FEDERAL STRUCTURES FOR INFRASTRUCTURE PROTECTION

Report to the
President's Commission
on Critical Infrastructure Protection
1997

This report was prepared for the President's Commission on Critical Infrastructure Protection, and informed its deliberations and recommendations. The report represents the opinions and conclusions solely of its developer, Institute for Defense Analyses. The publication of this document should not be taken to represent an endorsement by the Commission for the content of the material contained herein.

Preface

This paper was prepared by the Institute for Defense Analyses in response to tasking from The President's Commission on Critical Infrastructure Protection, to study "Organizational Options for Critical Infrastructure Protection." The paper was reviewed by Robert Anthony, William Barlow, and Michael Leonard. The authors gratefully acknowledge the contribution of the government officials interviewed for this task. We thank Bernie Aylor for support throughout the project, and Eileen Doherty for editing this final report.

Contents

Executive Summary

The options described in an earlier IDA paper called for the creation of a new federal leadership body for protecting the economic infrastructure.[1] The proposed body would lead or coordinate activities across the federal government in each of the five capability areas needed for infrastructure protection. These are strategy and policy formulation, prevention and mitigation, operational warning, consequence management and recovery, and counter-action. This paper examines alternative ways of sharing responsibilities between and among such a new structure for infrastructure protection and existing structures responsible for related activities.

The two current structures most closely aligned with the infrastructure protection mission are examined in some detail. First is the NSC's Coordinating Subgroup on Terrorism (CSG), established initially in NSDD 30 in 1982. Counterterrorism structures are concerned with providing counter-action capabilities against possible terrorist attacks of all kinds, including those involving infrastructure targets or those using cyber technologies. Second are the federal activities in place for responding to crises managed by FEMA through the Federal Response Plan (FRP). This structure provides a unified, "all-hazards" response to damages, regardless of the cause.

Many of the counter-action and response capabilities needed for infrastructure protection are closely related to those being provided by the CSG and FRP. There are gaps in their coverage, however, because neither structure has been tasked to focus explicitly on infrastructure protection. There are thus many potential scenarios in which infrastructure attacks might fall outside of their jurisdiction or missions. The gaps are even more pronounced in the other capability areas. There are no existing organizations providing a focal point for formulating infrastructure protection strategy and policy, fostering prevention and mitigation activities in collaboration with U.S. industry, or providing an integrated operational warning mechanism. Building these capabilities in existing structures would require significant expansion of current missions, the participation of a wider set of federal agencies, and the building of new ties between and among the federal government, state and local governments, and the private sector.

---

1 David R. Graham, Lexi Alexander, Michael Leonard, Paul H. Richanbach, John R. Shea, Richard H. White, et. al., "National Strategies and Structures for Infrastructure Protection," Institute for Defense Analyses, IDA P-3324, June 1997.

Because the relationships between current structures and the needed roles for an infrastructure protection structure vary so much across capability areas, there is no single "best" way to link infrastructure protection with the existing federal structures. In each capability area, it is necessary to consider whether it is better to expand the responsibilities of existing structures to include infrastructure protection, or whether it is better to create a new body that can focus exclusively on the new mission. Where feasible, there obviously are significant advantages in adopting an "all-hazards" approach, which consolidates common or related missions in a single structure. On the other hand, the responsibilities of the existing structures should not expanded to the point where this dilutes their focus on their current missions.

The paper, therefore, examines a range of alternative institutional arrangements for sharing infrastructure protection responsibilities between and among the current structures and a new structure. Three options are discussed. The first embeds infrastructure protection within the existing CSG and FRP structures. These bodies would assume the broader responsibilities and establish the wider set of relationships needed to address infrastructure protection. The second creates a new body—a "Domestic Preparedness Council"—that would take the lead for all five infrastructure capability areas. The third also creates a "Domestic Preparedness Council," but focuses its mission only on those capabilities where there is relatively little overlap with existing entities. This body would assume responsibility for strategy and policy formulation, prevention and mitigation, and certain aspects of operational warning. The CSG would assume responsibility for counter-action, the FRP structure would address recovery. The strengths and weaknesses of these options are discussed in the final section.

FEDERAL STRUCTURES FOR INFRASTRUCTURE PROTECTION

PCCIP ISSUE: NS05

A. INTRODUCTION

The options described in an earlier IDA paper called for the creation of a new federal leadership body for protecting the economic infrastructure.[2] Such a body is needed to address growing concern over the vulnerabilities of the U.S. economic infrastructure to both physical and cyber attack, vulnerabilities which could be exploited by a wide range of potential adversaries to damage the economy and harm American citizens. The proposed body would lead or coordinate activities across the federal government in each of the five capability areas needed for infrastructure protection. These are strategy and policy formulation, prevention and mitigation, operational warning, consequence management and recovery, and counter-action. This paper explores these options in greater depth.

- It describes the kinds of capabilities provided by existing federal structures that are already being used for infrastructure protection;
- It identifies the gaps that remain in each capability area that arise either because the jurisdictions of existing federal structures do not cover infrastructure targets, or because the capabilities needed to adequately address infrastructure vulnerabilities fall beyond their traditional missions; and
- It concludes with three alternative institutional arrangements for filling these gaps.

1. Counterterrorism and Emergency Response

The primary focus here in describing current federal capabilities is on those structures that deal with counterterrorism and the coordination of emergency response activities, because these are the most closely aligned with the infrastructure protection mission. Federal counterterrorism activities are coordinated under the NSC's Coordinating Subgroup on Terrorism (CSG), initially established in NSDD 30 in 1982. Counterterrorism structures are concerned with providing counter-action capabilities against possible terrorist attacks of all kinds, including those involving infrastructure

---

[2] David R. Graham, Lexi Alexander, Michael Leonard, Paul H. Richanbach, John R. Shea, Richard H. White, et. al., "National Strategies and Structures for Infrastructure Protection," Institute for Defense Analyses, IDA P-3324, June 1997.

targets or those using cyber technologies. The federal consequence management framework for responding to crises is managed by FEMA through the Federal Response Plan (FRP). Emergency response structures provide an "all hazards" response to damage, regardless of cause. Thus the CSG and FRP provide important capabilities needed to address infrastructure vulnerabilities in the areas of response and counter-action.

There also are a number of information security initiatives within the government focusing on prevention and mitigation of potential attacks on government information systems and data bases. They provide an important component of an overall federal structure. Their limited mandates and authority, however, restrict their ability to provide a structure for coordinating across the government, or for building relationships between and among the federal, state, and local governments and the private sector.

2. Vulnerabilities

There are many scenarios in which attacks exploiting infrastructures may trigger existing federal counter-action and response capabilities. At the same time, major gaps remain. There is a broad range of scenarios that falls outside the jurisdiction of these federal structures. For instance, cyber attacks may arise from new classes of adversaries that are outside the traditional mission of the CSG. Similarly, attacks on economic targets typically would not lead to a declared emergency, and thus would not trigger the FRP. Moreover, the requirements to respond to cyber attacks fall beyond the kinds of technical capabilities currently organized under the FRP. Hence, existing CSG and FRP structures only partially address the counter-action and response capabilities that will be needed for infrastructure protection.

In other capability areas, the gaps are even more pronounced. There are no existing organizations that provide a focal point for formulating infrastructure protection strategy and policy, that foster prevention and mitigation activities in collaboration with industry, or that provide an integrated operational warning mechanism. Thus, it will be necessary either to significantly alter the missions of the existing federal structures, or to create new structures that can bring focus to building these new capabilities.

3. Options for Addressing Infrastructure Vulnerabilities

Addressing infrastructure vulnerabilities demands a broader focus than that which exists in extant federal structures; it requires expanded federal roles and authorities. It also requires creating new capabilities, and building new federal, state, local, and private

sector relationships. There are advantages to embedding new missions within the existing structures that are already dealing with some aspects of the problem; these must be weighed against the advantages of creating an organization to focus exclusively on the new capabilities and relationships needed to address the new threats. The three options for federal structures outlined in this paper reflect these tradeoffs.

- The first would expand the missions of the existing CSG and FRP structures to encompass the infrastructure protection mission.
- The second would create a new "Domestic Preparedness Council" that would take responsibility for all new needed infrastructure protection capabilities.
- The third approach also would create a "Domestic Preparedness Council," but this option would focus the Council's activities on strategy and policy formulation, prevention and mitigation, and the cyber-specific aspects of operational warning. Under this option, the mission of the FRP framework would be expanded to include response and recovery from cyber attacks. The CSG mission also would be expanded to handle counter-action operations relating to cyber threats and vulnerabilities.

These three options and their strengths and weaknesses are discussed at the conclusion of this paper.

In addition to describing the CSG-FRP structures, three other existing federal structures were reviewed, in order to determine whether they should be meshed with infrastructure protection, or they might serve as a model in structuring new infrastructure protection institutions. Those reviewed deal with counternarcotics activities, counterproliferation, and continuity of government. These mission areas draw on many of the same resources as do the counterterrorism and infrastructure protection missions, and therefore must be coordinated at the national level. These missions do not, however, entail activities that need to be tightly linked with the infrastructure protection mission.

4. Organization of the Report

The organization of this paper is as follows: The current structures for counterterrorism are described in Section B; the structures for consequence management in Section C; and the government information security activities in Section D. Some related federal leadership structures are described in Section E. These sections describe the capabilities that are being provided in each of these areas. Section F then assesses the degree to which these capabilities support the infrastructure protection mission, and

outlines the three options. Section G assesses their strengths and weaknesses, and Section H offers some concluding observations.

B. THE COORDINATING SUBGROUP ON COUNTERTERRORISM

The Coordinating Subgroup on Counterterrorism (CSG) is the central federal coordinating mechanism for counterterrorism operations. Its jurisdiction includes terrorist activities or attacks, regardless of the target or method of attack. Whenever incidents occur, this group acts quickly to obtain needed Presidential authorities and to establish the roles of the participating federal departments and agencies. The CSG also serves as the standing interagency coordinating group, convening weekly to review ongoing counterterrorism policy and program issues. It fosters high-level interactions and consensus building among the various federal bodies having responsibilities to address terrorist-related contingencies and threats. CSG members formulate, coordinate, and recommend policies or actions through the National Security Council to the President. Once recommendations are approved by the President, the CSG coordinates and monitors implementation.

1. CSG Background and Mission

The concept for today's CSG has its roots in a 1982 National Security Decision Directive, NSDD #30. It established a Special Situation Group that was convened by the Assistant to the President for National Security Affairs at the direction of the Vice President. During terrorist incidents, the Special Situation Group advised the President. It was supported by a Terrorist Incident Working Group, comprising representatives from the Department of State, the DCI, DoD, FBI, FEMA and NSC, with augmentation from other agencies as required. This working group provided direct operational support, interagency coordination, and advice and recommendations during an incident.

Today, the Coordinating Subgroup on Counterterrorism is chaired by a Special Assistant to the President within the National Security Council, currently Dick Clark. The chairman sets the agenda for CSG meetings. The permanent members of the CSG are assistant secretary or equivalent level officials (see Figure 1). Membership comprises representatives from the Department of State (The Office of the Coordinator for Counterterrorism, Vice Chair to the CSG), DoJ, FBI, OSD (ASD/SOLIC), the Joint Staff (J-3, SOCOM), CIA (Counterterrorism Center, CTC), and the Office of the Vice President.

As needed, permanent members may be augmented by representatives from DOT (FAA), DoE, the Treasury Department (Secret Service, and Customs), OMB, HHS, and FEMA.

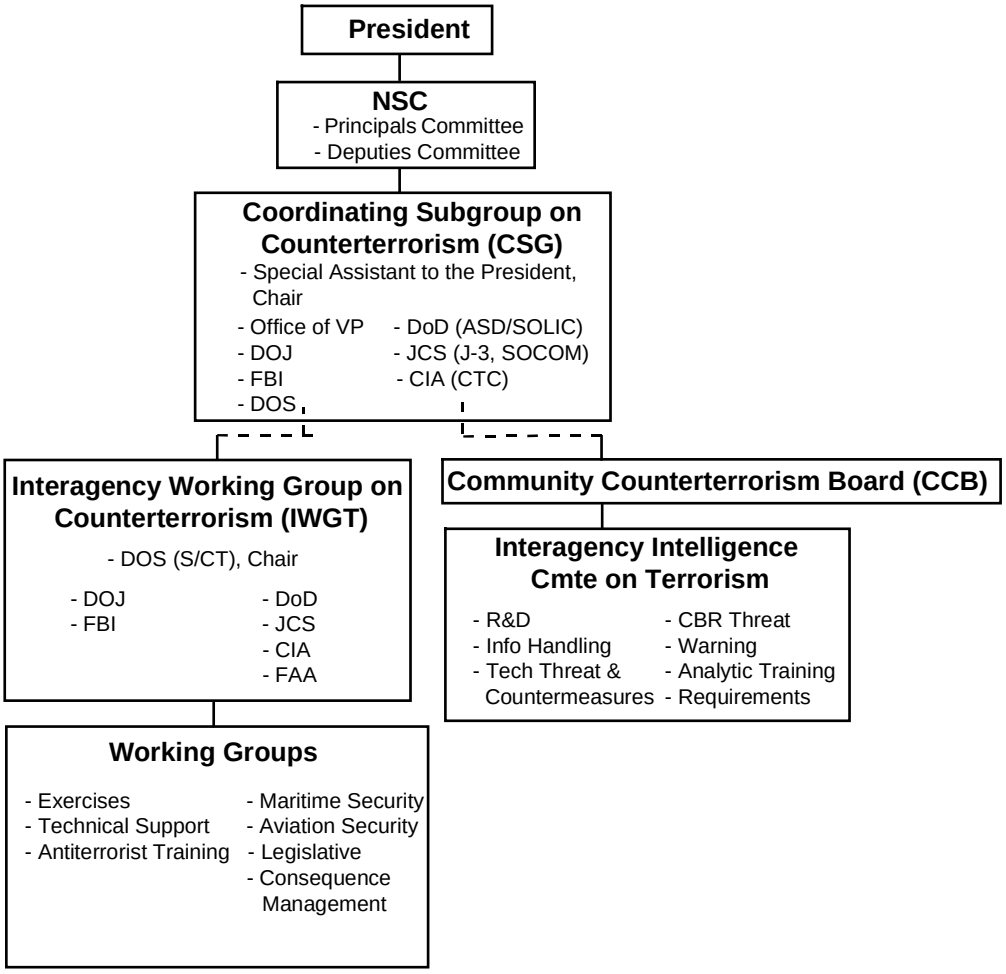

Figure 1. The Counterterrorism Framework

The permanent members of the CSG are brought together, physically or by secure video conference, at least weekly. In addition, any terrorist attack will trigger a meeting of the CSG, and representatives stand in constant alert for fast response. During a crisis, the CSG feeds information to a Deputies Committee of the NSC. The Deputies Committee is chaired by the Deputy Assistant to the President for National Security Affairs, and is the senior sub-Cabinet forum at NSC for policy issues affecting national security. Matters of the greatest importance and urgency are almost automatically elevated to the NSC principals.

The CSG draws on the capabilities of each of its member organizations. For example, the FBI contributes counter-action capabilities in support of the CSG's mission. Within the FBI are structures targeting international terrorists as well as domestic criminal and anti-social groups. DoD provides assets needed to address terrorism abroad. Each of these agencies also are developing assets to address cyber terrorism or information warfare. Within the last year, the FBI created the Computer Investigations and Threat Assessment Center (CITAC) in order to build capabilities for addressing cyber-crime and cyber-terrorism. The CITAC is developing capabilities in the areas of prevention and mitigation, operational warning, and counter-action. DoD provides information warfare assets, both offensive and defensive. The recent emphasis on developing these new capabilities suggests that the counter-action capabilities needed for infrastructure protection could be organized effectively through the existing CSG structure.

On the intelligence side, the CTC, created in 1986, focuses the national intelligence efforts to combat terrorism, and provides the NSC's and CSG's link to the intelligence community. The CTC comprises personnel from all four CIA directorates and from various agencies within the Counterterrorism community, including officers from more than a dozen government agencies, including NSA and DIA.

There are two important interagency bodies that coordinate counterterrorism initiatives and ongoing activities; the Interagency Working Group on Counterterrorism, and the Community Counterterroism Board.

2. The Interagency Working Group on Counterterrorism

Created in the 1970s as the Interdepartmental Group on Terrorism, the Interagency Working Group on Counterterrorism (IWGT) is organized under the leadership of the Department of State; it is chaired by Ambassador Phillip C. Wilcox, Jr. from the Office of the Coordinator for Counterterrorism at State. The IWGT provides a standing structure for coordinating a wide range of counterterrorism activities. It is responsible for developing policy on terrorism; it addresses organizational issues, proposes legislation, and coordinates interagency exercises and training activities. Membership includes all departments and agencies with responsibilities related to counterterrorism.

The IWGT operates through six functional subgroups, which provide an interagency forum comprising all eight departments and over sixty agencies. For

example, one of these subgroups is the Technical Support Working Group; Mike Jakub, also from the Office of the Coordinator for Counterterrorism, DoS, currently serves as its Executive Director. The Technical Support Working Group oversees the National Counterterrorism Research and Development Program, which coordinates resources and promotes information sharing among working group members. It also provides some of the funding for the research, development, and rapid prototyping of antiterrorism and counterterrorism technologies for use by federal, state, and local agencies.

Other sub-groups deal with such issues as training and exercises, aviation security, and maritime security. Many sub-groups are chaired by senior officers in the Office of the Coordinator for Counterterrorism, DoS.

3. The Community Counterterrorism Board

The Community Counterterrorism Board (CCB) is an arm of the DCI's Counterterrorism Center (CTC). It is the intelligence community's focal point for coordination of national counterterrorism intelligence, and for coordination and production of national-level intelligence assessments on terrorism. The CCB is responsible for initiating, facilitating, and coordinating terrorist threat assessments, advisories, and alerts; organizing warning and forecast meetings and agendas; and supporting special projects, such as the development and installation of the community's Automated Counterterrorism Information System. The CCB's Deputy Executive Director chairs the community's Incident Review Panel which meets monthly to review international incidents for inclusion in the community's terrorism data base.

Through the CCB, intelligence can be declassified and conveyed to targeted airlines, businesses, or the public. The actual dissemination of coordinated community threat assessments and warnings is the responsibility of several different departments and organizations. For example, the FBI uses its domestic Terrorist Threat Warning System to provide advisories and warnings to affected national, state, and local law enforcement officials; DIA disseminates threat advisories and warnings to DoD personnel around the world; and the FAA passes information to the airlines.

Under the CCB is the Interagency Intelligence Committee on Terrorism, chaired by the CCB's Executive Director. This Committee coordinates many initiatives, and assists the DCI with the coordination of national intelligence on terrorism and with the promotion of effective use of intelligence resources. It has several subcommittees that focus on specific topics.

- The Subcommittee on R&D. Chaired by the CIA, it provides a working-level interaction of technical officers within the Counterterrorism community who are involved in operations, research, development, or engineering activities.
- The Information Handling Advisory Group. Chaired by DoD, it exchanges information and provides a forum for discussion of information handling issues; it also coordinates information handling efforts within the Counterterrorism community.
- The Technical Threat and Countermeasures Subcommittee. Chaired by the CIA, it collects and assesses information on technical devices and techniques used by terrorist organizations; it also facilitates prompt evaluations of the technical threat posed by specific organizations and provides an avenue for timely guidance to the community on Countermeasures required to meet new threats.
- The Subcommittee on Chemical, Biological, and Radiological Threat. Chaired by DoE, it serves as the forum for examining present and future threats and vulnerabilities.
- The Subcommittee on Warning. Chaired by the State Diplomatic Security Bureau, it develops policies and procedures for operating an effective National Warning System for terrorist threats (alerts and advisories).
- The Subcommittee on Analytic Training. Chaired by DIA, it promotes training and career development for counterterrorism analysts and managers from throughout the Counterterrorism community; it also supports the community's Counterterrorism training program provided by the Joint Defense Training Facility.
- The Subcommittee on Requirements. Chaired by DIA, it identifies and translates consumer needs into prioritized requirements for intelligence collection, processing, analysis and dissemination programs; it also coordinates the community's Counterterrorism inputs to the Chief of the Counterterrorism Center in his role as the DCI's Issue Coordinator for Terrorism.

4. Operational Structures and Procedures

When an incident occurs that may involve terrorism, the Coordinating Subgroup on Counterterrorism is activated to quickly establish federal agency roles and responsibilities. Moreover, the federal response framework established by Presidential Decision Directive 39 also is implemented. PDD-39 divides the federal response to a terrorist incident into two major components: crisis management, and consequence management.

Crisis management involves measures to resolve a hostile situation, investigate an incident, and prepare a criminal case for prosecution. The Department of Justice is the lead federal agency for crisis management. It exercises its authority through the FBI.

Consequence management includes measures to protect health and safety, restore essential government services, and provide emergency relief for affected governments, individuals, and businesses. FEMA is the lead federal agency, and coordinates the activities of other departments and agencies through the Federal Response Plan.

Given an incident involving suspected terrorism or federal criminal activity, crisis management is the initial priority, and the FBI is given the federal lead. In this capacity, the FBI establishes a Domestic Emergency Support Team (DEST) to direct the activities of other federal agencies responding to the crisis, including DoD, DoE, or FEMA. The primary role of the DEST is to provide expert advice to the FBI's on-scene commander concerning the technical dimensions of the crisis, the capability of available assets, and the tactics for their employment. For a chemical, biological, or radiological terrorist incident, the FBI would implement an appropriate contingency plan. These plans bring together federal tactical, technical, scientific, and medical support to the FBI, and serve as a bridge between law enforcement and medical response communities.

Depending on the specific nature of an incident, at some point during a crisis the leadership may transition from the FBI to FEMA. This would occur when the Attorney General determines that law enforcement priorities are outweighed by health and safety concerns. In practice, the crisis management and consequence management structures operate in parallel.

C. EMERGENCY RESPONSE (CONSEQUENCE MANAGEMENT)

The three-pronged role of the federal government in consequence management is (1) to reinforce the state and local governments when they cannot cope with an emergency; (2) to provide for training, education, research, and planning for emergency management; and (3) to provide a focus for the national emergency management community. Federal departments and agencies also are responsible for managing emergencies and threats to their own installations and operations.

The Stafford Act (Public Law 93-288) defines the role of the federal government in emergency management and provides authority for the President to take action when necessary. The Presidential authorities generally are delegated to the Director of FEMA,

who is the person in the Executive Branch responsible for planning, preparing, and implementing the federal role in emergency management. FEMA is an independent agency with a staff of about two thousand employees and a multi-billion dollar annual budget, the bulk of which is in a Disaster Relief Fund.

The federal government is authorized to address legally declared emergencies or disasters. In layman's terms these are sudden, generally unexpected events that injure humans, damage property, and disrupt institutions. There are three basic kinds of emergencies for which the federal response system prepares: natural disasters, technological disasters, and the intentional actions of humans.

- Natural disasters include storms, floods, earthquakes, volcanic eruptions, tsunami, blizzards, forest fires, and drought.
- Technological disasters are unintentional man-made accidents, including structural fires, explosions, toxic spills, hazardous materials incidents, and pollution.
- Intentional actions include crime, terrorism, civil disorder, low-intensity warfare, conventional war, and nuclear attack.

Two basic principles govern the federal role in domestic emergency management: reinforcement, and all-hazards coverage.

The *reinforcement approach* is a legacy of the federal form of government in the United States wherein the primary responsibility for emergency management rests first with the local governments and then with the state governments. Responsibility for emergency response rests initially with the localities—the approximately 3,800 counties and municipalities, each of which has police, fire, emergency medical, and engineering services, to be the "first responders." They do this day-in and day-out for minor emergencies. When the local government cannot manage a large emergency, they call for reinforcement by state resources. Most emergencies are handled at the state or local level, without federal help. When the state cannot manage a major emergency, the Governors call for reinforcement from federal resources. In general, the system is set up so that lower levels of government have to request assistance before it can be sent.

This principle of reinforcement means that FEMA generally must wait until a Governor asks for help before help can be sent. This approach was criticized in the wake of recent hurricanes and earthquakes because the response by the federal government was perceived to be too slow. There is heavy pressure for the federal government to be more proactive and to send help in some cases before it is requested.

All-hazards coverage proposes that there is—or should be—a single national system to manage all emergencies, instead of unique systems for each kind of emergency. The all-hazards approach is generally feasible because the consequences of emergencies tend to be the same, regardless of cause: people killed or injured; people in need of food and shelter; transportation, communications, power, and other essential services disrupted; commercial and community institutions out of order; and normal life affected adversely. This idea is expressed in the thought that the results of an explosion are the same regardless of whether the explosion was accidental, purposeful, or incidental to some other event.

1. The Missions of FEMA

The current framework for federal emergency management activities began with the formation in 1979 of the Federal Emergency Management Agency. FEMA was established by President Carter to provide a single agency to coordinate the governmental response to the above defined emergencies. Five agencies were combined into one:

- The Defense Civil Preparedness Agency was moved from DoD; its charge was protecting the population, industry, infrastructure, and societal institutions in the event of nuclear attack, and lesser emergencies.
- The National Fire Prevention and Control Administration was moved from the Department of Commerce.
- The National Flood Insurance Administration was moved from the Department of Housing and Urban Development.
- The Federal Disaster Assistance Administration was moved from the Department of Housing and Urban Development.
- The Federal Preparedness Administration (mobilization) was moved from the General Services Administration.

These five separate agencies initially resisted integration, but after several years FEMA managed to establish a comprehensive emergency management system for the entire spectrum of emergencies.

During its formative years, FEMA not only had to find a way to deal with all its disparate parts, but also it had to accommodate the new kinds of threats that arose in the 1980s. Hazardous materials and pollution emerged as a significant cause of technological emergencies; after much debate, responding to hazardous materials and pollution were incorporated into the overall emergency management scheme. The Three Mile Island

incident made it necessary to deal with nuclear explosions or accidents, and to incorporate radiological emergency preparedness into the framework as well, including approval of local evacuation plans for nuclear power plants. Major earthquakes demanded attention, as did the need to strengthen the federal response to hurricanes.

Most of the time and attention dedicated to incorporating these additional missions into the overall federal framework was taken up in determining who would be responsible among the federal agencies. There was much turf-fighting. When no existing agency was obviously in charge, sometimes a new agency was created. For example, the Environmental Protection Agency was formed, in part, to institutionalize the management of environmental emergencies posed by toxic waste dumps.

Terrorist attacks comprise another class of emergencies of growing concern, and as counterterrorism has grown as a mission, there have been disputes over who would be in charge at the federal level. Only recently has a modus vivendi been reached, as outlined above in the discussion of PDD 39. Under the present system, the FBI is responsible for the incident itself; FEMA is responsible for the consequences of the incident. As with other emergencies, FEMA's role is to coordinate the actions of the other federal agencies responding to the crisis.

2. The Federal Response Plan

The Federal Response Plan (FRP) was prepared during the Bush Administration to obtain agreement from all participating federal departments and agencies on how emergency response would be handled. FEMA is the overall coordinator. An inter-agency Catastrophic Disaster Response Group (CDRG) was established at the national level, supported by an Emergency Support Team at the FEMA emergency operations center. The CDRG meets periodically and is activated for each major emergency. Each department and agency also has a team operating at its own emergency operations center.

Responsibility for coordinating emergency response activities on the scene is assigned to a Federal Coordinating Officer appointed by the Director of FEMA on behalf of the President. This Officer, who is normally a FEMA senior executive, operates a Disaster Field Office staffed by a core of FEMA workers and augmented by elements from other agencies.

Emergency Response is divided into twelve Emergency Support Functions (ESF); a primary agency and one or more support agencies are designated for each function.

Each primary agency's responsibility is to "plan and coordinate with their support agencies for the delivery of ESF-related assistance." Their functions are optimized for emergency response. These functions and their primary agencies are identified in Table 1.

Table 1. Emergency Support Functions and Primary Agencies

1. Transportation: DoT	7. Resource Support: GSA
2. Communications: NCS	8. Health and Medical: HHS
3. Public Works and Engineering: DoD	9. Urban Search and Rescue: DoD
4. Firefighting: USDA	10. Hazardous Materials: EPA
5. Information and Planning: FEMA	11. Food: USDA
6. Mass Care: American Red Cross	12. Energy: DoE

Source: Federal Response Plan

FEMA's role in the FRP and its success in executing field operations has relied on building consensus and support from other federal departments and agencies. It has no directive authority; it also has no role in policy making. The authority of FEMA was expanded, however, by the enactment in 1988 of the Stafford Act and the more recent modification of the Defense Production Act to permit the use of resource priorities and allocations authority for domestic emergency response. In a rush to discharge cold war artifacts, the Civil Defense Act was rescinded, but the Stafford Act and the Defense Production Act together continue to provide an adequate basis for protection of population, industry, infrastructure, and society.

FEMA's influence at the state and local level derives to a great extent from the fact that it provides federal funds to pay for state and local employees; it provides their training and subsidizes the construction and operation of their emergency operations centers. Analogous to their counterparts in the federal government, state and local officials are more interested in the day-to-day problems of crime and floods than in the remote (to them) possibility of terrorism and nuclear explosions. In most localities, it is only federal money with strings on it that motivates local responders to address these issues.

Soon after the formation of FEMA, all the state governments adopted the FEMA model, and formed their own emergency management offices to provide a single state

manager. There is, for example, a Tennessee Emergency Management Agency and a Pennsylvania Emergency Management Agency. There also has been a consolidation of emergency management planning, preparation, and response at the local level. Each county and municipality formed an emergency management office. Much of the time the police handle the situation, sometimes the fire service, and sometimes both.

One valuable legacy of cold war emergency preparedness activities is an elaborate infrastructure for the command and control of the nation's emergency management providers. Under the Civil Defense program, each state, county, and municipality built an emergency operations center with its own power source and communications center to manage emergencies. Each state employs full-time personnel who are trained either at FEMA's National Emergency Training Center or by FEMA mobile training teams. FEMA operates ten regional offices headed by a political appointee, and each has a full staff and one or more emergency operations centers with security, energy, communications, and emergency supplies. At the national level, each federal agency has its own emergency operations center, and is prepared to operate from alternate locations operated by FEMA. Taken together, these facilities constitute a formidable emergency command system that can be used to manage responses to multiple emergencies.

3. Recent Initiatives Addressing Acts of Chemical and Biological (C/B) Terrorism

As concerns about the possibility of chemical and biological terrorism have grown, the federal government has added a range of new C/B response capabilities to the existing response framework. As of June 21, 1996, medical response to C/B terrorism is officially coordinated through an appendix to the Health and Medical Services Annex of the FRP. Known as *The Department of Health and Human Services Health and Medical Services Support Plan for the Federal Response to Acts of Chemical/Biological (C/B) Terrorism*, this appendix provides the outlines for a timely, coordinated federal response to the health and medical aspects of a chemical or biological terrorist incident.

Each emergency support function is headed by a primary agency that has been selected based on its authorities, resources, and capabilities. Response actions for health and medical services' needs are directed by the Department of Health and Human Services (HHS) through its executive agent, the Assistant Secretary for Health. The Office of Emergency Preparedness is the action agent. The field operational agencies include the HHS Regional Health Administrator and the Environmental Protection Agency Regional Administrator.

Because a single act of C/B terrorism could quickly overwhelm state and local medical systems and necessitate urgent federal assistance, HHS has the authority to implement portions of the C/B Terrorism appendix prior to a Presidential Disaster Declaration and the formal implementation of the FRP. The federal health and medical response to a C/B terrorist incident may begin as either a crisis management response under the direction of the FBI, or as a consequence management response under the direction of FEMA.

The C/B Terrorism appendix lays out a comprehensive public health response to a chem-bio terrorist attack including the triage, treatment, transportation, hospitalization, and follow-up of victims. HHS assists the FBI in threat assessment, provides technical advice and assistance to federal, state and local governments, pre-positions resources, coordinates health-related public information, and prepares medical resources and services for mobilization and support. Additional specialized technical, scientific, and medical resources also can be called upon from HHS, DoD, DoE and EPA.

The appendix also calls for HHS to coordinate the federal health and medical services assistance that will be provided to state and local governments. HHS could provide incident-site management, and coordination of federal emergency health and medical services and technical support. Twenty specific, highly specialized, and time-critical health and medical service areas are identified; potential suppliers also are identified, primarily within DoD, EPA, and the Veteran's Administration.

Finally, in order to address large-scale crises, HHS can activate the National Disaster Medical System. This system is designed to care for as many as 110,000 victims, in cases where a crisis overwhelms the medical care capability of an affected state, regional, or federal health care system. To accomplish this, the National Disaster Medical System relies on a cooperative asset-sharing partnership among HHS, DoD, VA, FEMA, state and local governments, and the private sector. It provides for medical assistance in the form of a Medical Support Unit, Disaster Medical Assistant Teams, Special Teams, and medical supplies and equipment. It also oversees the evacuation of patients that cannot be cared for locally, and transports them to one of a national network of non-federal medical care facilities that are pre-committed to receive patients.

D. INFORMATION SECURITY

Information security is a critical aspect of infrastructure protection since it embodies the essential capabilities for the prevention and mitigation of cyber attacks.

This area has been of growing concern within the federal government, and a number of new activities has been initiated to address the vulnerability of federal information systems to compromise or attack.

Currently, there are two broad communities with the federal government dealing with information security. The first focuses primarily on national security concerns. The key actors in this community are NSC, DoD, DISA, NSA, and the National Communications System (NCS). The second community deals with civilian agencies and unclassified information. The key actors in this community are OMB, GSA, NIST, CERT and (potentially) the newly established Chief Information Officers' Council (CIO). GAO reviews of current programs find that there is a mixed record among federal organizations in the establishment of information security policies, programs, or regulations that govern the activities of private firms.[3]

Because these existing activities look inward at federal information systems, and because they currently lack a unified philosophy or approach to information security, none of them currently provides the same kind of basis for an infrastructure protection leadership entity as is provided by the CSG or the FRP. Nevertheless, these activities are providing needed capabilities, especially for prevention and mitigation, that are not being provided elsewhere, and therefore should be woven into any overall federal structure for infrastructure protection. These activities would provide technical support and leadership for prevention and mitigation activities under the umbrella of a federal leadership structure.

Some of the government's specific information security activities that provide important capabilities for infrastructure protection are reviewed in the remainder of this section.

1. National Security Community Responsibilities and Activities

The main capabilities for infrastructure protection are provided by NSC, DoD, DISA, NSA, and the NCS. The NSC's interagency Security Policy Board (SPB) oversees the development of federal security policy, including classification management, security countermeasures, personnel policies, and facilities protection. While the SPB has the potential to make an important contribution as a coordinating framework for the

---

[3] GAO, "Information Security: Opportunities for Improved OMB Oversight of Agency Practices." (Chapter Report, 9/24/96, GAO/AIMD-96-110).

government's information security activities, many observers believe it has not proven to be sufficiently powerful to forge an integrated prevention and mitigation program across the federal government. One criticism of the SPB is that its alignment and makeup is oriented toward the national security community, and therefore it is not fully attuned to the perspectives and needs of the civilian agencies.

At the operational level, DoD engages in a wide range of information security and information warfare-defense activities. These programs are distributed throughout OSD, the Joint Staff, the Services, and Defense Agencies. The Secretary of Defense is the executive agent for signals intelligence and communications security activities. NSA executes these responsibilities, and conducts research and development as necessary. It provides the products and services to protect classified and unclassified national security systems. NSA also is responsible for the protection of all classified information stored or transmitted using government information systems. The NSA Director is the executive agent for interagency operations security training.

NCS is an interagency activity supporting planning for and provision of national security and emergency preparedness telecommunications for the federal government in times of war and major emergency.

Within these agencies are many specific sub-activities playing key roles. There are several specific activities that should be incorporated into the overall structure for infrastructure protection:

- DoD's Defense Information Systems Agency (DISA): DISA is responsible for ensuring the availability, reliability, integrity, and security of the Defense Information Infrastructure (DII).
- Interagency Information Management Policy Group (IIMPG): This group addresses information security issues involving DoD and DCI organizations.
- The Information System Security Research Joint Technology Office: This office coordinates the information systems security research programs of DARPA and NSA, developing technologies to safeguard DoD information systems.
- NSA's Interagency OPSEC Support Staff (IOSS): NSA is the executive agent for federal operations security programs, and maintains the IOSS to execute this responsibility. Each agency with national security responsibilities must implement a formal OPSEC program.
- NSTAC: The National Security Telecommunications Advisory Committee provides an industry perspective on policy and investments in the National

Communications System. Members include top executives of major communications and information systems companies.

- The National Security Telecommunications and Information Systems Advisory Committee: An operational-level interagency group, this committee develops operational policies, guidelines, instructions, and standards. It also assesses national security systems, and interacts with an NSC committee of principals. The NSC provides a supporting secretariat.

2. Civilian Agency Responsibilities and Activities

On the civilian side of the federal government, the Office of Management and Budget has the overall responsibility for establishing information security policies and programs. OMB's Office of Information and Regulatory Affairs (OIRA) provides guidance, policy, and control for federal information technology procurement, and establishes minimum program requirements for security of federal automated information systems. It administers this program through OMB Circular A-130. Under this program, OMB issues guidelines for annual evaluations of federal accounting and administrative controls.

The other key civilian bodies are GSA, NIST, and the CERT. GSA provides many of the operational capabilities needed to implement OMB's guidance. NIST is responsible for issuing telecommunications standards for the federal government. NIST also is responsible for issuing government-wide, computer system security standards, as well as guidelines for training programs to protect sensitive unclassified information in federal computer systems. (NSA provides technical assistance, e.g., for encryption.) NIST assists federal agencies in complying with requirements for federal emergency response capabilities. It helps users when security incidents occur, and shares information concerning common vulnerabilities and threats.

The Computer Emergency Response Team (CERT) provides a wide range of prevention, mitigation, warning, and response capabilities. It publishes incident reports and threat and vulnerability analyses. It provides assessments and advice or organizations that seek advice. It issues notices and warnings of potential attacks. Finally, it responds to attacks when called. In sum the CERT provides a strong technical foundation for many infrastructure protection activities. It thus should be an important component of any overall national structure.

Some of the specific capability centers that contribute to infrastructure protection are as follows:

- GSA's Office of Information Security: The General Services Administration provides technical security services through its Office of Information Security, including systems engineering, network management, training, and procurement. It participates in the development of a security infrastructure to support government-wide applications, both classified and unclassified.
- NIST's Federal Computer Incident Response Capability (FedCIRC): FedCIRC supports the federal civilian community by publishing analyses of computer incident threat and vulnerability information, and issuing alerts. FedCIRC hosts incident-handling conferences, training sessions, and threat meetings. It also provides security evaluation of agency programs, and provides a 24-hour incident hotline to offer technical assistance and backup support to agency response teams.
- NIST's Computer System Security and Privacy Advisory Board: This Board identifies emerging managerial, technical, administrative, and physical safeguard issues relative to federal computer and telecommunications systems. The Board has twelve members drawn from the government, industry, and the science and technology communities.

Executive Order 13011, *Federal Information Technology*, created a Chief Information Officers Council as the principal interagency forum to improve agency practices for the mangement of information technology. The CIO council's charter states that its purpose is to provide a forum to "improve agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources." The CIO council first met in August, 1996, and has subsequently established a charter, strategic plan, and committee structure. It's main thrusts have been in the areas of interoperability, solving year 2000 problems, education and training, and capital planning and investment. It has discussed information security issues, but has not adopted these as a major focus of its activities. Thus the CIO council provides a possible leadership entity for information security, but at present it is not playing this role.

The mandates of the existing federal information security activities are focusing on many prevention and mitigation initiatives, but they continue to be too narrowly limited when viewed from the perspective of the infrastructure protection challenge. These entities are focusing of prevention and mitigation within the federal government. Hence, they provide an important part of an overall federal structure, but because of their limited mandates and perspectives, none of these bodies provides an appropriate structure

for coordinating across all of the four capability areas needed for infrastructure protection. Nor do any of these bodies, which focus nearly exclusively on internal government issues, provide an effective mechanism for coordinating public-private interactions across the government.

E. OTHER FEDERAL STRUCTURES

In reviewing federal leadership structures, a number of related activities were considered to determine the potential degree of overlap with the infrastructure protection missions. Three such entities are briefly described here. In general, we find that these structures draw on many of the same resources as do counterterrorism and infrastructure protection, and that the overall allocation of resources must be coordinated by the White House and the Congress. However, the day-to-day activities are not all that closely related, so a tight operational linkage is not needed.

1. Counternarcotics

Counternarcotics activities are directed by the "Drug Czar" in the Office of National Drug Control Policy (ONDCP). This office, established by Congress in 1988, is organized within the Executive Office of the President. The Director, currently General Barry McCaffrey, is appointed by the President. As a member of the President's Cabinet, the "Drug Czar" serves as a "drug issues advocate" within the cabinet by developing collaborative relationships with other Cabinet members and by keeping the Cabinet and the President apprised of the nature of the threat from illicit drug use. Reporting to the Director are the Deputy Director for Demand Reduction, the Deputy Director for Supply Reduction, and the Associate Director for State and Local Affairs. All three positions are filled by presidential appointees. The ONDCP Director personally appoints the Director of the Counter-Drug Technology Assessment Center. Also reporting to the Director is the Chief of Staff. The ONDCP organizational structure includes an Office of General Counsel, the Office of Planning, Budget, and Research, and the Office of Public Legislative Affairs.

The ONDCP is the focal point of the nation's counternarcotics efforts. It is tasked with developing, coordinating, promoting, and implementing the policies, priorities, and objectives of the nation's drug control program for reducing the manufacturing, trafficking, and use of illicit drugs; drug-related crime and violence; and drug-related health consequences. The ONDCP produces a National Drug Control Strategy, which

outlines and directs the U.S. anti-drug efforts. The National Drug Control Strategy also establishes a program, oversees a National Drug Control Strategy Budget, and provides guidelines for cooperation among federal, state and local entities. The ONDCP coordinates more than 50 federal government agencies with domestic and international counternarcotics responsibilities.

The ONDCP has divided its drug control priorities into four primary areas of interest: treatment, prevention, domestic law enforcement and interdiction, and international. In implementing its core responsibilities, the ONDCP conducts research and development in new supply and demand reduction technologies through the Counter-Drug Technology Assessment Center. ONDCP is also responsible for overseeing the High Intensity Drug Trafficking Area program, which provides resources to areas identified as having the highest, most far-reaching drug-trafficking problems.

There currently is little formal interaction between the Counternarcotics community and the Counterterrorism community. In part this reflects a degree of geographic specialization. The Counterdrug community tends to focus on Latin America, Central America, and Mexico. In these regions, counterdrug and counterterrorism activities are two aspects of a common problem, because the same criminal elements tend to be involved in both. Elsewhere around the world, groups involved in terrorism tend to be motivated by politics, nationalism, or religion, and so there is a lesser connection between terrorism and drug trafficking.

Officials within the counterterrorism community collaborate and coordinate with the counterdrug community at the working level. For example, officials serving on the IAWGs for counterterrorism often are supporting counterdrug activities, or working closely with those in their agencies who do. There is no formal coordinating mechanism across these communities. Issues that do arise are worked out within the NSC structure.

2. Counterproliferation

Recent legislation called for the creation of a “czar” to direct federal counterproliferation activities. Positioned within the Executive Office of the President, this official would chair an interagency group of Cabinet-level officials. Such an organization would help focus federal activities in this area, but in doing so would create resource demands that might compete with ongoing counterterrorism activities. Consequently, the President has not supported the creation of this new entity; instead, counterproliferation activities will continue to be coordinated through the existing

mechanisms within the NSC structure. Counterproliferation activities remain the responsibility of the NSC's Director for Arms Control.

3. Continuity of Government

This review has explored the roles and content of the existing Continuity of Government (COG) activities at the unclassified level. As this is a highly classified activity, these discussions have been very general and impressionistic. There is, however, a clear consensus among government officials that that continuity of government framework worked very effectively when there was high-level interest in this mechanism during the cold war. Many officials believe that the COG structure provided a useful model for dealing with important national issues—it provided a central leadership focus in the Executive Office of the President, and it had dedicated funding to buy services from other federal agencies. This combination allowed a significant network of capabilities to be established throughout the government. The COG operation has shrunk in size, funding, and influence in the post-cold war era. None of the government officials interviewed for this study felt that the existing COG framework could contribute much in addressing the infrastructure protection problem.

F. OPTIONS

The foregoing review of the CSG, FRP, and information security structures shows that many of the capabilities needed for infrastructure protection are already being provided within existing federal structures. In recent years, the nation has developed an extensive framework for creating and employing counterterrorism capabilities, and for dealing with a wide range of accidents and disasters. These capabilities are being extended to encompass chemical, biological, and radiological threats, as well as conventional terrorism. Since this framework already addresses many of the vulnerabilities facing the U.S. infrastructure, it is clear that any new structures must be linked in some way with this existing apparatus.

In considering options for new institutions, it is therefore appropriate to begin by asking what capabilities are *not* being provided within these existing structures. It is also appropriate to consider whether the commonalties between the new capabilities needed for infrastructure protection and those provided by the existing structure argue for incorporating the new mission within the existing structure, or whether the new

capabilities can be better provided under a separate, new structure focused on the new threat.

In addressing these issues, Table 2 presents a simple analysis of the roles of the current federal structures in terms of the threats they address and the kinds of capabilities they provide. The first two columns represent the threats associated with conventional terrorism ("bombs and bullets"), and terrorism using chemical, biological, or radiological weapons. The third represents the cyber threat. For each threat category, the table describes current roles and activities in each of the five infrastructure protection capability areas: strategy and policy formulation, prevention and mitigation; operational warning; response and recovery; and counter-action.

The table identifies the roles and jurisdictions of the existing structures. It also identifies some of the specialized technical structures that have been established to provide focus on new threats. In the case of the new chemical-biological-radiological threats, these specialized capabilities are being provided by new organizations that have been integrated within the existing CSG-FRP structures. The commonalties between conventional terrorism and CBR terrorism are sufficiently strong that it made sense to combine these missions within the existing federal framework. In the case of cyber threats, there also are many specialized structures. Many of these form the relatively decentralized information security communities, which have not been fully integrated into a coherent overall structure.

The CSG structure is providing leadership or coordination for activities relating to conventional and CBR terrorism. Performing this core mission requires the CSG to address all possible targets and attack technologies. Thus, if terrorists target infrastructure, their activities would fall within the jurisdiction of the CSG. If terrorists employ cyber attack technologies, this also would fall within the jurisdiction of the CSG.

Table 2. Federal Structures for Leadership or Coordination

CAPABILITY AREA	Threat Technologies		
	Conventional ("Bombs and Bullets")	**Chemical, Biological, Radiological**	**Cyber**
Strategy and Policy Formulation: -- prevention & mitigation -- operational warning -- response & recovery -- counter-action	**Lead Structure:** **NSC and CSG:** Provide national structures for developing federal policy and strategy **FEMA:** Chairs the Catastrophic Disaster Response Group (CDRG) which coordinates federal policy and strategy for consequence management in the Federal Response Plan	**Lead Structure:** **NSC and CSG:**: Conventional structure also used for CBR strategy and policy **FEMA:** A Core Group on Terrorism coordinates strategy and policy for CBR consequence management through specialized annexes to the FRP.	**Lead Structure:** **None:** No national structure in place for formulating strategy and policy to counter cyber threats to the economy
Prevention and Mitigation	**Lead Structure:** **CSG:** Interagency working group under CSG provides coordination, including coordination of funding for counterterrorism R&D **FBI and CIA:** Provide threat analysis, awareness, vulnerability assessments **FBI:** Provides funding for state and local preparedness activities	**Lead Structure:** **CSG:** Interagency working group under CSG provides coordination, including coordination of funding for counterterrorism R&D **Technical Structure:** **DoD:** Provides specialized prevention and mitigation activities to augment those for conventional threats	**Lead Structure:** **SPB & OMB (partial):** Provide some coordination of prevention and mitigation activities within the federal government **Technical Structure:** **CERTs and FedCIRC:** provide incident hotlines and publish analyses of computer incident threat and vulnerability information
Operational Warning	**Lead Structure:** **CIA's CTC & CCB:** Collects and analyzes counterterrorism intelligence; disseminates warning	**Lead Structure:** **CIA's CTC & CCB:** Collects, analyzes, and disseminates information pertaining to potential CBR attackers as part of overall mission	**Lead Structure:** **CIA's CTC & CCB (partial):** Collects, analyzes, and disseminates information pertaining to potential cyber attackers as part of overall mission **Technical Structure:** **CERTs and FedCIRC:** Issue alerts of cyber threats

Table 2. (Con't)

CAPABILITY AREA	Threat Technologies		
	Conventional ("Bombs and Bullets")	**Chemical, Biological, Radiological**	**Cyber**
Response and Recovery	**Lead Structure:** **FEMA:** Provides preparedness support for state and local governments Coordinates federal reinforcement of state and local response activities under FRP	**Lead Structure:** **FEMA:** Provides preparedness support for state and local governments—specialized contingency plans have been prepared for CBR incidents Coordinates federal reinforcement of state and local response activities under FRP	**Lead Structure:** **FEMA (partial):** Preparedness support and coordination under FRP will cover the physical consequences of cyber attacks **Technical Structure:** **CERTs:** Provide hotlines for cyber-attack response assistance
Counter-action	**Lead Structure:** **NSC and CSG:** Plan, exercise, and execute counter-action operations involving both law enforcement and **DoD** assets **FBI:** Coordinates and conducts counterintelligence and counterterrorism activities in the U.S. Supports local law enforcement in counterterrorism operations	**Lead Structure:** **NSC and CSG:** Plan, exercise, and execute counter-action operations involving both law enforcement and **DoD** assets **FBI:** Coordinates and conducts counterintelligence and counterterrorism activities in the U.S. Supports local law enforcement in counterterrorism operations	**Lead Structure:** **NSC, CSG, FBI, DoD (partial):** Existing counter-action capabilities for conventional and CBR attacks could address some cyber attackers **Technical Structure:** **FBI's CITAC and DoD:** Provide technical leadership for counter-action against cyber attackers

Similarly, the response and recovery capabilities organized under the Federal Response Plan are applicable to all kinds of declared disasters or emergencies. Whenever there is large-scale physical damage, loss of critical utilities, or major loss of life, the federal government provides reinforcing capabilities to back up private, or state and local responders. This is consistent with the "all-hazards" philosophy outlined earlier. Hence, the FRP is equipped to provide response and recovery capabilities to address the physical consequences of cyber attacks in cases where a federal disaster has been declared.

The gaps in the infrastructure protection capabilities provided under these structures arise because neither the CSG nor the FRP has focused explicitly on infrastructure protection. There are many potential scenarios in which infrastructure attacks might fall outside the jurisdiction of these structures. For example, individuals or

small groups involved in cyber attacks may not come under the jurisdiction of the CSG. Similarly, attacks that do not target federal property or trigger a disaster declaration may not trigger the FRP. Moreover, neither of these structures is designed to interact extensively with the private sector, and hence they do not provide an effective forum for collaborative mitigation and prevention initiatives. Although certain technical aspects are being addressed in the areas of warning, response, and counter-action, these existing structures lack the mandate to provide overall leadership. Many within these communities maintain that the cyber threat requires a different approach and culture from that of these existing structures.

Another theme illustrated by Table 2 is that the degree to which the existing structures are providing infrastructure protection capabilities varies significantly across the five capability areas. The CSG-FRP structures already provide many relevant capabilities in the areas of counter-action and response. In these areas, infrastructure protection represents a new set of technical challenges, but it will also draw on many capabilities in common with those already available within the existing CSG-FRP framework. However, in the areas of strategy and policy formulation, prevention and mitigation, and certain cyber aspects of warning, addressing cyber vulnerabilities presents a new set of challenges. It will require the participation of a new set of agencies, and new ties between and among the federal government, state and local governments, and the private sector.

The lesson to draw from these variations across capability areas is that there is no single way to link infrastructure protection with the existing federal structures that will necessarily be best across all five capability areas.

It is therefore appropriate to consider a range of alternative institutional arrangements for sharing infrastructure protection responsibilities among the current structures and a new structure. Three options are discussed here. The first embeds infrastructure protection within the existing CSG-FRP structures. The second creates a new body—a "Domestic Preparedness Council"—that would take the lead for all infrastructure protection activities. The third also creates a "Domestic Preparedness Council," but focuses its mission only on those capabilities where there is relatively little overlap with existing entities. This body would assume responsibility for strategy and policy formulation, prevention and mitigation, and certain aspects of operational warning. The strengths and weaknesses of these options are discussed subsequently.

1. Option 1: Embed All Infrastructure Protection Capabilities in the Existing Counterterrorism and Federal Response Plan Framework

This option places responsibility for each of the five capability areas within the existing CSG-FRP framework. The mission of the CSG would be expanded to include policy and strategy formulation, and the coordination of counter-action activities. The FRP would be expanded to address any new capabilities required for response to, and recovery from, infrastructure attacks. The warning mission would be assigned to the existing Community Counterterrorism Board. Finally, a new working group would be created within the existing Interagency Working Group on Counterterrorism to address prevention and mitigation. This new working group would integrate existing federal information security activities, and provide the mechanism for coordinating federal prevention and mitigation activities in collaboration with state, local, and private organizations. This option is illustrated in Figure 2.

Under this option, the CSG would have the overall *coordinating role* in developing infrastructure protection strategies and policies, and the missions of the existing CSG and the FRP mechanisms would be significantly expanded. This option thus provides a stronger coordination mechanism for response and counter-action than exists today, although it would remain a consensual process. A central function of the CSG would be to integrate the activities of the responsible federal law enforcement and national security agencies and departments in the infrastructure protection area, working as it does today for existing counterterrorism and law enforcement activities.[4]

The CSG also would have *coordinating responsibility* for the activities of the agencies responsible for prevention, mitigation, and operational warning. Interface with the private sector would continue to be handled through the network of agencies that already have working relationships with the private sector. Through the interagency working group process, the CSG would provide better coordination of the activities of responsible departments and agencies, which also could improve awareness and warning mechanisms at the sector level.

---

[4] In this framework, "responsible departments and agencies" are those already charged with responsibility for providing a needed infrastructure protection capability, or, in the absence of such assignment, where one will be assigned. An example of the former is the FBI, which is the responsible agency for most counter-action capabilities. An example of the latter is the Department of Energy, which may be designated as the responsible agency for interacting with the private sector in developing prevention and mitigation capabilities.

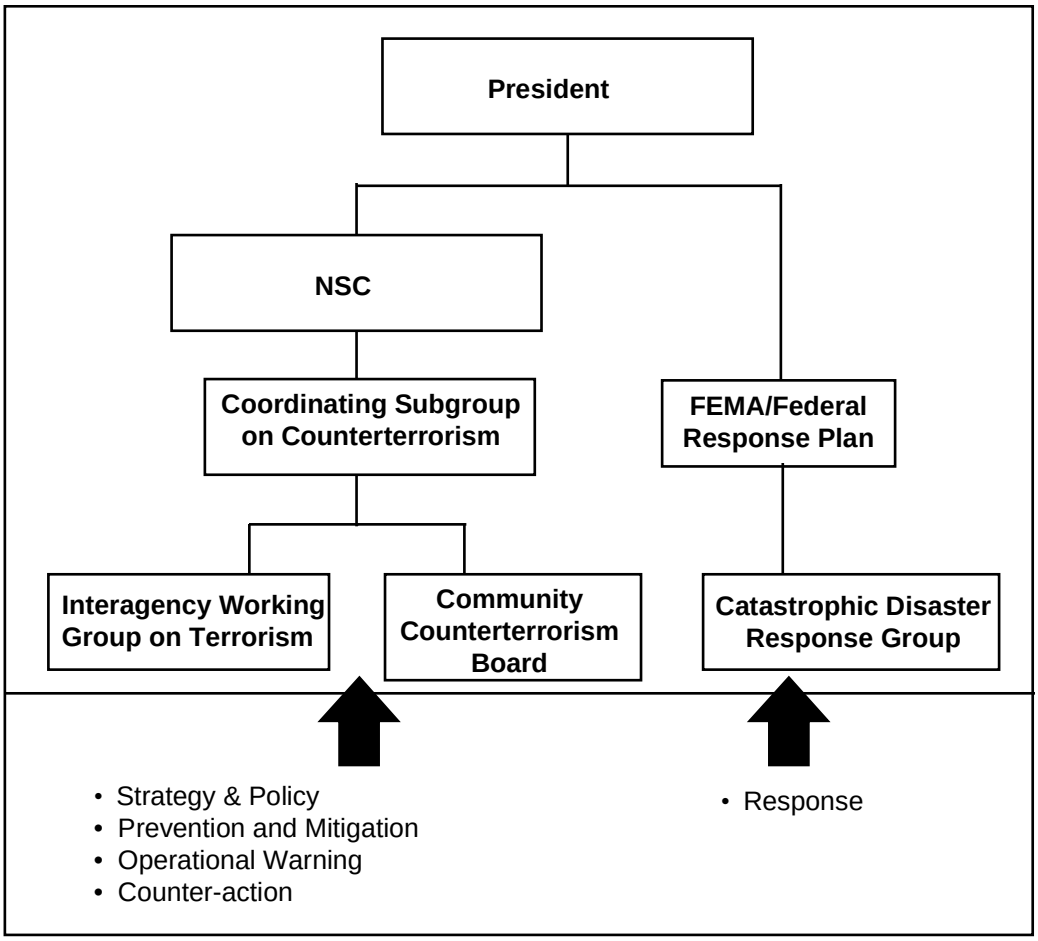

Figure 2. Option 1: Embed Infrastructure Protection Capabilities Within the Existing CSG-FRP Structures

The assignment of government roles for each of the five capability areas is summarized as follows:

Strategy and policy formulation roles: The CSG's mission would be expanded to give it responsibility for the *formulation* of federal policy for infrastructure protection, and coordination of national strategies.

Prevention and mitigation roles: This option maintains current relationships among government agencies and the private sector, while establishing a working group within the CSG structure to coordinate and integrate activities across responsible departments and agencies. Federal prevention roles are as follows:

- A working group under the CSG *coordinates* mitigation and prevention strategies and the related operations of responsible departments and agencies.

Current federal information security activities would be brought together under this mechanism.

- Responsible departments and agencies interact with the private sector through existing relationships. Their missions would be expanded to include infrastructure protection. (OMB would maintain its jurisdiction over federal departments and agencies for infrastructure protection.)

Operational warning roles: As with prevention activities, the main centers of responsibility remain with industry and the responsible departments and agencies. Initially, no formal integration activity would be established, but the CCB would encourage the growth of cross-sector exchanges and linkages. Federal operational warning roles are as follows:

- The CCB *coordinates* warning activities of responsible departments and agencies, and encourages cross-sector information exchanges.
- Responsible departments and agencies interact with the private sector through existing relationships.
- The CCB would coordinate the development of new operational warning tools and methods.

Response (consequence management) and recovery roles: FEMA would play the leadership role in developing and coordinating governmental responses to infrastructure attacks through the Federal Response Plan, parallel to the role already played by FEMA for natural disasters, conventional terrorist attacks, and NBC attacks. Annexes to the Federal Response Plan would be established to codify this role. Federal response roles are as follows:

- FEMA *coordinates,* through the FRP, the strategies and budgets of the departments and agencies responsible for response to infrastructure attacks.
- Responsible departments and agencies provide response capabilities.
- New technological capabilities needed to respond to infrastructure attacks (e.g. CITAC-like entities) would be developed and their employment *coordinated* through this FEMA-led mechanism.

Counter-action roles: This option would provide improved leadership for integrating the activities of the law enforcement and national security communities in the area of infrastructure protection. The mission of the CSG would be expanded to encompass infrastructure protection. The CSG would thus play the same role as it does for conventional and NBC terrorism today; it would coordinate strategies for joint action across these communities, support mechanisms for teaming to address specific tasks, and

establish leadership responsibilities in responding to incidents. Federal counter-action roles are as follows:

- The CSG *coordinates* the strategy and operations of the departments and agencies responsible for counter-action against infrastructure threats.
- Responsible departments and agencies provide law enforcement, military, intelligence and counterterrorism capabilities.
- New technological capabilities needed to counter-act infrastructure attacks (e.g. attack detection technologies) would be developed and their employment coordinated through this mechanism.

In summary, Option 1 defines an approach that focuses primarily on establishing stronger central leadership and on integrating the government's activities through the existing CSG mechanism and the Federal Response Plan. It draws exclusively on existing institutions and relationships, modifying these organizations and expanding their missions as required. This is analogous to the approach taken in recent years to expand the missions of existing structures to take on the growing threat of chemical, biological, and radiological attacks.

2. Option 2: Create a "Domestic Preparedness Council" for Infrastructure Protection

The second option would create a new leadership structure for infrastructure protection—a "Domestic Preparedness Council"—within the Executive Office of the President[5] (see Figure 3). This council would be comparable in level and function to the CSG, and would be responsible for each of the five capability areas. The council also would provide a framework for consultation and coordination, much the same as do the CSG and FRP mechanisms today.

The basic version of this option is to create a small council staff in the EOP entity that relies on federal departments and agencies to supply needed resources (this is "Option 1" of the earlier IDA study). A second, more ambitious variant is to supplement this leadership council with a supporting institution that provides supporting staff and resources ("Option 2" of the earlier IDA study).

---

[5] There are several possible variants of this option. The new council could be a parallel coordinating subgroup reporting through NSC; alternatively, it could report through OMB, or even directly to the President. A third alternative would be to make the council a stand-alone body outside the Executive Office of the President.

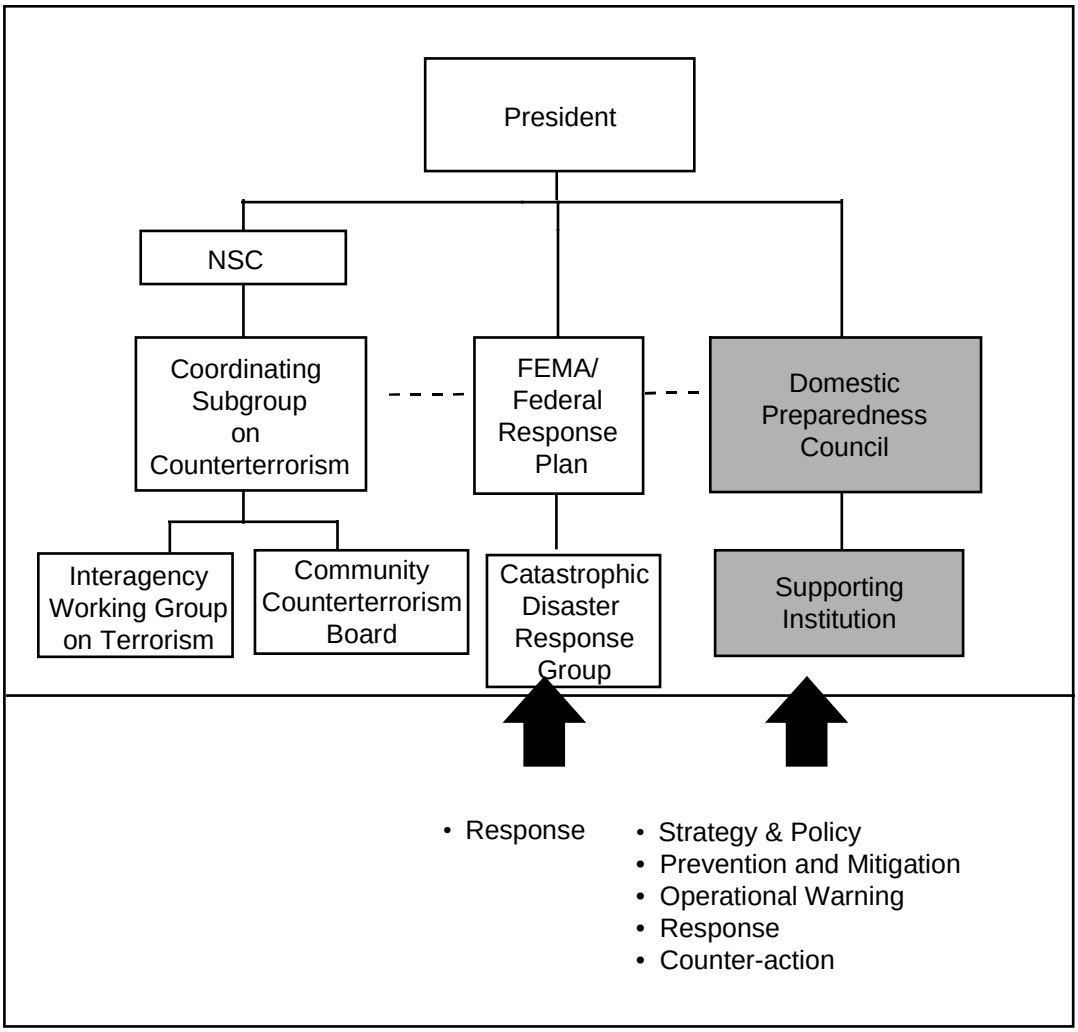

Figure 3. Option 2: A Domestic Preparedness Council Responsible for All Infrastructure Protection Capabilities

Under the council, an interagency working group structure would be established to coordinate the activities of the agencies responsible for prevention, mitigation, and operational warning. Ongoing information security activities would be subsumed within this structure. Interfaces with the private sector would continue to be handled through the network of responsible agencies that already have working relationships with the private sector, and would be assigned lead responsibility for coordinating infrastructure protection activities. As with Option 1, FEMA would take responsibility for shaping and coordinating the federal government's response and recovery activities.

The assignment of government roles for each of the capability areas is summarized as follows:

Strategy and policy formulation roles: The Domestic Preparedness Council would have responsibility for coordinating federal strategies and policies for infrastructure protection. These would be coordinated with the CSG for Counterterrorism and the FRP for response and recovery. Under the second variant of this option, the supporting institution would provide policy analysis and development in support of the Council.

Prevention and mitigation roles: This option establishes a new interagency working structure under the Domestic Preparedness Council to coordinate and integrate activities across responsible departments and agencies. This interagency mechanism *coordinates* strategies and policies for infrastructure protection. Federal prevention roles are as follows:

- The new leadership entity and working groups *coordinate* prevention strategy, policy, and operations of responsible departments and agencies. Ongoing information security activities would be subsumed under this structure.
- Responsible departments and agencies interact with the private sector through existing relationships.
- Under variant two, the supporting body would provide staff support to the Domestic Preparedness Council, and would interact extensively with the responsible departments and agencies.

Operational warning roles: As with prevention activities, the main centers of responsibility remain with industry and the responsible departments and agencies. Initially, the working-group framework under the Domestic Preparedness Council would encourage the growth of cross-sector exchanges and linkages. Federal operational warning roles are as follows:

- The working groups *coordinate* the warning activities of responsible departments and agencies, and encourage cross-sector information exchanges.
- Responsible departments and agencies interact with private sector through existing relationships.
- Under the second variant of this option, the supporting body would promote the development of operational warning capabilities, and would serve as an integrator of warning information.

Response (consequence management) and recovery roles: Federal response roles are as follows:

- FEMA *coordinates,* through the FRP, the strategy, policy, and budgets of the departments and agencies responsible for response to infrastructure attacks.
- Responsible departments and agencies provide response capabilities.
- New technological capabilities needed to respond to infrastructure attacks (e.g. CITAC-like entities) would be developed and their employment coordinated through the Domestic Preparedness Council.

Counter-action roles: The Domestic Preparedness Council would play a *coordination* role in developing the strategies, policies, and programs of those agencies and activities that conduct counter-action operations against potential cyber criminals or terrorists. The Council thus would play the same role for infrastructure protection as is played today by the CSG for conventional and CBR terrorism. The new leadership entity would work in close collaboration with the CSG, and would focus on capabilities and operations that complement those already provided by the CSG. In addition, the Council would provide leadership for developing specialized technical capabilities needed to address cyber attacks. Federal counter-action roles are as follows:

- The Domestic Preparedness Council would *coordinate* the strategy, policy, and budgets of the departments and agencies responsible for providing the specialized capabilities needed to operate against cyber and infrastructure threats. It would focus on capabilities and operations that would complement the existing roles of the CSG.
- Responsible departments and agencies provide law enforcement, military, intelligence and counterterrorism capabilities. This would be done in close coordination with the CSG.
- New technological capabilities needed to counter-act cyber or infrastructure attacks (e.g. attack detection technologies) would be developed and their employment coordinated through the Domestic Preparedness Council.

In summary, Option 2 establishes a new National Preparedness, with the responsibility of filling the gaps in the capabilities needed for infrastructure protection that are not being provided by existing federal structures. It would subsume ongoing information security activities, and carefully coordinate its other activities with the CSG and FRP.

3. Option 3: Create a "Domestic Preparedness Council" Focusing on Infrastructure Protection Strategy and Policy Formulation, Prevention, Mitigation, and Warning

As with Option 2, Option 3 creates a new "Domestic Preparedness Council." In this case, the mission is focused in the capability areas of strategy and policy formulation, prevention and mitigation, and operational warning (see Figure 4). The Council would address the specialized technological aspects of infrastructure protection, and build a network among responsible agencies involved with infrastructure protection. In the areas of counter-action and response, the missions of the CSG and FRP would be expanded to include needed new infrastructure protection capabilities. This option would thus maintain an "all-hazards" approach for coordinating response and counter-action activities within the existing leadership bodies.

Under this option, the CSG structure would be modified along the lines outlined for Option 1 above. CSG working groups responsible for infrastructure protection would play a *coordinating* role in developing the strategies, policies, and programs of those agencies and activities that conduct operations in the area of counter-action. As under Option 1, a central function of the CSG would be to integrate the activities of the federal law enforcement and national security communities in the infrastructure protection area, working as it does for other counterterrorism and law enforcement activities today.

The FRP mechanism would take the lead responsibility in coordinating strategies and programs for response and recovery. A new annex for infrastructure protection would be prepared, as described under Option 1.

The Council would focus on coordinating the activities of the agencies responsible for prevention and mitigation, and for operational warning. Existing federal information security activities would be subsumed under this new body. Interfaces with the private sector would continue to be handled through the network of responsible agencies that already have working relationships with the private sector. As outlined under Option 2 above, interagency working groups would be established under this new entity to coordinate the activities of responsible departments and agencies, which could also improve awareness and warning mechanisms at the sector level.

The assignment of government roles for each of the five capability areas is summarized as follows:

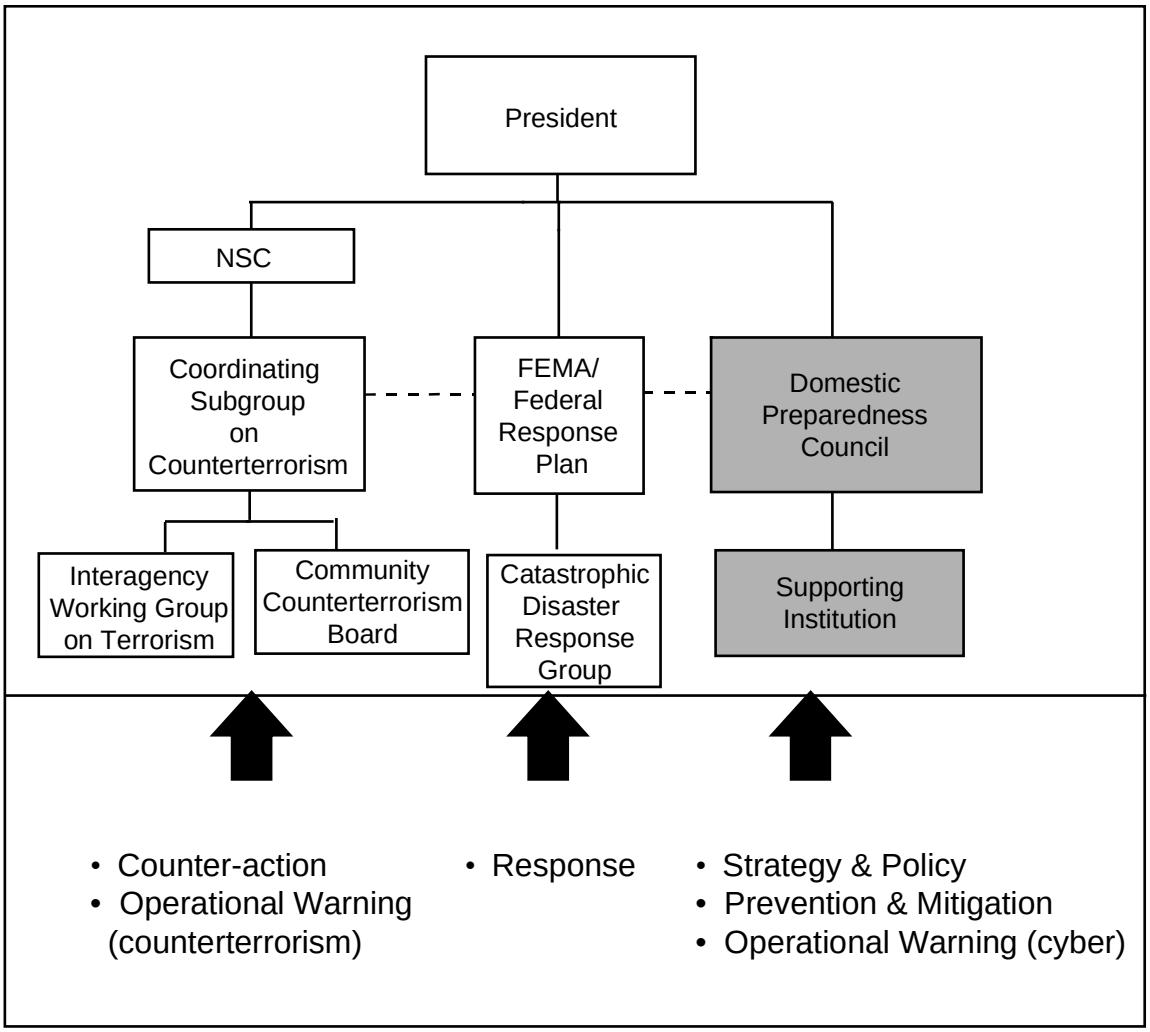

Figure 4. Option 3: A Domestic Preparedness Council Responsible for Strategy & Policy, Prevention & Mitigation, and Operational Warning

Strategy and policy formulation roles: The Domestic Preparedness Council would have responsibility for coordinating, with the CSG, federal strategies and policies for infrastructure protection.

Prevention and mitigation roles: The prevention and mitigation roles of the Domestic Preparedness Council would be the same as outlined for Option 2 above. (Specific roles are the same as outlined for Option 2.)

Operational warning roles: The operational warning roles of the Domestic Preparedness Council would be the same as outlined for Option 2 above. (Specific roles are the same as outlined for Option 2.)

Response roles: FEMA would play the same leadership role for developing and coordinating governmental responses under the Federal Response Plan as outlined under Option 1. (Specific roles are the same as outlined for Option 1.)

Counter-action roles: The CSG would play the same leadership role for counter-action as outlined under Option 1. (Specific roles are the same as outlined for Option 1.)

G. ASSESSMENT

Each of the three options outlined here provides a leadership body for infrastructure protection within the Executive Office of the President. The difference among these options is the degree to which the infrastructure protection entity employs the existing CSG-FRP structures.

Under Option 1, infrastructure protection is embedded within these existing structures. The main advantage of this approach is that it builds on a proven, existing coordinating framework. There are, however, disadvantages to this approach as well, because it will require significant expansion of the missions of these current entities. Infrastructure protection must address new threats, particularly the threat of cyber attacks, that will require entirely new technologies and the involvement of new communities of government and private organizations to address effectively. There is a risk that expanding the mission of the CSG could cause it to lose focus on its existing mission, or that this Coordinating Subgroup might not be able to provide adequate focus on the infrastructure protection mission. In addition, neither the CSG nor the FRP structure is intended to interact with the private sector as extensively as will be required to promote infrastructure prevention, mitigation, and warning activities. In summary, there are advantages to assigning the infrastructure protection mechanism to existing entities, but there is the risk that this approach would undermine the ability of those same entities to address their current missions, and may provide too little emphasis on developing needed infrastructure protection capabilities.

Option 2 creates a new body in the Executive Office of the President, a Domestic Preparedness Council, specifically for the infrastructure protection mission. This approach has the advantage of providing focused, high-level leadership for infrastructure protection. If structured properly, it could interact effectively with the full range of agencies that would have responsibilities for prevention, mitigation, and warning. It has the disadvantage of requiring the creation of a new organization, with the inevitable growing pains. This approach also would require careful management of the inevitable

"seams" and overlaps between the mission of this new entity and the missions of the existing CSG-FRP structures in the areas of counter-action and response. Indeed, there is the risk that this new entity could become a bureaucratic competitor of these existing leadership structures. In summary, creating a Domestic Preparedness Council has the advantage of providing needed focus on the prevention, mitigation, and warning capabilities, but it risks creating new coordination problems in the areas of counter-action and response with the existing CSG -FRP structures.

Option 3 shares the responsibilities for infrastructure protection between the new Council and existing structures. The responsibility for counter-action and response would be assigned to the existing CSG-FRP structures. The advantage of this is that it would retain an "all hazards" approach, without unduly expanding the missions of the existing leadership framework. The responsibility for strategy and policy formulation, prevention and mitigation, and warning would be assigned to a Domestic Preparedness Council, which could provide the needed focus and structures for these areas. There are two disadvantages of this option. First, as with Option 2, Option 3 would require creating a new organization; second, because this option splits responsibility for leadership, it would create its own set of coordination burdens across entities.

Table 3 provides a summary of the management principles used in evaluating the three options described above, and it provides an assessment of the relative strengths and weaknesses of each.

H. CONCLUDING REMARKS

Infrastructure protection will require the development of new capabilities and new relationships within and among the entities of the federal government and state, local, and private organizations. Many of the needed capabilities are closely related to those being provided under existing federal structures, particularly the Coordinating Subgroup for Counterterrorism and the Federal Response Plan.

Table 3. Assessment of the Options

Management Principles	Option 1: Embed Infrastructure Protection in Existing CSG and FRP Structure	Option 2: New EOP Entity for Infrastructure Protection (Possibly with Operational Arm)	Option 3: New EOP Entity focused on Prevention, Mitigation, and Warning (Possibly with Operational Arm)
1. Leadership for strategy, policies, and operational responsibilities for protecting the infrastructure	+++ provides strong institutional home -- Requires significant expansion of mission, and new mission may not get proper emphasis	+++ provides strong focus on infrastructure protection -- May lack needed linkages with the CSG and FRP structures for counter-action and response	+++ provides strong focus on infrastructure protection ++ Takes advantage of the CSG and FRP structures. -- Splits leadership responsibility between new entity and existing CSG and FRP structure
2. Build on existing institutional capabilities and working relationships	+++ Retains role of the CSG and FRP for counter-action and response -- Requires significant expansion of current roles for prevention, mitigation, and warning -- Existing framework does not involve many of the departments and agencies needed to address prevention, mitigation, and warning	--- Creates an entirely new structure	+++ Retains role of the CSG and FRP for counter-action and response
3. Interact effectively with the private sector	-- Existing CSG and FRP structures have limited interactions with the private sector	+++ New entity could provide strong focus on strengthening interactions with the private sector.	+++ Prevention, mitigation, and warning entity could focus on interactions with the private sector.
4. Evolve as the protection strategy matures	+++ This option provides significant flexibility for evolution ++ Requires minimal new resources and no new organization	+++ Allows relationships to evolve as needed -- Requires resources and new organization -- New organization may be resisted by existing government bodies for response and counter-action	+++ Allows relationships to evolve as needed -- Requires resources and a new organization ++ Does not threaten missions of any existing government bodies

Option Supports Principle: +++ Strongly ++ Moderately + Weakly

Option Undermines Principle: --- Strongly -- Moderately - Weakly

This raises the question of whether it is better to expand the responsibilities of existing federal structures to include infrastructure protection, or whether it is better to create a new body that can focus exclusively on the new mission. On the one hand, existing organizations should not be overburdened, nor should their focus on their current missions be diffused by adding a host of new responsibilities. On the other hand, new organizations should not be created if this duplicates ongoing efforts or creates unworkable management relationships between and among the old and new structures. These considerations argue that a mixed strategy, which shares missions among new and old structures, may be the best approach.

Glossary

ASD/SOLIC	Assistant Secretary of Defense for Special Operations and Low Intensity Conflict
C/B Terrorism	Chemical and Biological Terrorism
CCB	Community Counterterrorism Board
CDG	Continuity of Government
CDRG	Catastrophic Disaster Response Group
CGR	Chemical, Biological, Radiological
CIA	Central Intelligence Agency
CIO	Central Information Officer
CITAC	Computer Investigations and Threat Assessment Center
CSG	Coordinating Subgroup on Terrorism
CTC	Counterterrorism Center
DCI	Director of Central Intelligence
DEST	Domestic Emergency Support Team
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
EPA	Environmental Protection Agency
ESF	Emergency Support Functions
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigations
Fed CIRC	Federal Computer Incident Response Capability
FEMA	Federal Emergency Management Agency

FRP	Federal Response Plan
GAO	Government Accounting Office
GSA	General Services Administration
HHS	Health and Human Services
IDA	Institute for Defense Analyses
IICT	Interagency Intelligence Committee Terrorism
IIMPG	Interagency Information Management Policy Group
IOSS	Interagency Operational Security Support Staff
IWGT	Interagency Working Group on Counterterrorism
J-3	Director for Operations, Joint Staff
JCS	Joint Chiefs of Staff
NCS	National Communications System
NDMS	National Disaster Medical System
NIST	National Institutes for Science and Technology
NSA	National Security Agency
NSC	National Security Council
NSDD	National Security Decision Directive
NSTAC	National Security Telecommunications Advisory Committee
OIRA	Office of Information and Regulatory Affairs
OMB	Office of Management and Budget
ONDCP	Office of National Drug Control Policy
OPSEC	Operational Security
PDD-39	Presidential Decision Directive 39
R&D	Research and Development
SOCOM	Special Operations Command
SPB	Security Policy Board
USDA	U.S. Department of Agriculture
VA	Veteran’s Administration