiological module combines the expertise of representatives of the Bureau, the Department of Energy, the Department of Defense, the Public Health Service, and FEMA.

Through the utilization of these and other procedures, it is possible for the Department of Justice and the FBI, working together with other agencies to quickly mount a major, highly trained response to a terrorist threat or act. That response is designed to integrate the efforts of all involved through the Joint Operations Center, while using the SIOC to insure that nationwide and pertinent worldwide support from all appropriate Federal agencies is available in a prompt and coordinated manner.

While we believe that the response plan is sound, we recognize that the threat posed by chemical, nuclear, and biological weapons poses tremendous challenges that require that capabilities and coordination be enhanced at all levels of Government.

TRAINING EXERCISES

Training exercises are conducted frequently to evaluate progress. For example, the FBI's critical incident response group [CIRG] sponsors eight regional crisis management training exercises annually, many of which involve weapons of mass destruction. Each exercise involves personnel from FBI headquarters and multiple field offices, as well as other pertinent Federal, State, and local agencies.

ENCRYPTION

Let me briefly address one problem that is posed to our terrorism and enforcement efforts by developing technology. The widespread use of strong encryption by terrorists and other criminals, unless it provides for lawful access to plain text by law enforcement authorities, would have catastrophic implications for our ability to detect, prevent, and investigate terrorism. Unbreakable encryption allows terrorists to communicate about their criminal plans with impunity. Developing a balanced approach to robust encryption is an extremely serious public policy issue that urgently, urgently needs to be resolved, and requires attention from Federal, State, and local Government officials and from the private sector.

To this end, the administration has launched a focused initiative to work closely with the information technology industry to develop technical and policy solutions that represent balanced approaches to strong encryption. We have requested a legislative moratorium on encryption matters while we attempt to develop these solutions. Another problem posed by evolving technology relates, as you have pointed out, to cyberterrorism.

To date, U.S. interests have not been victimized by cyberterrorism. However, the potential is clearly present, and the significance of the threat is reflected in the work of the President's Commission on Critical Infrastructure Protection, which issued its report in October 1997.

CYBERCRIME

One unique challenge presented by computer crime is that it knows no geographic bounds. As a result, we have established local, regional, and national capabilities to provide the flexibility necessary to address this type of crime.

Additionally, we are working with our foreign counterparts through, for example, a subcommittee of the eight, the Council of Europe, and the Organization for Economic Cooperation and Development to develop effective mechanisms for coordination.

In February 1998, I announced the formation of the National Infrastructure Protection Center, which encompasses and expands the mission of the FBI's Computer Investigations and Infrastructure Assessment Center, which was formed in 1996.

One of the strengths of the NIPC is that it integrates the efforts of two Federal agencies which shared jurisdiction over cybercrime—the Secret Service and the FBI. Additionally, we have formed regional FBI computer crime squads with technical skills and equipment. These squads work closely with the computer telecommunications coordinator [CTC] in each U.S. attorney's office within their region. All U.S. attorney's offices now have a specially trained CTC.

Utilizing these resources and coordination arrangements, we are preparing ourselves to address potential acts of cyberterrorism. Investigators and prosecutors are trained to work backward through the chain of victim systems to locate the criminal at the source. They are also trained to work forward to identify other victims and to ascertain the full scope of the crime.

While we are at the early stages of our preparations to address this type of terrorist attack, much progress has been made in a short time, and we are committed to the expeditious continuation of this effort.

One aspect of this effort is to overcome the lack of up-to-date tools in the arsenal of the Federal Government, and to identify equipment that is necessary. In addition, Federal personnel sometimes lack the appropriate training and expertise in the cyber area to effectively interact with the private sector and to draw on its expertise.

It is critical that we reach out to industry and academia to identify areas in which we can be effective partners. I am committed to such a process, and the FBI, using the resources that you provided in fiscal year 1998 is undertaking such an effort.

We will be working with industry to enhance the skill of our employees, and to seek their advice on the latest state-of-the-art equipment and other tools necessary to meet our counterterrorism responsibilities. Although we have not yet reached a final conclusion, I think that we may need to develop an approach that would permit the Federal Government to accelerate the normal procure-

ment procedures, and quickly identify and deploy new technology in order to thwart terrorist threats.

These procedures would be used not only to buy new tools, but also, in some instances, to borrow tools or enter into effective partnerships with both academia and the industries as a way to address potential terrorist threats.

As part of our work with you to develop the 5-year counterterrorism strategic plan, we will be presenting proposals to you on how we can rapidly address these new issues. A major approach will be the establishment of partnerships with industry. Further, we anticipate establishing a mechanism for sharing the benefits of this overall effort, including the most recently developed technology and training with our State and local partners. You and I have talked about that issue, both with respect to forensic labs around this country, and with respect to these complex, expensive forensic tools. And I think we need to develop means of, regionally and on a State and local basis, sharing these tools so we do not have to spend a lot of money and duplicate each other's efforts.

OVERSEAS TERRORIST ACTS

Turning to terrorist acts overseas, during the past two decades, U.S. Government facilities in other countries, and Americans traveling outside the United States have been the target of choice for international terrorists. U.S. policy for responding to such acts combines diplomatic, intelligence, military, and criminal justice resources. The objective of that policy is to deter, defeat, and respond vigorously to all acts of international terrorism against U.S. interests.

It is a critical part of that policy that we apprehend and prosecute those who plan or perpetrate such attacks. It is not unusual for these investigations and the apprehension and rendition of defendants for trial in the United States to take years to complete. However, in our commitment to the effort, our effort is absolutely steadfast. Our memory is very, very long.

With deference to the committee's time this morning, I would refer you to my written statement for a full description of how we have responded in these instances. Much progress has been made during the past few years in preparing the United States to prevent acts of terrorism and to respond to the terrorist threats that do arise.

PREPARED STATEMENT

However, many challenges remain, including particularly those relating to the weapons of mass destruction and the cyberterrorism threat. Through the process of developing the 5-year counterterrorism and technology plan we will continue to address an interagency response to these challenges, and to work with the committee in this effort.

Thank you.

[The statement follows:]

PREPARED STATEMENT OF JANET RENO

INTRODUCTION

It is my privilege to appear before you today for the purpose of continuing the Department of Justice's discussions with you on our efforts to combat the scourge of terrorism.

When I testified before the Senate Appropriations Committee last September, I outlined the Government's policy in dealing with acts of terrorism, the government's strategies to deter and prevent terrorist acts, and the government's abilities to respond quickly and decisively to terrorist acts. I also addressed our growing capabilities to detect, prevent, defeat, and manage the consequences of nuclear, biological, and chemical material and weapons used by terrorists. I would like to use this opportunity today to highlight for you our progress in these areas. I would also like to address the challenges posed by our growing interdependence of critical infrastructures and the Department's response to the report and recommendations of the Presidential Commission on Critical Infrastructure Protection in October 1997. In particular, I will address the Department of Justice's creation of the National Infrastructure Protection Center (NIPC) within the Federal Bureau of Investigation. Finally, I would like to focus my testimony on the processes of interagency cooperation and consultation that we draw upon when we have to respond to and investigate terrorist incidents in the United States and abroad. These processes are increasingly indispensable to our efforts to confront the challenges posed by cyberterrorism, weapons of mass destruction, and protection of critical infrastructures against terrorist threats.

Mr. Chairman, you and this subcommittee have provided outstanding leadership focus on improving the processes for interagency cooperation and consultation in counterterrorism activities and on enhancing the technological capabilities of all entities with counterterrorism missions. The Conference Committee Report accompanying the 1998 Department of Justice Appropriations Act directs the Attorney General to develop a 5-year interdepartmental counterterrorism and technology crime plan to serve as a baseline strategy for coordination of national policy and operational capabilities to combat terrorism. The plan is to be representative of all agencies involved in the government's counterterrorism effort and to draw upon the expertise of academia, the private sector, and state and local law enforcement. The final plan must be submitted by December 31, 1998, and updated annually thereafter. In close cooperation with my colleagues across the government, I intend to devote the full resources of the Department of Justice to developing and implementing this plan. Accordingly, I have established an interagency resource and review group, composed of representatives of key federal agencies with counterterrorism responsibilities. Efforts are now underway to collect information and insights from them concerning their current and proposed programs and recommendations for action that need to be taken during the next five years to improve the counterterrorism capabilities of the United States.

You are correct in the assessment, Mr. Chairman, that for the Federal Government to carry out its counterterrorism efforts, we must develop and sustain effective partnerships not only with state and local law enforcement but also with industry, including the national laboratories, and academia as well. The threat, particularly in the area of cybercrime, requires expertise and equipment often difficult for the Federal Government to acquire through normal processes. We must develop flexible mechanisms that will allow us to engage in effective partnerships with industry and academia as well as enhance Federal resources in this area.

One of the criticisms that I have heard from experts in this area is that often the Federal Government does not have up-to-date tools and equipment within its own inventories. In addition, Federal personnel in some cases do not have appropriate training and expertise in the cyber area in order to effectively interact with the private sector and draw upon its expertise. You very ably pointed out during last year's hearing that we need to reach out to industry and academia to identify areas in which we can be effective partners. I am committed to such a process and have directed the FBI, using the resources that you provided in the fiscal year 1998 appropriation, to undertake such an effort. We will be working with industry to enhance the skills of our employees and to seek their advice on the latest state-of-the-art equipment and other tools necessary to meet our counterterrorism responsibilities.

The Congress has been generous in providing the Department additional resources, but I believe in the future we also will have to think outside of the normal Federal Government processes. Too often, the normal processes did not allow us to react to significant technological changes that impact our mission at the same pace at which the changes occur.

Although we have not come to a conclusion on this, Mr. Chairman, I think that we may need something along the lines of a Counterterrorism Technology Rapid Response mechanism. Such an approach would allow the Federal Government to accelerate the normal procurement procedures and quickly identify and deploy new technology in order to thwart terrorist threats. I am not saying these resources would only be used to buy new tools; they would in some cases allow us to borrow tools from or enter into effective partnerships with both academia and industry as a way to address potential terrorist threats. As part of our work with you to develop the Administration's five-year counterterrorism strategic plan, we will be presenting proposals to you on how we can rapidly address new threats. A major approach will be the establishment of partnerships with industry.

However, in the meantime, I think it is important that we focus on the resources that you have provided to us in fiscal year 1998 as well as those resources we have requested as part of the 1999 budget. I have asked Director Freeh to reach out to the appropriate experts in industry and academia to review with them our plans to acquire new tools to combat terrorism. We need to assure ourselves, the Congress, and the American people that we are acquiring the best available in this area. I will keep you apprised of our progress.

Not only do we need to acquire new technology in order to thwart terrorism, but we need to ensure that we have a federal workforce that can effectively deal with our new partners in industry and academia. One concern that has been brought to my attention is that often the federal government is not sufficiently grounded in the new technologies in order to be an effective partner with industry and academia. Using the statutory flexibility that you have given to us in the fiscal year 1998 appropriation, we are committed to developing a personnel process that will allow us to retain employees that can be effective partners with industry and academia in dealing with new emerging technologies. We also need to focus on how we provide continual training in these technologies to the federal workforce. Given the fact that new technologies appear to be deployed every 18 months, we must ensure that our workforce can keep abreast with the new developments.

I have also asked the FBI to establish a mechanism for sharing the benefits of this overall effort, including the most recently developed technology and training, with our state and local partners.

Let me emphasize again that the protection of our nation and its people from acts of domestic and international terrorism is among the greatest challenges faced by this Administration and one of the highest priorities of the Department of Justice. Over the past two decades, it has become clear that American citizens and interests may be the targets of terrorists.

Whatever the origin or misguided motivation of the particular terrorist or terrorist group, the potential consequences of a single terrorist incident can be enormous. For example, the magnitude of human suffering flowing from acts of terrorism such as the bombing of Pan Am Flight 103 is incalculable.

Events such as the World Trade Center bombing in New York City and the bombing of the Murrah Federal Building in Oklahoma City, pointedly demonstrated that acts of terrorism are not confined to foreign lands. Here at home, citizens going about their daily work, and even children entrusted to day care, may also be struck down without reason or warning.

The challenge that terrorism presents to a free society is that we must aggressively act to prevent and respond to such acts, using all the tools and techniques at our disposal, while still fully respecting the individual rights and liberties for which this nation stands. Striking this balance, we have made much progress in the past several years, successfully preventing a number of potentially deadly terrorist attacks at home and abroad while enforcing and strengthening the rule of law. We have demonstrated that our commitment is unflagging and our memory is long. But much work remains to be done.

The policy of our government in dealing with acts of terrorism, both at home and abroad, remains unchanged. We will do everything possible to deter and prevent terrorist attacks. When acts of terrorism do occur, we will respond quickly and decisively, with the full array of options that we have available. We will work with our friends throughout the world to interdict terrorists and ensure terrorist acts do not go unpunished. The strategic plan we are presently developing will provide a roadmap for the further refinement and implementation of this policy over the next five years.

Since I last testified on this subject before this Subcommittee, the President's Commission on Critical Infrastructure Protection (PCCIP) has submitted its report to the President. The PCCIP report properly emphasizes the vulnerability of each of our major infrastructures to willful misconduct, including terrorism. Terrorists can damage or destroy elements of our infrastructures either by physically attacking

them, or by launching cyber-based attacks aimed at disrupting the physical infrastructures' computer and communications systems. As we develop and position our resources to cope with these new threats, we must also remain vigilant against more traditional terrorist threats.

NATURE OF THE TERRORIST THREAT

Terrorist threats are both old and new. The heart-wrenching pictures of the nose section of the 747 that was Pan Am 103 in a field near Lockerbie, Scotland, or the half-standing building in Oklahoma City, remind us of long-used terrorist weapons: bombs. But newer threats abound. Chemical and biological weapons are now a potential part of the terrorists' arsenal, as made clear by the use of Sarin gas in the Japanese subway system. And software code may yet become another terrorist weapon. Indeed, seven years ago, the National Research Council predicted that "Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."

So what is the nature of the terrorist threat? It comes in three primary forms: conventional weapons (including incendiary devices), weapons of mass destruction, and cyberattacks.

Conventional Weapons

The bombings of the World Trade Center and the Murrah Federal Building are recent examples of the physical security vulnerabilities inherent in an open society. Such physical attacks could take on even more serious dimensions, however, if the bomb were placed at a carefully selected critical infrastructure facility. In addition to the death or destruction caused directly by the bomb, an explosion caused by a terrorist act could potentially destroy or disable elements of a specific infrastructure on a regional or national scale and could cause harm and possibly injury or loss of life to a significant portion of our population dependent upon that critical infrastructure.

Weapons Of Mass Destruction

As nuclear, chemical or biological weapons of mass destruction become more accessible, we face the potential of even more catastrophic acts of terrorism. In particular, chemical or biological weapons are relatively inexpensive to produce but have the capability of causing widespread death if released on an unsuspecting populace. The nerve gas attack in the Tokyo subway by members of the Aum Shinrikyo cult was a grim warning of this potential.

Further, as the United States and the former Soviet Bloc members proceed to dismantle their nuclear weapons, the potential exists that weapons-grade nuclear materials may fall into the hands of a terrorist group or a rogue political organization bent upon nuclear blackmail. Although our nation has not yet experienced such a threat, we must anticipate, plan and prepare for such an occurrence as we and former Soviet Bloc nations continue disarmament.

Cyberattacks

As we become increasingly reliant on the Global Information Infrastructure (GII), our information systems present an ever more attractive target for terrorists. At the same time, because the GII is itself a vast array of distinct networks with complex interrelationships and dependencies that are not yet fully understood, defining the vulnerabilities remains difficult. For example, a cyberattack on a telecommunications network may affect not just private communications, but transportation systems, banking systems, and the availability of critical government services, such as police and fire fighting.

By way of example, many energy facilities use Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems control a variety of energy facility components, such as electric power plants and oil and gas pipelines. As SCADA systems become more widespread and more interconnected, terrorists have increased opportunities to use publicly available as well as covertly obtained cyber techniques to damage critical energy infrastructures. More specifically, a large number of SCADA systems have simple dial-up access for remote maintenance which allows problems to be handled quickly by a computer engineer but also may make the system more vulnerable to cyber attack. Additionally, many SCADA systems use commercial off-the-shelf hardware and software with vulnerabilities known to individuals outside the energy industry. Other SCADA systems are connected to corporate computer networks with indirect connections to the Internet. As a result, many energy operating systems that were previously unknown or inaccessible to outside parties are now subject to possible cyber attack. An attack on a SCADA system would be potentially

devastating because it could affect not only the energy industry, but other critical infrastructures elements of which depend on the affected energy facilities.

Through the 5-year strategic plan we are currently developing in close coordination with other departments and agencies, we will outline how the federal government, in coordination with state and local authorities and the private sector, can improve its capabilities to prevent and deter all of these threats.

Moreover, the continuing development of technology itself is posing challenges to law enforcement's ability to keep pace with terrorists and others who seek to do harm to our nation and our nation's citizens using either conventional weapons, weapons of mass destruction, or cyberattack tools. For example, the widespread use of strong encryption by terrorists and other criminals, unless it provides for lawful access to plaintext by law enforcement authorities, would have catastrophic implications for our ability to detect, prevent, and investigate crime and terrorism. Unbreakable encryption allows terrorists to communicate about their criminal plans with impunity and to maintain electronically stored evidence of their crimes and records necessary to conduct their criminal operations immune from lawful search and seizure. Developing a balanced approach to robust encryption is an extremely serious public policy issue that requires attention and engagement by federal, state, and local government officials and by the people and businesses whose public safety law enforcement officers have sworn oaths to protect. To this end, the Administration has launched a focused initiative to work closely with the information technology industry to develop technical and policy solutions that represent balanced approaches to strong encryption. We have requested a legislative moratorium on encryption matters while we attempt to develop these solutions.

There can be no question that the policy issue of encryption urgently needs to be resolved. As noted, our counterterrorism mission will encounter serious difficulties if we are unable to obtain access to the plaintext of data and communications when lawfully authorized. Moreover, unless we achieve a balanced resolution of the issues presented by encryption, the private sector will only reluctantly, if at all, enter into the full spectrum of information, people, and technology partnerships with the government that are needed in order to prevent, deter, and effectively respond to terrorism. It is therefore vital that in the next several weeks, we in the government and our private sector partners pursue solutions that both address the immediate issue of encryption and also build up the trust and collaboration that are needed if we are to make progress on all counterterrorism fronts.

ORGANIZATION OF THE FEDERAL GOVERNMENT TO PREVENT AND RESPOND TO TERRORISM

In my appearances before the Senate Appropriations Committee last May and before this Subcommittee in September 1996, I described the Administration's strategies for preventing, responding to, and prosecuting terrorist activities against United States citizens and interests. Today I'd like to focus on a related subject, one which is complementary and equally important—the question of how the federal government has organized its resources and its decision-making processes to respond to terrorist events. My focus will be on how the departments and agencies of the federal government, together with state and local authorities, are increasingly working together to implement and advance the Administration's counter-terrorism strategies. These interagency mechanisms and resources to address terrorist threats are the baseline from which we will be developing the five-year strategic plan to further enhance our existing processes. Even today, the close interaction among agencies produces insights and strengths that no agency acting alone would have. To be frank, however, the close partnerships that Cabinet-level departments and other agencies have necessarily entered into also produces, on occasion, tensions arising from the organizations' differing statutory missions, authorities, restrictions, and perspectives that we all need to work through together.

I would like first to talk about intelligence production and the mechanisms for senior level coordination in the event of a terrorist incident, and then I will address how we respond to international and domestic terrorist incidents in turn.

Intelligence Collection and Assessment

Of course, our primary objective is to prevent terrorist acts before they occur. Intelligence is the lifeblood of prevention since it provides the United States with timely information about the identity, motives, movements, plans, resources, and possible allies of the perpetrators. The CIA is responsible for the collection, analysis and dissemination of foreign intelligence regarding terrorist groups. Its efforts are coordinated by its Counterterrorist Center (CTC). The Department of Defense, similarly, engages in the collection, analysis and dissemination of foreign intelligence that relates to the mission and security of U.S. Forces abroad. Where such informa-

tion concerns a possible attack upon United States interests here or abroad, it is furnished to the FBI which uses it either to assist in the development of an on-going investigation or to open a new one. In either event, the FBI disseminates the information to the responsible field office.

The FBI collects, analyzes, and disseminates intelligence on the activities of international terrorists targeting interests within the United States and terrorist groups operating in this country. This information is used to disseminate early warnings to targets of terrorist activity, and, when there is sufficient basis, to open investigations of individuals or organizations who are planning or preparing to commit terrorist acts.

Senior Level Interagency Coordination

Information concerning the possibility of an imminent terrorist attack may be developed by any one of a variety of federal agencies, including the FBI, CIA, DOD, and the State Department. Where credible information is developed, the government has specific procedures to facilitate a prompt, coordinated interagency response.

If the threat involves either a potential act of terrorism against U.S. interests overseas or an international terrorist act within the United States, coordination of issues requiring interagency review is handled through the Coordinating Sub-Group (CSG) of the Deputies Committee. The Deputy secretaries and equivalents of the Cabinet agencies comprise the Deputies Committee; its purpose is to increase interagency coordination, cooperation and decisionmaking at the chief operating officer level and to provide coordinated advice and views to the Cabinet secretaries and their equivalents and to the President. The agency coming into possession of the information immediately notifies the office of the NSC official who chairs the CSG, which has the capability of convening an emergency meeting of that group, via teleconference, in a matter of minutes. For potential acts of terrorism within the United States that are not of an international nature, the same expeditious coordination mechanism is available, except that the Department of Justice, through the FBI, is the organization which convenes and chairs the meeting.

The regular CSG members include the State Department, Defense Department, CIA, FBI, and Department of Justice. The CSG is also able to notify and involve its established points of contact in a variety of other federal agencies when the circumstances of the particular terrorist threat warrant the inclusion of one or more of those agencies. They include the Departments of Energy, Transportation, Treasury, Health and Human Services, Agriculture, as well as FEMA, EPA, and the NRC. For example, for a threatened terrorist act involving a chemical weapon, the CSG meeting would include, in addition to the regular components, representatives from the Public Health Service of the Department of Health and Human Services, the EPA, and FEMA.

Among the actions which the CSG can recommend to the Deputies Committee is deployment of either a Foreign Emergency Support Team (FEST) or a Domestic Emergency Support Team (DEST). Specialized modules of these teams can be called on as needed to address chemical, nuclear, and biological threats or acts of terrorism. Once activated, a FEST or DEST team can quickly assemble its components at the incident area within a few hours. Once on site, the FEST or DEST team is available to provide expert, highly specialized advice and guidance concerning the most appropriate response to the terrorist threat or incident. This on-site information, in turn, provides an informed basis for further decision making concerning the deployment of additional federal resources.

Interagency response capabilities are exercised, through either tabletop or field training exercises, to facilitate coordinated interaction.

Responding to Domestic Incidents

Crisis Deployment Strategy

Presidential Decision Directive 39, known as "PDD–39", sets forth lead agency responsibilities for combatting terrorism, including responding to terrorist incidents. The Department of Justice, and in particular the FBI, has lead responsibility for responding to terrorist threats and incidents occurring within the United States. As described in PDD–39, 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.

The Department has drafted "Guidelines for the Mobilization Deployment and Employment of U.S. Government Agencies In response to a Domestic Threat or Incident In Accordance With PDD–39." These Guidelines, which have not been fully approved yet but are in the final stages of interagency coordination, are also known as the "Domestic Guidelines"; they serve as coordinating measures within the framework of PDD–39 and are designed to enhance the capability of the U.S. Government to respond to terrorism. The Domestic Guidelines also were formulated to facilitate interagency coordination in support of the FBI's lead role in combating domestic terrorism, to delineate command responsibilities, and to address the use of the Domestic Emergency Support Team (DEST) and the Joint Operations Center (JOC). Additionally, the Domestic Guidelines:

—detail the roles and responsibilities of federal agencies in responding to a terrorist incident, including one involving a weapon of mass destruction (WMD). These include those of the On-Scene Commander and DEST Team Leader, DEST training and exercise programs, formation and structure of the DEST and JOC, and interagency responsibilities during WMD incidents.

—detail the roles and responsibilities of federal agencies in responding to a terrorism incident, including one involving nuclear, chemical or biological weapons of mass destruction;

—define the circumstances under which military resources can, consistent with federal law, be used for technical assistance or law enforcement support, detail the procedures for seeking such assets, and delineate the interrelation between military forces and the FBI. Under those procedures, the FBI on-scene commander will make an assessment whether military, technical or law enforcement assistance is necessary to address the crisis. His or her recommendation will be transmitted to the Attorney General who will, in turn, consult with the Secretary of Defense to determine whether the statutory prerequisites for such support are satisfied. In some instances, the President must also be consulted and he may be required by statute to issue findings and a Proclamation to disperse before military authorities can be employed for law enforcement purposes.

Let me briefly outline how components of the FBI's domestic terrorism apparatus will work and interrelate in the event of a terrorist crisis. Upon receipt of information concerning a credible threat, the FBI's Assistant Director for National Security will activate the Strategic and Information Operations Center (SIOC). The SIOC is staffed 24 hours a day and is used by FBI headquarters units as a command post to direct special operations or respond to terrorist incidents. The FBI Counterterrorism Center (CTC) includes representatives of eighteen federal agencies, including DOE, DOD, FEMA, Customs, Secret Service, and INS. The CTC, which was established in 1995, brings the resources and expertise of these eighteen agencies together, promotes communication of information among agencies, and helps to coordinate the response of the entire U.S. law enforcement community to terrorism. These agencies would be requested, when appropriate, to send a representative to the SIOC. That official would act as a liaison in coordinating needed support from parent federal agencies in responding to the crisis.

At the same time, the Domestic Emergency Support Team (DEST), a rapidly deployable interagency team of specialized advisors from several government agencies, including the Departments of Defense, Energy, and Health and Human Services, EPA, and FEMA, would be on call to provide assessment and expert technical advice to the FBI on-scene commander. Upon his or her request, and the concurrence of the Attorney General and the FBI Director, a task-organized element of the DEST would be deployed to the scene of the crisis for that purpose. In addition to its advice and assistance coordination role, the DEST would also ensure that decisionmakers, including those located in the SIOC, receive critical information on a timely basis and that the DEST agencies coordinate their on-scene operations in a manner that supports the commander's needs.

Finally, the FBI's Critical Incident Response Group (CIRG), which is headquartered at Quantico, Virginia, would coordinate support, as necessary, of several specialized FBI components. These include the Hostage Rescue Team, and Crisis Management Unit.

It is also important to understand that other law enforcement agencies play a significant role, not only in assisting the FBI as lead federal agency, but in supporting the state and local emergency responders. The Director of the FBI and I fully recognize that no single agency can tackle acts of terrorism—especially one involving a WMD—alone. Thus, our approach must be a unified one, bringing the expertise of the entire federal government to the front door of the state or municipality as needed. Improving the processes by which federal resources are made available to state and local authorities is one of the objectives of the five-year counterterrorism plan.

Among the groups of federal law enforcement authorities who play important roles in the battle against domestic terrorism are the Immigration Service, Customs Service, Border Patrol and Coast Guard. These agencies share the mission of protecting our borders, including the coastline, from foreign terrorists, weapons and other instrumentalities of potential use to terrorists. Their roles are crucial, for example, if intelligence sources indicate that a terrorist threat is presented by the clandestine importation of a WMD into the United States for use against a domestic target.

In cases involving arson or use of firearms or explosives, the FBI and the Treasury Department's Bureau of Alcohol, Tobacco and Firearms (ATF) have overlapping investigative responsibilities. When investigating violations which do not, at the outset, plainly fall within the investigative jurisdiction of one agency or the other, both participate in the effort. This joint approach includes coordination at both the headquarters and field levels until primary investigative jurisdiction is clearly established. The two agencies have established a working group to address areas of mutual concern. Topics considered by the group include investigative jurisdiction and protocols, crime scene and laboratory procedures, and training. In addition, the FBI and ATF have conducted a joint conference with the Special Agents in charge of FBI and ATF field offices to further develop a mutual working understanding. The FBI and ATF are also reviewing the current Memorandum of Understanding on bombing investigations in light of recent legislation which affects those investigations. Finally, ATF agents are present in the FBI Joint Terrorism Task Forces throughout the country and ATF has detailed an agent to the FBI's Counterterrorism Center.

Beginning in January 1996, the FBI developed two new units to address weapons of mass destruction (WMD) matters. Today, these units are comprised of nearly 40 employees, eight of whom are detailees from other federal agencies. The WMD Operations Unit (WMDOU) is the operational entity for all threats, threat assessments and domestic WMD incidents. It conducts WMD crisis planning and will coordinate the national response if state and local authorities require federal support during a crisis. A WMD Countermeasures Unit (WMDCU) was also established to coordinate the training of state and local first responders in support of the Domestic Preparedness Program. Additionally, it coordinates the preparation and planning of all WMD exercises within the Bureau in concert with CIRG. To deal with WMD crises, the FBI maintains an all-hour, full-time capability to conduct assessments of any threat involving such weapons. The FBI frequently receives information indicating an individual or group is professing an intent to use WMD materials. Upon receipt of such information, a preliminary assessment is made to determine if enough credible intelligence exists to warrant an interagency response. In such cases, an alert notification procedure is implemented to provide the threat information to all entities involved in the assessment process. The threat is evaluated by an assessment team which is tailored according to the threat; it may draw from expertise available at a number of federal agencies outside of the FBI, including the Department of Defense, the Department of Energy, the Department of Health and Human Services, the Environmental Protection Agency, and others.

When performed, the WMD threat assessment determines credibility of the threat from three points of view: technical feasibility, operational practicality, and behavioral resolve. Technical feasibility includes the capacity to obtain or produce the WMD material claimed; operational practicality refers to the feasibility of carrying out the threatened mode of deployment; and behavioral resolve addresses the psychological assessment of the likelihood of carrying out the threat. Using these three criteria, members of the team prepare an aggregate assessment of the credibility of the threat.

That information is then furnished to the appropriate FBI field office. At this point, further actions may be deemed necessary, to include initiating the deployment of assets to the affected location. The level of response may range from sending members of the FBI's Hazardous Materials Response Unit (HMRU) to help integrate scientific and technical responses and to retrieve evidence for further analysis, to a full scale deployment including the DEST and other assets to assist in detection and mitigation. The establishment of a Joint Operations Center (JOC) may also be deemed necessary to coordinate activities between the federal, state, and local agencies involved in responding to the incident. Members of all such agencies are involved in the operation of the JOC. If no immediate threat to public safety exists, normal investigative avenues are pursued to determine the identity and motivations of the subjects and, where warranted, to apprehend them.

The complexity of a threatened or consummated WMD incident requires that the FBI rely heavily upon the expertise of other federal agencies to assist in the resolution of the crisis through a specially configured DEST. In particular, the armed forces possess unique capabilities to locate, evaluate, isolate, disarm and dispose of

WMD devices, capabilities which can be placed at the FBI's disposal upon compliance with statutory requirements. HHS has responsibility for providing technical advice and assistance such as threat assessment, identification of contaminants, and public health guidance. EPA shares these responsibilities and, in addition, provides advice on decontamination. Finally, FEMA is responsible for coordination of federal consequence management response in support of state and local governments.

Prosecution of Terrorists

The prevention of terrorism also requires that we have the capacity to bring to justice those who are planning to or have committed a terrorist act. While we unfortunately may not be able to prevent all terrorist acts, we will vigorously investigate and prosecute terrorism cases. If an act of domestic terrorism occurs, federal prosecutors become involved with the FBI, as well as state and local law enforcement authorities, in an around-the-clock effort to develop evidence and to identify and apprehend those responsible. We have created an Attorneys Critical Incident Response Group, or ACIRG, composed of expert federal lawyers here in Washington and around the country, whose job it is to provide the Department's leadership with an improved capacity to manage the incident and, on occasion, support the United States Attorney in the on-scene response to the crisis. The ACIRG concept is flexible in nature; it contemplates the formation of task-tailored teams to fit the particular crisis. In some instances, the teams will involve monitoring events and periodic updates to senior Department officials. In others, the teams will provide a full-time presence at the FBI's SIOC to provide on-the-spot legal advice. Finally, where the crisis is a particularly grave one, team members will deploy to the field to provide expert advice to the local U.S. Attorney, coordinate multi-district matters and, in very rare cases, assume on-site responsibility.

During such exigencies, the Criminal Division's Terrorism and Violent Crime Section (TVCS), some of whose members are part of the ACIRG, will augment its legal advice and liaison functions as needed. To ensure preparation for their roles in a domestic terrorism crisis, TVCS has developed and conducted training for designated ACIRG members and the Assistant U.S. Attorneys selected to interact with them. In addition, as part of the Attorney General's "critical incident response plan," each U.S. Attorney's office has been tasked to develop a crisis response plan that includes a scheme for coordination with local, state and federal responders.

Through aggressive investigative techniques, and the subsequent prosecution of those who commit terrorist acts, the government seeks to incapacitate the perpetrators from further acts and deter others who would emulate them.

The rapid arrests and subsequent convictions of those involved in the World Trade Center bombing were the direct result of the effective cooperation of federal, state and local law enforcement agents working closely with assigned prosecutors. The conviction and death sentence of Timothy McVeigh for the Murrah Federal Building bombing, following a meticulous investigation and exemplary executed prosecution, will surely send an unmistakable message to others who might contemplate committing similar acts of terrorism.

Consequence Management

PDD–39 designates the Federal Emergency Management Agency (FEMA) as the lead agency for coordinating the consequence management of acts of terrorism, including the use of weapons of mass destruction incidents. During a terrorism crisis, FEMA acts in support of the FBI until the Attorney General is satisfied that addressing the consequences of the act should assume primacy over dealing with the immediate crisis situation. The domestic "Guidelines" address the procedures for the transfer of such responsibility.

When the Attorney General approves the decision to transfer the federal lead agency role from the FBI to FEMA, FEMA's designated Federal Coordinating Officer (FCO) will coordinate federal actions in support of state and local governments to provide effective consequence management appropriate to the incident. FEMA policy provides that, in fulfilling this role, it will employ the established structure of the Federal Response Plan (FRP). The FRP defines the relationships and roles of 28 federal departments and agencies and the American Red Cross in the consequence management of any disaster or emergency in which FEMA is called to respond.

Responding to international terrorism

Under PDD–39, the State Department serves as the lead agency for coordinating the U.S. response for acts of terrorism that take place outside of U.S. territory and within the jurisdiction of another nation. When a terrorist incident abroad occurs, the State Department acts as the on-scene coordinator for the U.S. Government. In response to a terrorist incident abroad, as I noted earlier, a Foreign Emergency Sup-

port Team (FEST) can be deployed when U.S. interests are threatened. The FEST consists of representatives of State, DOD, and the FBI. The purpose of the FEST is to provide the Chief of Mission, host government leaders, and incident managers guidance concerning U.S. capabilities in resolving incidents or crisis situations posing a serious and immediate threat to U.S. interests.

When the decision is made to deploy the FEST, which is led by a member of the State Department's Office of the Coordinator for Counterterrorism, a decision is also made concerning the composition of the team and the possible need for additional support from other U.S. government agencies, including the Department of Energy, Department of Transportation, and the Public Health Service. The FBI provides support to the FEST concerning U.S. law enforcement capabilities, crisis management assistance, contingency planning, hostage negotiations, evidence collection and guidance about U.S. extraterritorial jurisdiction. It is important to understand, however, that FBI FEST members are not, themselves, part of the investigative team that may be called upon to investigate an extraterritorial terrorism incident.

PDD–39 also assigns to the Federal Aviation Administration (FAA) primacy in dealing with terrorist acts involving air piracy. FAA has lead responsibility for the coordination of any law enforcement activity affecting the safety of persons aboard an aircraft within the special aircraft jurisdiction of the United States.

Developing a Criminal Case

As is the case with domestic incidents, whenever an act of international terrorism that violates federal law is committed, the FBI initiates a criminal investigation. In such cases, as the lead crisis management agency, the State Department seeks for the FBI the broadest possible access to the crime scene and foreign witnesses. The Department of Justice supports the Bureau's efforts to obtain access to evidence and witnesses through the use of Mutual Legal Assistance Treaty (MLAT) requests and, where required, letters rogatory. Additionally, where evidence or witnesses are located within the United States, the Department of Justice may convene grand jury proceedings to facilitate the investigation. As cases become prosecutable through the development of sufficient evidence and legal theories, Department of Justice prosecutors file a complaint or seek an indictment, and obtain arrest warrants. The arrest warrants may be sealed when necessary to facilitate apprehension of the defendants.

Once an arrest warrant is obtained, the U.S. works with the diplomatic, law enforcement and intelligence communities of foreign governments to locate the defendants, to effect their arrests and, whenever possible, to prosecute them in the United States.

As one illustration of our unrelenting commitment in undertaking these measures, in 1993 the FBI apprehended Omar Ali Rezaq in Africa and brought him to the United States to stand trial for aircraft piracy as the result of his participation in the hijacking in Southern Europe of an Air Egypt flight in November 1985 and the murder of one U.S. and one Israeli passenger. Rezaq was convicted in 1996 and sentenced to a life term. Similarly, in September 1996, the United States obtained custody of Tsutomu Shirosaki in Asia on charges emanating from his October 14, 1986, explosives attack on the U.S. Embassy in Jakarta, Indonesia. He was convicted in November 1997, and received a 30 year sentence.

International cooperation is particularly necessary when terrorists commit cyberattacks and other crimes through computer-based technologies. In cybercases, many incidents must be investigated in real-time because electronic trails may disappear once a hacker disconnects from the system or network that he is attacking. For this reason, the United States proposed creating, through the Group of Eight Nations, a Subgroup on High-Tech Crime, which has been examining ways to ensure that transnational cybercrimes can be swiftly investigated. As part of the Eight process, the Justice and Interior Ministers of the Eight met in December 1997 and adopted a ten-point Action Plan leading each country to designate a 24-hour point of contact so that high-tech criminals can be expeditiously pursued. The Subgroup is also seeking ways to expedite international trap-and-trace procedures.

Critical Infrastructures

The findings and recommendations of the President's Commission for Critical Infrastructure Protection, issued in October 1997, underscored the need to expand the nation's capabilities to respond to physical and cyber attacks on critical infrastructures. In particular, the PCCIP report focused on the need to enhance collaboration and cooperation between the public and private sectors to anticipate, deter, respond to, and investigate emerging threats to our infrastructure.

In response to these recommendations, and in consultation with other agencies across the Government, we have established within the FBI the National Infrastruc-

ture Protection Center (NIPC). Building on the former Computer Investigations and Infrastructure Threat Assessment Center (CITAC), the NIPC is to be an interagency partnership between federal agencies with responsibility for the nation's critical infrastructures and the private owners and operators of that critical infrastructure.

The NIPC's mission is to deter, prevent, assess, warn of, investigate, and coordinate the response to threats and unlawful acts targeting the critical infrastructures of the United States, including illegal intrusions into government and private sector computer networks. The NIPC will accomplish its missions by focusing its investigative and analytical efforts on critical infrastructures and technologies, and on how and by whom they are threatened and attacked. In addition, the Center will work with other organizations to ensure that federal, state and local cyber-investigators are properly trained and equipped. The NIPC will also evaluate, acquire and deploy computer equipment and cyber tools to support investigations and infrastructure protection efforts.

The NIPC, along with other federal agencies, will play an important role in an expanded partnership between government and the private sector. The FBI is hiring or developing partnerships with representatives of private industry, including private sector Computer Emergency Response Teams (CERT's), and will establish direct electronic connectivity with private industry, CERT's, state and local law enforcement entities and other government agencies. While we recognize that all of the interests of the private sector may not be represented in the NIPC and that private sector infrastructure owners and operators have responsibility for securing their own systems, through this partnership, the NIPC will facilitate the development of a world-class computer intrusion investigative capability with state-of-the-art tools, technologies, and intellectual capital related to computer intrusions and infrastructure protection. Additionally, the NIPC will help plan and develop a cyber emergency response capability.

The NIPC will be staffed by approximately 125 persons—eighty-five from the FBI, and approximately forty from other government agencies and from the private sector.

Having described the purpose and organization of the NIPC, let me focus now on the roles of NIPC and the other resources of the government in responding in particular to the new breed of potential terrorist attack—that of a cyberintrusion by a terrorist.

Cyber Intrusions

Until this point in my testimony, I have discussed our responses to international terrorism and domestic terrorism as largely distinct subjects. This is so because the roles, responsibilities, and interagency processes that are involved differ considerably between the two areas. One of the greatest challenges we face in the Department of Justice, and one that confronts all of the departments and agencies, is to determine whether a cyber intrusion is in fact an act of international terrorism, an act of domestic terrorism, or comes from some other malevolent source such as a non-terrorist criminal acting for illicit gain or vengeance, a hostile foreign intelligence service or, most seriously, a hostile state attacking the United States. In conventional terrorist attacks, the act often speaks for itself; the bombing at the World Trade Center would be classified as "terroristic" no matter who the actor. But although computer commands and digital manipulation of our information infrastructures have become potential terrorist weapons, it does not follow that every computer intrusion is in fact a terrorist act. And properly identifying the true nature of an attack is all the more difficult because the current information infrastructure can make it difficult or impossible to pinpoint the source of an attack or identify sponsorship of the activity.

To respond to this fluidity and uncertainty in cyberattacks, the FBI is creating the Computer Emergency Support Team (CEST). In the past, "foreign" attacks that at first seemed to be state-sponsored turned out to be U.S. hackers looping through foreign sites. It is therefore critically important not to make premature assumptions about the location or motive of the attacker. Such assumptions—that the attack is state-sponsored information warfare or an intelligence activity—have proved wrong in the past. Indeed, the only assumption that can safely be made at the outset of a cyberattack is that the attack constitutes a violation of federal law, and it must continue to be treated as a crime in the absence of evidence suggesting another motive.

Because of the uncertain nature of cyber intrusions, the Department of Justice maintains close coordination and communication with the National Security Council. The National Security Adviser and the NSC staff are charged with informing and advising the President about potential attacks on the national security of the United States. Therefore, it is important for these advisers to receive the necessary

information relevant to their responsibilities, and to participate, with me and the other Principals, in the ongoing consultation and decisionmaking process about whether and when a criminal matter has become an attack on our national security.

When a matter is the subject of a criminal investigation, powerful investigative tools offer the ability to quickly secure evidence wherever located. Moreover, NIPC personnel will be highly-sensitive to intelligence issues, ever vigilant for the national security implications of an investigation. Indeed, the nature of cyberattacks highlights the fact that any comprehensive approach to a cybercrime requires a multidisciplinary and interagency approach, bringing together the disciplines of computer security, law enforcement, counterintelligence, counterterrorism and foreign intelligence. Clearly, the level of technical, forensic, and legal ability necessary to combat these threats is extremely high and very specialized.

In responding to cyber incidents, the FBI draws heavily upon the skills of their Supervisory Special Agents assigned to the Computer Investigations and Operations section at FBI Headquarters, as well as teams in the other FBI offices. To deal with the complex legal issues raised by hacking cases, the FBI will consult with the Computer Crime and Intellectual Property Section (CCIPS) and those Assistant United States Attorneys, known as Computer and Telecommunications Coordinators (CTC's), who have been specially trained by CCIPS to deal with cyber events. Using these resources, and with the help of the Department of Defense and other agencies, the Department of Justice was able to respond quickly to the recent attacks upon numerous Department of Defense and other government and educational sites. As you are likely aware, that investigation has led investigators from California to Israel, with the resultant identification of the principal participants in the intrusions.

IMPROVING OUR CAPABILITY TO PREVENT AND RESPOND TO TERRORISM

Recent Successes

To date, our initiatives to combat international and domestic terrorism have had a number of notable successes. For example, in addition to the recent Rezaq and Shirosaki convictions, during the past year, the FBI, working with other federal agencies, captured Mir Amal Kasi from overseas so that he could be tried in Fairfax County, Virginia, where he was convicted and sentenced to death for the January 12, 1993, murders of two CIA employees.

During the past year, federal authorities, often working closely with their state and local counterparts, have also thwarted at least eight planned bombings or other acts of terrorism by homegrown extremist groups. One of these involved a scheme to bomb a large natural gas refinery in Wise County, Texas, to divert attention from a planned armored car robbery.

Additionally, on October 8, 1997, collaborative efforts of the Departments of Justice, State, and Treasury were an integral part of the process that culminated in the designation of 30 organizations as foreign terrorist organizations under Section 302 of the Antiterrorism and Effective Death Penalty Act of 1996. These designations trigger provisions that permit the prosecution of persons within the United States who knowingly furnish material support to designated foreign terrorist organizations. The provisions also call for U.S. financial institutions to block the assets of the designated organizations and render their members excludable from the United States.

New Programs and Initiatives

Nunn/Lugar and related efforts to develop state and local partnerships

We cannot, however, afford to rest on our laurels. Instead, in partnership with this subcommittee and the Congress, we must continue forging ahead to improve our capabilities to combat terrorism, and implement legislation enacted for that purpose. As a cornerstone of this effort, the five-year counterterrorism strategic plan will chart the course ahead for all of the agencies involved in counterterrorism. For now, let me highlight a few examples of our new programs and initiatives. In this respect, the Defense Against Weapons of Mass Destruction Act of 1996 was enacted as the Nunn-Lugar-Domenici Amendment (Nunn-Lugar) to the DOD Appropriations Act for Fiscal Year 1997. "Nunn-Lugar" imposes upon the Executive Branch a number of requirements relating to preparedness in responding to the terrorist use of weapons of mass destruction (WMD)—chemical, nuclear and biological weapons—within the U.S. Among other things, the legislation requires the Executive Branch to assess its capabilities to assist state and local governments in preventing and responding to terrorist incidents involving such weapons. It mandates that DOD, in coordination with other relevant federal agencies, establish programs to advise and train civilian emergency preparedness personnel at all levels of government in plan-

ning for and responding to WMD incidents. Additionally, it directs DOD to establish rapid terrorism response teams for the purpose of assisting such authorities in the detection, neutralization, containment, dismantlement and disposal of weapons of mass destruction.

The FBI and other federal agencies such as FEMA, the Department of Justice's Office of Justice Programs (OJP), the Department of Energy, EPA, and PHS, are supporting the Department of Defense in this initiative to provide WMD training to state and local "emergency responders." These consist of state and local police, fire, and emergency medical personnel who would likely provide the initial response to a WMD incident. This initiative, which commenced in late fiscal year 1997, will eventually train emergency responders in 120 cities throughout the United States. To date, officials from 19 cities have received training; an additional 31 cities are due to be introduced to the training in fiscal year 1998; and 35 more will be visited during fiscal year 1999.

In addition to these Nunn/Lugar-driven initiatives, the FBI pursues continuous crisis management planning in conjunction with other Federal agencies, as well as with local police, fire, and emergency medical personnel. For example, to further enhance the federal-state-local approach to combating terrorism, the FBI has, to date, established 16 Joint Terrorism Task Forces in field locations. The objective of the FBI in this respect is to ensure that all entities that would respond to an act of terrorism, involving either a WMD or a conventional weapon, are coordinated at the state and local, as well as at the national, level.

The Counterterrorism Fund

In 1998, Congress provided $52.7 million in the Counterterorrism Fund. Twenty-one million, two hundred thousand dollars has been allocated to ensure that State and local first responders have basic equipment and training to respond to chemical or biological incidents as well as those involving improvised explosive devices.

A total of $5.2 million is provided for the FBI's Hazardous Devices School at Redstone Arsenal, Huntsville, Alabama. These funds will be used for the expansion and renovation of the Hazardous Devices School to increase the number of bomb technicians trained each year on response to improvised explosive devices as well as nuclear, biological, and chemical incident matters. The funding will also provide certain items and articles of equipment for bomb squad use.

Further, $16 million is authorized for the provision of operational response equipment and training to state and local agencies that will enhance their capabilities to respond to an incident involving weapons of mass destruction. The Office of Justice Programs (OJP) will administer these funds as follows:

Working with the FBI, OJP is developing a $12 million grant program to provide equipment to state and local authorities who would be called upon to respond to an incident involving weapons of mass destruction. Such categories of equipment include items necessary for personal protection, detection, decontamination, and communication during an actual response. The FBI and OJP will coordinate with Nunn-Lugar and other efforts that also provide equipment to first responders to insure that overlap does not occur.

In addition, $2 million is provided for OJP to establish and administer a training center for state and local first responder personnel at Fort McClellan, Alabama. This Center will provide first responder personnel with state-of-the-art training, including "hands-on" field and laboratory exercises to improve their capabilities to respond to and manage terrorist incidents, including those involving chemical agents and explosive devices. This Center will work in cooperation with a consortium of universities and other specialized facilities which offer resources and expertise critical to first responder training. OJP will coordinate its administration of the Fort McClellan program, both training and curriculum, with the FBI. $2 million is also provided for the operation of a similar training center in conjunction with the Energetic Materials Research and Testing Center at the New Mexico Institute of Mining and Technology, in Socorro, New Mexico. OJP will administer this program as well, working with the Institute to define and develop curriculum and training appropriate to the Institute's capabilities and expertise in a manner that does not duplicate other available facilities and resources.

In addition to these disbursements, $20 million of the CTF is to be used to reimburse Departmental components for costs incurred in support of countering, investigating, and prosecuting domestic and/or international terrorism; to finance reward payments in connection with such activities; and to restore the operational capacities of offices destroyed or damaged by domestic or international terrorist acts. Since approximately $48 million ($20 million in 1998 appropriations and $28 million in carryover funds) was available at the beginning of 1998 for reimbursement, no additional reimbursement funding was requested in 1999.

The remaining $32.7 million in 1998 funds will be used for the following: development of the five-year interdepartmental counterterrorism and technology plan ($1 million); research and development ($10.5 million); and improving state and local response capabilities ($21.2 million).

For 1999, the Department seeks $52.703 million in funding for the CTF. Of this, $16 million would continue the program begun in 1998 to provide Weapons of Mass Destruction response equipment and training for state and local first responders. In addition, an enhancement of $3.1 million is requested to ensure the Continuation of Operations and the Continuity of Government during a time of emergency. The $3.1 million will fund an alternate crisis management/relocation facility to carry on essential Justice Department functions in the event the Department, or one of its components, is denied access to its facilities for various reasons, such as a terrorist act. The remaining $33.603 million is requested to implement certain recommendations of the President's Commission on Critical Infrastructure Protection, including funding for the expansion of the FBI's National Infrastructure Protection Center (NIPC). Funds not required for either ensuring the continuity of essential Department functions during an emergency or for critical infrastructure protection would remain available for the other authorized purposes of the CTF, including countering, investigating, and prosecuting domestic or international terrorism.

Senator GREGG. Thank you, Madam Attorney General. If you will make a note, or if your staff will make a note, to get us language you want on the equipment issue, we will get that in the bill.

DIRECTOR FREEH'S STATEMENT

Director.

Mr. FREEH. Thank you, Mr. Chairman. I will just make a very brief statement. Let me also join the Attorney General in commending the committee, and particularly your own personal leadership in this critical area.

HISTORY OF COUNTERTERRORISM

I think if you look at the history of counterterrorism activity by the Federal Government, you will see an historic change beginning in about 1995, with respect not only to the emphasis, but to the resources and infrastructure which this Congress and this committee, particularly, has spearheaded, in terms of the delivery of those services for the protection of the people that we are obligated to protect.

Let me just contrast very briefly incidents of a few years ago, given the available tools and resources, and what we are prepared to react to today in 1998, thanks to the resources and the leadership of this committee.

If you take the bombing of the World Trade Center, if you take the Khobar bombing in Saudi Arabia, even the Oklahoma City bombing, those were catastrophic acts of terrorism, both domestic and foreign, to which the Federal Government, the State and local officials, and particularly the Department of Justice reacted to very quickly, in my view very ably, and very expertly, given the results of those investigations, and the speed with which the individuals at least in the World Trade Tower case and the Oklahoma case were identified and apprehended, convicted, and sentenced.

We did not have at that time the many resources which are now part of our routine table of tools to deal with these kinds of cases. For instance, we did not have a Counterterrorism Center during those events, which this committee has provided to us, where now 18 Federal agencies can co-locate and work, not just to analyze in-

formation and intelligence, but to respond in a unified fashion when an attack such as those occurred.

We did not have the structures that we now have with respect to the Infrastructure Protection Center. We did not have the hazardous materials response unit in our laboratory which responded very recently to the threat in Las Vegas of an anthrax attack.

We did not have the weapons of mass destruction operations unit. We did not have the expanded legat program, which this committee also was responsible for supporting successfully, which gives us the ability to work overseas, not only to prevent these kinds of acts, but also to solve them quickly.

We were not engaged in first responder training, as we are now. We did not have the expanded capabilities in our operations center, that the new SIOC facility which was funded under the leadership of this committee will have when it is opened in August of this year.

We did not have the relationships in place between the FBI and the CIA on the one hand which now result in apprehensions of people like Kasi and their return back to the United States.

We did not have the PDD–39 which clearly specifies the FBI's leadership role in counterterrorism acts in the United States, as well as the lead supporting role in overseas activities.

We did not have the designated Department of Justice attorneys in the critical areas relating to counterterrorism, both in terms of acts of violence and also cybercrimes and attacks against our infrastructure.

We did not have the plan and the framework for putting together the resources which are needed to further focus our mission and coordinate what we are doing. We did not have the equipment that is now provided to our CIRG unit in Quantico for dealing with hazardous material investigations and responses.

And I could go on, actually, at some length. What I think is critical is that beginning in 1995, and continuing this year and now into the 1999 request, this committee, and you, Mr. Chairman and Mr. Hollings, really, turned around the question of resources and capability, and infrastructure. And we will be better prepared to protect this country and its people in the years to come as a result of that.

COUNTERTERRORISM THREATS

The threats change, of course, from year to year. We have individuals, even very recently, shutting down a small airport in New England by a computer attack against its infrastructure. We have other individuals trying to shut down 911 systems in Florida, systems which are critical to the protection of everyone.

We know that we have terrorists and spies, and even more common, white collar criminals looking to exploit information systems to commit crimes. We see that most glaringly in the *Innocent Images* case, which again, your leadership and the leadership of this committee have been responsible for giving us the tools to deal with these issues.

We are in a formative stage in the sense that we are still planning how to carry out these functions, to use the resources wisely, to make sure we do not duplicate what other agencies are doing.

The Attorney General, in particular, has emphasized to us the need to insure that our State and local partners not only receive the training and equipment which this committee has authorized, but that they have direct input into our Counterterrorism Center, that their interests are represented in the new National Infrastructure Protection Center, and to make sure in all of our endeavors that we work with them closely and cooperatively.

We have other issues and problems to deal with. The Attorney General mentioned encryption. These are issues that need to be addressed, to give us the capability which I know your committee and the Congress intend us to have by the appropriations and the leadership that they have shown in this area.

So let me add my appreciation to that of the Attorney General, and tell you that as the FBI Director I am confident that in 1998 we are twice as prepared to deal with these threats, both at home and overseas, both truck bombs as well as infrastructure attacks, and we are twice as prepared because of the resources, the leadership, and the focus which this committee in particular and the Congress has given to this problem.

Thank you.

COUNTERTERRORISM COORDINATION

Senator GREGG. Thank you, Director.

I agree. We are at least twice as prepared, but we are still, as you mentioned, in the formative stages. I want to go over a little bit where we are, because I would like to get a sense of how this is playing out. In your opinion, who is coordinating the national effort on counterterrorism for anticipating events in the area of weapons of mass destruction, and where should that responsibility be, and is that coordination being done correctly?

Ms. RENO. Let me address it initially. The coordination, under PDD–39, between agencies ultimately lies with the National Security Council. Where it relates to domestic terrorism and the use of chemical, biological or nuclear weapons within the United States, the FBI is the lead agency, and the Department of Justice and the FBI are planning on a regular basis and developing through the 5-year strategy that plan.

As part of the 5-year strategy, as I mentioned, we have submitted to you an outline. But we will now be meeting with the different agencies, both those that you have mandated that we meet with, and we are bringing in other agencies to ensure that there is full consultation and that we develop an organized plan with relationship to all terrorist issues as well as weapons of mass destruction.

With respect to immediate issues, we are in the process of doing the Nunn-Lugar initiatives in a number of cities, and learning from those experiences what can be done to improve our coordination with the Department of Defense.

As you noted before the hearing began, the Department of Defense has undertaken certain steps with the National Guard to be prepared through teams that would be available for responding. As I indicated, we will be having regular meetings. We have already had our first meeting with the Department of Defense, and one of the issues that we have identified for discussion is how we handle

these matters together, and what we do with respect to coordination at the scene.

I would let Director Freeh respond further.

Mr. FREEH. I just would echo what the Attorney General has said. I think the current structure with respect to response and playing the leading, coordinating role in response to these particular events, particularly domestic events, is really successfully placed with the Attorney General, and the FBI as the lead agency in the planning for events, where opportunities of attack and targeting are obvious or contemplated, and also in responding to those events.

I think that the PDD–39 formula which puts that responsibility with the Attorney General and the FBI is prudent. I do not think it should be altered.

ROLE OF THE NSC

Senator GREGG. I guess my question is, is it working? We did read some reports that the NSC has stepped into the arena in maybe a way that has put it in the process of making law enforcement types of decisions, versus being a coordinating agency. Is there a positive, constructive coordinated effort, or are we running into turf problems between different agencies?

Mr. FREEH. My view is that the current coordination is successful, and we are having discussions, not only with the NSC, but other agencies, with respect to refining that cooperation. There are some areas of disagreement. We are engaged in those discussions now, and we are hopeful that they will maintain what I think is the current, successful formula.

Senator GREGG. How do you feel, Madam Attorney General, relative to the NSC's role, and specifically who should be doing what?

Ms. RENO. I have found that the PDD–39 mechanism as it exists today has been very, very satisfactory. I have pointed out on a number of occasions that the NSC has an important coordinating role. The PDD–39, as it is drafted, specifically provides that it does not mean that the NSC can direct action with respect to domestic law enforcement. But what I have found is that they are just exactly that—a good coordinator. They have not directed action. They have faithfully communicated my position to the President of the United States when I am in the minority, and I have felt that it has been a good working relationship with proper deference to the fact that the law enforcement agency should be responsible for domestic law enforcement and terrorism issues.

ROLE OF NATIONAL GUARD AND DOD

Senator GREGG. And the National Guard and the Defense Department, which is really the biggest part of the equation out there outside the FBI for domestic issues. Obviously CIA when we get into international issues, and State. But to what extent is there a coordinated, comprehensive domestic preparedness effort that ties in the National Guard and Defense Department?

Ms. RENO. I think we have much to do on that. Under the program announced by Secretary Cohen, the Department of Defense has just established the Consequence Management Program Integration Office. That office will oversee the integration of both Na-

tional Guard and Reserve elements into overall agency weapons of mass destruction preparedness programs.

Part of the effort is the establishment of 10 rapid assessment and initial detection elements. As Secretary Cohen has said, it will be dedicated solely to assisting local civilian authorities in the event of a chemical or biological attack. In other words, their main focus is consequence management, and for that reason they will be aligned with 10 FEMA regions to provide a more flexible and immediate capability to support a State's response.

In addition to that, I understand that the DOD initiative also provides for additional training of existing reserves so they will be better able to assist at home. We need to have further conversations with the Department of Defense, and as I indicated, we are having regular meetings with them now, and this has already been identified as one of the areas that we should address.

And we need to look at what is happening in the field with the initiatives that have been undertaken in the field to see what we can do to improve that coordination.

DOMESTIC PREPAREDNESS PROGRAM

Senator GREGG. When I went over there and got briefed by those folks, they talked about the fact that they have targeted the first, the top, I think, 120 cities in the country to bring them up to speed, bringing their fire departments and police departments up to speed in their capacity to respond to a weapons of mass destruction attack.

Now, obviously that should be coordinated with the Justice Department and the FBI. To what extent is it coordinated with the FBI, this actual education and structuring of the response on the ground by the community leadership, which is then followed up by the FBI and FEMA and the first response teams coming in from wherever they are located?

Mr. FREEH. With respect to not only the designation of the 120 cities, but the carrying out of the first response training, the FBI has been a participant, a full partner participant in the planning and is now taking it to the training and implementation stage.

We hope that all of the 120 cities will receive that training over the next 18 months to 2-year period. And although the authorization and appropriation is a DOD funding, we have been working very closely with them and are satisfied that that part of the responsibility is being implemented in a way that will not only give them the technical training, but the liaison to the Federal counterparts which would be triggered in the event of an emergency.

Senator GREGG. I am going to have to go vote. I apologize. I will be back.

[A brief recess was taken.]

DOD-JUSTICE COORDINATION

Senator GREGG. I apologize for the delay.

On the issue of the National Guard and what DOD is doing, I recognize that you are trying to coordinate with the Defense Department, and I know it is preliminary and everybody is going off and trying to do their own thing. What the Defense Department is doing is excellent. I respect what they have attempted to do, espe-

cially with the National Guard and with the education, in bringing their various communities up to speed. Is there anything further we could do to make sure this was a little more coherent exercise so that Justice knows what Defense is doing, and vice versa?

Ms. RENO. What I have asked is that we take the initiatives that have already been pursued in the first of the 120 cities, and that we analyze those—I think they have been analyzed in after action reports, but I have not received those—to see what the problems were, and what we can do to organize better.

Some of these initiatives, and correct me if I am wrong, my people in the back, have been done, and I understand that they have been carried out very efficiently and effectively. But there has not been a coordination through to the Department of Justice that I am aware of, up to the highest levels that would involve us all.

Senator GREGG. So how do we get that?

Ms. RENO. Well, I think we are going to get that now. And then I think we have got to work with the Defense Department, who has committed, and Deputy Secretary Hamre has committed, to participating in the National Infrastructure Protection Center. That should be resolved very quickly. There will be a presence there, and I think that will be the place that so many of these issues can be ultimately resolved.

At the same time, as I mentioned, this is one of the highest priorities in the table of issues that we have identified for discussion with our meetings with the Defense Department. So I think these issues will be addressed in short order.

STATUS OF TITLE V EXEMPTION

Senator GREGG. Well, let us also make sure we have the National Guard at the table, because I think their responsibility here is going to grow exponentially, because they are a very logical resource, an underutilized resource. And I know as a former Governor that they would be an extremely appropriate agency to turn to, as a Governor, to try to be the coordinating agency within a State.

Now, on the issue of attacks against the infrastructure, you have the CITAC effort. You have a number of efforts going forward to try to coordinate. The Attorney General mentioned that you folks needed access to better equipment. Obviously, if you need some legislative language to do that let us know.

You also need personnel. How are we doing on the title V issue with the OMB? Have we got that straightened out yet, so we can actually hire people who are capable of doing that stuff?

Mr. FREEH. Senator, we are working with OMB and OPM very intensely to get to them what they have required, which is a paper which addresses recruitment and retention issues, as well as the authority, which the Congress has now given us, to hire critical employees in key areas without the restriction of title V.

I have given our people, and we are working in close conjunction with the Department's personnel people, within a very short timeframe, to get the plan up to the requirements and we think the expectations of the OPM and OMB people.

At that point we will expect them to approve it, and then we can move forward, and begin these hires.

Senator GREGG. I appreciate that, and this is not directed at you, but the Congress has been pretty specific on saying that we want you to have this flexibility. I find it unconscionable that OMB is standing in the way of all sorts of efforts in the area of detecting criminal activity in this country, but specifically the terrorist threat by their unwillingness to move expeditiously on this issue. That is an editorial comment.

Ms. RENO. Mr. Chairman, can I just make sure there is no misunderstanding about that. We owe OMB something.

Senator GREGG. Yes; but they owe the Congress something, too, which is action.

Ms. RENO. Well, it is our step to be taken, and we are pursuing it as vigorously as possible, and in my discussions with OMB I think we will find a receptive ear.

INFRASTRUCTURE PROTECTION

Senator GREGG. OK. Let us hope so.

Now, on these attacks on the infrastructure that come through technology activity, to what extent do you perceive these to be internationally driven, and, second, to what extent are they driven by Government-sponsored international activity?

Mr. FREEH. Many of them, in fact, most of the ones that have been publicized, quite apparently, have been individual actors. In many cases, juveniles, even though the juveniles resided outside the United States.

We are aware of, and we do have information with respect to planning, at least planning operations by foreign counterterrorism services, as well as external services, to attack infrastructure targets. We have gotten that information through a series of sources. We have not seen any attacks that we can identify as foreign state-sponsored attacks, but we do know that it is an area of expertise that many foreign services have developed, but not to my knowledge as yet utilized here in the United States.

Senator GREGG. Do you need significantly more resources in this area?

Mr. FREEH. I think it is an area where we do need resources, precisely because the nature of these attacks, as documented by a recent Department of Defense exercise, indicates that the subtlety, as well as the transparency, of the intrusions are very capable of not being detected, and that the more resources and the more interconnectivity, the ability to trace back upstream bits and pieces of evidence maybe not apparent on a piece-by-piece analysis, but in a computerized type of matrix, make a lot more sense.

So I think it is an area where both the Department of Defense and criminal justice efforts will require more resources over the years. And I think our budget contemplates the initiation of that phase.

ISRAELI HACKER CASE

Senator GREGG. I notice that there was a recent incident with Israel, and Israeli, not Israel—well, Israel, too, in a hacker attacking an American Government agency. It did not seem to me that the Government of Israel was very cooperative in allowing us to

handle that individual from a standpoint of law enforcement. What is your reaction?

Mr. FREEH. From a law enforcement point of view, we did get very quick access to the information, as well as the interviews which were conducted in Israel. Our legat in Tel Aviv immediately made contact with his counterparts.

I think from an investigative point of view, not maybe a——

Senator GREGG. I am talking about a prosecutorial point of view.

Mr. FREEH. Well, with respect to extradition, those are issues which have been problems not only in Israel but in many other countries.

But in terms of access to the information and quick facts relating to the methodology of the attack, the Israelis were very forthcoming with us.

Ms. RENO. One of the areas that we are focused on, and we had an excellent meeting beginning with the P–8 countries in December, is we are much further advanced than most other countries in the development of information technology, and in the reliance on it in our infrastructure.

But the other major industrial countries are right behind us. And one of the things that is clear and that we have committed to try to do is to recognize that locating the intruder is one of the more difficult issues. It requires for us to really be effective 7 days a week and have the round-the-clock ability and capacity to respond. And so we are trying to move in that direction. It requires an ability to locate, and we are trying to move in that direction.

We are looking at the development of common statutes. Now that is just the major industrial countries. One of the things that we have learned with respect to this whole issue is that a country that is not industrially advanced can be the source of an intrusion from some very bright young person that can cause us fits. And so we need to develop the capacity worldwide.

The second point is one that Director Freeh alluded to, and one that I have concentrated on a great deal during my time as Attorney General. That is, if we are going to build a hemisphere and a world of trust, then we are going to have to trust each other to extradite nationals and to let the crime be tried and prosecuted where the crime was committed. That is a slow process, but we are making some progress, not enough.

INTERNATIONAL CYBERCRIME

Senator GREGG. Well, do we need a new international convention of some sort to address the issue of cybercrime? I mean, should there be an international symposium of some sort on this?

Ms. RENO. As I mentioned in my prepared remarks, we are spending a great deal of time with the P–8 countries, with the Council of Europe, and with the OECD in developing just this. I do not think we are to the point yet where we could develop an international convention, but this is certainly what we should be moving toward.

Senator GREGG. How high is this on the agenda of the White House, when they meet with the G–7, or they meet with the ASEAN countries? Does this type of topic ever come up? Is it ever put on their agenda as an item?

Ms. RENO. It has been very much on their agenda, as I understand it. I have not been there. But the meeting of the ministers of justice, or the ministers of interior, my counterparts, this past December was as a direct result of the priorities established by the leaders of the P–8, and I think reflects their commitment to this issue.

I know the President is very sensitive to this issue. The President's Commission on Critical Infrastructure Protection is a clear example of that, and I think he is, I have felt that he is very supportive in this effort.

Senator GREGG. Should we have a freestanding operation under the Justice Department somewhere that specifically addresses this type of crime?

Ms. RENO. I would like Director Freeh to comment as well, but one of the problems that you face is that you do not know what it is going to be. When you see it, you do not know where it is coming from or who it is. It may turn out to be a domestic juvenile hacker. It may turn out to be a foreign power. It may turn out to be a terrorist. We do not know coming into it, but we have got to have the flexibility to move on to a different stage of investigation if it should be determined to be an act of a foreign power, or if it should be determined to be a terrorist who is systematically taking down the structures around the country.

This is the reason it is so important, and the initiatives undertaken by the Department of Defense in conjunction with the Department, eligible receiver, and our initiatives with respect to the recent intrusion that you referred to have been so important.

The National Infrastructure Protection Center, I think, will be the ideal place to focus responsibility because if you leave it just as a cyber issue, you will not be able to fully coordinate the issue when it is both a cyber attack and a physical attack.

And the way the FBI has set up that structure with this Counterterrorism Center immediately available to the National Infrastructure Protection Center I think provides the ideal coordination with representation. I said 19 on the Counterterrorism Center, but it is 18 other agencies represented in the Counterterrorism Center.

If we can build the same capacity in the National Infrastructure Protection Center, if we can involve the private sector and State and locals, we will have a system there both on the terrorist side, the physical terrorism side, and the cyber side that can be fully coordinated through the FBI's SIOC, if there is a situation which brings in both physical terrorism and the cyberterrorism together.

Senator GREGG. Did you want to expand on that?

Mr. FREEH. Yes; I think we are really at the beginning of what will be seen ultimately as a revolution with respect to the methodologies by which criminals and terrorists and spies commit crimes and the ability of the Government, particularly the Department of Justice, to respond to that.

I think the advent of computers, networks of information, infrastructures, really does represent a revolution in terms of what we are charged with combating. I think it is a little bit akin to the use of the automobile.

The advent of the automobile in the early 1930's, allowing criminals to commit crimes and to escape and to get access to new areas to commit crimes really caused a change, a graphic change in the tools, resources, and authorities required by Federal agencies to respond to that, as well as the State and locals.

So I think going back to your question, you will see very shortly the establishment of new components, particularly in the Department of Justice. And as the Attorney General described it, the NIPC is exactly that component which is responsible for criminal investigation, for early warning, for research, for State and local training, and to take both the counterterrorism as well as the criminal aspects of this technology and put it where it belongs, which is in the operational capacity of the Department of Justice.

Department of Defense and national security reasons require other capability on that level. But those two have to be connected, and I think the NIPC is the first attempt to do that. But you will see, I think, increasingly in this Department of Justice, in the FBI, and in your State and local law enforcement agencies, whole new components which will be responsible for dealing with a whole new genre of crime.

TECHNOLOGY EXPLOITATION

Senator GREGG. As you say, this is a revolutionary event. As the technology moves, so must you. Is there a review system that you feel comfortable with that is going to allow you to anticipate the technology threats and respond to them, rather than having them occur before you know they exist?

Mr. FREEH. Yes, exactly. The research capacity and the resources that you and the committee have given to us will be a first step in that direction. We will report to you by the end of the year the contours of that research and the objectives as well as the anticipated benefits.

But the precise idea behind that, which I thought was a great idea—was not mine, by the way—was to begin looking at the technology in terms of prevention and acquisition of techniques and equipment to prevent and defeat attacks, as opposed to just solving them and reacting to them.

So I think that is the first investment in that, and I think it is a wise one. I think there will be much more required, significantly more, as the type of crime that we deal with grows quickly.

Senator GREGG. How close are we to——

Ms. RENO. Could I add something there, because I think it is vitally important. With the information infrastructure as it is in this country today, with so much of the private sector dependent on it, banking and finance, energy, utilities, transportation, it becomes absolutely critical that law enforcement form a partnership with the private sector unlike perhaps anything that we have seen before, because it is all interrelated. And one of the things that we have got to understand is the interconnectivity and how one industry or sector can affect another, and how we can engage in preventative efforts.

I think there is, to some extent, a distrust between the private sector and law enforcement. That distrust is being broken down by experts from both sides coming together. I had a wonderful oppor-

tunity about 3 weeks ago to speak to scientists and academics and private sector representatives at the Lawrence Livermore National Laboratories when I announced the National Infrastructure Protection Center.

It is so important that we build on that knowledge. They can give us new ideas about evolving equipment, and evolving technology that can be vital to our efforts. They can give us information concerning intrusions that are absolutely vital.

So the steps that we are also undertaking are reaching out, and the center, as the FBI has designed it, provides for an outreach component. They are already engaged in that. It is also important that we reach out to the State and locals in the same way. And I think not just the expertise, not just the equipment, but the outreach will be vital, and the partnership that is developed from that outreach will be vital to our success.

ENCRYPTION

Senator GREGG. How close are we to reaching an agreement on encryption?

Mr. FREEH. I think we have a lot of work to do. There is still a——

Senator GREGG. But without an agreement on encryption you basically do not have a——

Mr. FREEH. Without an ability to deal with robust encryption with a court order, a lot of these counterterrorism efforts, a lot of our drug efforts will be defeated. There is no question about that.

Ms. RENO. My sense is that it is very important for law enforcement, for the Department of Justice, to pursue these discussions with the private sector, to build trust, to build understanding.

We are all in this together, and from my conversations with the private sector, they are saying, recognize that we are in this together, and let us see how we can work together. Do not tell us what to do. Describe the problem to us, and you may find that the private sector may have more than one solution to the problem that can be more effective for you.

So it is absolutely critical. Nothing will work unless we solve this encryption issue. But I think if we just keep working very hard we will make some real progress in these next 60 days.

Senator GREGG. I think people need to understand that if we do not solve the encryption issue, the country is basically open to all sorts of threats—terrorist threat, and obviously drug dealers.

Ms. RENO. Since this is a forum where people may hear and say, well, just what does encryption mean, I think it is important for them to understand what we do today.

Today to get a drug dealer, Director Freeh's agents can prepare a wiretap application that is very detailed, it requires probable cause to take it to the court, and the court approves it. It is clearly authorized and sustained under the law. We do that in our fight against drug dealers and our fight against terrorists. What the issues with respect to encryption are, is not expanding what the FBI can do, but only adapting to modern technology, which encrypts, and very strong encryption that cannot be broken, messages, stored data, and even online access.

So we are not asking for additional authority to surveil. We are asking that our authority be adapted to modern technology.

ANTHRAX THREAT IN LAS VEGAS

Senator GREGG. Absolutely. Now, on the anthrax threat in Las Vegas, what did you learn from that that you did not know? And what should we be doing as a result of that?

Mr. FREEH. Of course, one thing was apparent, which was a positive event, and that is the fact that the FBI office in Las Vegas, in conjunction with the other Federal agencies, particularly with FEMA, with the Department of Defense, and with the State and local agencies, including the emergency and rescue operations, and the mayor's office, there was very, very strong prior cooperative efforts—not particularly in an exercise involving anthrax—but in exercises involving crisis management.

The SAC had received that training. The State and locals were aware of the system that would be triggered, and was triggered, with the FBI taking the lead in conjunction with FEMA, and using Department of Defense elements who facilitated the transportation and analysis back here in Washington.

We are in the midst of doing a postincident review to see what we could have done better in that regard. We are, however, pleased with the result, in terms of the response time. The warning system was triggered, we think successfully, and it took relatively short time to resolve a very difficult and complex scientific analysis.

We want to do that quicker in the future. We want to look at field testing equipment that could be safely and successfully used to do a more positive and earlier identification. Although that technology is not where it needs to be, and is not available now, it probably will be in a short time, again, as a result of these efforts and resources that you have given us.

But the coordination was very well done, and that is not my own view. It is the view of the State and local participants, the other Federal agencies. And if we had a blueprint for working together in that kind of incident, it certainly was evidenced there.

INTERNATIONAL COORDINATION

Senator GREGG. There was a comment made in a GAO report that came out dealing with terrorism, if I can find it. It seemed to imply that we needed to do more in the area of international coordination. Unfortunately, I cannot find it immediately. But can you just give us your thoughts on where we stand in coordinating our overseas efforts with the State Department, the CIA, and with various agencies, in trying to anticipate terrorism threats?

Mr. FREEH. With respect to the CIA, and I think I have said this before, Mr. Chairman, even in this committee, the relationships between the Bureau and the CIA, not just in the counterterrorism area, but in all of our across the board responsibilities could not in my view be stronger. And that is a testament to George Tenet's leadership, to John Deutsch's leadership. The Kasi operation, although a fugitive operation, really put into play the critical elements that are required for our successful operation together overseas, which is the headquarters component, and then the foreign, on-the-ground, coordination.

The State Department was also a key player in that. Under the PDD–39, the State Department is the lead coordinator for acts of terrorism outside the United States. We have assembled, using them in Peru and in some other occasion, the foreign emergency support team [FEST], the foreign deployed team of American experts, which represents all of the responsible and expert agencies to deploy physically and immediately in response to a counterterrorism attack.

The level of expertise and awareness by the Ambassadors around the world with respect to counterterrorism has been in my view enhanced, and better coordinated with our legat program, the people that we have overseas.

So I think the overall coordination overseas, particularly with the agency, is good. We are talking about doing with the State Department what we have done with the CIA, which is exchanging officers or deputies in key areas of our counterterrorism responsibilities and international operations. So we can have that kind of seamlessness. We have an FBI agent who is a deputy in the counterterrorism center. We have a CIA officer who is a deputy in our international terrorism section. We found that that kind of exchange probably does more than anything else to insure smooth reactions and cooperative efforts. So in all, I would report very positively on those endeavors.

Ms. RENO. I would raise one additional point which I think is important. I think we have got to also continue our efforts to develop law enforcement capacity in the emerging democracies in those nations that are coming into democracies.

What the FBI has done with Budapest I think has just been excellent. I have had a chance to visit there. But anytime a minister of justice from the Middle European countries comes to visit, it is just a very eloquent, almost plaintiff plea for law enforcement training, for institution building, for courts, for prosecutor training. You realize how fragile democracy is, and how fortunate we are.

I have had the opportunity to talk with the State Department, and I am hopeful that we can build capacity around the world with our allies, and with those nations that work with us, so that they can respond as well.

I mean, there are different grades and different capacities now, and the more we can build that capacity for those first responders, the more it will be helpful, whether it be in drug enforcement, or anything else.

PAN AM BOMBING

Senator GREGG. Do we still presume that the two people responsible for the Pan Am, Lockerbie bombing are in Libya?

Mr. FREEH. Yes, sir; that is our current information. As you know, there are two defendants who are on our top 10 list, and efforts are consistently and intensely being followed.

Senator GREGG. Has there been any progress in those efforts?

Mr. FREEH. No; there are discussions now which have been publicly reported about agreement on a venue for the trial in exchange for the delivery of the two defendants. But those have not concluded in any regard.

Senator GREGG. But we are still pursuing it.

Mr. FREEH. Yes, sir; we are.

IMPROVING RESPONSE TO TERRORISM

Senator GREGG. Is there anything you need from us as a Congress to make your ability to respond to the issues of terrorism which we have gone over here, or any other issues relative to that question more effective?

Mr. FREEH. Senator, we would just note a couple of things, and you have really noted many of them in your statements and your questions. Certainly the continued support for these initiatives at this particular time is critical.

As I said, I think we have really turned the corner on our capacity and abilities, and the follow up which will occur in the next couple of years, based on this type of strong support by you and your colleagues is obviously critical.

We need assistance on the encryption issue. We are trying to work that, as the Attorney General said, in a consensus manner with the industry. We hope that that works. We hope that we are not required to come back and seek legislation.

There are some other aspects of what we do, from a technical point of view, and we can certainly provide those to you and the committee in a separate submission. But minor amendments to some of the current statutory authority, could be done, I think, with little trouble.

For instance, the addition of terrorist offenses to the Federal racketeering statute would certainly be a very prudent and appropriate use of a statute, which tends to accumulate and predicate offenses when there is an overriding enterprise dedicated to committing serious harm, as anybody involved in terrorism certainly would be.

Authorizing the interception of communications for certain terrorism-related offenses. In other words, expanding the title III statute to include as predicates some of the terrorist offenses. Giving us the ability to do multipoint wiretaps. Not being able to choose between techniques and coverage, if the terrorist decides to use a phone or instead talk in an area where we have probable cause to intercept conversations.

Authorizing the use of pen registers to trap and trace devices in foreign intelligence and international terrorism investigations. We do not quite yet have that authority, although we have asked for it for several years.

Providing temporary emergency wiretap and pen register authority for terrorist crimes. We can do that now for most serious criminal offenses. We cannot do it for the terrorism crimes.

Extending the statute of limitation provision for the National Firearms Act would be one slight amendment which would help us in these kinds of cases. Modifying the statutory exclusionary rule under the wiretap statute to exclude from coverage those situations where good faith exists.

Clarifying the removal ground of engaging in terrorist activity in order to permit full and effective utilization of the alien terrorist removal court. And I think a number of other provisions. We would be happy to submit those to the committee in writing, and follow

up with type of documentation or hearing that you would think necessary and appropriate.

Senator GREGG. Thank you. We would like to get those.

We probably would not be able to stick them all in our bill or we would be shot by the chairman of the Judiciary Committee, but we can put as many of them in as the Judiciary Committee can tolerate.

We are joined by the chairman of the Intelligence Committee, and it is an honor to have him here. I will turn to you.

PREPARED STATEMENT OF SENATOR SHELBY

Senator SHELBY. Mr. Chairman, I appreciate you inviting me over here today, but I have a written statement I would like to be made part of the record.

Senator GREGG. Of course.

[The statement follows:]

PREPARED STATEMENT OF SENATOR RICHARD C. SHELBY

I would like to thank Chairman Gregg and the members of the Subcommittee for allowing me to sit in on today's hearing and commend Chairman Gregg for convening a hearing on this important matter.

We all learned from the World Trade Center bombing and the Murrah building bombing, among other incidents, that terrorist acts can occur on American soil. While these acts caused great damage and loss of life, they are only examples of the impact of conventional explosive devices. I am concerned that we recognize the full range of weaponry available to terrorist actors.

As Chairman of the Select Committee on Intelligence, I am currently holding a series of hearings in conjunction with Senator Kyl, the Chairman of the Terrorism Subcommittee of the Judiciary Committee regarding the full spectrum of terrorist threats—from international groups and state sponsors of terrorism, to domestic terrorists producing homegrown poisons. So far we have learned that there is a significant capability for terrorist groups to use destructive devices involving chemical and biological agents. I intend to continue to investigate the various terrorist threats and hold future hearings on these matters.

However, as we develop an understanding of the existing threat we must also take action—the United States must prepare for any of the many kinds of terrorist acts that could occur. I commend Chairman Stevens and Subcommittee Chairman Gregg for instituting the process to develop a national preparedness plan and I am pleased by the hard work of the Attorney General and the men and women of the Justice Department as they design and work toward implementation of this plan.

Specifically, I am encouraged by the conceptual discussions regarding the creation of an Executive Office for Domestic Preparedness within the Justice Department. I hope this proposed office quickly becomes a reality as I believe that it will facilitate the creation of an effective and comprehensive national counterterrorism strategy.

I recognize that we are only in the developmental phase of this process. We have much work ahead of us. It is no small feat to develop a national response plan that integrates local, state, and federal assets in the counterterrorism effort. As I stated earlier, as Chairman of the Select Committee on Intelligence, I intend to continue to hold hearings to investigate the nature of the terrorist threat which I believe will produce findings useful to the development of a national counterterrorism strategy.

Again, Chairman Gregg and members of the Subcommittee, I appreciate the opportunity to participate in today's hearing and look forward to hearing the testimony of the Attorney General and FBI Director Freeh.

Senator SHELBY. I think the hearing that you are having is very appropriate. Timeliness is everything. I have worked with the Attorney General, and will continue to work with her, and also Judge Freeh of the FBI, in dealing with terrorism in every form.

We have focused on a good bit of this, in the Intelligence Committee, and as they both know we have some upcoming hearings when we get back—one closed and one open, because this is a real

threat to America. And how we respond to it, and what we do with it will depend a lot on what we do here, what you do on policy, what we do to help you, I believe.

But I want to thank you, Attorney General Reno. Your leadership as the Attorney General of the United States has been real focused here. Judge Freeh, you have been outspoken on this on many occasions before the Intelligence Committee, the Judiciary Committee, the Appropriations Committee.

It is something that is not going to go away, and we cannot ever, ever look the other way on, is it?

Mr. FREEH. No, sir.

Senator SHELBY. So thank you, Mr. Chairman.

Mr. FREEH. Thank you, Mr. Chairman.

Senator GREGG. Thank you, Senator Shelby. You see, like you have turf issues in the administration, we have turf issues here, but we get over them by just having the chairman of the Intelligence Committee stop by so we get it all straightened out. I very much appreciate that.

Senator SHELBY. I do not know if we have straightened out anything. But I think that working together, and with the leadership that the Attorney General brings to the table, and the Director of the FBI brings to the table, we will make a significant difference, Mr. Chairman.

Senator GREGG. Well, that is absolutely key. Cooperation and coordination.

ADDITIONAL COMMITTEE QUESTIONS

And so I thank you both for your time. You have been very courteous, giving us over a 1½ hours here, and we very much appreciate it.

[The following questions were not asked at the hearing, but were submitted to the Department for response subsequent to the hearing:]

QUESTIONS SUBMITTED BY SENATOR PETE V. DOMENICI

U.S. ATTORNEYS

Question. Attorney General Reno, I regret that I was unable to attend the hearing on February 24th when you gave testimony on the President's overall budget request for the Department of Justice for fiscal year 1999. The following week when the heads of the Immigration and Naturalization Service (INS), Federal Bureau of Investigation (FBI), and Drug Enforcement Administration (DEA) were before the Subcommittee, we discussed the Administration's proposal to provide additional law enforcement resources to Indian country. I indicated that I would like to submit a question to you regarding the activities of the United States Attorneys on Indian reservations. I would appreciate it if you would accept that question now.

Could you provide the Committee with an idea of the current role the United States Attorneys play in assisting Indian tribes and pueblos in their law enforcement efforts?

Answer. The United States Attorneys provide assistance and training to tribal governments to enhance their ability to address violent crime and juvenile crime at the tribal level. Federal law enforcement is the only avenue of protection for the victims of these crimes. United States Attorneys in Indian Country are effectively district attorneys for the citizens in their districts; they have the sole responsibility for prosecuting all major crimes committed by or against Indians on the reservations in their districts.

Question. Has the overall level of activity of the United States Attorneys on Indian reservations across the nation increased over the past one to two years? If so,

in what specific areas have United States Attorneys focused their resources in Indian Country?

Answer. The primary focus has been on violent crimes committed in Indian Country. Case filings have increased from 330 in 1993 to 531 in 1997, an increase of nearly two-thirds. These cases include all types of violent crimes from felony basic assaults and murder to child sexual abuse. However, many instances of violent crime go unreported as there is limited investigative agency presence. The Administration's proposal addresses this need and adds a concomitant number of prosecutors required to direct investigations and prosecute acts of violence.

Question. The fiscal year 1999 budget request includes $3.47 million and 35 positions (26 attorneys) to focus on reducing violent crime, including gang-related and juvenile crime, on Indian reservations. How would these additional resources be specifically utilized if provided by the Congress?

Answer. Our strategies, if these resources were provided, include:

—Fully implementing the Major Crimes Act, the Indian Country Crimes Act, the Indian Child Protection Act, the Violent Crime Control and Law Enforcement Act of 1994, the Anti-Terrorism Act of 1996, and the Anti-Gang and Youth Violence Act of 1997;

—Supporting comprehensive strategies to target and fight overall violent crime, violent gangs, and youth crime through the establishment and continuation of multi-agency and federal and tribal task forces, such as the Safe Trails Initiatives and Weed and Seed designations in Indian Country;

—Continuing the United States Attorneys' support of the Department of Justice's Anti-Violent Crime Initiative;

—Providing additional assistance and training to tribal governments to enhance their ability to address violent crime and juvenile crime at the tribal level; and

—Assisting tribes in developing and implementing Child Protection Teams and Multi-Disciplinary teams to address the serious problem of child physical and sexual abuse.

Question. I am under the impression that in New Mexico at least there is a recognition by the Department and the United States Attorneys that more must be done to assist Indian tribes and pueblos with law enforcement efforts? Has the Department recognized this need? Is that recognition adequately reflected in the fiscal year 1999 budget request?

Answer. The Department and the Administration recognize the critical need to assist Indian tribes with law enforcement needs. After the Presidential initiative was issued, an Executive Committee consisting of leaders from the federal and tribal governments examined the law enforcement problems and determined that a substantial infusion of resources into Indian Country law enforcement is essential. At the request of the Executive Committee, United States Attorneys led an unprecedented series of tribal consultations on Indian Country law enforcement across the country during September and October 1997. A report was presented to the Attorney General and the Secretary of the Interior in October 1997 providing options for improvement in public safety and criminal justice in Indian Country. The needs of the New Mexico Office were included as were all offices that have exclusive federal jurisdiction in Indian Country.

COUNTERTERRORISM TECHNOLOGY R&D

Question. With the leadership of our distinguished Chairman, Senator Gregg, this Subcommittee began a significant counterterrorism initiative in the 1997 bill. These initiatives were greatly expanded for fiscal year 1998.

The 1998 Commerce, Justice, State, and the Judiciary Appropriations bill established a Counterterrorism Fund, providing $52.7 million for several initiatives. The Fund included $11.5 million to undertake a counterterrorism technology research and development program. The Subcommittee provided $1 million for the Attorney General, in consultation with other federal agencies, to develop a five-year, interdepartmental counterterrorism and technology crime plan.

Ms. Reno, can you provide the Subcommittee with a status report on the development of this counterterrorism and technology crime plan?

Answer. The Conference Committee Report accompanying the 1998 Justice Appropriations Act requires the Department of Justice to develop an interdepartmental Counterterrorism and Technology Five Year Plan by December 31, 1998. In response to this Congressional directive, representatives from the Department and the FBI developed an ambitious 13-page outline of issues to be addressed in the final Five Year Plan. This outline has been circulated to other agencies with key counterterrorism responsibilities and their comments incorporated into the outline.

A projected work plan has also been developed to assist the Department in meeting the deadline of December 31, 1998 for submission of the final Plan to Congress. In order to ensure the maximum amount of interdepartmental participation in the development of the Five Year Plan, a Core Agency Group, consisting of high ranking representatives of 15 other federal agencies which have various counterterrorism responsibilities within the government, has been established to help develop the Plan. The Core Agency Group had its first meeting on March 5, 1998. Each agency was asked to complete a lengthy questionnaire soliciting information about current and anticipated programs, training, research and development projects, and projected resource needs in order to fight the perceived terrorist threat over the next five years. Responses to the questionnaire will form the basis of a discussion paper for use by specialized working groups to be constituted from experts identified within the Core Agencies.

The working groups will meet during the spring to address major areas of concern, such as crisis management, consequence management, cyber-terrorism, information sharing and intelligence, critical technologies/research and development. The working group discussions and recommendations will form the basis for developing an interim Plan that will be circulated to state and local officials, academic experts and experts in the private sector for review and discussion during the summer. The drafting of the final Five Year Plan will therefore reflect consultation with the major federal agency participants in efforts to combat terrorism as well as consultation with affected state and local representatives, and experts from academia and the private sector. As a result, the Department expects that the final Plan will be a truly comprehensive one.

Question. Has the Department submitted a prospectus with estimated time lines and major milestones for completion of this plan to the Committees as was requested by February 1?

Answer. The Department has submitted to the Committees the 13-page outline as well as an organizational chart and a chart of key dates and milestones for completion of specific phases of the project through submission of the Five Year Plan to the Committees.

Question. Which specific federal agencies are involved in this interagency effort?

Answer. We have sought input from more than 20 federal agencies and components in the development of the Plan. These agencies all have counterterrorism responsibilities as part of their mission and have identifiable programs and activities in which they are engaged in order to carry out those responsibilities. We have asked each of these agencies to reach down to all their relevant components in responding to a survey we distributed as our primary information-gathering tool. The responses we have received thus far indicate that these agencies are doing just that: they are providing candid and comprehensive responses. The agencies involved include those with which Congress directed me to consult in the development of the Five Year Plan: the Departments of Defense, State and the Treasury, and the Central Intelligence Agency (CIA) and FBI. In addition, I have sought the involvement of additional federal agencies and components: the Departments of Energy (DOE), Commerce, Transportation, and Interior, the National Security Agency, the Public Health Service (PHS), Federal Emergency Management Agency (FEMA), the United States Information Agency, the Nuclear Regulatory Commission, the Environmental Protection Agency (EPA), the White House Office of Science and Technology, the General Services Administration, and the United States Postal Service. Throughout the development of the Plan, we will consult with the Office of Management and Budget (OMB) as well as the National Security Council (NSC), to ensure that proposals being considered for inclusion in the Five Year Plan comport with other vital budgetary and national security priorities in the area of counterterrorism.

Question. Do you anticipate consulting with Congress as this plan is developed? Would you expect to complete this plan by the end of this calendar year as directed by the Appropriations Subcommittees?

Answer. The Department recognizes the great interest that Congress has in the development of the Five Year Plan. Understanding this interest, the Department has been consulting with members of the Congressional Subcommittees, as well as members of the staff of each subcommittee, in creating the outline for the Plan and discussing the proposed development of the Plan from that outline. The Department anticipates additional consultation with Congress as the Plan develops during the next several months at the working group level. The Department has developed the organizational plan and the work plan with the expectation that the final Plan will be completed and submitted to Congress by December 31, 1998. The breadth of the outline, as well as the directive to create a plan that is truly interdepartmental in nature, however, demonstrates that the project is an extremely ambitious one.

The Department is committed to working to complete the Plan and submit it to Congress by the end of this calendar year; the scope of the project and the amount of interagency coordination required to finalize a comprehensive Five Year Plan may make that deadline a challenging one to meet. We will advise the Subcommittees, as the project progresses during the next several months and as the various expert working groups meet to develop their recommendations, as to any necessary adjustments to the present timetable.

Question. How much is requested in the President's fiscal year 1999 budget for the Department of Justice to continue counterterrorism initiatives?

How does this compare to the funding provided for these programs in fiscal year 1998? Could you provide these estimates by agency and program?

Answer. The Department's fiscal year 1998 budget includes $652 million related to counterterrorism/antiterrorism efforts, including prevention, investigation, prosecution, detention, and incarceration. This level reflects recent counterterrorism enhancements received in 1995, 1996, 1997, and 1998, as well as prorated segments of agency program resources related to, or supporting, counterterrorism activities. In 1999, the Department's counterterrorism-related resources total $666 million. The chart below breaks out these resource levels, by agency and by function.

In addition, the following identifies the $60.3 million in specific agency program enhancements requested in the 1999 budget related to counterterrorism and threats to the nation's critical infrastructure/Cybercrime, as well as the current 1998 funding for these programs:

Counterterrorism/Cybercrime Initiative

The United States relies heavily upon its interconnected telecommunications and automated information systems for basic services such as energy, banking/finance, transportation, and defense. Any broadly successful effort by an individual, group, or country to disrupt, destroy, or deny access to the National Information Infrastructure (NII) could result in serious economic, defense, national security consequences. This threat is heightened by the increasing number of incidents of computer intrusions by individuals who, although possessing limited resources, have demonstrated the capability to extensively compromise sensitive computer and telecommunications networks.

1999 COUNTERTERRORISM AND CYBERCRIME INITIATIVE BY COMPONENT [1]

	Positions	Agents/Attorneys	Amount
Federal Bureau of Investigation (FBI)	133	(75)	$22,019,000
Criminal Division (CRM)	17	(13)	1,552,000
Attorney General's Counterterrorism Fund (CTF)			36,703,000
Total	150	(88)	60,274,000

[1] Excludes requested United States Attorney resources of 36 positions and $3,630,000, associated with the prosecution of persons responsible for the commission of criminal offenses involving the use of computers and computer systems.

CURRENT 1998 COMPONENT CYBERCRIME PROGRAM RESOURCES

	Positions	Agents/Attorneys	Amount
Federal Bureau of Investigation (FBI)	167	(99)	$23,909,000
Criminal Division (CRM)	21	(16)	2,345,000
Attorney General's Counterterrorism Fund (CTF) [1]			
Total	188	(115)	26,254,000

[1] Of the $52.7 million provided within the CTF in 1998, $20 million is to be used for reimbursing Departmental components for extraordinary costs incurred in support of efforts to counter, investigate, or prosecute terrorism, and to restore the operational capabilities of offices destroyed or damaged by terrorist acts. The remaining $32.7 million in 1998 funds will be used as follows: $1 million to develop a comprehensive intergovernmental counterterrorism and technology strategy, $10.5 million for counterterrorism research and development, $16 million for State and local first responder training and equipment, and $5.2 million for State and local bomb technician training at FBI's Hazardous Devices School.

The Department's 1999 budget includes $60.3 million in additional funding for counterterrorism/Cybercrime for the following:

Cybercrime and Counterterrorism Investigations.—The FBI's request includes 124 positions (75 agents) and $11.6 million to establish six additional Computer Crime Squads in Atlanta, Boston, Charlotte, Miami, Minneapolis, and Seattle.

Cybercrime/Counterterrorism Coordination, Threat Assessment, and Early Warning.—The FBI's request includes 9 positions and $10.4 million in additional resources for the National Information Protection Center (NIPC), formally the Computer Investigations and Infrastructure Threat Assessment Center. Of this amount, $4.6 million is to conduct infrastructure vulnerability assessments and $4.3 million is to develop a comprehensive Early Warning System. In addition, the request includes funding for training, Computer Crime Squad equipment, and staff to expand the operations of the Watch and Threat Analysis Unit.

Legal/Technical Challenges.—The Criminal Division's request includes 17 positions (13 attorneys) and $1.6 million for the Computer Crime and Intellectual Property Section (CCIPS) to keep pace with the rapidly changing legal and technological environment associated with Cybercrime cases. The Criminal Division plays a critical role in the Federal effort to protect critical infrastructure, secure lawful use of the Internet, and respond to information warfare. The Division provides advice to and coordinates Federal efforts with State, local and foreign governments.

Implementation of the Recommendation of the President's Commission on Critical Infrastructure Protection.—The Attorney General's Counterterrorism Fund request includes $36.7 million, including $33.6 million to implement the recommendations of the President's Commission on Critical Infrastructure Protection, including funding for the expansion of the NIPC and $3.1 million to ensure the continuance of essential DOJ/FBI functions during an emergency.

In addition to the requested enhancement, the Counterterrorism Fund includes $16 million in recurred funding to continue efforts to equip and train State and local first responders to terrorist incidents.

Question. The FBI has requested $11.6 million and 124 positions (including 75 agents) to establish new Computer Investigations and Infrastructure Threat Assessment Squads in six major cities to prevent computer-related, or "Cybercrime." How does this fit into the counter-terrorism efforts by the Department?

Answer. The establishment of the Computer Investigations and Infrastructure Threat Assessment (CITA) squads is due, in part to the inclusion of the National Information Infrastructure with the FBI's National Security Threat List, as well as the Presidential Decision Directive—39, in July 1995. These attacks, which could be carried out by terrorists, criminals, hackers, or foreign agents, might be directed against the United States Government or United States corporations, establishments, or persons and could target physical facilities, personnel, information, or computer, cable, satellite, or telecommunications systems. These teams have responsibilities over both the criminal investigative and the potential national security implications of computer intrusions.

FIRST RESPONDER TRAINING

Question. Attorney General Reno, I am concerned about the Administration's proposal for the Counterterrorism Fund for fiscal year 1999.

The fiscal year 1998 Commerce, State, Justice and the Judiciary Appropriations bill established a Counterterrorism Fund, providing $52.76 million for several initiatives. The Fund included $21.2 million to improve State and Local Response Capabilities in cases of possible chemical or biological agents or explosive devices. This would be achieved through the purchase of equipment and gear for first responder training efforts by experts in the field.

What is the department doing to fully utilize facilities and expertise in First Responder Training for Weapons of Mass Destruction? How do you envision this initiative getting some practical results—in other words, getting training out to the field so that our law enforcement agencies have the ability to respond to terrorists incidents if called upon?

Answer. In 1998, Congress provided $21,200,000 in the Counterterrorism Fund to improve state and local response capabilities in case of possible chemical or biological agents or explosive devices. Of this amount, $5,200,000 was provided for the FBI's Hazardous Devices School at Redstone Arsenal, Hunstville, Alabama. These funds will be used for the expansion and renovation of the Hazardous Devices School, which will allow the FBI to double the number of bomb technicians trained each year for improvised explosives and WMD matters. In addition, the funding will provide certain items and articles of equipment for response to improvised explosive devices by bomb squads, including Percussion Actuated Nonelectric disrupters, robots, and reference materials.

Congress also provided $16,000,000 in the Counterterrorism Fund for first responder equipment and training, specifically: (1) $12,000,000 to provide grants for acquisition of terrorism-related equipment for state and local agencies; (2) $2,000,000 for support operations of the state and local training center for First Responders at Fort McClellan, Alabama; and (3) $2,000,000 for operations of a similar training center at the New Mexico Institute of Mining and Technology. On March 26, 1998, I signed a memorandum delegating responsibility for these programs to the Assistant Attorney General, Office of Justice Programs (OJP).

OJP's long history and experience working with state and local jurisdictions provides the knowledge and infrastructure to effectively and efficiently administer these programs. OJP will work extensively with the FBI in curriculum development and determining state and local requirements for the equipment program. OJP will also coordinate its efforts with OJP's National Institute of Justice's Office of Science and Technology and Bureau of Justice Assistance, the Executive Office of National Security, and other federal agencies as appropriate.

OJP has a long history of working with state and local agencies to administer and implement grant programs and has established strong, positive relationships with these jurisdictions. This, combined with OJP's proven record of designing and implementing anti-terrorism training for state and local jurisdictions, speaks strongly for OJP's ability to administer these initiatives and provide first responders with hands-on training, technical assistance and the field exercises required to prepare them to meet the challenges of responding to terrorist acts.

OJP will develop a comprehensive state and local assistance "umbrella" that will administer the new equipment program and the training initiatives at Fort McClellan, Alabama and at the New Mexico Institute of Mining and Technology, along with OJP's current $5 million First Responder Training Program for Fire and Emergency Medical Personnel. This umbrella will provide a focused, responsive, long-term national capability to execute a comprehensive and highly coordinated first responder training, test, and exercise program.

OJP's efforts will also include the utilization of a consortium of universities, research institutions and other facilities that have resources and expertise critical to the success of any program designed to assist state and local jurisdictions respond to terrorist acts. Initially, OJP will coordinate efforts with the several university and research facilities included in the Conference Report. This will further ensure that appropriated funds are used in a coordinated and complementary manner. Further, such a consortium will provide OJP a means to identify and coordinate resources and expertise that exist at other universities and institutions across the nation.

OJP's existing grant-making infrastructure will enable it to effectively and efficiently develop and implement the equipment acquisition grant program, and will ensure these funds are obligated as quickly as possible. Such equipment will include protective gear and detection, decontamination and communications equipment. These discretionary grants will be jurisdiction-specific and will be awarded based on guidelines and criteria being developed by OJP in cooperation with the FBI, which will consider the equipment needs of fire, emergency medical services, hazardous materials response teams, and law enforcement. This equipment list is also being coordinated with the National Fire Academy and the International Association of Fire Chiefs. OJP will provide necessary technical assistance to the applicant agencies to ensure that the equipment acquired through this program is the most appropriate and technologically advanced available. The demand for first responder equipment is tremendous; there are an estimated 3,000,000 to 5,000,000 first responders working across the Nation.

With respect to the training program under development at Fort McClellan, OJP is designing an incident management course for fire and command staff as well as a tactical considerations course for hazardous materials units and emergency medical personnel. OJP is in the process of determining what personnel should be trained at the Fort, although first responder training could be appropriate for state and local law enforcement, firefighters, emergency medical personnel, public works personnel, and state and local emergency management employees.

OJP is also working with the New Mexico Institute of Mining and Technology, which already has a training program in place, to establish agreements as to training curriculums, trainers and trainee groups.

Question. Is it your intention to develop a comprehensive and integrated first responder training program that utilizes existing expertise and resources that are currently available?

Answer. Yes. The Attorney General's decision to delegate to the Office of Justice Programs (OJP) the responsibility to administer the first responder training programs at Fort McClellan and the New Mexico Institute of Mining and Technology

was based on OJP's experience in working with state and local jurisdictions and its existing infrastructure, which allow it to efficiently implement training and grant programs. In accepting the responsibility, OJP will coordinate its national first responder training activities—including curricula and exercise development—with other federal agencies including the: FBI, Executive Office of National Security, Department of Defense (DOD), and FEMA, as well as those universities and national research facilities with the expertise necessary to provide for a full range of resources. This collaboration will ensure that our nation's first responders receive training that is (1) of the highest quality and utility; (2) non-duplicative; and (3) engineered to provide for the sustainment of knowledge and lessons learned.

Question. What is the current schedule for the implementation of the First Responder training program?

Answer. OJP is committed to having the Fort McClellan training facility operational immediately following the resolution of the outstanding environmental assessment (EA) that is required by the National Environmental Policy Act (NEPA). OJP has drafted an Interagency Agreement (IAA) with the Army Corps of Engineers to assist us in determining if OJP's planned training activities at Fort McClellan will pose any significant adverse impact on the environment. This agreement should be in place soon. Barring any unusual circumstances, the EA should be complete by June 30, 1998. In the meantime, OJP is working with the Fort McClellan Reuse and Redevelopment Authority (FMRRA), and entered into an IAA with them on May 4, 1998. This IAA will allow FMRRA to begin the pre-implementation planning activities for OJP such as: refinement of the Program of Instruction; inventory of existing facilities and equipment; development of a short-term (18 month) planning strategy and a long-term use plan; and development of the memorandum of understanding (MOU) with the Department of the Army for use of specific facilities at Fort McClellan (classrooms, offices, dormitories, etc). These activities will be conducted concurrently with the EA.

OJP is also collaborating with the New Mexico Institute of Mining and Technology (NMI) to develop a first responder training initiative—similar to the one at Fort McClellan. OJP has had planning meetings with NMI to discuss NMI's training capabilities and options for how NMI efforts can support an overall national training approach for first responders. As a result of these meetings, OJP and NMI have defined a critical unmet need for NMI to focus its efforts on in 1998.

NMI's principle task will involve building on OJP's progress in providing critically-needed awareness training to local fire and emergency medical personnel; specifically, OJP will task NMI to modify OJP's Emergency Response to Terrorism: Basic Concepts curriculum, which currently targets local fire and emergency medical personnel, to target the unmet need for a similar curriculum for local law enforcement personnel. In addition to modifying the existing curriculum, NMI will deliver this 16-hour awareness program through training that will provide both a train-the-trainer component for targeted jurisdictions, as well as support on-site training by the certified trainers trained through the train-the-trainer component. This OJP/NMI effort focuses on local law enforcement and does not duplicate any Nunn-Lugar-Domenici training activities.

NMI has submitted a preliminary grant application to OJP for review. A final NMI application will be submitted by May 22, and OJP plans to make an award to NMI by June 12. In the interim—during the expected 30-day grant award process—OJP will provide NMI with standard pre-agreement costs so it can begin its planned program/assessment activities.

Bringing these two facilities online will provide OJP with two critical elements in its overall approach to developing and conducting a national program to train first responders to more effectively and efficiently respond and manage terrorist incidents, and will complement OJP's ongoing training, which targets local fire and emergency medical personnel.

Question. Attorney General Reno, the fiscal year 1999 budget request includes $52.7 million for the Counterterrorism Fund, the same as the 1998 level. However, the budget eliminates funding for technology R&D which is funded at $10.5 million this year. These funds will be used for first responder training.

Does the 1999 budget request of the Department of Justice include any funding to continue support for first responder training?

I understand that the Department is planning a $40 million program for 1999 for first responder training. However, these resources are not in the Department of Justice budget. What funding does the Administration plan to use for this purpose in 1999 to continue this initiative?

Answer. The Department's 1999 budget request includes funding to continue support for first responder training. The Department has requested $16 million from the Counterterrorism Fund to continue to provide Weapons of Mass Destruction re-

sponse equipment and training for state and local first responders. In addition, the Department has requested $5 million in 1999 to continue the first responder training program for local firefighters and emergency medical service personnel.

The Department is not planning a separate $40 million first responder training program for 1999. Rather, it is involved, through the FBI, in the five-year Nunn-Lugar-Domenici Domestic Preparedness Program (NLDDPP) that provides training and assistance to first responders. This effort is funded solely through the DOD as authorized by the National Defense Authorization Act (Public Law 104–201). The DOD received $39.8 million in 1998 to provide training under NLDDPP and will receive $49.2 million in 1999. None of these DOD funds have been provided for use by the Department of Justice in the past, and at the present time I am not aware of plans to distribute the funds to the Department of Justice or any other federal agency.

In an effort to consolidate first responder training, I signed a memo on March 26, 1998, assigning the authority to the Office of Justice Programs (OJP) to administer three counterterrorism programs appropriated to me through the Counterterrorism Fund. These programs include (1) $12 million to provide grants for the acquisition of terrorism-related equipment for state and local agencies; (2) $2 million to support operations of a state and local training center for First Responders at Fort McClellan, Alabama; and (3) $2 million for operations of a similar training center at the New Mexico Institute of Mining and Technology. This action streamlines these first responder resources under an organization—namely OJP—that has (1) extensive experience working with state and local jurisdictions and (2) can provide the knowledge and infrastructure to administer such programs effectively and efficiently. OJP will coordinate extensively with the FBI in curriculum development and recognizing State and local requirements.

OJP has initiated a discussion with the National Emergency Management Association (NEMA), the association representing the State directors of emergency management. OJP officials made presentations on available terrorism training at NEMA's membership conference held in September 1997, in Boston, MA and February 1998, in Washington, D.C. Subsequent to the February conference, NEMA officials asked to meet with OJP to discuss areas where OJP and the state emergency management agencies could work more cooperatively in the terrorism area. A meeting was held with the President of NEMA, the NEMA Executive Director, and selected state emergency management officials on March 26, 1998, in Washington, D.C. to begin joint efforts to examine opportunities for Department of Justice and NEMA cooperation in the area of domestic terrorism and training and exercises to enhance state and local preparedness.

OJP will also work with a consortium of universities, research institutions and other facilities that have resources and expertise critical to the success of any program designed to assist state and local jurisdictions respond to terrorist attacks. Initially, OJP will coordinate with the several university and research facilities included in the conference report accompanying the 1998 appropriations act. This consortium should provide OJP with a means to identify and coordinate resources and expertise that exist at other universities and institutions across the Nation.

In addition, the OJP will administer the $5 million first responder training program for local firefighter and emergency medical services personnel, which is authorized under section 819 of the Antiterrorism and Effective Death Penalty Act of 1996. This training program provides basic counterterrorism training and incident management concepts to 120 targeted metropolitan jurisdictions across the nation, which represent 80 percent of the country's population. The 1999 requested funding of $5 million will allow for seamless continuation of this local training effort, which began in 1997, and will provide for the training of an estimated 30,000 individuals.

Question. Is it Nunn-Lugar-Domenici funding that will be provided through the DOD for use by the Department of Justice?

Answer. The DOD's Domestic Preparedness Program was formed under the fiscal year 1997 Defense Authorization Bill (Public Law 104–201), commonly known as the Nunn-Lugar-Domenici legislation. The bill provides funding for DOD to enhance the capability of Federal, State, and local emergency responders in incidents involving nuclear, biological, and chemical terrorism.

DOD received $39.8 million to provide training under Nunn-Lugar-Domenici in 1998. DOD retains these monies, but in conjunction with FBI, EPA, FEMA, DOE, and PHS, provides training and reimburses agencies for costs incurred. The Department of Justice was not appropriated Nunn-Lugar-Domenici funding from Congress.

Question. Why doesn't the Justice Department budget include funding to assist in what will surely be an ongoing effort to train state and local law enforcement and emergency response personnel in counterterrorism methods and response?

Answer. The Department's 1999 budget request includes funding to continue support for first responder training. The Department has requested $16 million from the Counterterrorism Fund to continue to provide Weapons of Mass Destruction response equipment and training for state and local first responders. In addition, the Department has requested $5 million in 1999 to continue the first responder training program for local firefighters and emergency medical service personnel.

NATIONAL INFRASTRUCTURE PROTECTION CENTER

Question. The 1999 budget does include $33.6 million in the Counterterrorism Fund to implement the recommendations of the President's Commission on Critical Infrastructure Protection (PCCIP). I do not believe that this report has been widely distributed, so could you describe the various uses to which this proposed funding would be directed?

Answer. Executive Order 13010 designated as critical certain infrastructures whose incapacity or destruction would have a debilitating impact on our defense or economic security. Eight were named: telecommunications; electrical power; gas and oil storage and transportation; banking and finance; transportation; water supply; emergency services (including emergency medical services, police, fire and rescue); and government services.

On October 13, 1997, the PCCIP submitted its report, entitled Critical Foundations: Protecting America's Infrastructures, to the President. The Commission noted that all of the designated critical infrastructures are increasingly dependent on information and communications systems that criss-cross the nation and span the globe. That dependence was cited as a source of rising vulnerabilities. While the Commission found no evidence of an impending cyber attack or electrical disaster which would have a debilitating effect on the nation's critical infrastructure, the panel did find widespread capability to exploit infrastructure vulnerabilities. Because the infrastructures are mainly privately owned and operated, the Commission concluded that critical infrastructure assurance is a shared responsibility of the public and private sectors. The Commission's report includes a variety of recommendations for improving the government's focus on infrastructure assurance, as well as suggestions for collaborative public and private organizational partnerships. The Administration is carefully weighing the findings and recommendations of the Commission and developing appropriate policies.

In recognition of the broad range of the threat to critical infrastructures, and to bring about an interagency capability to detect, assess, and act upon threats and intrusion, the Department and the FBI developed a plan to expand the scope and responsibilities of its former Computer Investigations and Infrastructure Threat Assessment Center into a NIPC. As proposed, the NIPC would be jointly staffed by the FBI, other federal agencies, including the DOD, and the public sector. The NIPC will serve as a national resource that supports both cyber and physical emergency response efforts and helps determine if an incident, or series of incidents, is either a criminal or terrorist act, an effort to collect intelligence, or a hostile attack initiated by a foreign power. The NIPC was presented to the Administration for consideration since it makes policy decisions regarding the findings and recommendations of the PCCIP.

Funding proposed for the Counterterrorism Fund would be used in 1999 to implement the policies being developed by the Administration, including the NIPC. As proposed, this funding could be made available by the Attorney General to any federal agency, not just components of the Department of Justice, consistent with Administration policy decisions.

Question. Which organizations would be the recipients of these funds?

Answer. The funding proposed in the Counterterrorism Fund would be made available to federal agencies to implement Administration policy decisions to protect the nation's critical infrastructures.

The FBI, as the host for the NIPC, would be a recipient of the funds. All entities associated with the NIPC, DOD, United States Secret Service (USSS), NSA, CIA, other government agencies, state and local authorities, and members of the private sector will benefit from the use of these funds as the NIPC mission will be forged as a joint effort.

Question. Has the Department done an assessment of what resources might currently be available to meet some of these identified needs rather than creating a new use for the Counterterrorism Fund?

Answer. Yes, the Department has worked closely with OMB to assess what resources are currently available to meet the above mentioned needs to prevent a duplication of effort.

Question. Why is the Department of Justice the lead agency in this regard?

Answer. The Department of Justice, acting through the FBI, has been given the lead role because of the FBI's unique role and authorities in the criminal investigative, counterintelligence, and counterterrorism area. Threats to the infrastructure can arise from a broad spectrum of sources, ranging from a disgruntled insider or juvenile hacker operating within the United States to a foreign intelligence or military service operating from abroad. Accordingly, the FBI may need to utilize its criminal investigative authorities and/or its foreign counterintelligence authorities effectively to investigative and respond to a cyber threat, depending on the source and nature of the threat.

In addition, in the cyber world, it is often not possible to determine in the early stages of an intrusion the source, nature, scope, objective, or methodology of an attack. Therefore, it is impossible to determine whether it is a purely domestic, criminal matter, or involves a threat to the national security. It is also impossible to determine in many cases whether other agencies like the DOD or State, or intelligence agencies, have a role to play. However, in almost all instances, the intrusion will constitute a potential violation of federal criminal law, providing the FBI with jurisdiction to investigate. Both private sector owners and operators of the critical infrastructures have significant roles to play in protecting the nation's critical infrastructures. The NIPC, as an interagency, public-private partnership, brings representatives from the affected entities and establishes direct electronic connectivity with them.

MEXICO DRUG CERTIFICATION

Question. I regret that I was unable to attend the hearing earlier this year where the Attorney General testified about the Department of Justice budget. I wanted to ask a question of the Attorney General which is unrelated to today's topic.

Once again this year, the Administration has taken the controversial step of certifying that Mexico is fully cooperating with the United States in the drug war. It has been widely reported that you disagree with that decision, particularly in light of the continued corruption and increased drug violence in Mexico in the last year.

What role does the Justice Department play in the certification process?

Answer. The process begins with identification by the President of the major drug producing and drug transit countries; in 1997, there were 30 such countries. With respect to each country, the Department of Justice provides factual information and assessments to Administration personnel regarding the cooperation, or lack thereof, and compliance with the goals and objectives of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. The subject areas in which the Department of Justice provided an assessment were: efficacy of narcotics laws and enforcement, including legislative initiatives and bilateral law enforcement cooperation; extradition; mutual legal assistance; money laundering and asset forfeiture; control of precursor and essential chemicals; maritime cooperation; political and official corruption; political will; and progress on any benchmarks set for the country. Various components of the Department of Justice also reviewed all parts of the draft International Narcotics Control Strategy Report (INCSR), including the country chapters and special chapters on money laundering and chemical control.

DEA and FBI support the annual certification process by preparing country briefings on the major drug producing and transit countries. These agencies also provide assessments of narcotics enforcement; money laundering and asset forfeiture; control of precursor and essential chemicals; maritime cooperation; official and political corruption; and political will.

Question. Did the Justice Department recommend to the Administration that it not certify Mexico this year? What specific facts led the Justice Department to make the recommendation it made?

Answer. It would not be appropriate to reveal the internal discussions and deliberations regarding the Administration's ultimate certification decisions. We provided factual information to support our subject area assessments regarding Mexican cooperation and the other "major" countries.

Mexico is an indispensable partner in combating drug trafficking. While we believe that the Government of Mexico attained some significant achievements in 1997, there is more that needs to be done. In 1997, in the Department of Justice's view, President Zedillo continued to demonstrate his strong commitment to combating narcotics trafficking, which he recognizes to be the primary threat to Mexico's national security. In carrying out that commitment, the Government of Mexico continued to strengthen its national counter-drug efforts in certain respects.

Extradition and Mutual Legal Assistance.—On November 13, 1997, I signed with Attorney General Madrazo a protocol to the existing bilateral extradition treaty to

authorize the temporary surrender of persons for trial purposes and their return after prosecution to complete the process or sentence against them in the country of their initial arrest. In addition, the Government of Mexico extradited 13 fugitives to the United States during 1997, six of whom were sought on drug charges; the Government of Mexico also expelled 10 other fugitives whose extradition had been requested (one wanted for narcotics-related offenses).

Moreover, the Mutual Legal Assistance Treaty (MLAT) with Mexico was used with increasing frequency during 1997 in a wide range of cases, including narcotics and money laundering investigations. Under the MLAT and Mexico's Organized Crime Law, the Government of Mexico is now empowered to transfer important cooperating witnesses from prison in Mexico to the United States to testify in United States criminal proceedings.

Money Laundering and Asset Forfeiture.—Further, we have seen some progress in the area of money laundering and asset forfeiture; the Mexican Government issued regulations establishing legal requirements for financial institutions concerning customer identification, reporting of suspicious transactions, and recording and reporting of large-value currency transactions.

The Zedillo Administration also introduced new forfeiture legislation for consideration by the Mexican legislature; the bill addresses issues relating to the administration and disposition of forfeited assets and international asset forfeiture assistance. In addition, the Government of Mexico has provided useful asset forfeiture assistance in three drug cases: a $9 million civil forfeiture case against former Deputy Attorney General Mario Ruiz Massieu in Houston (Southern District of Texas); the criminal forfeiture judgment for $350 million against Juan Garcia Abrego; and the seizure and ongoing forfeiture actions in the Amado Carrillo Fuentes matters in the Southern Districts of New York and Florida.

Chemical Control.—In December 1997, the Government of Mexico passed a comprehensive chemical control law, which for the first time reaches "essential chemicals" used in the manufacture of cocaine and heroin. Once implemented, this law would bring Mexico into substantial compliance with the 1988 U.N. (Vienna) Convention.

While the Government of Mexico has made strides in counterdrug efforts, we would like to stress that more action must be undertaken by the Mexican Government. Specifically, we would like to see improvements in the following areas: corruption remains widespread and disabling within all government institutions; the Bilateral Border Task Forces (BTF's) continue to be beset by numerous problems, including slow "vetting" of investigators and prosecutors, leading to delayed staffing, and inadequate funding; although Mexican courts have found several Mexican citizens "extraditable," the appeals process needs to move inexorably towards the goal of actually extraditing Mexican citizens on drug charges; there were no successful money laundering prosecutions in 1997; the Mexican PGR has yet to establish its money laundering/financial investigations unit; the Government's inability to follow up on United States leads regarding the illicit diversion of precursor and essential chemicals; and in an emerging area of cooperation, we hope to make progress against pharmaceutical drug diversion, for many licitly manufactured but dangerous prescription drugs legally sold in Mexican pharmacies are ending up on the black market in the United States.

Question. Do you think it would bring more credibility to the certification process if a law enforcement agency like the Justice Department (including the DEA and FBI) took the lead role in the certification decision?

Answer. Ultimately, the certification decisions are for the President to make, with the most fair and objective input possible from all pertinent government components. The President as the Chief Executive chooses the lead agency for this purpose. We note that Congress has designated the United States Department of State to take the lead in coordinating United States counter narcotics assistance to foreign countries. See 22 U.S.C. § 2291(b). No other department has a presence like the State Department by way of embassies in virtually every country. This puts the State Department in an excellent position to assess counterdrug performance of each country. Typically, they do so in very close collaboration with Department components, including the DEA and FBI.

Question. What role does the State Department play in the work the Justice Department (including the DEA and FBI) does with Mexico regarding drug trafficking?

Answer. The State Department through the Narcotics Affairs Section takes the lead at the political level in our international counter narcotics cooperation with Mexico. The State Department also plays a major role in coordinating cooperation and assistance with Mexico. The law enforcement country officers are housed in the United States Embassy in Mexico City. The State Department, through the Bureau of International Narcotics and Law Enforcement Affairs, provides a large share of

the funding for training, technical assistance and other resources provided by the United States government. Moreover, it does so in areas that are broader than law enforcement, including demand reduction and alternative development.

Question. Which federal agencies are the most informed about the specific counternarcotics activities undertaken by a particular country and the level of cooperation the United States receives from particular countries?

If Congress were to change the certification law, is there any reason why the Justice Department or DEA could not assume the lead responsibility for advising the President on whether a country is fully cooperating with the drug effort?

Answer. Each federal agency is obviously best informed in its areas of responsibility, e.g., the DEA for operational drug law enforcement, the CIA for intelligence, the Department of Treasury for money laundering, the United States Coast Guard for maritime interdiction, and Health and Human Services for demand reduction.

We are not recommending that Congress should change the certification law at this time. Other components could fulfill this role, but the State Department has the broadest mandate, and perhaps the best perspective, to coordinate all international counterdrug assessments.

Question. Do you agree with the Administration's decision to decertify Colombia, but grant it a national interest waiver, while fully certifying Mexico? Were these decisions consistent given each country's level of cooperation? How would you compare the level of cooperation received from Colombia with that of Mexico? Did Mexico do a better job, a worse job or about the same?

Answer. The Department provided factual information to Administration personnel regarding the cooperation (or lack thereof) of Colombia. I am happy to discuss with you the Department's law enforcement/legal assessment of Colombia. However it would not be appropriate to discuss the internal discussions and deliberations regarding the Administration's ultimate certification decisions.

From a law enforcement/judicial perspective more action must be undertaken by the Colombian Government. We are particularly disappointed with: political corruption at the highest levels of the Colombian Government; lack of real political will; the Colombian reform of narcotics sentencing laws which provided excessively lenient sentence reduction provisions; Colombian drug kingpins' abilities to continue to operate their criminal enterprises from prison; the Colombian legislature's failure to enact a law amending their Constitution to address retroactively the extradition of Colombian nationals; ineffective chemical control; and failure to forfeit any assets in 1997.

Nevertheless, the Colombian Government has, in recent months, made some strides in the two areas: the Government of Colombia did conduct some narcotics investigations in 1997; and they intensified eradication efforts, assigning more pilots and airplanes to the mission, which continued even in the face of armed resistance. Regrettably, however, new cultivations in areas that were not subject to the spray campaign have left Colombia with an increase in net coca cultivation—thus making Colombia number one in the world for coca cultivation.

QUESTIONS SUBMITTED BY SENATOR ERNEST F. HOLLINGS

CYBERCRIME

Question. General Reno, as we all know, the protection of our nation's computer infrastructure is vital to national security. However, recent events, such as the one involving an Israeli teen breaking into a United States Defense Network, have clearly demonstrated the vulnerabilities that exist in this nation's computer systems. And as more and more public and private organizations are connected to the Internet, there is an ever growing potential for cyber terrorism.

General Reno, how much money are you proposing to spend on combating threats to our nation's information systems?

Answer. The United States relies heavily upon its interconnected telecommunications and automated information systems for basic services such as energy, banking/finance, transportation, and defense. Any broadly successful effort by an individual, group, or country to disrupt, destroy, or deny access to the National Information Infrastructure (NII) could result in serious economic, defense, national security consequences. This threat is heightened by the increasing number of incidents of computer intrusions by individuals who, although possessing limited resources, have demonstrated the capability to extensively compromise sensitive computer and telecommunications networks.

1999 Budget Request Related to Cybercrime/Infrastructure Protection

The Department's 1999 budget includes $60.3 million in additional funding for Cybercrime and threats to our Nation's critical infrastructure.

1999 COUNTERTERRORISM AND CYBERCRIME INITIATIVE BY COMPONENT [1]

	Positions	Agents/Attorneys	Amount
Federal Bureau of Investigation (FBI)	133	(75)	$22,019,000
Criminal Division (CRM)	17	(13)	1,552,000
Attorney General's Counterterrorism Fund (CTF)	.....	.....	36,703,000
Total	150	(88)	60,274,000

[1] Excludes requested United States Attorney resources of 36 positions and $3,630,000, associated with the prosecution of persons responsible for the commission of criminal offenses involving the use of computers and computer systems.

Cybercrime and Counterterrorism Investigations.—The FBI's request includes 124 positions (75 agents) and $11.6 million to establish six additional Computer Crime Squads in Atlanta, Boston, Charlotte, Miami, Minneapolis, and Seattle.

Cybercrime/Counterterrorism Coordination, Threat Assessment, and Early Warning.—The FBI's request includes 9 positions and $10.4 million in additional resources for the NIPC, formally the Computer Investigations and Infrastructure Threat Assessment Center. Of this amount, $4.6 million is to conduct infrastructure vulnerability assessments and $4.3 million is to develop a comprehensive Early Warning System. In addition, the request includes funding for training, Computer Crime Squad equipment, and staff to expand the operations of the Watch and Threat Analysis Unit.

Legal/Technical Challenges.—The Criminal Division's request includes 17 positions (13 attorneys) and $1.6 million for the CCIPS to keep pace with the rapidly changing legal and technological environment associated with Cybercrime cases. The Criminal Division plays a critical role in the federal effort to protect critical infrastructure, secure lawful use of the Internet, and respond to information warfare. The Division provides advice to and coordinates federal efforts with state, local and foreign governments.

Implementation of the Recommendation of the President's Commission on Critical Infrastructure Protection.—The Attorney General's Counterterrorism Fund request includes $36.7 million, including $33.6 million to implement the recommendations of the President's Commission on Critical Infrastructure Protection, of which approximately $27 million would be made available to the NIPC. Resources from the fund could also be available to reimburse other Federal agencies for their costs associated with protecting our Nation's critical infrastructure. Also included in the $36.7 million request is $3.1 million to ensure the continuance of essential DOJ/FBI functions during an emergency.

The FBI National Infrastructure Protection Center

The FBI's NIPC will take on a larger, interagency role in fighting Cybercrime and computer intrusions, and will serve as the government's lead mechanism for responding to an infrastructure attack. To provide this capability, the NIPC's 1999 requirements are projected to be 85 FBI positions (17 agents) and $51 million, of which 9 positions and $37.4 million represent program enhancements addressed above.

FBI NIPC RESOURCES

[Dollars in thousands]

	Positions	Agt.	Amount
1999 FBI Budget Enhancement	9	.....	$10,412
1999 CT Fund Enhancement	.....	.....	26,985
Subtotal, 1999 Enhancements	9	.....	37,397
1999 Base NIPC Resources [1]	76	17	13,865

FBI NIPC RESOURCES—Continued

[Dollars in thousands]

	Positions	Agt.	Amount
1999 Total Requirements	85	17	51,262

[1] Note: 1999 base reflects the FBI's planned internal reallocation of 7 support positions in 1998.

Question. Will the money you are requesting get our nation's vital computer systems to a level at which they could be considered "safe?"

Answer. There is no question that the money we request will make the nation's vital computer systems much safer and, we hope, will achieve a level of security reasonable and acceptable for the critical services they provide. But this will be a difficult, long-term task, and achieving a nationwide standard of complete network safety is unlikely in the near future for several reasons. One of these reasons is that most of the nation's critical information infrastructure is neither owned nor controlled by government. While government can lead, teach, promote, deter, and defend, and can even regulate or legislate, many of the everyday decisions that separate a secure computer from an exposed one will be made by the private sector. In addition, whether a computer system is public or private, real computer security rests on at least four complex elements—all of which must be present and integrated.

Technical solutions.—As in the physical world, ease and economy of access to data are constantly at odds with the security of that data. Every technical advancement that enhances the power, flexibility, and utility of information networks invites opportunity for technical errors that create unwitting vulnerabilities. The Boston teenager who acquired root control of a telephone company switch (and twice disrupted phone service for significant periods) did so by stumbling into a vulnerability unknown either to the phone company or to the manufacturer of the switch. Technology—expertly designed and employed—can solve many of our computer security problems, and the Department's initiative is aimed in large measure at promoting technical solutions. But technology is not perfect and will not be invulnerable anytime soon. Emerging technologies may also continue to create communications systems that enhance anonymity and make it more difficult to attribute harmful or illegal conduct to a particular individual. As technology develops, we must insure that while privacy is enhanced, accountability is maintained.

Personnel security.—Even if technology could create perfectly secure systems, these systems are still administered and used by people who make mistakes or betray trust. Much of the former can be addressed by training, which is a large part of the Department's program. But other aspects of this issue are extremely complex. In these days of corporate downsizing, outsourcing, deregulation, and multinational mergers, it is harder than ever for owners or operators of vital networks to control or even know who has unlimited access. Both in government and in industry, we have seen cases where, through a series of subcontracts or international mergers, for example, some surprising fingers have gained authorized access to sensitive keyboards.

Law enforcement response.—When security breaches occur, government must have a coordinated network of agents and prosecutors, well-trained and equipped with state-of-the-art technical tools, to quickly ascertain the facts, stop the attack, and bring the criminals to justice. National and international laws—both substantive and procedural—must be updated and integrated to facilitate rapid global investigations. This, clearly, is the primary focus of the Department's program.

Public opinion.—For reasons apparent in the three items discussed above, computer security is neither easy nor free, but this is not yet common knowledge. Nor is it widely understood that computer security can be just as important to national well-being as traditional physical or national security. As in the physical world, it is much simpler, cheaper, and faster to access data in a system with no technical security—no firewalls, one-time password-generators, encryption, or network security monitors. It is much more convenient not to practice secure computing or worry about personnel security. It will be very difficult for industry to ask the public to spend the money and bear the inconvenience of secure information systems if the public does not see the need. Thus, working toward public education and awareness is also an important way in which government can strongly support the efforts of the private sector to enhance the security of our information systems.

Question. What are we doing to help private industry safeguard their vital computer networks?

Answer. Both the Department's CCIPS and the interagency NIPC housed at the FBI have worked formally and informally with industry to enhance the security of the private infrastructure. In broad terms, the Department is supporting industry by working in all four of the areas discussed above. Some of these efforts include CCIPS's six-year-old Industry Information Group, countless presentations to industry and technical conferences, participation with groups such as the Computer Emergency Response Team (CERT) at Carnegie-Mellon University, the National Security Information Exchange (NSIE), and the Bankers' Information Technology Secretariat (BITS). Further, both CCIPS and the NIPC work closely with industry on security incidents and issues, not only for criminal investigative purposes, but also for incident prevention.

The Department and the private sector are increasingly sharing information and expertise, and the Department is looking for ways to expand this partnership. Indeed, the NIPC is creating an Outreach and Field Support Unit to enhance industry ties. The NIPC is also including industry as a customer of its Watch and Warning Unit so that current information about system vulnerabilities can be disseminated quickly and securely. The Department is also experimenting with solutions like Infraguard, a law enforcement-industry initiative in Cleveland that establishes protocols for reporting and disseminating information about security problems.

Question. General Reno, surprisingly, a number of illegal incursions into restricted computer networks are perpetrated by teenagers. To many of them, breaking into restricted networks is seen as a challenge or mischievous prank, and is not intended as a terrorist act. Nevertheless, their actions are certainly considered criminal activity, and therefore take valuable investigative resources away from the investigation of other possible terrorist activity.

So, what will your agency do to impress on young people that this type of activity is not a game, and that offenders will be prosecuted to the fullest extent possible?

Answer. First of all, we are prosecuting them to the fullest extent possible and publicizing that fact, both to deter them and to deter others. When the statute requires United States Attorneys to obtain declinations from state prosecutors (where the state has a concurrent offense), we are doing this in appropriate cases. As you know, the Boston teenager who interrupted telephone service was prosecuted federally and his case announced (without his name) at a press conference by the United States Attorney and Bell Atlantic. News of this case, specifically written for children (titled "You CAN Get in Trouble for Hacking"), will soon be posted on the Department's Web Page devoted to children, called the DOJ KidsPage (found at www.usdoj.gov/kidspage). There is material on the KidsPage for children, parents, and teachers on many topics, and our Cybercrime materials were created by the prosecutors at the Computer Crime Section. Already posted are our Internet Rules of the Road—rules by which children can protect themselves and respect the rights of others. Also at the site are information and teaching plans to assist instructors in presenting these issues to children in the classroom. Soon to be added is an interactive game called "Are You a Good Citizen?"

The prosecutors in our Computer Crime Section frequently raise exactly these issues in presentations to industry and the public, and have for some time argued the importance of teaching computer ethics in interviews with the press. Moreover, the Department is beginning plans for a more extensive public education campaign, which we hope will elicit the support of industry. We believe strongly that parents, teachers, and the rest of the adult world must teach our children not only how to use computers, but also how not to use them.

STATE AND LOCAL COOPERATION

Question. General Reno, as you know, no federal emergency plan will be successful unless there is close coordination with state and local governments. In many circumstances, state and local emergency agencies will be the first responders to a terrorist act. For this reason, the Nunn-Lugar-Domenici Amendment mandated that contingency plans be established in the event of a terrorist act involving weapons of mass destruction (WMD). This preparation includes the establishment of programs to train emergency personnel at all levels of government in how to respond to incidents involving WMD. This legislation also required that the DOD, along with the FBI, FEMA, EPA, DOE, and other relevant agencies, establish rapid terrorism response teams. These teams will assist state and local emergency authorities in the detection, containment, and disposal of WMD. You are requesting $16 million to continue these initiatives.

General Reno, as you have stated, to date 19 cities have received weapons of mass destruction training from the federal government, and 101 cities are scheduled to

receive training in the future. Could you give us a more detailed description of what that training consists of?

Answer. Training is being coordinated by a federal interagency team composed of representatives from the FBI, FEMA, DOE, EPA, PHS, and DOD. Courses were developed to provide the necessary information and job skills, beyond those that currently exist in the first responder community, to safely and effectively respond to an incident involving weapons of mass destruction. These courses are designed to train the trainers in each of the cities that normally provide instruction to the first responders. The program uses a team approach combining the skills and expertise of the nation's nuclear, biological, and chemical specialists with the skills and expertise of emergency response experts. Six train-the-trainer courses are offered: Emergency Responder Awareness; Emergency Responder Operations; HazMat Technician; EMS Technician; Hospital Provider; and Incident Command. Two additional courses are offered directly to the specific audience. These include Basic Awareness, which is a 30-minute video targeted for non-responders, and a Senior Officials' Workshop designed to instruct cabinet level officials and department heads.

One hundred twenty cities were selected to receive training under Nunn-Lugar-Domenici through a collaborative effort. The DOD, with other federal agencies is authorized to provide training and assistance to enhance the capabilities of first responders to an incident involving a weapon of mass destruction. The United States Army Chemical and Biological Defense Command (CBDCOM), Aberdeen Proving Ground, Maryland, the center of DOD's chemical and biological expertise, is the lead DOD agency charged with enhancing existing metropolitan response capabilities to include nuclear, biological, and chemical incidents.

DOJ's contribution to Nunn-Lugar-Domenici includes one class taught by the FBI. The FBI provides a terrorism threat briefing course that consists of a video that discusses the terrorism threat nationally, followed by information from field office representatives regarding the local threat.

Following the initial training, table-top, and functional exercises provide opportunities for trained city participants to demonstrate practical decision-making applications of the training.

Question. Have the training sessions been successful? Is there any type of follow up on the part of the federal government? How do we know that these cities are maintaining their state of readiness?

Answer. The DOJ believes DOD's Nunn-Lugar-Domenici training program has been lacking; however, efforts are being made to improve the program. Many cities have voiced their frustrations that initial training has fallen short of expectations. A process has been developed to incorporate the cities' suggestions for improvement into subsequent training classes.

The training is designed to train-the-trainer after which the city trains itself. Approximately six months following the initial training, the DOD returns to the city and provides full field chemical training exercise (FTX). A biological table top exercise is conducted approximately one month later. Through these exercises, the cities can assess their readiness levels and make appropriate adjustments to their training and response levels. DOD contract personnel currently maintain a listing of individuals whom they train in each city. However, further records are not compiled by the United States government.

While Nunn-Lugar-Domenici training is supposed to be tailored to the specific needs of a local jurisdiction, based on preliminary assessments, actual experience has revealed that much of the training offered to date is centered on a standard, introductory course. Because this training is not tailored to the different types of first responders, it does not meet the specific operational requirements of firefighters, EMS personnel, or police officers.

The FBI is working to improve communications between DOD and local public safety agencies through the established channels and close working relationships that have developed over the years between FBI field offices and their counterparts in the communities they serve. In addition, the DOJ is considering structuring the DOJ's State and local first responder WMD training and equipment programs to provide a city with more specialized training and the equipment to better prepare and outfit response agencies after the Nunn-Lugar-Domenici training.

Question. How many state and local task forces have been established throughout the country? Will these state and local "emergency responders" have access to the type of equipment necessary to effectively deal with an incident involving WMD?

Answer. The Defense Against Weapons of Mass Destruction Act of 1996, enacted as the Nunn-Lugar-Domenici Amendment (Nunn-Lugar II) to the DOD Appropriations Act for 1997, mandates that the Executive Branch undertake a number of requirements relating to preparedness to respond to the terrorist use of chemical and biological weapons within the United States. The Act mandates that DOD, in coordi-

nation with other relevant federal agencies, establish programs to advise and train civilian emergency preparedness personnel at all levels of government in planning for and responding to WMD incidents. In addition, it directs DOD to establish rapid terrorism response teams for the purpose of assisting such authorities in the detection, neutralization, containment, dismantlement, and disposal of weapons of mass destruction.

Although the FBI does not have "emergency responder" task forces to address life and safety consequences of a WMD incident, i.e., decontamination and remediation, the FBI pursues crisis management planning with federal, state, and local law enforcement groups in order to prepare and respond, as directed under PDD–39, to WMD incidents.

To enhance the federal, state, and local approach to terrorism, the FBI has established 16 joint terrorism task forces (JTTF) throughout the country. These JTTF's have been formed by the FBI to maximize interagency cooperation and coordination to create cohesive units capable of addressing terrorism problems within the United States. The mission of each JTTF is to detect, prevent and investigate individuals or groups carrying out terrorist acts directed against the United States.

The JTTF's are composed of 212 full and part-time, federal, state, and local law enforcement personnel. Federal participants include the INS, USSS, Bureau of Alcohol, Tobacco and Firearms, United States Customs, and Postal Inspection Service, among others. Personnel on these JTTF's also may be members of the FBI's Evidence Response Team or certified bomb technicians. As such, they will receive training and related equipment that will allow them to respond to a terrorist incident involving a WMD.

WIRE TAPPING/ENCRYPTION

Question. General Reno, court ordered telephone intercepts are critically important to combating all types of crime, including domestic and international terrorism and counter intelligence threats.

Could you please bring us up to speed regarding implementation of CALEA and encryption negotiations?

Answer. This information will be forwarded to the Committee as soon as available.

Question. Have you met with FCC Chairman Kennard to discuss these issues yet?

Answer. This information will be forwarded to the Committee as soon as available.

Question. What do you believe is the cost estimate if the communications industry gets its way on slipping the compliance date and other CALEA demands?

Answer. This information will be forwarded to the Committee as soon as available.

NSC DOMESTIC ANTITERRORISM CZAR

Question. General Reno, a recent Washington Post article stated that a Domestic Anti-Terrorism Czar may be appointed within the National Security Council. The article stated that this individual would "assign roles to the 18 federal departments or agencies—including the FBI, CIA, and Pentagon—now involved in the counterterrorism effort, and have authority over everything from the development of yearly budget plans to rescue efforts after a terrorist attack."

General Reno, I thought it was your responsibility to coordinate efforts dealing with domestic terrorism? Are you comfortable with the proposal to establish an Anti-Terrorism Czar within the NSC? Do we really need this additional layer of bureaucracy?

Answer. I strongly support the need for greater coordination of the counterterrorism plans, resources, and programs of the many departments and agencies that have important roles in our counterterrorism and infrastructure protection efforts. The need to achieve greater coordination and eliminate overlap and redundancy, as you know, is one of the drivers for the five-year counterterrorism and technology crime plan that I, along with my colleagues at the Departments of Defense, State, Treasury, Energy, the CIA, FEMA, and other agencies are developing. Similarly, I support a more focused effort within the National Security Council focused on infrastructure issues in order to ensure that programs across the government and outreach to the private sector are properly coordinated. I also believe that the President's National Security Adviser and his staff, in order properly to advise the President, require a mechanism through which they can receive timely information about matters in which the Department of Justice is engaged that affect the President's national security responsibilities. The NSC, for example, will play a key role in the President's decision on whether a criminal law enforcement investigation into a seri-

ous cyber intrusion should be treated as an attack on the United States. I believe that we can develop appropriate procedures that will enable Department of Justice prosecutors and other personnel to fulfill their law enforcement missions while facilitating the NSC's role as adviser to the President.

CONCLUSION OF HEARING

Senator GREGG. This hearing will be recessed, and we will move on to marking up the bill in the near future.

[Whereupon, at 11:20 a.m., Tuesday, March 31, the hearing was concluded, and the subcommittee was recessed, to reconvene subject to the call of the Chair.]

○