NATIONAL STRATEGIES AND 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 has been prepared by the Institute for Defense Analyses (IDA) in response to tasking from The President's Commission on Critical Infrastructure Protection under task order, "Organizational Options for Critical Infrastructure Protection." It is submitted in fulfillment of this task order.

The IDA study group wishes to express its appreciation to the members of the expert panel convened to review organizational approaches. The panel was chaired by General Larry Welch, President of IDA; its members were Mr. Duane Andrews, Mr. Colin Crook, Dr. Edward David, Dr. Robert Kupperman, Mr. Oliver "Buck" Revell, The Honorable James Schlesinger, Mr. Jeffrey Smith, and The Honorable James Woolsey.

The authors are grateful for the support received from all members of the IDA study group; from Julian Nall, who arranged the expert panel meeting; from Eileen Doherty, who provided editorial assistance; and from Donna Rivoire and Rhonda Cook, who provided secretarial support.

IDA STUDY TEAM

David A. Graham
Lexi Alexander
Michael Leonard, Project Leader
Paul H. Richanback
John R. Shea
Richard H. White

Robert W. Anthony
William J. Barlow
John R. Brinkerhoff
Terry Mayfield
Julian C. Nall
Michael S. Nash
Ronald S. Ross
Robert D. Turner

CONTENTS

NATIONAL STRATEGIES AND STRUCTURES FOR INFRASTRUCTURE PROTECTION

I. THE ISSUE AND BACKGROUND

In the coming decades, the U.S. economy will prosper in an era of free trade, open borders, global corporations, advanced computing and telecommunications, and extensive information networking and interconnections. There are, however, underlying risks. Inherent in these economic trends toward an open and integrated economy is an increased susceptibility to physical or cyber attacks. These could emanate from criminals, anti-social groups, sub-national terrorist groups, or perhaps nation states. Protection of the country's economic infrastructure is thus becoming a critical dimension of the overall national challenge posed by the danger of attacks on U.S. citizens and their property. In the future, sophisticated attacks may be directed at high-value economic targets, with the goal of shaping U.S. policies by undermining the economy, the national will, and ultimately the confidence in the government.

The President's Commission on Critical Infrastructure Protection has been tasked to provide a better understanding of this national problem and offer a strategy for addressing it. This report summarizes work performed by the Institute for Defense Analyses in support of the Commission. This work has focused on developing federal government strategies and structures for meeting the threat of attacks on the U.S. infrastructure, particularly attacks employing cyber technologies.

A. Infrastructure Protection: An Amorphous and Ambiguous National Problem

Several factors indicate that the threat of physical or cyber attacks on the U.S. economy is a problem of strategic importance to national security, public safety, and economic well being. First, the every-day incidence of random violence and terrorism is rising both in this country and against our interests abroad. U.S. citizens have been victims of the Pan Am 103 bombing, the World Trade Center bombing, the Oklahoma City bombing, the Olympic Village bombing, and the Khobar Towers bombing of U.S. military personnel in Saudi Arabia. Lower profile bombings or other acts of sabotage against property are practically a weekly occurrence around the nation. The will and the

ability of small groups to inflict harm is a fact of life in America today. Second, the continuing diffusion of technology will expand the power of individuals, or small groups, to harm American citizens and their property. Looking to the future, if terrorists and other anti-social groups gain access to more modern or more sophisticated explosives; to chemical, biological, or radiological weapons; or to advanced computer and communications technologies, their ability to inflict harm will multiply.

A third factor is the increasing possibility that the engagement of U.S. military forces overseas will provoke attacks on the United States. Potential opponents could readily come to embrace a doctrine of "asymmetric response," based on the premise that while U.S. military forces are unbeatable, the political will of the country can be undermined if sufficient damage can be inflicted on U.S. citizens or our economy.[1] Hence, the necessary engagement of the nation in world affairs will continually raise the risks of attacks at home.

These threats are real and growing, but today they remain amorphous and ambiguous in the eyes of the American public. Even experts in the field do not yet agree on the magnitude of the risks posed or how best to address them. We currently do not have a good understanding of the intentions or (to a lesser degree) the specific capabilities of potential attackers. Large-scale or technically sophisticated attacks require combinations of ill-will, knowledge, skills, and leadership that — at least until now — have not often come together. To achieve country-wide consequences, an attack may in fact require an effective intelligence apparatus to provide detailed knowledge, targeting assistance, and sustainment.

It has been argued further that, even though the capability exists for devastating attacks, other factors will constrain the use of such violence. Social taboos on weapons of mass destruction might, for example, limit attacks from all but the most sociopathic groups. Moreover, U.S. policies may effectively deter the use of terrorism as a political tool. Thus, some contend that the problem is overblown. Many others, however, believe

---

1 In a recent address, Secretary of Defense Cohen observed: "If the United States cannot be challenged directly, head to head, then our superiority may encourage adversaries to use indirect, or what they call asymmetric, means to attack our forces and interests abroad, and even our people here at home, and …. our adversaries are likely to be students of Sun Tsu and have read "The Art of War" and seek advantage over us by using unconventional strategies to circumvent our strengths and exploit our vulnerabilities." Keynote Address by Secretary of Defense William Cohen to the Conference on Terrorism, Weapons of Mass Destruction, and U.S. Strategy, The University of Georgia, April 28, 1997

that in this age of potent capabilities to inflict harm, we are living in the calm before the storm — a storm we are having difficulty forecasting and preparing for adequately.

While the full risks and consequences of attacks are uncertain, the prospects for significant casualties and damage appear to be rising. Recent experience with conventional explosives and the growing threat that nuclear, chemical, or biological weapons could be employed have given physical attacks truly catastrophic potential. And in the past several years, attention has begun to focus heavily on the possibility (some would say *probability*) of both physical and cyber attacks on the critical infrastructures that underlie all economic activity, government, and lifestyles.[2] Infrastructures of concern include computer networks, telecommunications, electric power, banking, gas and oil storage and distribution, and transportation. Strong interdependencies exist among these infrastructures (e.g., all depend on computer networks, telecommunications, and electric power). This raises the prospect that successful attacks on one infrastructure sector could have serious, "cascading" effects on others, resulting in potentially catastrophic damage and disruption.

There is mounting concern that advances in technology and business practices are making the economy increasingly vulnerable to cyber attacks. Unfortunately, secure methods of operating new technologies often lag behind their initial deployment. Thus, the growth in distributed computing networks, the convergence on a few standard software packages, the reliance on computer controls (particularly for energy supplies and manufacturing processes), and the tight coupling of business processes and logistics with computer-based information networks all raise the potential for a single attack, or attack mode, to inflict widespread damage.

The high degree of uncertainty surrounding the threat of attacks on the United States has frustrated attempts to address them effectively. Attacks can come from any direction, occur at any time, and target any aspect of American life. How does the U.S. prepare itself to fend off or respond to such threats?

By their very nature, the challenges posed by potential attacks on U.S. infrastructures do not fall neatly within existing institutional arrangements and assignments of responsibility. The U.S. government is not structured to take quick, decisive action to address problems that cut across the many departments and agencies that typically deal with specific segments of the economy and supporting infrastructures.

---

[2] While threats to infrastructure are typically considered to be *destructive* in character, cyber attacks can also cause major harm through *exploitation*. Electronic espionage is a good example.

The nation also has established a clear divide between the national security community, which is responsible for addressing external threats, and the federal law enforcement community, which is responsible for dealing with domestic crime. Differences in their legally defined missions and cultures make it very difficult for these communities to collaborate.

Public-private roles also are not well defined. Most of the nation's economic assets — including the key infrastructures — are designed, built, and operated privately. Our legal system limits the role of government with respect to such assets. In addition, when normal service outages, vandalism, or natural disasters occur, most of the capability to respond is provided by the private sector. Hence, as a practical matter, the job of protecting the U.S. infrastructure is — and will remain — largely in private hands.

But the government also possesses important capabilities for protecting the infrastructure, and it is clearly responsible for ensuring that broader national security and public safety concerns are addressed. Private firms have strong incentives to protect their assets, reputations, customers, and employees, but their concerns tend to be narrower than those of the government. Private business decisions are based on their own "cost-effectiveness" calculations, which may not capture the full damage to society that could result from a purposeful attack. Moreover, many government officials believe private firms do not yet recognize how serious this threat really is. For both reasons, private firms are unlikely to take all of the protective measures that are desirable from the public standpoint.

Given the ambiguity and uncertainty of the risks, considerable further clarification will be required to determine what additional governmental capabilities are needed and will be supported by the private sector and the American public. Concerned government officials face the challenge of convincing the public to react to the still-abstract possibility of catastrophic attacks on the U.S. economy. At present, most industry experts see some useful roles the government can play, but they do not want the government to interfere with their internal business decisions.

B. The Commission's Mandate and Tasking to IDA

The President's Commission on Critical Infrastructure Protection has been asked to address this national problem. Its specific tasks have been to scope the problem at hand, to cut through the fog of ambiguity surrounding it, and to recommend to the President an appropriate course of action.

The Commission builds on a number of studies and initiatives undertaken within the government in recent years. As concern has grown over the potential for attacks on the infrastructure, so too has the concern that the nation needs to better understand the problem and potential responses, organize appropriately, and take the necessary actions. Accordingly, the federal government established a Critical Infrastructure Working Group (CIWG) in 1995 to address this problem, and the CIWG in turn led to the President's Commission, which was established by Executive Order in 1996. In addition, a wide range of studies addressing various aspects of infrastructure vulnerability and protection have been conducted, both by the government and by private organizations.

The Commission tasked IDA to provide an independent view on possible governmental strategies and to consider options for developing needed federal capabilities, structures, roles, and responsibilities. IDA interviewed government officials, industry executives, and technical experts to obtain their views on the threats to the infrastructure, the current state of protection capabilities, and suggested improvements. In addition, available studies and reports on this issue were reviewed, and a compilation of the existing roles and responsibilities of government and private organizations was prepared. Based on the interviews and these materials, a set of structural issues and options was prepared. IDA then convened a panel of senior advisors who reviewed these materials and offered additional proposals for developing needed government structures.[3]

This report summarizes this work and the main findings of this task. Section II describes the general nature of the threats that plausibly could emerge over the next decade. It then identifies the capabilities needed to address such threats. These capabilities provide a framework for describing possible assignments of roles and responsibilities to industry and government; they also suggest the kinds of institutional structures that will be needed to address the problem. Section III describes several principles for the design of such structures, offers three broad structural options, and discusses the main advantages and disadvantages of each approach. Some final remarks are included in Section IV. Several appendices contain the details of IDA's threat scenario, its organizational research, and some additional issues.[4]

---

[3] The review panel was chaired by IDA's President, General Larry Welch, and included Mr. Duane Andrews, Mr. Colin Crook, Dr. Edward David, Dr. Robert Kupperman, Mr. Oliver "Buck" Revell, The Honorable James Schlesinger, Mr. Jeffrey Smith, and The Honorable James Woolsey.

[4] Appendix A provides the details of IDA's threat scenario. Appendix B presents the work done to establish a "baseline" describing existing organizational roles and responsibilities. Appendix C notes three additional issues.

In summary, this paper argues that (1) threats to critical infrastructures, particularly of cyber attack, are both real and growing; (2) there is a clear need for greater federal involvement in coordinating national infrastructure protection efforts; and (3) the effectiveness of any protection strategy will depend heavily on the degree of cooperation between government and the private firms that own and operate the critical infrastructures.

II. TOWARD AN INFRASTRUCTURE PROTECTION STRATEGY

The logical starting point for strategy development is a clear statement of the problem that needs to be addressed. In simplest form, the problem is that current infrastructure vulnerabilities to both physical and cyber attack could be exploited by a wide range of potential adversaries to severely damage the U.S. economy and harm its citizens. Subsection A focuses first on the new, cyber dimension of the problem. It starts with a description of weaknesses known to exist in the types of information systems that are widely used in the critical infrastructures. It then merges vulnerability considerations with existing, or anticipated, infrastructure attack capabilities that could be employed by prospective opponents. This is done by positing a threat scenario that depicts a series of physical and cyber attacks on several types of critical infrastructures in multiple U.S. cities. Using both cyber vulnerabilities and the threat scenario as benchmarks, Subsection B then identifies the kinds of capabilities required to help prevent or respond to infrastructure attacks.

The capabilities and general roles described in Subsection B by no means comprise a complete protection strategy. The capability areas are intended to describe the general outlines of a strategy; no doubt, many additional kinds of capabilities will be identified as more is learned about the problem. Moreover, there are many elements of a complete strategy that are not addressed, such as resource requirements, staffing, and a detailed delineation of the appropriate roles and responsibilities of the private sector, state and local governments, and the federal government. The work presented here can best be described as an outline for the development of a strategy.

A. Vulnerabilities and Threats

1. A Vulnerabilities Perspective

Technical experts agree that there are extensive *vulnerabilities* in current information systems that could be exploited by knowledgeable individuals or groups. But

they disagree on how likely this is, because there are few groups with both the *intentions* and the *capabilities* to exploit such vulnerabilities.

Intentions are inherently difficult to predict, notwithstanding the observation that current events show no lack of enmity to the United States or malicious intent in the world. The most likely cause for an information attack could well be as a response to actions taken in the future by the U.S. government. But such actions — and the situations and motives that might result — are virtually impossible to forecast with any precision.

On the other hand, an analysis of the *vulnerabilities* in current on-line systems, and the ready availability of tools to exploit them, can structure the problem in more concrete terms. It is the existence of these weaknesses that helps give prospective opponents the *capabilities* needed to conduct cyber attacks. The Defense Science Board identified a wide range of typical software and other vulnerabilities, as summarized in Table 1.

Table 1. Cyber Vulnerabilities of Current On-Line Information Systems, Identified by the Defense Science Board

HUMAN FACTORS - Information freely available - Poor password choices - Poor system configuration - Vulnerability to "social engineering"	PROTOCOL-BASED - Weak authentication - Easily guessed sequence numbers - Source routing of packets - Unused header fields
AUTHENTICATION-BASED - Spoofing - Password sniffing/cracking - Social engineering	DENIAL OF SERVICE - Network flooding - "Spamming" - Morris worm
DATA DRIVEN - Data corruption/deletion - Error handling - Mobile code	CRYPTOSYSTEM WEAKNESSES - Inadequate key size/characteristics - Mathematical algorithm flaws
SOFTWARE-BASED - Viruses - Flaws - Root access - Access privileges - Unused security features - Trap doors - Poor system configuration	UNPROTECTED KEY MANAGEMENT - Key installation - Key storage - Key generation - Key interception BYPASSING - Capture data before encryption - Turn off encryption - Replay - Denial of service

Source: Defense Science Board & IDA

The nature of the problem varies with the software in question, but a cyber attack can be successful if it succeeds in exploiting even a single area. Among the more pressing features of the threat *capabilities* thus engendered are that:

- tools to exploit known vulnerabilities are widely available for downloading from the Internet, at little or no cost;
- many of these tools can be exploited by individuals with limited training (e.g., undergraduate level courses in computer science, or less); and
- individuals and groups — some of them criminal — advertise openly on the Internet to sell their services in applying such tools.

Only limited manifestations of cyber attack have actually been experienced to date, but large-scale indications should not necessarily be expected (not least because penetrations often go unreported). For more than three years, DoD has noted intrusions by unidentified entities showing more sophistication than normally would be expected from school children or other benign hackers. Banking and financial institutions have experienced persistent losses from cyber intrusions, although the details and the extent of the losses have been guarded to protect the reputations of franchises. Moreover, stealing money from accounts without being detected takes significantly more sophistication than merely corrupting data or closing down systems. The reason that more "service-denial" attacks have not been seen, in banking or other infrastructure sectors, may simply be that those capable of such dramatic actions have not yet had sufficient motivation.

In summary, the vulnerabilities inherent in our information systems, and the ease with which they can be exploited, offer prospective opponents a broad spectrum of cyber attack capabilities. These capabilities have not yet produced a significant information disruption in this country, but they clearly could do so in the future. The next section addresses possible motivations for large-scale information attacks and posits a threat planning scenario along these lines.

2. A Plausible Threat Scenario

Cyber threats to the United States range across a continuum from isolated "hackers" (e.g., teenagers penetrating high school web sites); to small scale criminal individuals or groups (e.g., perpetrating credit-card fraud); to large criminal conspiracies (e.g., conducting money laundering, extortion, or cyber bank robberies); to terrorist groups (e.g., carrying out attacks on the power grid); to nation states (e.g., committing full-scale information attacks).

Major information attacks by rogue states or terrorist groups (domestic or foreign) are of primary interest here for two reasons. First, such attacks fall toward the more demanding end of the threat spectrum, thus providing a suitably challenging set of benchmarks for defining needed capabilities. And second, they are considered plausible by a number of experts. For example, the current Directors of the Joint Staff for Operations (J-3) and Command and Control (J-6) both regard information attacks on the United States to be among the more likely of the serious national security threats currently facing the country.[5] Their reasoning is that if future adversaries cannot match U.S. forces directly, then large-scale cyber attacks offer them the prospect of an effective, inexpensive, and perhaps anonymous means of achieving their objectives.

While the main focus here is on the new cyber threat, it is necessary to consider physical attacks against critical infrastructures as well. Threats from conventional explosives and other, more traditional means of attack have been present for some time, but the growing likelihood of nuclear, biological, or chemical use has increased dramatically the potential for serious damage and disruption. Chemical and biological capabilities warrant particular attention because — as with cyber capabilities — they are relatively cheap and easy to acquire, and they can have even more devastating effects.

The scenario developed for this study posits a coordinated series of physical and information attacks on critical infrastructures. (Scenario details are provided in Appendix A.) These acts are instigated by one or more foreign entities in response to a deployment of U.S. forces into an overseas crisis situation, with overt opposition from both domestic and foreign sources.

The cyber components of the attack scenario could be carried out by perhaps two dozen persons. Some of the leadership of that group would need to be knowledgeable in computer networking defenses (i.e., they would need to have undergone some graduate-level training), but most of the group would only need to be computer-literate and to receive a modest additional amount of training. The physical aspects of the scenario would require another several dozen people trained to conduct terrorist-style operations and capable of moving about in U.S. cities without attracting undue notice. The postulated scenario is thus clearly within the technological capacity of virtually any hostile nation, and of some terrorist groups operating today.

---

5 Interview with Lt. General Pete Pace, Director for Operations (J-3), and Lt. General Doug Buchholz, Director for C4 (J-6), 29 April 1997.

The dominant focus of the scenario is on urban attacks, which are postulated to take place over a two-week period, in three waves, affecting seven or eight cities each time. The attacks consist of cyber interruptions of electric power, followed by physical damage to power distribution systems. Uncontrolled fires resulting from diminished water pressure, and a breakdown of civil order caused by impaired law enforcement, inflict most of the damage. Concurrent cyber attacks also threaten the financial system, denying service in financial exchanges and corrupting depositor information in many banks.

The scenario generates substantial damage, despite low success rates for individual attacks (10 to 20 percent). Seven cities sustain major damage over the two-week period, through fires, looting, and parallel biological or chemical incidents. Widespread attacks on many banks, with publicity introduced by the terrorists themselves, lead to a significant decrease in trust for the financial system. Runs on the banking system severely impede commerce, and associated transactions threaten to overwhelm the telecommunications system.

This scenario presents a convincing rationale for federal involvement, serves as a means to identify important defensive capabilities, and provides a useful context for assessing protection options.

3. Additional Concerns

Two other important concerns deserve brief mention in connection with infrastructure vulnerabilities and threats. Both relate to cyber attacks. The first is that strong market forces are leading to greater infrastructure vulnerabilities. Current management trends point toward increased consolidation, reduced redundancy, wider-scale standardization, and greater dependence on networks. All of these factors exacerbate the information system weaknesses that are already abundantly present in critical infrastructures. Moreover, the same economic pressures that mandate these management efficiencies also work to reduce the willingness of infrastructure owners to provide cyber protection measures that are not justified by careful calculations of business interests. The second concern is that cyber attacks can occur — and their effects can propagate — very rapidly. Compared with previous infrastructure threats, major cyber attacks could foreshorten response times dramatically.

The preceding description of growing U.S. cyber vulnerabilities and the potent infrastructure attack capabilities that they provide to our prospective enemies — coupled with careful analysis of the stresses and demands that could result from a concerted series

of physical and cyber attacks on infrastructures (as postulated in the threat scenario) — suggest the following serious weaknesses and problems in protecting critical U.S. infrastructures today:

- lack of an overall strategy and poor coordination of federal-level crisis management activities;
- inadequate provisions for prompt operational warning of attacks and for sharing of information between government and the private sector;
- poor awareness in some infrastructure sectors of the types and magnitudes of threats confronting them, and of the easily exploited flaws in their important information systems; and
- widespread private sector reluctance to cooperate with government efforts to provide better protective measures.

In the absence of a well-planned, coordinated, public-private approach, a concerted infrastructure attack of the type described in the threat scenario will continue to pose a serious threat to the citizens and economy of this country.

B. Needed Capabilities — Government and Private Roles

Four broad kinds of capabilities would be useful to meet the threat of attacks such as those illustrated in the preceding scenario: prevention and mitigation; operational warning; response; and counter-action. Each capability area is defined and discussed in this section. For each, the appropriate relationship between the government and private sector will differ; hence, the appropriate roles and structures should be tailored to suit the circumstances. The key features of this discussion are summarized in Table 2, which identifies each of the capability areas and describes the associated private and government roles.

1. Prevention and mitigation

Prevention and mitigation activities reduce the likelihood of successful attacks or mitigate the damage that can be inflicted. Physical hardening, dispersal, and diversification of facilities are important components of prevention, as these help reduce vulnerabilities, particularly to unsophisticated attacks. Redundant and backup systems are key elements of mitigation, since both can decrease the operational down-time resulting from successful attacks. Prevention and mitigation are complemented by the full spectrum of counter-action capabilities that are discussed later.

Table 2. Private and Governmental Roles in Providing Needed Capabilities

NEEDED CAPABILITIES	PRIVATE ROLES	GOVERNMENT ROLES
Prevention and mitigation * Threat analysis and information sharing * Research and development * Norms for infrastructure assurance * Policies to limit proliferation of potential attack technologies	Private sector designs, builds, owns, and operates most infrastructure Private sector currently builds in "cost effective" prevention for understood risks based on potential private (vs. social)costs	Provide threat analysis and awareness programs; evaluate protection programs and vulnerabilities Support R&D Establish norms for infrastructure protection reflecting public needs (regulation, standards, incentives, etc.) Negotiate international agreements and set domestic technology access policies
Operational Warning * Incident reporting * Analysis * Notification and dissemination	Industry and professional associations provide operational problem identification and incident reporting suitable for common, understood risks	Coordinate and integrate incident reporting across sectors, and merge with government information sources Establish an analysis and assessment center to develop and apply warning indicators Disseminate warning
Response * Federal leadership for response * Response preparation * Consequence management	Industry provides first response to common problems Industry is typically well-prepared to respond to common, understood problems, including natural disasters	Federal government leads in developing strategies, plans, and exercises, and in coordinating responses Federal government provides preparedness support (training, financial support, exercise support) for federal, state, and local responders Government acquires and operates local, state, federal response assets (people, technical expertise, equipment)
Counter-action * Federal leadership for crisis management * Military action * Law enforcement * Counterterrorism	Private security is extensive and growing; primarily focuses on "cost effective" security for individual firms based on potential private (vs. social) costs	Federal government leads in developing strategies and plans, promulgating rules of engagement, conducting exercises, and coordinating national counter-action operations Federal government acquires and operates military and intelligence assets for counter-action Federal, state, and local governments acquire and operate assets for law enforcement and counterterrorism

Prevention and mitigation capabilities are primarily developed by the owners and operators of the infrastructure. For example, prevention against cyber attacks includes system hardware and software design, and the design and administration of information networks. User procedures and training are extremely important. Redundant and backup systems are commonly used in all information systems where reliability and information assurance are valued. Private firms thus effectively address routine threats to reliability and assurance, but they generally do not deal with the risks associated with large-scale, purposeful attacks.

In every infrastructure sector reviewed, there also are trade or professional organizations that concern themselves with service reliability.[6] The emphasis of these organizations, however, is on conventional reliability problems, criminal activities, or natural disasters. Industry decision making is driven by a focus on profitability, and a firm's decisions reflect its understanding of risks in terms of potential losses in customers and revenue; for the most part, these decisions do not take account of the broader social costs that might arise if the firm were attacked. Consequently, with the exception of the banking industry (which largely absorbs the costs that result from successful cyber attacks), there appears to be little recognition or emphasis on preventing or mitigating purposeful attacks on information systems. Because prevention and mitigation are largely in the hands of the private sector, the primary role of the federal government is to provide inducements or pressures to bring private decisions into line with the level of protection desirable from a public standpoint.

The federal government can play a number of useful roles in supplementing or encouraging the private sector's prevention and mitigation activities:

- *Threat analysis and awareness*: Improving the threat and vulnerability information available to private firms could influence their decisions to invest in prevention or mitigation capabilities. The government could, for example, share information obtained through intelligence channels or through the operation of its own

---

6 For example, the American Bankers Association (ABA) studies new technologies, e.g., the security of electronic banking and payments systems; the Edison Electric Institute (EEI), an association of privately owned electric utilities, sponsors a security committee; the North American Electric Reliability Council (NERC) uses reports on major outages to raise industry awareness; the Association for Computing Machinery (ACM) has a committee that promotes the reliability, integrity, and security of computer operating systems; the Telecommunications Industry Association (TIA), which represents manufacturers, develops voluntary standards; and the American Water Works Association (AWWA) cooperates with the Environmental Protection Agency (EPA) to prevent microbial contamination of drinking water.

information incident-sharing channels.[7] It could provide an "information clearinghouse" that collects and organizes information provided by private firms, particularly information affecting multiple infrastructure sectors. More proactive analysis and awareness activities could include sponsoring exercises or "red teaming" activities that test a firm's or a sector's existing prevention and mitigation capabilities.

• *Research and development*: The Defense Advanced Research Projects Agency, the National Security Agency, and the military departments sponsor most government-funded research on information assurance; the National Institutes for Science and Technology and the Department of Energy also sponsor a modest amount. In the private sector, consortia such as the Electric Power Research Institute, the Financial Services Technology Consortium, and the Association of American Railroads develop technologies to improve infrastructure, including its safety and security. Academic research focused on computer security is being conducted at several universities, including the Computer Operations, Audit, and Security Technology (COAST) program at Purdue University and the Computer Security Research Laboratory at the University of California at Davis. This research is sponsored primarily by the government, but the private sector also contributes some funding.

By improving available technologies, and reducing the costs of protection, such research could help induce firms to adopt improved prevention and mitigation capabilities. "Designing in" hardening and redundancy should be given high priority in the development of future hardware and software used in connection with critical infrastructures.

• *Norms for prevention and mitigation*: In those sectors where private prevention and mitigation efforts are inadequate to meet public needs, the government could employ regulatory- or standards-setting authority to pressure private firms to meet certain minimum norms. Existing regulatory or oversight authorities may be available; these could be expanded to serve this purpose, or entirely new authorities could be established to address protection issues. Alternatively, the government could encourage

---

7 For example, network security information exchanges (NSIEs) have been established to communicate threats, incidents, and vulnerabilities affecting public network software, with the National Communications System (NCS) representing the government and the National Security Telecommunications Advisory Committee (NSTAC) representing private industry. Also, the FBI's Development of Espionage, Counter-intelligence, and Counter-terrorism Awareness (DECA) program includes a communications network to inform industry of industrial spying and (soon) computer crime threats; and its Computer Investigations and Infrastructure Threat Assessment Center (CITAC) will deal with computer infrastructure threats.

the development of voluntary industry standards or guidelines for infrastructure protection; this could be done as part of an awareness and outreach program. [8]

The establishment of norms could also be encouraged by using the government's influence as a buyer to lead by example — that is, to demand assurance in acquiring its own information services. In many sectors, however, the government has limited influence, because it represents a very small fraction of the overall market. In addition, previous government attempts to encourage market demand for "trusted" technology were not subsequently supported by government acquisition; this failure will undercut the credibility of future efforts along these lines.

A complementary approach would be to encourage the development of a legal liability framework that would establish norms for information assurance. Under such a system, firms would be induced to provide "customary" levels of information assurance in order to limit exposure to liability suits.

- *Access control policies for related technologies:* A final element of prevention could be to limit access to possible attack technologies. Current restrictions on the export of high-end computer equipment, for example, attempt to limit the access of unfriendly nations to hardware that could be used in an attack. However, such restrictions are damaging to U.S. business interests abroad and therefore are staunchly resisted by industry. Moreover, the increasingly sophisticated technologies now being marketed worldwide by other nations will sharply reduce the effectiveness of unilateral U.S. export limitation measures. Government-private agreement on the right approach here is likely to remain elusive.

Although the government has a number of tools at its disposal, prevention and mitigation generally will remain a cooperative, creative activity calling for a high degree of voluntary participation by the private sector. The government can pressure or provide incentives, as well as tools, to private sector firms, but in the final analysis it is up to the private sector to adopt appropriate prevention and mitigation capabilities. Government

---

8 In the private sector, standards for infrastructure safety and reliability are developed, for example, by the American Petroleum Institute (API) and NERC while professional certification programs include the Certified Information System Security Professional and the Certified Information Systems Auditor. NIST and NSA standards designed for Federal information protection are sometimes adopted by private industry as well. Federal regulators also issue mandatory standards, including the EPA for drinking water, the Federal Reserve System and the Office of the Comptroller of the Currency for physical and cyber security at banks, and the Nuclear Regulatory Commission for the safe civilian use of nuclear materials.

and private roles will depend importantly on the characteristics of each sector. Two key characteristics are:

- The "*public criticality*" of the sector: Service failures in infrastructure sectors that support other infrastructures or economic activities — such as computer processing, systems control, data base management, electricity generation, and telecommunications —have broad "spillover" potential. The government's interest in assuring service will be higher for such sectors than for those where collateral effects are of less consequence.[9]
- *Existing public-private roles* in the sector: Some sectors are already subject to extensive federal oversight, regulation, and statutory control, which includes security concerns; thus, it would be reasonable to build on this framework of existing government roles to address infrastructure protection. In contrast, there is no comparable regulatory framework in place for the computer services industry. The government also has limited influence over several of the other infrastructure sectors. In these areas, establishment of an effective role for government will be much more difficult.

It can be expected that the government's engagement of the private sector will start small — with current relationships and responsibilities — and evolve. It is essential that the government's first steps be measured and successful, in order to encourage further progress. For this reason, the infrastructure protection strategy and associated government structures need to emphasize collaboration, and they should try to provide early and significant value-added from the perspective of private firms. A "grand solution" seems less likely to succeed than an evolutionary approach that allows for learning and building on successes.

2. Operational warning

The fact that cyber attacks and their consequences can develop very rapidly has the effect of shrinking drastically the time available for effective reaction. The capability to provide warning of impending attacks — or indicators of attacks under way — would contribute significantly to the nation's ability to muster resources for responding, and to engage effectively the nation's national security, law enforcement, and counterterrorism assets. Such a capability requires a well-structured incident reporting system and a sophisticated understanding of potential warning indicators that would permit attacks to be distinguished from common problems.

---

9 Indeed, some have argued that the government should identify the "minimum essential infrastructure," based on a concept employed in early emergency preparedness activities. This concept would establish a formal — and active — federal role in protecting designated infrastructures.

Some incident reporting systems already exist within the private sector. [10] Others are managed by the government.[11] Most of these are not focused on possible cyber attacks, however, and they operate within existing sector "stovepipes." Nevertheless, these mechanisms may provide a good starting point for developing a useful warning system.

There are several important roles the government could play in establishing an effective operational warning mechanism.

- *Data collection and integration*: The government is in the position to integrate information across sectors, from government operations, and from the intelligence and law enforcement communities, and thus to obtain a cross-cutting view of warning indicators.

- *Analysis and correlation*: The government could develop and operate the analytical capabilities required to compile and analyze these indicators. And the government is the logical sponsor of R&D programs that will be needed to develop such capabilities.

- *Dissemination*: Finally, the government could provide the mechanisms needed for disseminating warning. A warning analysis center can be closely linked with government focal points for response, law enforcement, and counterterrorism; it also could provide for the real-time alert of infrastructure firms, and thus trigger protective countermeasures.

Some experts question the feasibility of developing a useful warning system for cyber attacks. The technical feasibility has been challenged by those who doubt it will be possible to identify an attack in time to intercept it, mount a useful response, or counterattack. They emphasize that it will be difficult to distinguish attacks from normal system failures caused by day-to-day problems. Moreover, attackers can be expected to

---

10 The New York Stock Exchange (NYSE) maintains continuous electronic surveillance of its market for noncompliance with its rules and unusual price and volume activity. NERC has established 22 regional security coordinators to monitor operations and exchange information.

11 Several federal regulators require that certain events be reported to them expeditiously, including major telecommunications outages (to the Federal Communications Commission (FCC)), electric power outages (to the Department of Energy (DOE)), and releases of oil and other hazardous materials (to the Department of Transportation (DOT), the EPA, DOE, and the U.S. Coast Guard (USCG)). Some agencies seek to issue specific warnings when attacks seem imminent, e.g., the Central Intelligence Agency (CIA) informs the Federal Aviation Administration (FAA) of threats so that the FAA can inform industry, and the Department of State (DOS) operates programs to warn U.S. interests overseas of possibly impending attacks.

disguise their attacks in a variety of ways. Doubts also have been raised as to whether private firms will be willing to share information with a government warning center.

These problems notwithstanding, it is generally agreed that warning should be a central element in infrastructure protection strategy. Considerable thought and cooperation will be required to define a system and a set of institutions that are legally and technically capable of providing such warning, and that will induce firms to report problems voluntarily. For this reason, government structures are needed that can take a proactive role in fostering the development of warning indicators and techniques, develop collaborative relationships with industry for the sharing of information, and help institutionalize the needed incident reporting systems.

3. Response

Response includes those capabilities needed to resolve an infrastructure crisis and manage its consequences. Response activities thus range from initial efforts to halt further destruction of the infrastructure and protect public safety, to subsequent efforts to provide disaster relief and eventually facilitate recovery of communities and infrastructure. Any response must draw on private sector assets, which provide the vast majority of response capabilities. Response also embraces existing governmental capabilities provided by FEMA, other federal departments and agencies, and state and local governments. In many cases, the consequences of purposeful attacks on infrastructures will be similar to those already addressed by these communities. Power and telephone outages, bank holidays, suspension of mail delivery and other government services, and physical destruction of property all can occur on massive scales when there are floods, hurricanes, tornadoes, or earthquakes. The capabilities developed for these situations can be applied to purposeful infrastructure attacks as well.

Serious attacks on infrastructure add an important dimension to the challenges that must be met by response functions. Weapons of mass destruction disperse chemicals, biological agents, or radiation that could impede response capabilities. Similarly, cyber attacks may create misinformation and confusion, and undermine the information systems needed to coordinate response activities. Response coordination assets may therefore need to be hardened against attack, and response personnel may require greater protection than is widely available today. In addition, these communities must develop new technologies and tactics if they are to respond to purposeful attacks on

infrastructure; this includes expanding the capabilities and availability of computer emergency response teams.[12]

Three government roles are needed to address the challenges of responding to purposeful attacks:

- *Federal leadership*: A lead government entity must be assigned responsibility for developing the strategy, programs, and policies needed to provide response capabilities suitable for meeting the threat of broad attacks on the U.S. infrastructure. One focus of this leadership would be to determine what capabilities are needed that are not already being provided by the response community, and to ensure that these capabilities are developed and deployed. Leadership also must be capable of creating close collaboration within the federal government, with state and local governments, and with the private sector.

- *Response preparedness:* The federal government, through FEMA and other agencies, already conducts a wide range of preparedness activities with state and local governments. It also funds state and local preparedness investments, and supports preparedness tests and exercises. Recently, under the Nunn-Lugar legislation, federal preparedness programs were expanded to help state and local governments deal with chemical, biological, and radiological emergencies.[13] In a similar way, preparedness programs could be extended to prepare for purposeful physical and cyber attacks on the infrastructure.

- *Response operations:* The federal government frequently mobilizes assets in response to emergencies, and it provides leadership in coordinating the activities of a wide range of responders. Much of this capability exists within the Department of Defense, which, with its active, reserve, and National Guard forces, possesses the manpower and logistics capabilities typically needed to restore order and basic services. There are, however, other very important capabilities found throughout the federal government. To name one key example, the federal response to release of hazardous materials is carried out under the National Oil and Hazardous Substances Pollution

---

[12] DARPA sponsors the well-known Carnegie Mellon computer emergency response team (CERT), which provides 24-hour technical assistance for responders to computer security events. NIST supports a federal computer incident response capability (FedCIRC) to support responders to computer security incidents at federal civilian agencies, utilizing capabilities at CERT and DOE.

[13] Under 1996 legislation, DoD conducts exercises to improve federal, state, and local responses to emergencies involving biological or chemical weapons or materials; DOE conducts similar exercises addressing nuclear and radiological weapons or materials.

Contingency Plan. The Environmental Protection Agency has been designated as the lead agency for this mission. However, it may call upon one or more support agencies, including DoD, DoE, and the Coast Guard for assistance. FEMA also provides other essential emergency governmental services, and it coordinates overall response activities at the federal level.

It is generally accepted that the existing response framework performs adequately in addressing the kinds of situations for which it has been designed. The challenge will be to expand the missions of this existing framework — or possibly to supplement it with new institutions — to address situations involving concerted attacks on the U.S. infrastructure. This may require additional coordination assets; it may also require the development of new response capabilities. Expanded missions must be accorded high priority in order to ensure that existing organizations adapt to meet them. Federal structures must lead the response community firmly in coping with purposeful attacks on the infrastructure, and helping foster the development of the new capabilities that are needed.

4. Counter-action

This category includes capabilities to preempt or intercept would-be attackers; possibly counterattack physically or using U.S. offensive information warfare tools; or track down, apprehend, and prosecute attackers in the wake of an attack. In sum, counter-action includes all of the measures at the nation's disposal to deal directly with the individuals, groups, or states that perpetrate attacks.

While law enforcement and counterterrorism are generally considered government functions and most such capabilities are within the government, private security provides most of the day-to-day protection for U.S. businesses. For example, it was Citibank's private security team that found the Saint Petersburg gang that broke into their system. Their private security then provided the information to government authorities, which allowed the gang members to be apprehended. Citibank has adopted an information assurance strategy that includes as an important element pursuing anyone who unlawfully enters their information systems.

Such private security has much to contribute, but it is limited in scope, leaving the bulk of the law enforcement and counterterrorism work to be done by the government. Three main federal capabilities are needed in this area.

• *Federal leadership:* Government leadership is needed for creating the strategy, programs, and policies necessary to bring the government's intelligence, military, law enforcement, and counterterrorism capabilities to bear on countering attacks on the U.S. infrastructure. A main purpose of this leadership would be to better integrate the international missions of the national security community with the law enforcement and domestic counterterrorism missions. In doing so, it would clarify the responsibilities of the various communities, and help establish teaming relationships among them to address a wide range of cross-cutting infrastructure protection problems. (It is important to draw a clear distinction here between leadership of federal-level *strategy development and coordination*, as described above, and *actual conduct of military operations*. Any military action that is required would clearly be the responsibility of the nation's unified military commands. The same distinction applies to law enforcement actions, which would be carried out by the appropriate law enforcement agencies.)

A second function of strong federal leadership would be to determine what capabilities are needed that are not already being provided by the national security, law enforcement, and counterterrorism communities, and to ensure that these capabilities are developed and deployed. Finally, this organizational entity must be capable of creating close collaboration within the federal government, and with state and local law enforcement agencies.

• *Law enforcement and counterterrorism operations:* The Federal Bureau of Investigation, as the leading federal law enforcement body, plays a key role in preventing, halting, and investigating terrorist crimes and apprehending terrorists. The FBI has the principal authority to conduct and coordinate counter-intelligence and counter-terrorism investigations and operations in the U.S. The FBI also investigates terrorist threats and crimes against U.S. citizens and interests abroad in cases where extraterritorial jurisdiction applies. The FBI maintains an on-line database of suspected terrorist groups and individuals. With its new Computer Investigations and Infrastructure Threat Assessment Center (CITAC), the FBI will conduct computer infrastructure threat assessments as well as investigate computer-related crimes. The FBI supports state and local law enforcement through training, laboratory services, and operational assistance, including joint terrorism task forces and SWAT teams located around the country.

The national security community provides the military and intelligence assets for addressing terrorist threats abroad. The Coordinating Sub-Group on Terrorism within the NSC coordinates the activities of the national security, law enforcement, and other communities working on this problem. The CSG establishes policy and assigns

responsibility for operations. It coordinates the capabilities needed to counter possible attacks on the infrastructure, but as yet it has not been assigned this mission explicitly, or any mission associated with information attacks.

In summary, the government already posses significant intelligence, law enforcement and counterterrorism capabilities, along with a truly formidable capacity for military operations. There are, however, important gaps that need to be filled in addressing the threat of attacks on the U.S. infrastructure. A new federal structure is needed to provide clear missions and tasking to the existing agencies, and to establish collaborative working relationships among them. These relationships are needed especially at the federal level, but also between national and state/local governments, and between government and the private sector. These measures are especially critical for effective reaction to fast-breaking cyber attacks.

C. Observations

The representative threats and the four capability areas discussed here — prevention and mitigation, warning, response, and counter-action — provide the outline of a strategy for infrastructure protection. Much detailed work remains, and there are many residual questions about the most effective approaches, how quickly to proceed, resource levels, and the precise assignment of roles and responsibilities.

It is in fact probably premature to develop a very detailed strategy, because there is so much uncertainty regarding the nature and extent of the threat, and because the threat can be expected to change over time. To an important degree, the strategy must rely on learning by doing: many roles and relationships might best be left open to refinement as more is learned. Government institutions appropriate for this approach should strive initially to generate capabilities that contribute a high value-added from both government and industry perspectives, and they should be designed to foster mutual collaboration and trust with the private sector.

A number of structural issues were raised in the context of describing the four capability areas and general roles and responsibilities. It seems clear that the structures need to be tailored for each of the capability areas. The structures best suited for prevention and mitigation activities should be designed to promote public-private collaboration. The structure for warning should be capable of fostering a program of research on warning methods and building needed reporting relationships. The structures for response and counter-action need to provide strong leadership and coordination within the federal government, while at the same time fostering collaboration with state and

local governments and the private sector. Options for building these kinds of institutional structures are the subject of the next section.

III. ALTERNATIVE FEDERAL STRUCTURES

Section II identified the kinds of capabilities that might be developed to address the dangers of attacks on the U.S. infrastructure, and it described the roles that can be played by government and the private sector. Each of the governmental roles requires capabilities that are not readily found within the current organizational structure of the federal government. Moreover, the kinds of structures needed cannot be "cobbled together" quickly once a serious threat has emerged. Thus, the strategy for infrastructure protection will entail creating some new federal structures that begin to lay the groundwork of needed capabilities and relationships

In designing and evaluating potential options, it is useful to start with some guiding principles oriented toward ensuring that new structures are both relevant and effective. Several management and organizational principles have been suggested by experts; to a large degree, these reflect lessons learned in prior efforts to provide focused leadership for national problems. These principles stipulate that federal structures should be designed in such a way that they: (1) provide leadership for developing strategies and policies, and assigning operational responsibilities for protecting the infrastructure; (2) build on existing institutions, capabilities, and working relationships; (3) interact effectively with the private sector; and (4) evolve as the protection strategy matures. These principles are described in greater detail in Subsection A.

Drawing on these principles, three broad structural options are described in Subsection B. Each of these options has received significant support from current and former senior government officials, and experts in infrastructure protection, and each has identifiable strengths and weaknesses. The first option focuses on establishing a small senior leadership entity within the government for federal response and counter-action activities. Under this option, interactions with the private sector and state/local governments for prevention and mitigation activities, and for operational warning, would initially continue to rely on currently existing relationships. The second option augments this small leadership entity with an operational institution that would perform additional federal functions, and provide more structured interaction with the private sector and state and local governments. The third option establishes a new public-private organization reporting to the President that would perform both leadership and operational roles. The relative advantages and disadvantages of these options are discussed in Subsection C.

A. Management Principles

Any new federal organization established to address infrastructure protection concerns must overcome extant weaknesses in the federal structure, while avoiding the pitfalls that have been encountered in the past in creating new federal entities to address national problems. Therefore, to the extent possible, new organizations should conform with the four principles listed above.

Principle 1: Provide effective leadership for developing strategies and policies, and assigning operational responsibilities for protecting the infrastructure

Leadership and responsibility for the development and execution of strategies and policies is diffused, and needs to be more focused at the highest levels of government. Getting the government to address effectively issues that cut across organizational boundaries is always a complex task; it is difficult to coordinate and lead a multi-agency process, and yet it is the agencies that have the capabilities needed to do the job. Leadership must be provided in setting federal policy, and in marshaling and coordinating federal resources. In fact, many believe that for a strategic policy focus to be fully developed and implemented, a stronger role will have to be played by the President and the Executive Office of the President.

To be successful, a federal leadership entity requires independent authority, operational focus, and "clout." Thus, it may be a mistake to make this a subsidiary responsibility to an organization with other important missions; it may make sense instead to establish a strong, new organization within, or reporting to, the Executive Office of the President. Alternatively, it may be possible to establish a strong organization outside the White House that is both empowered and responsive to the policy directives provided by the White House. It may be that no existing agency is right for the job, or it may be that, with strong central leadership and coordination, existing organizations can work together effectively. Several existing leadership bodies have been proposed as possible models.

Coordinating Sub-Group model: The first model is a coordinating-type mechanism like the Coordinating Sub-Group (CSG) on Terrorism. The CSG provides a venue for federal agencies to work out, in advance, responsibilities for responding to terrorist events. This includes affirming who the lead agency is in specific circumstances, and informing each prospective lead agency of capabilities throughout the government that might be of value during a crisis. The CSG has no prevention and mitigation, or

indications and warning capabilities; these are not part of its charter. The CSG is chaired by a senior National Security Council staff member.

Independent Agency model: A very different model is provided by the Federal Reserve Board. The "Fed" is an independent regulatory agency that, among its other responsibilities, manages risks to the banking system. Because of its regulatory powers over, and its close working (operational) relationships with member banks, it is able to exert considerable influence over bank behavior; it is also able to obtain detailed information from the banks whenever it wishes. Its role as regulator is key to its relationship with industry, and thus central to determining whether it is, or is not, a model for other government agencies and industry sectors.

Other models of an independent agency for leadership that have been proposed include creating a new public-private entity (e.g., similar to a Federally Funded Research and Development Center, or the Centers for Disease Control (CDC)) that would be a focal point for the development and analysis of policy and operational options. Such an entity might report directly to the head of a White House Infrastructure Office, should such an office be created.

Executive Agency model: A third leadership model, illustrated by the Office of National Drug Control Policy (ONDCP), creates an agency within the Executive Office of the President. ONDCP actively leads and coordinates strategy, policy, and the assignment of operational drug control responsibilities among many different agencies. Unlike the chair of the CSG at the National Security Council, the head of ONDCP reports directly to the President, and has greater responsibility for directing the allocation of resources and operational responsibilities to the agencies. However, the serious difficulties experienced by this office at various times caution against establishment of an "Infrastructure Czar." Another alternative some have suggested is to have an office such as ONDCP that reports to an established entity, like the National Security Council or the Office of Management and Budget.

The Continuity of Government (COG) model is an example of an executive agency that reportedly worked quite successfully. It had control over resources and significant top level support, particularly during the Reagan Administration. However, this organization had the advantage of being able to focus intensively on a single (albeit important), well-defined mission that was clearly a federal responsibility. Infrastructure protection is more complex, and the federal role therein is contentious.

Clearly, federal leadership is needed for developing an infrastructure protection strategy and implementing needed policy and program changes. While a number of other organizational approaches have been taken to solving national problems that cut similarly across federal structures, the list above reflects the more promising models for infrastructure protection.

Principle 2. Build on existing institutional capabilities and working relationships

Although federal leadership may be lacking, there are nonetheless a multitude of both government and private organizations that are already dealing with certain aspects of the infrastructure protection problem. They involve every important sector of the infrastructure and the economy. Government organizations often work closely with industry organizations in a collaborative effort to achieve both private and public goals. In addition, many government agencies have unique capabilities that can and should be used to address infrastructure protection issues. The existing talents and capabilities of both government and private organizations, including their working relationships with industry, have much to offer.

Existing capabilities: This report cites a wide range of examples of existing government organizations with impressive and growing capabilities in the cyber and infrastructure protection areas, or in closely related fields. (Appendix B provides details.) The Department of Defense, in particular, has extensive information warfare capabilities, both offensive and defensive, spread throughout the Department. There is considerable awareness of these issues, particularly as they affect DoD activities. But in considering the possible contribution of DoD to national infrastructure protection, a critical distinction will always need to be made between DoD's responsibilities for and capabilities to handle its own assets, and the responsibilities it can legally assume with respect to protecting infrastructure in general.

The FBI provides another essential capability; it is the lead agency for investigating terrorist attacks, and it provides most federal involvement in investigating domestic crimes. The Bureau views all attacks, including cyber, as crimes, and it is organized to investigate and solve crimes. The FBI clearly has significantly fewer cyber-related capabilities than the Defense Department (although its focus is directly on events affecting U.S. citizens, companies, and property, whereas DoD's focus is on external threats and its own assets). The FBI's Computer Investigations and Infrastructure Threat Assessment Center (CITAC) was established to provide a focus for cyber and

infrastructure crimes, but is still new and relatively small. Furthermore, when the FBI is called in on a case, its focus on evidence collection and crime-solving often disrupts ongoing business. Consequently, companies are often reluctant to call them for assistance.

In the area of response, FEMA is a central player for developing programs and policies for addressing natural disasters, and it should play an equivalent role in the response system for infrastructure protection.

Existing relationships: This report also has cited a number of effective relationships among organizations of the type that will be needed to establish infrastructure protection capabilities. (Additional information is provided in Appendix B.) One typical example of a close government-private relationship is that of the Federal Aviation Administration within the Department of Transportation (DOT), which oversees the air traffic control system and has a comprehensive working relationship with the airline industry. DOT also oversees the safety of oil and gas distribution. The Federal Reserve Board provides another example, as does the Federal Energy Regulatory Commission, with its regulatory authority over the distribution of electric power and other energy supplies. These relationships can be built upon to deal with infrastructure protection capabilities.

The examples cited here, and earlier in the report, illustrate that many of the capabilities and working relationships that eventually will comprise an infrastructure protection strategy are already being provided, exist in similar form, or are under development. The institutions built for infrastructure protection should be designed to take advantage of these existing capabilities and relationships to the extent practicable. However, if the federal leadership entity cannot generate a critical mass of support for infrastructure protection within extant organizations, then a reorganization that consolidates related activities in a single organization may be necessary.

Principle 3. Interact effectively with the private sector

There is broad agreement that the primary responsibility, and most of the capabilities required, for infrastructure protection rest with the private sector owners and operators. At the same time, there is also agreement that the government has valuable assets for addressing this problem, and that the government has important responsibilities complementary to those of private industry. Collaborative relationships are needed, and much of the responsibility for building such relationships lies with the federal government.

One important government responsibility in building relationships is to increase education and awareness, and thus improve understanding of the problem. Many in the private sector assert that their greatest need is for threat information, and that government has much that is unique and important to contribute here. Public officials generally agree with this assessment. Improving the flow of information to the private sector — including potentially sensitive intelligence information, in a sanitized form — may be an important prerequisite of success. Overcoming procedural and cultural impediments to sharing classified information will be challenging. Even more challenging will be determining what private sector information is of greatest value for infrastructure protection, and developing workable mechanisms for sharing it.

Government can also play an important role in helping to set norms for infrastructure protection. This role may range from a directive one to simply facilitating voluntary industry standards or agreements. As discussed previously, there is often a sharp divergence between private and public sector calculations of the costs and benefits of prevention and mitigation measures – private estimates tend to underestimate risks to themselves, and they take little account of ripple effects on others, or of broader national security or public safety concerns. Education regarding larger threats and careful consensus-building are important prerequisites for establishing effective protection standards.

Examples of existing working relationships between industry and government have been discussed previously. To a large extent, these are "bilateral" in nature, between an industry organization and a government agency that has close ties with that sector. The examples cited include the Federal Reserve Board, with banking; the Federal Energy Regulatory Commission, with electric power companies; and the Federal Communications Commission, with the telecommunications industry. These are relationships that can be built upon in order to meet expanded infrastructure protection requirements.

There are significant hurdles that must be overcome, however. The private sector is highly skeptical of any government involvement in its activities. There are numerous concerns over privacy, proprietary data, and government intrusion into business decisions. Trust will need to be developed and improved between government and the private sector.

Another challenge in building public-private relationships is that many key government organizations with infrastructure protection responsibilities or capabilities

simply lack effective ties to the private sector. This is particularly true for the counter-action area. The Coordinating Sub-Group on Terrorism (CSG), for example, has no direct responsibility for dealing with the private sector, and has no responsibility for indications and warning. Relations between government and industry are handled separately by each CSG member agency, if at all. In the Defense Department, the people developing offensive information warfare capabilities talk to no one, and defensive information warfare organizations are primarily concerned with protecting DoD assets. The FBI has a program that provides threat briefings to industry, but these tend to be general in nature; this program is not designed to share sensitive information that might expose sources, or to promote two-way sharing. And the intelligence community has little contact with the private sector on infrastructure-related issues.

Governmental institutions for infrastructure protection must promote effective collaboration between the federal government, state and local governments, and the private sector. Some "building blocks" for such relationships exist, and these can be built upon, particularly for prevention and mitigation activities and for collaboration on response. At the same time, no such relationships are in place with respect to several important capability areas, particularly for indications and warning, and counter-action; it is within these areas especially that considerable work will be required to overcome cultural differences and to build trust between the public and private sectors.

Principle 4. Evolve as the protection strategy matures

Creating and implementing an infrastructure protection strategy is a journey, not a single point solution. There is a need to build trust, both among government organizations and between government organizations and the private sector. Specific responsibilities will evolve as issues and problems are better understood, and as working relationships develop.

Thus, it may be that many relationships and responsibilities should not be spelled out in detail, at least for some period of time. Aggressive action by the federal government to direct private-sector activities, or to devote extensive resources to the problem, is likely to be viewed by industry as an over-reaction. These considerations argue that the best tactic for enlisting industry support is an evolutionary approach, one that initially establishes a federal structure that focuses on understanding the problem, sharing information, and maturing an infrastructure protection strategy. Such an organization would invite industry to review and comment on proposed initiatives, and it would foster needed organizational relationships within the federal government, and with

state and local governments and the private sector. As organizational structures and the desired interactions evolve and mature, increasing attention would be focused on developing prevention and mitigation measures, and on the more critical task of reducing the timelines for effective warning, response, and counter-action.

B. Options

Drawing on these principles and on preliminary research and interviews, the IDA study team developed a number of initial organizational options designed to provide the capabilities outlined earlier. These options were presented to the IDA panel, discussed at length, and developed into an amended set of options. This section describes the results. For each option, an organization chart is provided, along with a description of the federal roles to be played by the proposed organization(s).

Option 1: A Lead Agency within the Executive Office of the President

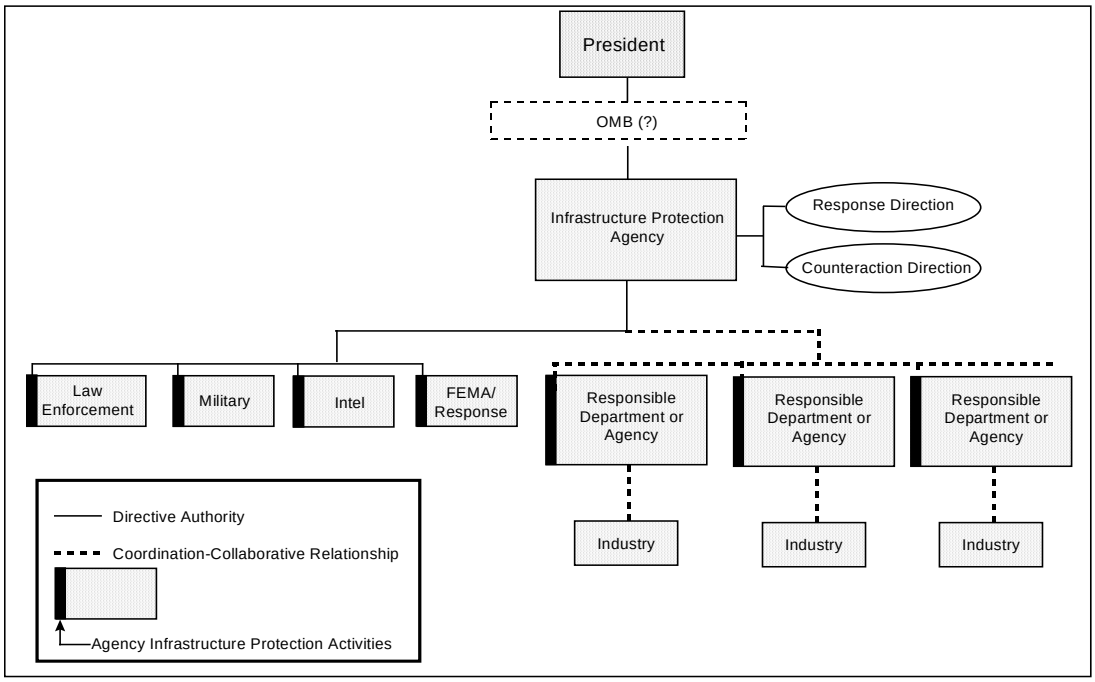
Option 1 entails the creation of a strong Presidential-level office — a "Lead Agency" — to direct the government's infrastructure protection activities. An overview of this option is presented in Figure 1. This Lead Agency would be in the White House, and would have a very small staff. The head of the Lead Agency would report directly to the President or the Vice President. Alternatively, the agency could be placed within, or subordinated to OMB, which has recently started coordinating the federal government's internal information assurance efforts. The primary advantage of this placement is that of providing the Lead Agency a strong institutional home and direct access to resources; the main disadvantage is that Lead Agency responsibilities would have to compete with other important OMB functions for the attention of its leadership, which may in turn dilute the agency's authority.

The Lead Agency would have *directive* authority over the strategies, policies, programs, and budgets of those agencies and activities that conduct operations in the areas of response and counter-action. This option thus provides for much tighter coordination for response and counter-action than exists today. A central function of the Lead Agency would be to integrate the activities of the federal law enforcement and national security communities in the infrastructure protection area.

The Lead Agency would have *coordinating* responsibility for the activities of the agencies responsible for prevention and mitigation, and for operational warning. Interfaces with the private sector would continue to be handled through the network of agencies that already have these working relationships. (The intent here is to let these

connections evolve; the same applies for integration *across* infrastructure sectors.) The Lead Agency would provide tighter coordination of the activities of responsible departments and agencies, which could also improve awareness and warning mechanisms at the sector level.

Figure 1. Option 1: A Lead Agency with the EOP



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

Prevention roles: This option takes an evolutionary approach. It maintains current relationships between government agencies and the private sector, while establishing a Lead Agency to coordinate and integrate activities across responsible departments and agencies. Federal prevention roles are as follows:

- The Lead Agency *coordinates* prevention strategy, policy, and operations of responsible departments and agencies.
- Responsible departments and agencies interact with the private sector through existing relationships.

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 leadership agency

would encourage the growth of cross-sector exchanges and linkages. Federal operational warning roles are as follows:

- The Lead Agency *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.

Response roles: The Lead Agency would actively shape and integrate the federal government's response activities; it would play a leadership role in developing and coordinating governmental responses to infrastructure attacks, similar to the role played by FEMA for natural disasters. Clearly, tight coordination and collaboration between the agency and FEMA would be essential. Federal response roles are as follows:

- The Lead Agency directs the strategy, policy, and budgets of the departments and agencies responsible for response to infrastructure attacks.
- Responsible departments and agencies provide response capabilities.

Counter-action roles: This option is intended to provide strong leadership for integrating the activities of the law enforcement and national security communities. The Lead Agency would establish strategies for joint action across these communities, and it would establish mechanisms for teaming to address specific tasks. Federal counter-action roles are as follows:

- The Lead Agency *directs* the strategy, policy, and budgets of the departments and agencies responsible for operations against infrastructure threats.
- Responsible departments and agencies provide law enforcement, counterterrorism, military, and intelligence capabilities.

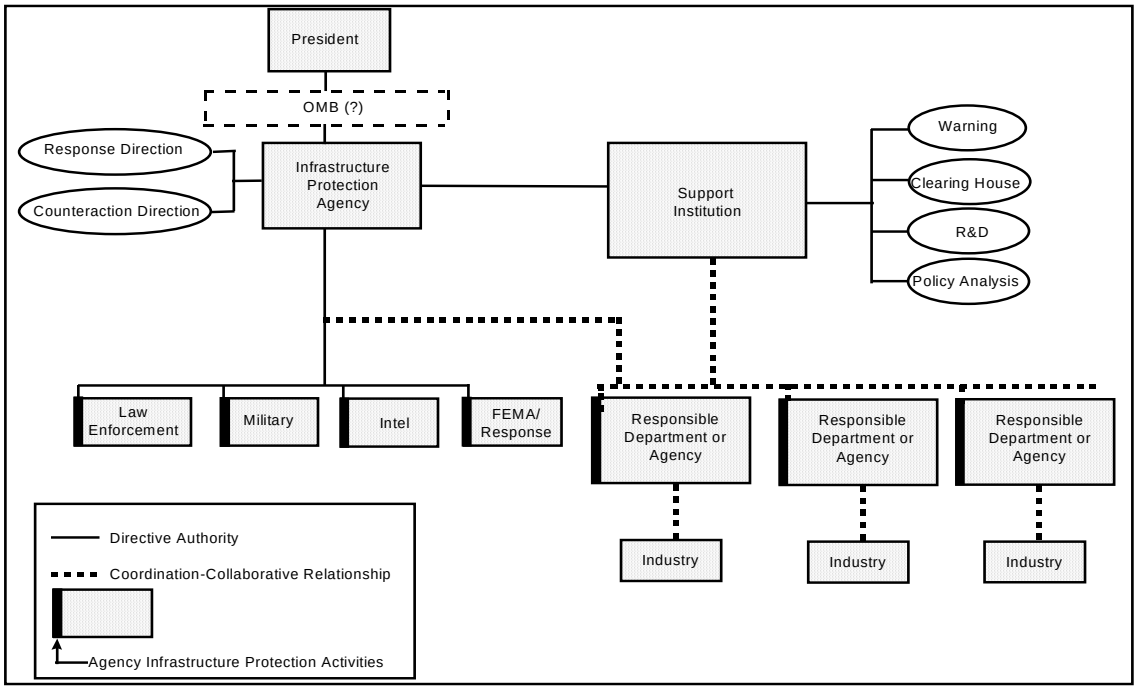
In summary, Option 1 defines an approach that focuses primarily on establishing strong central leadership and integrating the government's own activities. It takes a go-slow approach with respect to government-private interaction, relying heavily on building on existing relationships.

Option 2: Double-barreled approach: EOP Lead Agency and a supporting operational institution

Under this option, a Lead Agency within the Executive Office of the President is created to manage federal activities. Just as in Option 1, the head of this office would report to the President or to the Vice President, or the office could be housed within OMB. The Lead Agency would provide the same kinds of leadership for response and counter-action activities as outlined for Option 1.

The additional feature of Option 2 is that this agency is complemented by a supporting institution and a substantial staff to engage in a more proactive program of protection activities. The director of this institution would report directly to the leadership agency. Its operational staff would focus on information sharing, research and development, and on developing operational warning mechanisms. It would also provide policy analysis support to the agency across the full range of protection activities. This supporting institution might be a government body, or it might be a public-private entity such as a Federally Funded Research and Development Center. Figure 2 presents a pictorial overview of Option 2.

Figure 2. Option 2: EOP Lead Agency with a Supporting Institution



The assignment of roles for each of the four capability areas is as follows.

Prevention roles: In contrast with Option 1, new institutions would play a much larger role in promoting prevention and mitigation activities. The federal roles under Option 2 for prevention are as follows:

- The Lead Agency *coordinates* prevention strategy, policy, and operations of responsible departments and agencies.
- The Support Institution
  - Provides an information clearinghouse
  - Conducts awareness activities with government and industry

    - * Coordinates and directs R&D
    - * Supports policy development & analysis.
- Responsible departments and agencies interact with private sector through existing mechanisms.

Operational warning roles: The new institutions would take a proactive role in developing the organizations and technical tools needed to establish warning capabilities. This option thus creates a much more vigorous role for the federal government in establishing a centralized warning capability. The federal roles under Option 2 for operational warning are as follows:

- The Lead Agency *coordinates* activities of responsible departments and agencies.
- The Support Institution
    - * Provides a warning analysis center
    - * Integrates information across departments
    - * Provides a dissemination mechanism.
- Responsible departments and agencies continue to interact with the private sector through existing mechanisms.

Response roles: The role of the Lead Agency in Option 2 is essentially the same as outlined for Option 1. The main difference is that it can draw on a dedicated supporting staff in establishing strategies and policies for response, and for reviewing budgets and addressing resource allocation issues. The federal roles under Option 2 for response are as follows:

- The Lead Agency *directs* strategy, policy, and budgets for response to infrastructure attacks.
- The Support Institution supports strategy, policy, and budget development.
- Responsible departments and agencies provide response capabilities.

Counter-action roles: As under Option 1, the Lead Agency has a central role to play in integrating the federal government's capabilities in this area. It can draw on the supporting institution for this role. The federal roles under Option 2 for counter-action are as follows:

- The Lead Agency *directs* strategy, policy, and budgets for operations against infrastructure threats.
- The Support Institution supports strategy, policy, and budget development.
- Responsible departments and agencies provide law enforcement, counterterrorism, military, and intelligence capabilities.

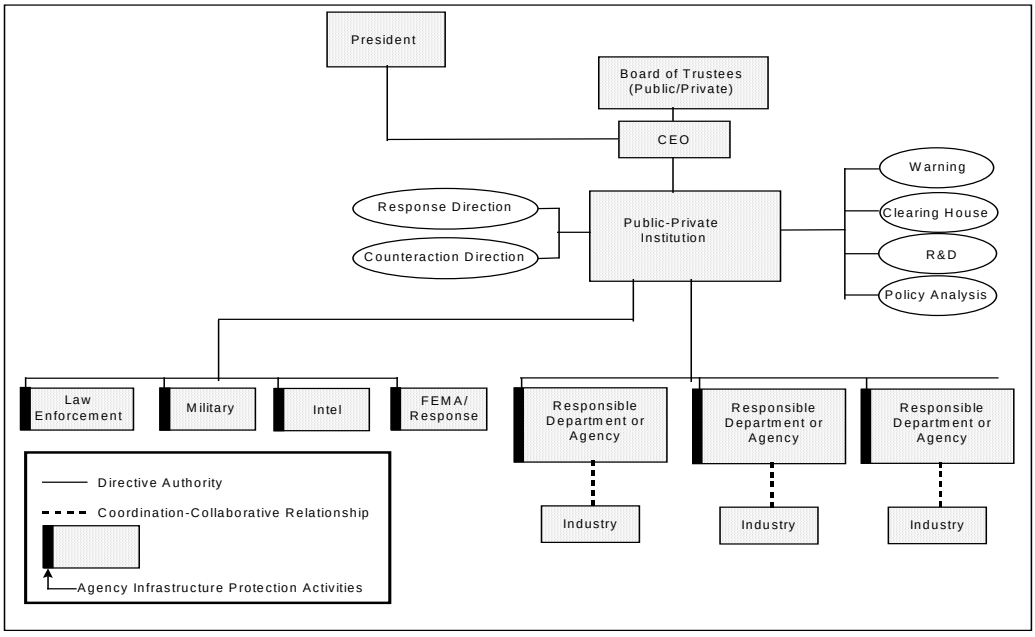
In summary, Option 2 establishes a strong federal leadership entity, as under Option 1, and augments this organization with an operational arm that can provide muscle in the intra-governmental policy process and better support the development of needed capabilities in cooperation with the private sector.

Option 3: A Dedicated Public-Private Institution for Infrastructure Protection

This option envisions the creation of an independent institution, reporting to the President, which would lead both public and private efforts to protect critical infrastructures. This would be an organization with a public-private board of trustees appointed by the President. The CEO would report to the trustees and to the President. The trustees would comprise a mix of senior government officials, industry executives, and others from the private or non-profit sectors. The Institution would maintain a large, expert staff. It would have regulatory and standards-setting authority for prevention norms. This authority would govern federal departments and agencies, as well as private firms.

The Institution would work with responsible departments and agencies and the private sector. It would provide clearinghouse and warning capabilities, and it would set norms for protection. Further, the Institution would have the authority to direct departments and agencies responsible for response, law enforcement, and counterterrorism. Figure 3 provides an overview.

Figure 3. Option 3: Government-Private Institution for Infrastructure Protection



Under Option 3, the public-private institution is given responsibility for all federal leadership activities, as well as for developing federal infrastructure protection capabilities, such as an information clearinghouse and a warning mechanism.

Prevention roles: The Institution would provide federal leadership for prevention activities. It would continue to work through the existing network of departments and agencies that interact with the private sector, but it would have strong authority to direct their infrastructure protection activities. The Institution also would develop significant substantive capabilities through its administration of the federal information clearinghouse, the management of an R&D program, and involvement in policy development and analysis. The federal roles under Option 2 for prevention are as follows:

- The Institution
  - * *Directs* activities of responsible departments and agencies through regulation or standards.
  - * Provides an information clearinghouse
  - * Conducts awareness activities with government and industry
  - * Coordinates and directs R&D
  - * Supports policy development and analysis.
- Responsible departments and agencies continue to interact with the private sector, but do so under Institution direction.

Operational warning roles: The Institution leads the development of warning mechanisms and works to establish needed organizational relationships. The federal roles under Option 2 for operational warning are as follows:

- The Institution
  - * *Directs* the activities of responsible departments and agencies through regulation and standards.
  - * Provides a warning analysis center
  - * Integrates information across departments
  - * Provides a dissemination mechanism.
- Responsible departments and agencies continue to interact with the private sector, but do so under Institution direction.

Response roles: The Institution assumes the federal leadership role for response to infrastructure attacks. It has directive authority over the infrastructure protection activities of agencies that provide needed response capabilities. It has a staff in place to assist in executing this authority. The federal roles under Option 2 for response are as follows:

- The Institution *directs* strategy, policy, and budgets for response to infrastructure attacks.
- Responsible departments and agencies provide response capabilities.

Counter-action roles: The Institution takes the federal leadership role for integrating the capabilities of the law enforcement and national security communities for infrastructure protection. The Institution has directive authority over the protection activities of agencies. The federal roles under Option 2 for counter-action are as follows:

- The Institution *directs* strategy, policy, and budgets for operations against infrastructure threats.
- Responsible departments and agencies provide law enforcement, counterterrorism, military, and intelligence capabilities.

C. Evaluation of the Options

Each of the three options outlined here — EOP Lead Agency, EOP Lead Agency with a support institution, or a new, public-private body — is intended to address the weaknesses in the current federal structure for performing infrastructure protection capabilities. Obviously, there are many possible variations on these options. In particular, a range of alternative models was discussed in the principles section. The best approach will depend importantly on the relative priority one places on developing each of the capabilities outlined in Section II, on how aggressive one believes the federal role should be, and on how one judges the appropriate relationships between the public and private sectors.

Each of the three options addresses important organizational weaknesses for implementing infrastructure protection capabilities, and, in this regard, each has considerable merit as compared with the *status quo* federal structure. Still, there are significant differences among the options, and associated with these are certain strengths and weaknesses. This subsection provides a framework for evaluating the three options that also could be applied to comparing others.

Option 1: The first option only provides federal leadership to strengthen the integration within the federal government of response and counter-action capabilities. It attempts to marshal the capabilities of the federal law enforcement and national security communities to address infrastructure protection concerns. The principal strength of this option is that it focuses on getting the federal government's own house in order. It also provides a central focal point for the continued development of an infrastructure protection strategy. A second advantage is that it would be relatively easy to implement.

It does not require significant, explicit resource commitments, since the new office will be small. It also does not require the creation of a new *type* of organization, and it does not disturb existing relationships between federal departments and agencies and the private sector. A third advantage of this option is that it provides the greatest flexibility to allow relationships to evolve as the protection strategy is developed.

There are three significant weaknesses of the first option. First, the Lead Agency in the White House possesses no significant staff, and therefore it is limited in both the resources and operational focus required to accomplish its mission. Second, the existing working relationships between the law enforcement and national security communities have been very difficult to integrate in the past, and such a leadership agency may not have the authority and resources necessary to improve these relationships significantly. Finally, this agency lacks the resources, institutional clout, and past relationships needed to work effectively with the private sector. It is questionable whether such a small office, even in the White House, could influence strongly the activities of the responsible agencies and departments in their dealings with the private sector.

In sum, Option 1 provides a modest but clearly feasible first step in developing needed federal structures. It creates a structure that can begin working to build some of the most important relationships within the federal government, particularly between the federal law enforcement and national security communities. It also can begin to exert leadership pressure in support of programs for prevention and mitigation. But many of the capability needs outlined in Section II would not be addressed very effectively by this organization.

Option 2: Option 2 includes the same leadership agency within the Executive Office of the President as described for Option 1. Under this option, however, this agency is augmented by a support organization located outside the White House. Its advantage over Option 1 is that it provides for the staff and other resources needed to generate a far more vigorous effort to interact with the private sector in encouraging prevention and mitigation, and it could push the development of a warning system more effectively. The expertise contained within this organization would also substantially strengthen the ability of the Lead Agency to integrate federal capabilities for response and counter-action.

There are two clear shortcomings of Option 2. First, it will be significantly more difficult to implement than Option 1, because it will require substantially more resources and the creation of a new organization. Both actions will be resisted in a time of federal

budget cutting. Second, some may argue that this arrangement represents an over-reaction to currently perceived dangers, and accordingly may fight the creation of the new entity. Third, the authority of the operational entity may also be resisted by those organizations within the government that have traditional — and perhaps competing — infrastructure responsibilities. There is thus a risk that the new entity will reinvent capabilities rather than work within existing structures.

In summary, Option 2 combines the needed leadership role in the federal government with the strengths of a supporting operational arm outside the White House. Potentially, this combination could muster both the leadership authority (from proximity to the President) and institutional clout (from a substantial operational staff) that is necessary to build needed infrastructure protection capabilities. The main difficulties with this option are that it directly challenges the *status quo*, and will therefore be difficult to implement.

Option 3: This option would create a new type of public-private entity that would combine federal leadership and operational responsibilities. There are a number of important advantages to this option. First, it would consolidate many of the needed leadership functions with operational functions, providing a more substantial critical mass for addressing infrastructure issues than would be the case under either Options 1 or 2. Second, this option signals a much greater commitment to addressing the infrastructure protection challenge. It provides a high profile and demonstrates greater private buy in. Third, this entity would combine leadership, a dedicated staff, and a solid institutional identity. Fourth, this institution would have strong authority to shape government programs and policies; it could thus provide the leadership needed to integrate response and counter-action activities. It could also better integrate the activities of the other responsible departments and agencies, and thus build a more coherent program for interacting with the private sector on prevention, mitigation, and warning.

Many of the strengths of Option 3 are also its weaknesses. In general, implementation of this option will be very difficult. Establishing and operating such a new, "bicameral" entity with directive authority over other departments and agencies will generate significant legal issues. Assuming that these disputes can be resolved favorably, the creation of *any* strong new organization is always resisted in the federal government. While some of this resistance stems from turf battles, there also are legitimate concerns about the creation of a powerful, single-purpose institution. Consolidating functions within a single-purpose agency inevitably uproots extant relationships within the government and between the government and private sector. Since such functions benefit

to some degree from their home in their prior department or agency, real losses in capabilities may result from centralization.

A second weakness of this option is its lack of proximity to the President. While the government-private institution would have directive authority, such authority is not always effective in practice. In particular, it may be difficult for such a unique, stand-alone body to effectively influence, much less genuinely integrate, the activities of the law enforcement and national security communities. (The experience of ONDCP provides a relevant case in point.) Finally, the envisioned government-private entity reflects the need to build a partnership between the government and industry, but it also represents an untried organizational structure, which raises numerous practical feasibility questions.

Table 3 summarizes the subjective evaluations above, and attempts to rate them objectively.

Table 3. Assessment of the Options

Management Principles	Option 1: EOP Office	Option 2: EOP Office with Support Arm	Option 3: Government Private Body
1. Leadership for strategy, policies, and operational responsibilities for protecting the infrastructure	+++ strong leadership for government response, and counter-action - lacks resources and operational focus for prevention and warning	+++ strong leadership for government response, and counter-action ++ provides operational focus and resources for prevention and warning activities	+ creates central focus for government response and counter-action, but independent body may lack clout over agencies +++ provides operational focus and resources for prevention and warning activities
2. Build on existing institutional capabilities and working relationships	+++ retains existing relationships between responsible departments and industry - agency may lack resources needed to build relationships, particularly between law enforcement and national security communities - agency may lack resources to coordinate activities of responsible departments	+++ strong leadership with needed resources to coordinate government agencies +++ support institution provides neutral clearinghouse + largely retains existing relationships between responsible departments and industry	- - employs an unproved model for government-private collaboration - - - significant legal problems must be overcome - - regulatory authority for protection may undermine existing relationships between responsible departments and industry
3. Interact effectively with the private sector	+ some leadership from EOP agency - - lacks resources for sustained interaction with private sector	+ some leadership from EOP agency ++ operational focus for sustained interaction; neutral clearinghouse	+++ operational focus for sustained interaction with industry +++ regulatory authority provides considerable clout - institution lacks proximity to President
4. Evolve as the protection strategy matures	+++ allows relationships with industry to evolve as needed +++ requires minimal resources and no new organization	+++ allows relationships with industry to evolve as needed -- requires resources and creation of new organization -- new operational entity may be resisted by existing government agencies	++ government-private institution still provides flexibility for relationships to evolve --- regulatory authority for prevention and warning will be resisted as an over-reaction --- requires significant resources and creation of a new institution -- new operational entity may be resisted by existing government agencies

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

IV. CONCLUDING REMARKS

Several elements of an infrastructure protection strategy have been touched on in this report. An initial discussion of threats and vulnerabilities helps to define the challenge that must be met in protecting the infrastructure. These considerations also help to identify how the challenge will be addressed, and the kinds of capabilities that will be needed. Four capability areas are identified: prevention, warning, response, and counter-action. For each, it has been possible to describe in general terms the roles that are to be played by the private sector, state and local governments, and the federal government. Finally, a number of institutional options for fulfilling the federal government's roles are described, and their strengths and weaknesses are discussed.

The ideas presented here suggest the broad outlines of an infrastructure protection strategy. Substantial additional work is needed to fully develop a complete strategy, the implementation of which will require a significant commitment of political will and resources.

It should not be expected that a comprehensive strategy can, or should, be stipulated at this point. Because of the immense uncertainties in this area, it would be best to adopt a gradual, somewhat experimental approach. It is appropriate to begin working on certain aspects of the problem, with the understanding that additional problems and needed capabilities are yet to be identified. Over time, a complete set of capabilities and institutions can be expected to evolve as the nature of the challenge and of the possible options becomes more clear.

There are logical first steps to be taken by the government in each of the capability areas. In the prevention area — where the major responsibility lies with the designers, builders, owners, and operators of the infrastructure — the government should inform the public of potential dangers, and it can take steps to induce industry to incorporate desired preventive measures. The government also can support — both politically and financially — the research and development intended to enhance prevention technologies. And it can promote measures designed to limit access to technologies that could be used by attackers. These activities all require extensive collaboration between the government and the private sector.

In the warning area, the government can begin to build the kind of reporting and analytical capabilities that could provide warning of cyber attacks, either impending or

actually under way. Developing these capabilities will require a sustained organizational focus, as well as a greater degree of public-private trust than now exists.

In the area of response, the government's extensive organizational capabilities and response assets could be adapted to meet the challenges of purposeful attacks on the infrastructure. This will require strong top-level leadership. In addition, the government can begin to identify and invest in any new capabilities — equipment, training, etc. — that will be needed to respond to such attacks.

With respect to counter-action, the federal government can expand the missions of responsible agencies to address the new dangers, and it can better coordinate their activities. It will be necessary to establish new teaming relationships that employ more effectively the assets of the national security community and the law enforcement communities at the federal, state, and local levels.

APPENDIX A

Infrastructure Attack Scenario

The infrastructure attack scenario described here was constructed specifically to provide three main needs of the current study effort:

- Plausible justification for Federal involvement,
- Identification of useful/relevant capabilities for prevention and mitigation, operational warning, response and counter-action,
- An operational framework to help develop and compare organizational options.

In order to meet these objectives, a number of other conditions are important as criteria for suitability:

- Incidents with unity of purpose that might be motivated by hostile agendas of one or more entities,
- Plausibility that hostile entities could conceivably launch such attacks,
- Overall impact of sufficient severity to warrant government involvement,
- Coverage of most aspects of infrastructure vulnerability that are known and of greatest concern.

In so far as possible, the scenario was developed to exhibit the four characteristics above in order to meet the three main objectives. In constructing the scenario, it became clear that the criterion for sufficient severity to warrant National response could be met with fewer incidents than were eventually devised. The additional events were added to broaden the scope of the overall attack to cover more of the known points of vulnerability.

The scenario places an unpopular U.S. expeditionary force in the Balkans with a number of nations (and possibly other entities) objecting to that presence. As in the RAND 'Day-After' scenario, a key point of the situation is that the opposition is sufficiently diffused, and mixed with domestic factions, that it will not be clear who is doing the damage. The hostile forces have three objectives for their attacks:

- to inflict significant damage on urban areas,
- to discredit the financial system, and
- to disrupt the transportation and gas distribution systems with spectacular media events.

In the attacks, the hostile forces use a combination of cyber attacks of various types, some aided by insiders, and physical attacks. The details of 22 types of incidents in the scenario were developed on a spreadsheet (included below) that lists each incident, its critical aspects to include the observable signatures of the early phases of the attack, and the means infrastructure users and operators would have to determine what was happening to their networks.

The main message from the scenario is that significant damage can be inflicted from widespread attacks, even if the individual incidents are not particularly effective.

The dominant focus was on urban attacks, which took place over a two week period in three waves, affecting seven or eight cities each time. The attacks consisted of cyber interruptions of electric power, followed by physical damage. Fires associated with diminished water pressure, and looting associated with less effective law enforcement, inflicted most of the damage.

In the urban attacks, attacks on the power system were assumed to have no effect in 10 percent of the cases, and to cause nothing more than a temporary power outage in the majority of other cases. (Significant traffic problems can result from power outages.) Seven cities sustained major damage over the two week period, through either fires, looting, or parallel NBC incidents. The overall success rate per incident to inflict such severe damage would need to be no higher than 10 to 15 percent.

Dramatic results also could follow from the financial system attacks. Closing major stock or commodity exchanges while the sources of corrupted data were determined could lead to significant financial losses. Also, widespread attacks on many banks (two per state would cover 100 banks), with publicity introduced by the terrorists themselves, could lead to significant decrease in trust for the banks. Litigation could arise from those victimized by the attacks, as well as by those wishing to cash in on a good opportunity.

The attacks on transportation and distribution could easily lead to great loss of life. In winter, during a period of high demand for natural gas, such attacks could lead to wide-spread collateral damage due to frozen pipes.

The impact on National policy would be to hand those opposing U.S. military intervention an obvious argument: "If the US cannot defend its own cities, why is it sending troops overseas?"

Table A-1. Working Scenario

Location	Target	Symptom	Reporting of Symptom	Forensic Tools	Cause	Incident Reporting	Steps to Mitigate Problem
Incidents Attacking Urban Centers							
Chicago, and cities throughout US	Local Emergency Response System	Multiple cities note increased incidence of repeated calls by computer modems to 911	Reports from 911 offices to local police	Police follow-up to local homes, tech. examination of affected computers. Investigation by local phone company may be a useful tool.	Malicious virus, spread through popular version of an on-line game, causes home computers to dial 911 repeatedly after pre-determined time		Rapid response when a virus has been detected can limit its spread using COTS anti-virus software. Assignment of liability for spread of virus may motivate measures to limit spread (routine CRC checks, etc.)
Tennessee	Regional Electric Power System	Unscheduled/ unanticipated reset of power control system suggests attempt to affect major power grid in Southeast	Reports are generally directed through local utility companies to regional Power Grid Management.	System status log examination	Unauthorized access to SCADA systems; and/or an interaction with malicious software inserted by insiders	Incident Report forwarded to TVA HQ after reports of problems by client cities.	Ensure IA measures are in-place; ensure incidents are reported; develop a means of correlating minor incidents to detect broader IW attack
Target City, First wave	Electric Power Distribution	Power blackout over entire urban area, followed by system shut-down	Calls to local police and subsequent notice of appropriate state and federal law enforcement agencies as necessary.	Built-in system diagnostic tools; review of system activity log	Manipulation of utility through manipulation of SCADA system and/or an interaction with malicious software inserted by insiders		Intel warning can raise alert level, enabling special watch of critical nodes; maintain levels of IA; mandatory reporting; correlation of incidents
Target City, First wave	Water supply systems	Fish kill noted in local reservoir	Local media note fish kill. Emergency warning to consumers	Chemical tests on reservoir system and fish	Deliberate chemical contamination	Report to local and state law enforcement agencies	Intel warning can raise alert level, enabling special watch of critical nodes; isolate reservoir from public water system; flush affected lines; warn public

Table A-1. Working Scenario

Location	Target	Symptom	Reporting of Symptom	Forensic Tools	Cause	Incident Reporting	Steps to Mitigate Problem
Target City, First wave	General Population	Bomb explosion in subway, followed by release of chemical (nerve gas); many people incapacitated	Calls to local police, ER teams, and CDC; local and national news coverage	Medical tests on affected people in hospitals; post-explosion equipment and air testing in subway	Nerve gas attack	Reporting through local police, FBI, and state emergency response systems.	Special training/equipment to aid ER personnel react to CBR incidents; timely dispatch of Intel warnings and alerts; In-place rapid mobilization plans for regional CBR assets
Target City, First wave	Local water utilities and transp systems	Stoppage of all rail and air traffic by power outage; all vehicular traffic control signals out; water pressure drops to 5% of normal levels	Local police, state and federal law enforcement as appropriate; local and national news coverage.	On-site reporting of police, utility investigators, fire personnel	Power failure	Reporting through local police, FBI, and state emergency response systems.	Back-up power for traffic signals, rail signals, water pressure maintenance
Target City, First wave	Electric Power Distribution Nodes	7 of 8 primary urban power distribution nodes physically destroyed by short-circuits	Local police, state and federal law enforcement as appropriate; local and national news coverage.	Physical and chemical examination of damaged hardware and facilities.	Physical installation of short-circuit devices by hostile agents masquerading as power company repair crews during early period of power outage	Reporting through local police, FBI, and state emergency response systems.	Intel warning procedure can raise alert level, enabling special watch of critical nodes; maintain levels of IA; mandatory reporting; correlation of incidents.
Target City, First wave	City Law Enforcement	Response reduction by local law enforcement leads to breakdown of civil order; looting breaks out in urban areas.	Local police, state and federal law enforcement as appropriate; local and national news coverage.	Intel reports on domestic terrorists and extremists	Power outage limits the ability of local police to direct mobile units; reduced manpower resources	Local police, state law enforcement, and FBI, as appropriate	Timely Intel dissemination and warning for local police; back-up power sources for police dispatches; rapid mobilization of National Guard
Target City, First wave	City, Fire	Spreading of fires over five areas of city.	Fire fighters, local, state, federal law enforcement agencies; local, national news coverage.		Fire departments hampered by insufficient water pressure to fight fires effectively	Reporting through local police, FBI, and state emergency response systems.	Back-up power sources for fire alert and dispatches; back-up power sources for maintenance of water pressure

Table A-1. Working Scenario

Location	Target	Symptom	Reporting of Symptom	Forensic Tools	Cause	Incident Reporting	Steps to Mitigate Problem
Target City, First wave	Water supply system	Numerous cases of acute poisoning reported by area hospitals.	Local police, state law enforcement, and federal as appropriate; local and national news coverage.	Chemical evaluation of reservoir system and water supply lines.	Contamination aggravated by shut-down of power and water treatment facilities and generally stagnant condition of municipal water lines	Reporting through local police, FBI, State Health Dept., CPC, and state emergency response systems.	Intel warning procedure can raise alert level, enabling special watch of critical nodes; mandatory reporting; correlation of incidents can enable early detection of chemical and biological contamination.
Target City, First wave	Combined Public Utilities	Local utilities for electric, gas and telephone, housed in one building, blown up	Local police, state law enforcement, FEMA, and FBI as appropriate; local and national news coverage.	Physical and chemical examination of damaged facilities.	Single point of vulnerability for multiple critical utilities	Local police, state and federal law enforcement as appropriate; local and national news coverage. No mechanism to handle incident reporting during crisis conditions.	Encourage diversification of location for critical nodes of critical utilities; Intel warning procedure can raise alert level, enabling special watch of critical nodes; mandatory reporting; correlation of incidents
Philadelphia Newark	Telecom-munications	Unanticipated malfunction and reset of major urban switching system; potentially relevant to detection of broader attack, but locally a minor incident	Report of minor disruptions in service.	Correlation of other events in other locations and industries	Unauthorized electronic or physical access to PSN systems.	Local police, state law enforcement , and FBI as appropriate; local and national news coverage.	Ensure IA measures are in-place; ensure incidents are reported; develop a means to synthesize reports to identify broader IW attack

Table A-1. Working Scenario

Location	Target	Symptom	Reporting of Symptom	Forensic Tools	Cause	Incident Reporting	Steps to Mitigate Problem
Incidents Attacking Financial System							
New York City	Stock Exchanges	Brokers in a stock exchange observe corruption of data from several recent transactions	Irregularity reported to the SEC.	Technical system diagnostic tools	Malicious software triggered in latest release of network operating system. Systematic attacks by financed hackers.	Lack of a mechanism reduces the timely identification of hostile actions	Ensure IA measures are in-place; ensure incidents are reported; develop a means to synthesize reports to identify broader IW attack
Capital Cities, most states	Banks	Account holders notice discrepancies between bank records and local records in bank accounts	No reporting requirement. Account holders may complain to media if banks are not responsive in correcting accounts	Tracing of disputed transactions	Hostile users entering system with false I&A certification	Reporting of fraud/ misappropriation of funds to FBI	Ensure IA measures are in-place; ensure incidents are reported; develop a means to synthesize reports to identify broader IW attack
Chicago	Commodity Exchanges	Brokers for the Commodities Exchange observe corruption of data from recent transactions	Irregularity reported to the Commodity Futures Trading Commission.	Technical system diagnostic tools	Malicious software triggered in latest release of network operating system	Lack of a mechanism reduces the timely identification of hostile actions	Ensure IA measures are in-place; ensure incidents are reported; develop a means to synthesize reports to identify broader IW attack
Nationwide	Banks	In restoring backups of corrupted records, numerous banks discover that the back-up data have been corrupted, as well	No reporting of back-up difficulty	Accounting diagnostics to check data	Subtle errors introduced into back-up data over 2-3 weeks prior to crisis	Press reports anonymous claim that depositor records in hundreds of banks have been destroyed in retalia-tion for 'unjust' pre-sence of US troops in the Balkans	Ensure IA measures are in place; develop strategies other than secrecy and denial to deal with public relations and cyber attacks.

Table A-1. Working Scenario

Location	Target	Symptom	Reporting of Symptom	Forensic Tools	Cause	Incident Reporting	Steps to Mitigate Problem
Incidents Attacking Transportation and Distribution Systems							
Houston	Air Traffic Control System	Unanticipated disruption of air traffic control communications to major airport; 5 min outage for reset, but repeated 3 times during day	Potentially relevant to detection of attack, but locally a minor incident	Correlation of other events in other locations and industries; intrusion detection tools	Cyber attack on FAA comm system	FAA HQ, FBI	Ensure IA measures are in-place; ensure incidents are reported; develop a means to synthesize reports to identify broader IW attack
Mississippi River	Major Bridges	Truck bombs explode on 7 major bridges crossing river, severing communications and pipelines	Local police, state and federal law enforcement as appropriate; local and national news coverage.	Physical and chemical examination of damaged bridges, facilities, and pipelines.		Local police, state law enforcement, and FBI as appropriate,DOT, Corps of Engineers; local and national news coverage.	Warning of potential infrastructure attack to local and state traffic enforcement organizations can enable enhanced security against truck bombs
Colorado		Pilots report incidents to Air Traffic Controllers; Reports of jamming local GPS reference signal.	DOD, DOT (USCG)	None.	Low tech interference with GPS downlink.	DOD, DOT (USCG)	Intel warning procedure can raise alert level, enabling special watch; correlation of incidents

Table A-1. Working Scenario

Location	Target	Symptom	Reporting of Symptom	Forensic Tools	Cause	Incident Reporting	Steps to Mitigate Problem
Other Incidents							
Baltimore	Federal Funds Distribution System	Discontinuity in non-Nat'l Security Govt. Services - Indication of diversion of electronic Medicare payments nationwide	Health providers complain to Dept. of Health and Human Services that payments are delayed without explanation. They complain to media if DHS is not responsive.	Tracing of disputed payments	Malicious software inserted by insiders to redirect payments to selected health care providers	FBI	Ensure IA measures are in-place; ensure incidents are reported; develop a means to synthesize reports to identify broader IW attack
Columbus, OH		Discontinuity in Nat'l Security Govt. Svcs; corruption detected in unclassified DOD data base critical to deployment planning		Local system diagnostic tools	Insider suspected of accessing and damaging data	DOD, FBI, and NSA. Criminal incident report	Reporting, if done, could support assessment of a more general cyber attack.
Texas	Natural Gas Distribution System	Bomb located near major natural gas pumping station	Local police, state law enforcement, and FBI as appropriate; local and national news coverage.	Physical and chemical examination of bomb site, pumping station, and associated facilities		DOE, State Utility, Dept. of Interior	Intel warning procedure can raise alert level, enabling special watch of critical nodes; mandatory reporting; correlation of incidents

APPENDIX B

BASELINE ROLES AND RESPONSIBILITIES

CONTENTS

Baseline Roles and Responsibilities

This appendix presents information describing the current activities of organizations relevant to the protection of critical infrastructures. Section 1 gives a general description of roles and responsibilities for different types of organization; Section 2 introduces and summarizes a data base of specific organizations and their relevant activities; and Section 3 presents selected examples from the data base of different types of protective activities.

1. TYPES OF ORGANIZATION

A. Owners

The responsibility for critical infrastructure protection rests in the first instance on infrastructure owners. For the most part, this means private corporations, e.g., banks, power and telephone companies, pipeline owners, and railroads. In some cases, however, critical infrastructure is owned and operated by government organizations.

- Infrastructures for providing general government services, emergency services, and water supplies are usually government-owned at the federal, state, or local level.
- Governments often own and operate key components of the infrastructure in other sectors, e.g., the Federal Reserve's interbank payments network, the FAA's air traffic control system, and local and national highway systems.

It is the owners who invest in robust systems, install safeguards, and train and supervise operators. It is the owners who recognize the occurrence of breakdowns, accidents, and attacks. And it is the owners who take action to halt the propagation of problems and restore service. For the most part, other entities can affect infrastructure protection only by influencing, aiding, or supplementing owners.

B. Owner Associations and Suppliers

Private (and government) owners of infrastructure have formed a multitude of associations, consortia, and not-for-profit corporations to promote common sectoral interests.

- Trade and professional associations promote general sectoral interests, but focus on infrastructure protection when that becomes an important issue. Associations form task forces, for example, to develop industry positions on pending legislation or regulations. Trade associations may also be instrumental in establishing permanent organizations to deal with protection issues.
- R&D consortia exist in many sectors to sponsor or conduct projects to develop useful technologies. Research projects often address infrastructure improvement, including tasks focused on infrastructure protection. Some R&D organizations evaluate technical standards or test products for standards compliance.
- Standards bodies develop standards, guidelines, and protocols to promote general sectoral interests, e.g., interoperability. Standards may be influenced by security concerns, or may directly address infrastructure protection. Types of standards organizations include trade associations that develop consensus industry standards, professional organizations that certify practitioners, and R&D entities that develop technical standards. Some sectoral standards bodies work closely with government regulators, writing standards that are accepted or promulgated by the regulators.
- Operational consortia are formed to manage support infrastructure needed by the companies in a sector; for example, management of commercial interactions among the companies. In some cases, infrastructure protection is the prime concern.
- Manufacturers of infrastructure components address issues of reliability, security, and compliance with standards in the design and manufacture of their products. Frequently, manufacturers participate actively in sectoral organizations.
- For-profit consultants offer infrastructure protection services; for example, evaluation and testing of existing security systems.

Associations are not themselves responsible for infrastructure protection and generally cannot commit infrastructure owners to particular investments or protective activities. Associations nevertheless represent owners to some degree and can be a useful intermediary for communicating with them. Moreover, work by associations in R&D and standards may contribute directly to infrastructure protection.

C. Governments

federal, state, and local governments play a number of distinct roles in infrastructure protection. They influence the behavior of infrastructure owners through voluntary

programs and mandatory regulation. They also conduct those protection activities that are traditionally considered a governmental responsibility.

- Governments promote voluntary infrastructure protection activities by owners through awareness and training programs, exercises, research and development, cooperative development of standards, and product testing and certification.
- Governments regulate most critical infrastructures, for example, mandating that private owners implement safeguards in the interest of public safety. The nature of regulation varies among industries, depending on the scope of authorizing legislation, the balance of economic and safety interests, and the susceptibility of protection issues to regulation.
- Governments also play a direct role in protecting critical infrastructures through such activities as collecting intelligence, issuing warnings, foiling planned attacks, prosecuting perpetrators, providing emergency services, and coordinating and providing resources for relief efforts.
- Finally, governments play a direct role in protecting critical infrastructures that they themselves own and operate, including internal systems needed for the provision of government services, and external infrastructures such as the FAA's air traffic control system. Indeed, government operation of external infrastructures is sometimes viewed as a method of protecting them.

The role of government also varies among the local, state, and federal levels. To some extent, different levels specialize in different activities, but there are overlaps.

- Local governments provide initial emergency response and consequence management services. They typically have mutual aid agreements with other local jurisdictions and can request state aid when necessary. They also own certain critical infrastructures — for example, transit systems, roads, and water supply systems — and regulate others.
- State governments play a major role in regulating the providers of critical infrastructures, especially providers not subject to federal regulation. State governments support preparedness and training of local responders; state Governors have primary responsibility for consequence management in major disasters.
- The federal government is the primary regulator of critical infrastructure providers, overseeing those engaged in interstate commerce. The federal government has unique responsibilities for intelligence collection and counter-terrorism overseas and for the enforcement of federal laws. The federal government provides training and other support to state and local authorities and cooperates with them in law enforcement, crisis response, and consequence management activities.

Government entities frequently establish joint mechanisms for cooperation and coordination.

- A multitude of inter-agency boards and committees have been established at the federal level to address common problems or make recommendations to the President or other authorities.
- Joint task forces are established between federal and state and local authorities to address specific problems, for example, counter-terrorism.
- State and local authorities develop mutual aid agreements with neighboring jurisdictions, for example, for emergency response.

D. Other Actors

Certain other organizations also influence the protection of critical infrastructures:

- Federal advisory committees are groupings of private-sector executives and experts to advise the federal government on particular issues, including topics related to the protection of critical infrastructures. Such entities may have a time-limited charter to complete a specific study or a continuing charter to study issues and offer advice as requested.
- Academic institutions conduct research related to infrastructure protection, including research sponsored by the federal government. Some also operate federally sponsored centers designed to disseminate protection information.

2. ORGANIZATIONS WITH RELEVANT ACTIVITIES

Many organizations contribute to the protection of critical infrastructures or are positioned to do so in the future. The balance of this appendix discusses current relevant activities of such organizations.

A. Activities Data Base

The study team has assembled a data base containing brief descriptions of current activities related to the protection of critical infrastructures. Each record in the data base includes:

Responsible organization
Description of activity
Type of activity
Infrastructure sector
Legal reference
Data source
Other comments.

The data base identifies over 260 activities or responsibilities, including approximately 200 within or directed by federal agencies. The remainder are primarily the work of national associations. The data base does not include activities of state and local governments, regional associations, or private companies. Because the data base was assembled quickly, there are undoubtedly omissions of noteworthy activities. Experts in particular sectors were interviewed to identify and fill the most glaring gaps. Principal data sources are as follows:

- Agudo, Michael E., *Assessment of Electric Power Control Systems Security*, Joint Program Office for Special Technology Counter Measures, September 30, 1996
- DARPA, *Defense Information Warfare Study*, ISAT-95
- FEMA, *Federal Response Plan*, April 1992
- JCS and NDU, *Information Warfare: Legal, Regulatory, Policy, and Organizational Considerations for Assurance*, Second Edition, July 4, 1996
- Office of Technology Assessment, *Information Security and Privacy in Network Environments*, September 9, 1994
- PCCIP Draft Sector Reports
- Presidential Decision Direction 39, June 21, 1995
- Relevant regulations and legislation
- Worldwide Web Home Pages

It is important to note that the activity descriptions in the data base are based on formal responsibilities and office descriptions. In most cases, no attempt has been made to assess whether an activity is being implemented effectively.

B. Summary Table

Table B-1 provides a summary of the data base activities, listing the organization responsible for each activity in the data base.

- Column headings identify the PCCIP infrastructure sectors to which the activities apply.
- Row headings classify the activities based on the types of infrastructure protection they provide (these row headings are explained further below).
- Organizations shown in the shaded areas are associations; those in the clear areas are federal agencies, interagency groups, federal contractors, or federal advisory committees.

- Organizations are color-coded based on the relevance of their activities. Blue indicates that the activities explicitly address protection against hostile attack; green indicates activities that protect against traditional safety and reliability concerns; black indicates activities of general interest. It is believed that green activities could be re-directed to protect against hostile attack or may incidentally provide such protection already. Black activities could also be re-directed in the future.
- For organizations with multiple activities of the same type, the number of activities is shown in parentheses. Organization names include suffixes to identify sub-offices or major programs. Table B-2 provides definitions for these acronyms.

Table B-2: Acronyms and Abbreviations for Baseline Summary

AAR	Association of American Railroads
AASHTO	American Association of State Highway and Transportation Officials
ABA	American Bankers Association
ACM-SIGOS	Association for Computing Machinery-Special Interest Group on Operating Systems
AGA	American Gas Association
API	American Petroleum Institute
APWA	American Public Works Association
ASIS	American Society for Industrial Security
Assn of Old Crows	Association of Old Crows
ATA	Air Transport Association
ATIS-NRSC	Alliance for Telecommunications Industry Solutions-Network Reliability Steering Committee
AWWA	American Water Works Association
AWWARF	American Water Works Assn Research Foundation
BECCA	Business Espionage Controls and Countermeasures Association
Bellcore	Bell Communications Research
BRT	Bankers' Roundtable
CFCA	Communications Fraud Control Association
CIA	Central Intelligence Agency
CMellon-CERT	Carnegie Mellon-Computer Emergency Response Team
CSI	Computer Security Institute
CVA	Computer Virus Association
DCI-NIC	Director of Central Intelligence-National Intelligence Council
DOC-BEA	Department of Commerce-Bureau of Export Administration
DOC-NTIA	Department of Commerce-National Telecommunications Information Administration
DOD	Department of Defense
DOD-AFIWC	Department of Defense-Air Force Information Warfare Center
DOD-ASD(C3I)	Department of Defense-Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
DOD-COE	Department of Defense-Corps of Engineers
DOD-DARPA	Department of Defense-Defense Advanced Research Projects Agency
DOD-DDNSCC	Department of Defense-Defense Data Network Security Coordination Center
DOD-DIA	Department of Defense-Defense Intelligence Agency
DOD-DISA	Department of Defense-Defense Information Systems Agency
DOD-ERAP	Department of Defense-Emergency Response Assistance Program
DOD-ISSR	Department of Defense-Information System Security Research-Joint Technology Office
DOD-NRL	Department of Defense-Naval Research Laboratory
DOD-SOCOM	Department of Defense-Special Operations Command
DOD-TSWG	Department of Defense-Technical Support Working Group
DOD-USD(P)	Department of Defense-Undersecretary of Defense for Policy
DOE	Department of Energy
DOE-ANL	Department of Energy-Argonne National Laboratory
DOE-CIAC	Department of Energy-Computer Incident Advisory Capability
DOE-CIST	Department of Energy-Center for Information Security Technology
DOE-DP	Department of Energy-Defense Programs
DOE-ESRTF	Department of Energy-Electric System Reliability Task Force
DOE-FERC	Department of Energy-Federal Energy Regulatory Commission
DOE-NN	Department of Energy-Non-Proliferation and National Security
DOE-NPC	Department of Energy-National Petroleum Council
DOE-NTS	Department of Energy-Nevada Test Site
DOI-BOR	Department of Interior-Bureau of Reclamation
DOJ-AG	Department of Justice-Attorney General
DOJ-Antitrust	Department of Justice-Antitrust Division
DOJ-BJA	Department of Justice-Bureau of Justice Assistance

DOJ-Criminal	Department of Justice-Criminal Division
DOJ-INS	Department of Justice-Immigration and Naturalization Service
DOJ-NCB	Department of Justice-National Central Bureau
DOJ-NIJ	Department of Justice-National Institute of Justice
DOJ-OIPR	Office of Intelligence Policy and Review
DOS	Department of State
DOS-BIOA	Department of State-Bureau of International Organization Affairs
DOS-DS	Department of State-Bureau of Diplomatic Security
DOS-DS	Department of State-Diplomatic Security
DOS-FEST	Department of State-Foreign Emergency Support Team
DOS-INR	Department of State-Bureau of Intelligence and Research
DOS-OSAC	Department of State-Overseas Security Advisory Council
DOS-S/CT	Department of State-Office of the Coordinator for Counterterrorism
DOT	Department of Transportation
DOT-FAA	Department of Transportation-Federal Aviation Administration
DOT-FHWA	Department of Transportation-Federal Highway Administration
DOT-FRA	Department of Transportation-Federal Railroad Administration
DOT-OET	Department of Transportation-Office of Emergency Transportation
DOT-OHMS	Department of Transportation-Office of Hazardous Materials Safety
DOT-OPS	Department of Transportation-Office of Pipeline Safety
DOT-TSI	Department of Transportation-Transportation Safety Institute
DOT-Volpe	Department of Transportation-Volpe National Transportation Systems Center
DTC	Depository Trust Company
EEI	Edison Electric Institute
EPA	Environmental Protection Agency
EPA-ERNS	Environmental Protection Agency-Emergency Response Notification System
EPA-STORET	Environmental Protection Agency-Storage and Retrieval Water Quality Data Base
EPRI	Electric Power Research Institute
ERRI	Emergency Response & Research Institute
FASB	Financial Accounting Standards Board
FBI	Federal Bureau of Investigation
FBI-CART	Federal Bureau of Investigation-Computer Analysis and Response Team
FBI-CIRG	Federal Bureau of Investigation-Critical Incident Response Group
FBI-CITAC	Federal Bureau of Investigation-Computer Investigations and Infrastructure Threat Assessment Center
FBI-DECA	Federal Bureau of Investigation-Development of Espionage, Counterintelligence, and Counterterrorism Awareness
FBI-DEST	Federal Bureau of Investigation-Domestic Emergency Support Team
FBI-EU-BDC	Federal Bureau of Investigation-Explosives Unit-Bomb Data Center
FBI-NCCS	Federal Bureau of Investigation-National Computer Crime Squad
FBI-TIS	Federal Bureau of Investigation-Terrorist Information System
FCC	Federal Communications Commission
FCC-EAS	Federal Communications Commission-Emergency Alert System
FDIC	Federal Deposit Insurance Corporation
FEMA	Federal Emergency Management Agency
FEMA-RRIS	Federal Emergency Management Agency-Rapid Response Information System
FEMA-USFA	Federal Emergency Management Agency-US Fire Administration
FFIEC	Federal Financial Institutions Examination Council
FRS	Federal Reserve System
FRS-FEDNET	Federal Reserve System Network
FSTC	Financial Services Technology Consortium
GISB	Gas Industry Standards Board
GRI	Gas Research Institute
GSA	General Services Administration
GSA-ISOO	General Services Administration-Information Security Oversight Office

HHS-CDC	Health and Human Services-Centers for Disease Control and Prevention
HHS-OEP	Health and Human Services-Office of Emergency Preparedness
IACP	International Association of Chiefs of Police
IAFC	International Association of Fire Chiefs
IEEE-PES	Institute of Electrical and Electronic Engineers-Power Engineering Society
IETF	Internet Engineering Task Force
IITF-RVWG	Internet Engineering Task Force-Reliability and Vulnerability Working Group
IITF-SIF	Internet Engineering Task Force-Security Issues Forum
IMPWG	Information Management Policy Working Group
INGAA	Interstate Natural Gas Association of America
ISACA	Information Systems Audit and Control Association
ISC2	International Information Systems Security Certification Consortium
ISPAC	Information Security Policy Advisory Council
ISSA	Information Systems Security Association
MIT-WWW	Massachusetts Institute of Technology-World Wide Web Consortium
NACHA	National Automated Clearing House Association
NASA	National Aeronautics and Space Administration
NASDV	National Association of Security and Data Vaults
NCCCD	National Center for Computer Crime Data
NCS	National Communications System
NCS-GETS	National Communications System-Government Emergency Telecommunications Service
NCS-TSP	National Communications System-Telecommunications Service Priority
NEMA	National Emergency Management Association
NERC	North American Electric Reliability Council
NERC-SCC	North American Electric Reliability Council-Security Coordinator Subcommittee
NERC-SPSSTF	North American Electric Reliability Council-Security Process Support System Task Force
NFPA	National Fire Protection Association
NGA	National Governors' Association
NIST	National Institute of Standards and Technology
NIST-CSSPAB	National Institute of Standards and Technology-Computer System Security and Privacy Advisory Board
NIST-FACSPMF	National Institute of Standards and Technology-Federal Agency Computer Security Program Managers' Forum
NIST-FIRST	National Institute of Standards and Technology-Forum of Incident Response and Security Teams
NIST-TTAP	National Institute of Standards and Technology-Trusted Technology Assessment Program
NRC	Nuclear Regulatory Commission
NRC-CSTB	National Research Council-Computer Science and Telecommunications Board
NRC-IRD	Nuclear Regulatory Commission-Incident Response Division
NRC-NMSS	Nuclear Regulatory Commission-Nuclear Material Safety and Safeguards
NRC-WSTB	National Research Council-Water Science and Technology Board
NRIC	Network Reliability and Interoperability Council
NRT	National Response Team
NSA	National Security Agency
NSA-IOSS	National Security Agency-Interagency OPSEC Support Staff
NSA-MISSI	National Security Agency-Multilevel Information Systems Security Initiative
NSA-NCSC	National Security Agency-National Computer Security Center
NSA-SNAC	National Security Agency-Systems and Networks Attack Center
NSC	National Security Council
NSTAC	National Security Telecommunications Advisory Committee
NSTAC-NSIE	National Security Telecommunications Advisory Committee-Network Security Information Exchange
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NTSB	National Transportation Safety Board
NYSE	New York Stock Exchange
OMB	Office of Management and Budget

OMB-ISSO	Office of Management and Budget-Information Security Oversight Office
OMB-OIRA	Office of Management and Budget-Office of Information and Regulatory Affairs
OSTP	Office of Science and Technology Policy
Purdue-COAST	Purdue University-Computer Operations, Audit, and Security Technology
PWGFM	President's Working Group on Financial Markets
SEC	Securities and Exchange Commission
SEC-DE	Securities and Exchange Commission-Division of Enforcement
SPB	Security Policy Board
SRI-IIII	SRI International-Information Integrity Institute
State Govt	State Governments
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TIA	Telecommunications Industry Association
Treas	Treasury Department
Treas-OCC	Treasury Department-Office of the Comptroller of the Currency
Treas-FinCEN	Treasury Department-Financial Crimes Enforcement Network
Treas-IRS	Treasury Department-Internal Revenue Service
UC Davis-CSRL	University of California at Davis-Computer Security Research Laboratory
USCG	U.S. Coast Guard
USCG-FOSC	U.S. Coast Guard-Federal On-Scene Coordinators
USCG-NRC	U.S. Coast Guard-National Response Center
USCM	U.S. Conference of Mayors
USGS	U.S. Geological Survey
USPS	U.S. Postal Service
WRC	Water Resources Council
XIWT	Cross-Industry Working Team

C. Analysis of Table: Dispersion of Federal Activity

Federal efforts at infrastructure protection are widely dispersed. We have identified 164 relevant activities at 24 federal agencies, involving at least 70 separate offices or sub-agencies. The obvious need for coordination has given rise to at least 19 interagency groups carrying out 21 relevant activities. We also have identified activities at five federal contractors, and 12 federal advisory committees.

The dispersion of federal activities reflects the specialized responsibilities assigned to federal agencies. For example, on average each of the 24 federal agencies engages in seven relevant activities concentrated in only two separate infrastructure sectors. Moreover, most individual offices within federal agencies deal with only one sector.

Each individual sector is overseen by an average of five federal agencies conducting 18 relevant activities. The division of responsibilities among these agencies often reflects the heterogeneity of the sector. For example, the banking and finance sector includes different classes of banks as well as non-bank financial institutions and securities markets.

These distinctions have led to multiple federal regulators for banking and finance. Similarly, the transportation sector includes movement by air, water, rail, and truck, and the Department of Transportation oversees separate offices for each of these modes. On the other hand, for the continuity of government sector, the assignment of responsibilities among OMB, NSA, NIST, and GSA represents a functional division of labor to oversee the relatively homogeneous federal infrastructure.

3. EXAMPLES OF ACTIVITIES BY TYPE OF CAPABILITY

This section provides additional comments on Table B-1, including examples of specific activities represented on Table B-1. The discussion is organized in accordance with the categories of protective activity shown as row headings on Table B-1. The acronyms used in this section are defined above on Table B-2.

A. Prevention and Mitigation

1) Awareness

There are a number of organizations attempting to assess infrastructure vulnerabilities, disseminate information, and promote improved security. Activities that address hostile attacks dwell primarily on cyber attacks and are concentrated in the continuity of government and telecommunications networks/computers sectors. Most other sectors are concerned with such traditional issues as protection against fraud, reliability in the face of natural disasters, and technical breakdowns. Examples of current activities include:

- NIST manages FedCIRC, which supports the federal civilian community by analyzing computer incidents, issuing alerts, evaluating agency security programs, providing training, and hosting conferences.
- DOE has established a task force (ESRTF) to examine the reliability of the national electric power grid.
- NERC sponsors a threat assessment group that interfaces with DOE on possible terrorist threats against electric power facilities.
- The FBI-DECA program includes a communications network to inform industry of industrial spying and (soon) computer crime threats.
- The NSA-SNAC program seeks to identify systems and network vulnerabilities and network attack technologies.

- NRIC addresses telecommunications reliability and interoperability and will advise on FCC participation in network planning.
- NSTAC-NSIE (with industry representatives) works closely with its government counterpart to exchange information on threats, incidents, and vulnerabilities affecting public network software.
- The HHS-CDC and EPA maintain a surveillance system to collect, analyze, and report data on waterborne-disease outbreaks.

2) Research and Development

Sector-specific R&D centers have been established by industry associations and, in several cases, by the federal government as well. The federal agencies also sponsor R&D by academic and other contractors. R&D to protect infrastructure against hostile attack is most prominent in the continuity of government and telecommunications computers sectors, focusing on cyber attacks. R&D in the emergency services sector addresses primarily physical terrorism. In the remaining sectors, most R&D seems to be focused on infrastructure development and traditional safety issues. Examples of current activities include:

- FSTC sponsors R&D on financial services, e.g., Internet access to existing bank payment systems. Security and interoperability are prime concerns.
- DoD-ISSR coordinates the information systems security research programs of DARPA and NSA.
- DoD-TSWG develops counter-terrorist technologies, focusing on explosives detection and detection and protection against CBR threats.
- DOJ-NIJ develops technologies to combat terrorism, including technologies to assist state and local law enforcement authorities.
- DOE-CIST utilizes Oak Ridge National Laboratory for R&D, demonstration, and application testing and evaluation of information security technologies.
- DOC-NTIA provides grants to promote development and availability of advanced telecommunications technologies.
- DOT-Vole conducts technical research on all modes of transportation, with one business area focusing on safety and security.
- AWWARF sponsors drinking water R&D, addressing treatment, monitoring, and health effects as well as reliability assessments and Scads.

3) Norms (Standards)

NIST and NSA dominate federal efforts to develop security standards for telecommunications and information systems, with NIST focusing on the protection of sensitive unclassified information and NSA addressing encryption technologies and the protection of classified information. NIST and NSA standards are intended primarily for federal agencies and contractors, but the private sector sometimes finds them useful as well. In addition, there are sector-specific associations developing standards to address traditional safety and reliability issues for particular sectors. Examples of current activities include:

- NIST develops Federal Information Processing Standards (FIPS) and validates product compliance. Its TTAP program proposes to allow certain security products to be evaluated by third parties certified by the government.
- NSA-NCSC assigns trust levels to computer systems, software, and components and publishes the Information Systems Security Products and Services Catalog.
- Professional certification programs include SCI's Certified Information System Security Professional and ISACA's Certified Information Systems Auditor.
- NERC ensures the reliability of interconnected electric systems by developing and monitoring compliance with policies, criteria, and standards.
- API develops standards for design, construction, and O&M of refineries and pipelines, addressing fire prevention and control, operational safety, and oil spill response.
- ISSA is developing generally accepted, system security principles in an international effort.
- AASHTO develops standards and specifications for highway design and construction, many of which are incorporated in FHWA regulations.
- FASB establishes accounting and reporting standards that are accepted by the SEC for its regulatory purposes.

4) Norms (Regulations)

The sectors providing critical infrastructure have attracted federal regulation for many years. Regulators focus primarily on traditional concerns, for example, reliability and public safety. In a few sectors, regulators also have addressed the possibility of hostile attack; this is most evident in the regulation of security at federal agencies. The SPB, under NSC direction, develops federal security policy. NSA serves as the executive agent for

federal operational security programs. OMB develops and implements policies for information resource management, setting minimum program requirements for the security of federal automated information systems. GSA oversees implementation of the uniform system for classifying, declassifying, and safeguarding national security information. Other examples of current activities include:

- FFIEC prescribes uniform federal principles and standards for bank examiners, addressing physical and cyber security and contingency planning.
- OMB establishes guidelines for federal agencies to conduct annual evaluations of their internal accounting and administrative controls. Some have recommended extending this type of oversight to computer security as well.
- The NRC oversees the safety and security of civilian use of nuclear materials, including activities to deter and protect against threats of radiological sabotage, theft, or diversion.
- NRT's Integrated Contingency Plan enables facilities handling oil and hazardous substances to meet the emergency planning requirements of nine overlapping federal regulations issued by DOT, EPA, OSHA, and DOI.
- DOE-FERC regulates the interstate transmission of natural gas, including pipeline construction and operation. At the same time, DOT-OPS regulates safety for the transportation of natural gas by pipeline, including design, construction, O&M, and emergency response.
- DOT-FRA enforces federal railroad safety laws, conducting safety inspections and issuing emergency orders.
- EPA sets standards and guidelines for U.S. drinking water. Public water systems and state standards must comply.

5) Norms (Self Protection)

Government ownership of critical infrastructures is sometimes viewed as a means of enhancing safety and reliability. For example, government owners might place greater emphasis on public safety and less emphasis on profitability or proprietary advantage. It is not clear how widely applicable such arguments are in a country with a strong preference for private ownership, but the government does own and operate certain critical infrastructures. One example is the air traffic control system operated by the FAA; another is the interbank payments system operated by the FRS. Incidentally, there also are private clearinghouse associations that operate payments systems in conjunction with the FRS system.

B. Indications and Warning

A number of organizations collect, evaluate, and disseminate information that could indicate that an infrastructure attack is imminent, or in progress. Some organizations provide specific warnings and alerts (as opposed to the general threat awareness activities discussed above). Others monitor infrastructure operations to detect anomalies that could indicate an attack is in progress. Still others collect anomaly reports from those who monitor operations. The identification of anomalies could trigger crisis response activities and, in theory, could be used to alert other infrastructure owners who might be at risk. As the examples below suggest, many indications and warning mechanisms are in place, although, for several sectors, they focus on identifying traditional operational problems rather than on hostile attacks.

Several organizations aspire to provide specific warnings and alerts:

- The Central Intelligence Agency issues terrorist threat warnings to civilian agencies, e.g., the FAA, that in turn notify private industry.
- DOS-OSAC provides unclassified security information and terrorist warnings to U.S. firms overseas, using corporate and government sources.
- FinCEN is an intelligence and analytical network supporting law enforcement agencies combating financial crimes.
- FCC-EAS enables the President and state and local officials to distribute emergency messages via broadcast stations and digital devices, e.g., pagers.

Other organizations monitor critical infrastructures to detect anomalies:

- NYSE maintains continuous electronic surveillance of its market for noncompliance with its rules and unusual price and volume activity.
- AFIWC is a focal point for intelligence data and operates sophisticated tools to detect, document, and evaluate apparent attacks on Air Force systems.
- DOE-CIAC (at the Lawrence Livermore National Laboratory) disseminates fast-breaking threat and vulnerability information throughout DOE and to its contractors.
- DOE-DP operates aerial measuring systems and a monitoring and assessment center to detect and assess nuclear accidents and other radiological releases.
- EPA requires large public water systems to monitor for microbial contaminants and disinfection byproducts, using EPA-approved labs.

- DOI-USGS monitors streamflow data at 7,292 sites in near real-time, and monitors water quality in 679 watersheds at least once per month.

Still other organizations collect reports of anomalies detected by others:

- Electric utilities are required to report expeditiously to DOE events affecting adequacy or reliability such as loss of system load, voltage reductions, and acts of sabotage or terrorism.
- Telecommunications' common carriers must report to the FCC service outages that affect 30,000 or more potential users for 30 minutes. Outages affecting major airports or the emergency 911 service must be reported first to the NCS. Outages affecting nuclear power plants or major government or military facilities must be reported first to DISA.
- Hazardous materials transporters must report immediately by telephone to DOT-OHMS all major incidents, substantial marine releases, and instances of radioactive contamination. Infectious substance incidents may be reported instead to CDC.
- USCG-NRC receives reports on all oil, chemical, radiological, biological, and etiological discharges to the U.S. environment.

C. Response

1) Crisis Response Preparation

Infrastructure owners must plan and prepare for emergencies, in their own interest and often to satisfy federal, state, and local regulators. At the federal level, preparation for crisis response and consequence management naturally occurs primarily in the emergency services sector, although there are also a number of sector-specific activities. FEMA plays a major role in emergency preparedness, in coordination with individual agencies. In most cases, preparations focus on response to natural disasters and traditional infrastructure breakdowns, but some recent activities also address response to CBR attacks. As suggested by the following examples, preparation activities include developing response capabilities as well as training and exercising responders:

- NCS coordinates planning for national security and emergency preparedness telecommunications for the federal government.
- EPRI is developing disaster mitigation and recovery technologies to foster the early recovery of large or critical electric utility customers.
- DoD conducts exercises to improve federal, state, and local responses to emergencies involving biological or chemical weapons or materials. DOE

conducts similar exercises addressing nuclear and radiological weapons or materials.

- DOE-NTS operates a spill center for hazardous materials, used by government agencies and private companies to exercise emergency response capabilities.
- DOE-OHMS funds preparedness and responder training programs to upgrade local response capabilities for hazardous materials emergencies.
- AAR operates an emergency response training center addressing train and truck derailments and rollovers involving hazardous materials.
- FEMA-USFA's National Fire Academy trains local fire departments in fire prevention and control as well as emergency medical services.
- DOE-ANL calculates protective distances for responders to transportation accidents involving hazardous chemicals or radiological materials and supports related training and preparedness exercises.

2) Crisis Response

Crisis responders must protect public safety, mitigate infrastructure damage, and quickly restore service. In the first instance, these responsibilities fall to the infrastructure owners and to local public safety officials. However, there are a number of federal activities designed to support local responders, remotely or on the scene. Agencies maintain operations centers to coordinate response and often provide deployable response teams. Especially in the case of the emergency services sector, many of these activities explicitly address hostile attacks, including those involving CBR materials. Some significant response capabilities have also been developed by sector associations. Examples of current activities include:

- NERC's regional security coordinators assess security, provide near real-time operating information to control areas, and coordinate emergency operations.
- NRC-IRD's operations center receives event reports and manages the incident response interface with FEMA and with NRC regional offices.
- DoD-ERAP advises (including by hot line) federal, state, and local agencies on emergency responses to use or threatened use of WMD or related materials.
- DoD's domestic terrorism rapid response team aids federal, state, and local officials in the detection, neutralization, containment, dismantlement, and disposal of chemical or biological weapons or materials.

- DOE-DP maintains teams to respond to nuclear accidents and terrorism worldwide, providing technical and first responder assistance and medical and health physics support.
- HHS-CDC will move multidiscipline emergency response teams to CBR disaster locations within hours to assess the situation, identify contaminants, and advise on public health concerns.
- HHS-OEP grants support Metropolitan Emergency Medical Response Teams that provide medical services in response to use or threatened use of WMD.
- CMellon-CERT supports response to computer security events involving Internet hosts, providing 24-hour technical assistance.
- NIST-FedCIRC supports response to computer security incidents at federal civilian agencies, providing hotline technical assistance and backup support to agency response teams.
- USCG-NRC relays environmental discharge information to EPA, provides emergency telecommunications, and operates automated chemical identification and dispersion information systems.
- FEMA-RRIS provides a data base on chemical and biological agents, munitions characteristics, and safety precautions as well as an inventory of federal assets that could aid state and local officials manage and mitigate WMD disasters.
- AAR offers a data base of response information for transportation accidents involving hazardous materials, covering 3900 transported chemicals.
- PWGFM provides interagency coordination during a crisis affecting financial markets.
- FRS acts to forestall financial crises or to manage crises once they occur, e.g., by providing liquidity to financial markets.

3) Consequence Management

Consequence management includes the provision of disaster relief to affected communities and assistance in recovery and rebuilding, as well as containing the damage caused by the original incident. Primary responsibility lies with local governments and infrastructure owners; however, federal agencies provide supplemental assistance, both technical and financial. FEMA coordinates planning for and execution of the federal effort in accordance with the Federal Response Plan, which identifies the primary agency responsible for federal emergency assistance in each of 12 functional areas. Examples of current activities include:

- FEMA is directed to ensure that the Federal Response Plan and state response plans are adequate for terrorism directed against large populations.
- NCS-TSP authorizes priority provisioning and restoration of service on public switched networks for high priority users.
- DOJ-AG coordinates emergency federal law enforcement or military assistance to civil authorities, including response to civil disturbances.
- DOT-OET operates a crisis center to deploy transportation resources to assist federal and state response and track the flow of relief supplies and personnel.

D. Law Enforcement and Counter-Terrorism

State and local officials play a key role in law enforcement and against terrorist crimes. The federal government also has a major role because certain terrorist acts are federal crimes and because many terrorist activities have a foreign connection. There are many federal activities directed against terrorism, but only a few specifically address cyber threats.

The assignment of counter-terrorism responsibilities is divided among several federal agencies:

- DOS is the lead agency for terrorist incidents outside the U.S. (except U.S.-flag vessels in international waters, or control of military force, if directed).
- The FBI investigates terrorist threats and crimes against U.S. citizens and interests abroad where Congress applies extraterritorial jurisdiction.
- The FBI has the principal authority to conduct and coordinate counter-intelligence and counter-terrorism investigations and operations in the U.S.
- For air piracy, the FAA has exclusive responsibility for coordinating law enforcement activity affecting the safety of persons aboard aircraft.
- USCG is responsible for maritime enforcement of U.S. laws and has authority to prevent or respond to terrorism within or adjacent to the marine environment.
- DOJ-INS enforces entry prohibitions on aliens who have incited serious terrorist activity or who are associated with foreign terrorist organizations.

Federal agencies engage in a number of counter-terrorism activities:

- The CIA collects foreign intelligence, supports counter-terrorist actions, and operates a multidisciplinary center for counter-terrorism.
- DOS-DS offers up to $2M for information preventing acts of international terrorism against U.S. persons or property or leading to the arrest or conviction of such terrorists.

- DOS-S/CT leads an interagency emergency response team that deploys promptly anywhere in the world in response to international terrorist incidents.
- DoD-SOCOM includes counter-terrorism primarily among its missions.
- DOS-INR operates a computerized system to link visa sections at U.S. missions abroad with a master data base of terrorists, criminals, and drug traffickers.
- FBI-TIS is an on-line data base of suspected terrorist groups and individuals.
- FBI-CITAC manages computer infrastructure threat assessments and assists the FBI investigations involving computers.
- The FBI and the Secret Service have a coordination group with several banking associations to combat financial fraud and computer crimes.

Federal efforts to assist state and local authorities include:

- The FBI funds joint terrorism task forces with state and local law enforcement agencies in a number of major cities.
- The FBI supports local law enforcement agencies through laboratory facilities, training, and operational assistance.
- FBI-CIRG addresses hostage-taking, barricade situations, and terrorist activities, with SWAT teams located around the country.
- DOJ-BJA grants to state and local agencies support planning, training, and technical assistance for the investigation and prevention of terrorism.

Table B-1: Baseline Organization Summary: Organizations with Relevant Activities

6May97	Banking/ Finance	Continuity Govt Svcs	Electrical Power	Emerg Services	Gas & Oil Transport	Telecommunications Networks	Telecommunications Computers	Transport	Water Supply
1. PREVENTION and MITIGATION									
Awareness	Treas-OCC BRT SEC-DE	**GSA** **IMPWG** **NIST-FACSPMF** **NIST-FedCIRC** **NSA**		**DOD-USDP**	DOT-OPS	**IITF-RVWG** **IITF-SIF**	**FBI-DECA** **MITRE** **NSA-SNAC** DOJ-Antitrust	**NTSB** DOT-TSI DOT-Volpe	EPA-STORET HHS-CDC DOI-BOR WRC
	ABA	**NIST-CSSPAB** **NSTAC**	**NERC** DOE-ESRTF NERC(2) EEI	**ERRI** BECCA IACP	DOE-NPC GRI INGAA	**NSTAC-NSIE** ATIS-NRSC NRIC TIA	**ACM-SIGOS** **ASIS** **SRI-IIII** NASDV		AWWA APWA
R&D		**DOD-ISSR** **NSA(2)**		**DOD** **DOD-TSWG** **DOJ-NIJ**		DOD-NRL DOC-NTIA	**DOD-DARPA** **DOE-CIST** **NSA-MISSI**	DOT-Volpe	**DOD-COE** DOD-COE
	FSTC		EPRI		GRI	**AOC**	**Purdue-COAST** **UC Davis-CSRL** IETF NRC-CSTB	AAR	AWWARF NRC-WSTB
Norms (Standards)		**NIST** **NSTISSC** GSA				**NIST** **NSA** NIST DOC-NTIA DOS-BIOA	**NIST-TTAP** **NSA-NCSC(2)** **NSC** **Treas**	**USCG** NTSB	
	NACHA FASB	**ISPAC**	IEEE-PES NERC	NFPA	API API GISB	Bellcore	**CSI** **ISC2** **ISSA** ISACA MIT-WWW XIWT	AASHTO ATA	
Norms (Regulations)	**FFIEC** SEC FRS(3) Treas-OCC(2)	**GSA-ISOO** **NSA-IOSS** **OMB-ISSO** **SPB** OMB(3)	**NRC-NMSS** DOE-FERC NRC		DOE-FERC(2) DOT-OPS NRT	FCC(2)		**DOT-FAA** DOT-FRA DOT-OHMS DOT-FHWA	EPA(2) DOD-COE(2)
				State Govt					
Norms (Self Protection)	FRS-FEDNET	**DOD-ASD(C3I)** **DOD-DISA(2)** **GSA** NASA USPS						**DOT-FAA**	
2. INDICATIONS and WARNING									
Reporting Fusion Dissemination	Treas-FinCEN	**DOD-AFIWC** **DOE-CIAC** Treas-IRS	**DOE**	**CIA** **DOE-DP** FCC-EAS		DOD-DISA FCC NCS	**CIA** **DCI-NIC** **DOD-DIA** **FBI-CITAC**	DOT-FAA DOT-OHMS USCG-NRC	DOI-BOR DOI-USGS EPA EPA-ERNS
	NYSE	**DOS-OSAC**	NERC-SPSSTF						

Notes: --Non-Federal activities are listed in shaded areas.
--Activities are graded based on their focus: **Security against Hostile Attack**, Ordinary Safety and Reliability, General Sector Issues.
--(#) indicates number of activities recorded for same organization and grade.

(Table B-1 Continued)

	Banking/ Finance	Continuity Govt Svcs	Electrical Power	Emerg Services	Gas & Oil Transport	Telecommunications Networks	Telecommunications Computers	Transport	Water Supply
3. Response									
Response Preparation		**NCS** **NIST**		**DOD** **DOE** DOC-NTIA DOE-NTS DOT-OHMS FEMA-USFA				DOE-ANL DOT-FRA	DOI-BOR
			EPRI NERC-SCC	**NGA** APWA IAFC NEMA USCM	AGA			AAR	
Crisis Response	FRS PWGFM	**DOD-AFIWC** **DOD-DDNSCC** **DOE-CIAC** **NIST-Fed-CIRC**	**NRC-IRD** DOE	**DOD** **DOD-ERAP** **DOD-USDP** **DOE-DP** **DOE-NN** **FBI-EU-BDC** **FEMA-RRIS** **HHS-CDC** **HHS-OEP(2)** DOD DOT-OHMS	USCG-NRC		**CMellon-CERT**	USCG-FOSC	
			NERC				**CVA** **NIST-FIRST`**	AAR	
Consequence Management	FDIC	**FEMA** FEMA NCS-GETS NCS-TSP DOC-NTIA	DOE	**DOJ-AG** **DOS** **FEMA** FEMA(2) FBI	EPA	NCS OSTP		DOT-OET	DOD-COE
4. LAW ENFORCEMENT and COUNTER-TERRORISM									
Law Enforcement **Counter-Terrorism**	FBI SEC-DE	**DOS-DS**		**CIA** **DOD(2)** **DOD-SOCOM** **DOJ-BJA** **DOJ-INS** **DOJ-OIPR** **DOS(4)** **DOS-INR** **FBI(6)** DOD DOJ-AJ DOJ-NCB		**DOC-BEA**	**FBI-CITAC** **FBI-NCCS** DOJ-Criminal FBI FBI-CART	**DOT-FAA** **FBI** **USCG**	
						CFCA	NCCCD		

Notes: --Non-Federal activities are listed in shaded areas.
--Activities are graded based on their focus: **Security against Hostile Attack**, Ordinary Safety and Reliability, General Sector Issues.
--(#) indicates number of activities recorded for same organization and grade.

APPENDIX C

ADDITIONAL ISSUES

CONTENTS

Additional Issues

In the course of researching this issue paper, the IDA study group developed observations and opinions concerning a number of issues that, while not directly related to the PCCIP study task, are clearly relevant to the broader topic of infrastructure protection. The three most important concerns that arose in this context pertain to (1) the need for a high-level public statement defining major aspects of U.S. policy for infrastructure protection; (2) the plausibility of concerted infrastructure attacks generated by rogue states; and (3) the requirement for some sort of "follow-on" entity to coordinate federal infrastructure protection efforts while new organizational structures are emplaced. A brief elaboration on these subjects follows.

1. POLICY STATEMENT

A good model here is the U.S. declamatory policy that has evolved with respect to counter-terrorism. Such a statement need not be lengthy, but it must be comprehensive and clear. It would define, at a minimum:

- the very serious concern that the United States accords to threats against its infrastructure;
- the absolute U.S. commitment to defending its citizens and economy against such threats;
- the range of actions and counter-measures that the U.S. government would be *prepared* to employ in response to infrastructure attacks (linkage between types/sources of attack and specific responses should be left purposefully vague);
- the broad aspects of U.S. internal strategy and organization for infrastructure protection; and
- the approach that the United States proposes for international collaborative efforts to protect infrastructures and, in particular, to interdict global infrastructure threats.

2. ROGUE STATE THREATS

In several interviews and discussions, and during the April 30th panel session at IDA, questions arose as to the validity of threats by *nation-states* against the infrastructure. The range of disagreement on this issue is quite wide. One view, citing evidence that countries such as China are becoming very interested in all aspects of information warfare, argued that nation-state threats are quite plausible and must be taken

very seriously. The contrary view is that — given U.S. conventional and nuclear capabilities to effectively control escalation at all levels — direct attacks on the United States are simply not a viable option for future nation-state adversaries.

As a practical matter, it is unnecessary to reach a firm conclusion as to the efficacy of a direct infrastructure attack on the United States. Such a judgment is inherently difficult to make, given the range of contexts and conflict circumstances that must be considered. For planning purposes, it is instead more useful to assume that direct attacks on U.S. infrastructures *could easily become* a reasonable option for a "rogue" state enemy (with all that this implies for the scope and sophistication of physical/cyber threats) in any situation where the relative vulnerability of the United States is perceived as disproportionately greater. For example, a rogue state leader might calculate that his ability to continue inflicting highly disruptive, service-denial attacks on a U.S. infrastructure sector would be a sufficient threat to force the United States to compromise its political objectives rather than resort to military retaliation.

It is also possible that a rogue state could conduct broad cyber attacks on U.S. infrastructure anonymously, with the objective of sowing confusion during a crisis situation. A third possibility is that such attacks could be carried out in a way that makes another country appear responsible. In this event, the United States could find itself embroiled in a needless confrontation, or perhaps even be provoked to retaliate against an adversary of the rogue state actually conducting the cyber attack. Should the true attacker be identified, however, both of these cases become similar to the first in that retaliatory measures would need to be weighed against the harm that could be inflicted through continued infrastructure attacks.

An important subject for further exploration — by the PCCIP or another group — is the changing calculus of escalation in the cyber age. Useful insights might be derived here from the community that thought about all aspects of nuclear strategy during the Cold War, and more recently has turned its attention to WMD more generally.

3. FOLLOW-ON ORGANIZATION

At present, the President's Commission (along with its Infrastructure Protection Task Force counterpart) is the *only* U.S. organization charged broadly with critical infrastructure protection. Following submission of its strategy recommendations to the President, there will be a hiatus of indeterminate length while these recommendations are considered, decisions are made, and perhaps new institutions are established with responsibilities of comparable scope. During this interval, it is important that some organizational entity continue as a focal point for infrastructure protection matters. The organization could be the PCCIP itself (or a portion thereof), or it could be a new interim body created for this purpose. In addition to serving as an information source supporting high-level government infrastructure protection deliberations, such a body could initiate further research, expand upon the PCCIP's on-going industry outreach efforts, and perform many other useful tasks.

An explicit proposal, or options, for a follow-on organization, with associated functions and responsibilities, could be included with PCCIP's strategy recommendations.