Order Code RL30153

Report for Congress

Received through the CRS Web

Critical Infrastructures: Background, Policy, and Implementation

Updated July 18, 2002

John D. Moteff
Specialist in Science and Technology Policy
Resources, Science, and Industry Division

Congressional Research Service ❖ The Library of Congress

Critical Infrastructures:
Background, Policy and Implementation

Summary

The nation's health, wealth, and security rely on the production and distribution of certain goods and services. The array of physical assets, processes and organizations across which these goods and services move are called critical infrastructures (e.g. electricity, the power plants that generate it, and the electric grid upon which it is distributed). Computers and communications, themselves critical infrastructures, are increasingly tying these infrastructures together. There has been growing concern that this reliance on computers and computer networks raises the vulnerability of the nation's critical infrastructures to "cyber" attacks.

In May 1998, President Clinton released Presidential Decision Directive No. 63. The Directive set up groups within the federal government to develop and implement plans that would protect government-operated infrastructures and called for a dialogue between government and the private sector to develop a National Infrastructure Assurance Plan that would protect all of the nation's critical infrastructures by the year 2003. While the Directive called for both physical and cyber protection from both man-made and natural events, implementation focused on cyber protection against man-made cyber events (i.e. computer hackers). Those advocating the need for greater cyber security felt that this was a new vulnerability not fully appreciated by system owners and operators in either the private or public sectors. However, given the impact of the September 11 attacks on the communications, finance, and transportation infrastructures, physical protections of critical infrastructures is receiving greater attention.

PDD-63 was a Clinton Administration policy document. Following the events of September 11, the Bush Administration released two relevant Executive Orders (EOs). EO 13228, signed October 8, 2001 established the Office of Homeland Security. Among its duties, the Office shall "coordinate efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks." EO 13231 (Critical Infrastructure Protection in the Information Age), signed October 16, stated the Bush Administration's policy and objectives for protecting the nation's information infrastructure. These are similar to those stated in PDD-63 and assumes continuation of many PDD-63 activities. E.O. 13231, however, focuses entirely on information systems. E.O. 13231 also established the President's Critical Infrastructure Protection Board. The mission of the Board is to "recommend and coordinate programs for protecting information systems for critical infrastructures." On June 6, 2002, President Bush, along the lines of congressional efforts to do the same, proposed the establishment of a new Department of Homeland Security. The Department would assume and integrate offices and agencies from other departments responsible for implementing various aspects of homeland security. The President's proposal identified four primary areas of responsibility that he suggested should constitute major divisions within the new Department. One of these would be Information Analysis and Infrastructure Protection. The Boards, Councils, and advisors established in the above mentioned E.O.s remain in effect.

Contents

Latest Developments 1
Introduction 1
The President's Commission on Critical Infrastructure Protection 3
Presidential Decision Directive No. 63 4
Implementation of PDD-63 8
Selection of Sector Liaison Officials and Functional Coordinators . . . 8
Identifying and Selecting Sector Coordinators 9
Appointment of the National Infrastructure Assurance Council 10
Selection of Agency CIAOs 10
Internal Agency Plans 10
National Critical Infrastructure Plan 12
Information Sharing and Analysis Center (ISAC) 12
Restructuring by the Bush Administration 15
Pre-September 11 15
Post-September 11 16
Department of Homeland Security 18
Issues 21
Roles and Responsibilities 21
Costs 24
Information Sharing 26
Privacy/Civil Liberties? 27
Congressional Actions 29

Appendix 31
For Additional Reading 32

List of Tables

Table 1. Lead Agencies 5
Table 2. Lead Agencies as Proposed in the National Strategy for Homeland Defense 8
Table 3. Sector Coordinators 10
Table A.1. National Plan for Information Systems Protection Version 1.0 31

Critical Infrastructures: Background, Policy, and Implementation

Latest Developments

One June 6, President Bush announced that the Administration would propose the establishment of a new Department of Homeland Security. On June 18, the Administration presented establishing legislation. It is beyond the scope of this report to track the developments and issues associated with this proposal in total. However, the President's proposal does seek to establish, within the new Department, a division for Information Analysis and Infrastructure Protection. Issues and developments regarding this element of the proposal (i.e. Information Analysis and Infrastructure Protection) and how it complements or supersedes existing activities in these two areas, are discussed in this report (see Section on **Department of Homeland Security**).

On July 16, 2002, the Office of Homeland Security released a National Strategy for Homeland Security. The draft legislation above captured much of the activities and responsibilities assigned to the Department of Homeland Security by the National Strategy. However, the National Strategy elaborates further on some of those responsibilities and introduces a few more. Information contained in the National Strategy that is relevant to the discussions in the report is incorporated in the appropriate sections.

The House Select Committee on Homeland Security is about to mark up its version (H.R. 5005) of the President's proposal, after having received input from a number of the permanent committees. The Senate Government Affairs Committee, too, is about to mark up a version of S. 2452. (See **Congressional Actions**).

Introduction

Certain socio-economic activities are vital to the day-to-day functioning and security of the country; for example, transportation of goods and people, communications, banking and finance, and the supply and distribution of electricity and water. These activities and services have been referred to as components of the nation's critical infrastructure. Domestic security and our ability to monitor, deter, and respond to outside hostile acts also depend on some of these activities as well as other more specialized activities like intelligence gathering and command and control of police and military forces. A serious disruption in these activities and capabilities could have a major impact on the country's well-being.[1]

[1] As a reminder of how dependent society is on its infrastructure, in May 1998, PanAmSat's (continued...)

These activities and capabilities are supported by an array of physical assets, processes, information, and organizations forming what has been called the nation's critical infrastructures. The country's critical infrastructures are growing increasingly complex, relying on computers and, now, computer networks to operate efficiently and reliably. The growing complexity, and the interconnectedness resulting from networking, means that a disruption in one may lead to disruptions in others.

Disruptions can be caused by any number of factors: poor design, operator error, physical destruction due to natural causes, (earthquakes, lightening strikes, etc.) or physical destruction due to intentional human actions (theft, arson, terrorist attack, etc.). Over the years, operators of these infrastructures have taken measures to guard against and to quickly respond to many of these risks.[2] However, the growing dependency of these systems on information technologies and computer networks introduces a new vector by which problems can be introduced.[3]

Of particular concern is the threat posed by "hackers" who can gain unauthorized access to a system and who could destroy, corrupt, steal, or monitor information vital to the operation of the system. Unlike someone setting off a bomb, hackers can gain access to a critical site from a remote location[4]. The ability to detect and deter their actions is still being developed. While infrastructure operators are also taking measures to guard against and respond to cyber attacks, there is concern that the number of "on-line" operations is growing faster than security awareness and the use of sound security measures.

Hackers range from mischievous teenagers, to disgruntled employees, to criminals, to spies, to foreign military organizations. While the more commonly reported incidents involve mischievous teenagers (or adults), self-proclaimed "electronic anarchists", or disgruntled (former) employees, the primary concern are criminals, spies, military personnel, or terrorists from around the world who appear to be perfecting their hacking skills and who may pose a potential strategic threat to the reliable operations of our critical infrastructures.[5]

[1] (...continued)
Galaxy IV satellite's on-board controller malfunctioned, disrupting service to an estimated 80-90% of the nation's pagers, causing problems for hospitals trying to reach doctors on call, emergency workers, and people trying to use their credit cards at gas pumps, to name but a few.

[2] Following September 11, these protections will undoubtedly be reexamined.

[3] Efforts to integrate the computer systems of Norfolk Southern and Conrail after their merger in June, 1999 caused a series of mishaps leaving trains misrouted, crews misscheduled, and products lost. See, "Merged Railroads Still Plagued by IT Snafus," Computerworld, January 17, 2000,pp 20-21.

[4] See, Cyber-Attacks by Al Qaeda Feared, Washington Post. Thursday June 27, 2002 ppA1,A10. Among the topics discussed in the article, is a man in Australia who was able to remotely gain access to the digital control system of a sewage treatment plant to cause raw sewage to leak into the surrounding environment.

[5] The Director of the Central Intelligence Agency testified before the Senate Committee on (continued...)

Prior to September 11, critical infrastructure protection was synonymous with cyber security to many people. Recent policies, and implementation of those policies, also focused on cyber security. Consequently, much of this report discusses cyber related activities and issues. However, the terrorist attacks of September 11, and the subsequent anthrax attacks, demonstrated the need to reexamine physical protections and to integrate physical protections into an overall critical infrastructure policy.[6] To the extent this happens, this report will capture it. However, specific protections, physical or cyber, associated with individual infrastructures is beyond the scope of this report. For CRS products related to specific infrastructure protection efforts, see **For Additional Reading**.

The President's Commission on Critical Infrastructure Protection

This report takes as its starting point the establishment of the President's Commission on Critical Infrastructure Protection (PCCIP) in July 1996.[7] Its tasks were to: report to the President the scope and nature of the vulnerabilities and threats to the nation's critical infrastructures (focusing primarily on cyber threats); recommend a comprehensive national policy and implementation plan for protecting critical infrastructures; determine legal and policy issues raised by proposals to increase protections; and propose statutory and regulatory changes necessary to effect recommendations.

The PCCIP released its report to President Clinton in October 1997.[8] Examining both the physical and cyber vulnerabilities, the Commission found no immediate crisis threatening the nation's infrastructures. However, it did find reason to take action, especially in the area of cyber security. The rapid growth of a computer-literate population (implying a greater pool of potential hackers), the inherent vulnerabilities of common protocols in computer networks, the easy availability of hacker "tools" (available on many websites), and the fact that the basic tools of the hacker (computer, modem, telephone line) are the same essential technologies used by the general population indicated to the Commission that both the threat and vulnerability exist.

[5] (...continued)
Governmental Affairs (June 24, 1998) that a number of countries are incorporating information warfare into their military doctrine and training and developing operational capability. It should be noted that the U.S. military is probably the leader in developing both offensive and defensive computer warfare techniques and doctrine.

[6] Besides loss of life, the terrorist attacks of September 11 disrupted the services of a number of critical infrastructures (including telecommunications, the internet, financial markets, and air transportation). In some cases, protections already in place (like off-site storage of data, mirror capacity, etc.) allowed for relatively quick reconstitution of services. In other cases, service was disrupted for much longer periods of time.

[7] Executive Order 13010.Critical Infrastructure Protection. Federal Register. Vol 61. No. 138. July 17, 1996. pp. 3747-3750.

[8] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, October 1997.

The Commission's general recommendation was that greater cooperation and communication between the private sector and government was needed. Much of the nation's critical infrastructure is owned and operated by the private sector. As seen by the Commission, the government's primary role (aside from protecting its own infrastructures) is to collect and disseminate the latest information on intrusion techniques, threat analysis, and ways to defend against hackers.

The Commission also proposed a strategy for action:

- facilitate greater cooperation and communication between the private sector and appropriate government agencies by: setting a top level policy-making office in the White House; establishing a council that includes corporate executives, state and local government officials, and cabinet secretaries; and setting up information clearinghouses;
- develop a real-time capability of attack warning;
- establish and promote a comprehensive awareness and education program;
- streamline and clarify elements of the legal structure to support assurance measures (including clearing jurisdictional barriers to pursuing hackers electronically); and,
- expand research and development in technologies and techniques, especially technologies that allow for greater detection of intrusions.

The Commission's report underwent interagency review to determine how to respond. That review led to a Presidential Decision Directive released in May 1998.

Presidential Decision Directive No. 63

Presidential Decision Directive No. 63 (PDD-63)[9] set as a national goal the ability to protect the nation's critical infrastructure from intentional attacks (both physical and cyber) by the year 2003. According to the PDD, any interruptions in the ability of these infrastructures to provide their goods and services must be "brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States."[10]

PDD-63 identified the following activities whose critical infrastructures should be protected: information and communications; banking and finance; water supply; aviation, highways, mass transit, pipelines, rail, and waterborne commerce; emergency and law enforcement services; emergency, fire, and continuity of government services; public health services; electric power, oil and gas production, and storage.[11] In addition, the PDD identified four activities where the federal

[9] See, *The Clinton's Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, White Paper, May 22, 1998, which can be found on [http://www.ciao.gov/ciao_document_library/paper598.html].

[10] Ibid.

[11] The National Strategy on Homeland Security has expanded the list of critical infrastructures identified.

government controls the critical infrastructure: internal security and federal law enforcement; foreign intelligence; foreign affairs; and national defense.

A lead agency was assigned to each of these "sectors" (see **Table 1**). Each lead agency was directed to appoint a **Sector Liaison Official** to interact with appropriate private sector organizations. The private sector was encouraged to select a **Sector Coordinator** to work with the agency's sector liaison official. Together, the liaison official, sector coordinator, and all affected parties were to contribute to a sectoral security plan which will be integrated into a **National Infrastructure Assurance Plan** (see **Table 3** below). Each of the activities performed primarily by the federal government also were assigned a lead agency who will appoint a **Functional Coordinator** to coordinate efforts similar to those made by the Sector Liaisons.

Table 1. Lead Agencies

Department/Agency	Sector/Function
Commerce	Information and Communications
Treasury	Banking and Finance
EPA	Water
Transportation	Transportation
Justice	Emergency Law Enforcement
Federal Emergency Management Agency	Emergency Fire Service
Health and Human Services	Emergency Medicine
Energy	Electric Power, Gas, and Oil
Justice	Law Enforcement and International Security
Director of Central Intelligence	Intelligence
State	Foreign Affairs
Defense	National Defense

The PDD created the position of **National Coordinator** for Security, Infrastructure Protection, and Counter-terrorism. The National Coordinator reported to the President through the Assistant to the President for National Security Affairs.[12] Among his many duties the National Coordinator chaired the **Critical Infrastructure Coordination Group**. This Group was the primary interagency working group for developing and implementing policy and for coordinating the federal government's own internal security measures. The Group included high level

[12] President Clinton designated Richard Clarke (Special Assistant to the President for Global Affairs, National Security Council) as National Coordinator.

representatives from the lead agencies (including the Sector Liaisons), the National Economic Council, and all other relevant agencies.

Each federal agency was made responsible for securing its own critical infrastructure and was to designate a Critical Infrastructure Assurance Officer (CIAO) to assume that responsibility. The agency's current Chief Information Officer (CIO) could double in that capacity. In those cases where the CIO and the CIAO were different, the CIO was responsible for assuring the agency's information assets (databases, software, computers), while the CIAO was responsible for any other assets that make up that agency's critical infrastructure. Agencies were given 180 days from the signing of the Directive to develop their plans. Those plans were to be fully implemented within 2 years and updated every 2 years.

The PDD set up a **National Infrastructure Assurance Council**. The Council was to be a panel that included private operators of infrastructure assets and officials from state and local government officials and relevant federal agencies. The Council was to meet periodically and provide reports to the President as appropriate. The National Coordinator was to act as the Executive Director of the Council.

The PDD also called for a **National Infrastructure Assurance Plan**. The Plan is to integrate the plans from each of the sectors mentioned above and should consider the following: a vulnerability assessment, including the minimum essential capability required of the sector's infrastructure to meet its purpose; remedial plans to reduce the sector's vulnerability; warning requirements and procedures; response strategies; reconstitution of services; education and awareness programs; research and development needs; intelligence strategies; needs and opportunities for international cooperation; and legislative and budgetary requirements.

The PDD also set up a National Plan Coordination Staff to support the plan's development. Subsequently, the **Critical Infrastructure Assurance Office** (CIAO, not to be confused with the agencies' Critical Infrastructure Assurance Officers) was established to serve this function and was placed in the Department of Commerce's Export Administration. CIAO supports the National Coordinator's efforts to integrate the sectoral plans into a National Plan, supports individual agencies in developing their internal plans, helps coordinate a national education and awareness programs, and provides legislative and public affairs support.

In addition to the above activities, the PDD called for studies on specific topics. These included issues of: liability that might arise from private firms participating in an information sharing process; legal impediments to information sharing; classification of information and granting of clearances (efforts to share threat and vulnerability information with private sector CEOs has been hampered by the need to convey that information in a classified manner); information sharing with foreign entities; and the merits of mandating, subsidizing or otherwise assisting in the provision of insurance for selected infrastructure providers.

Most of the Directive established policy-making and oversight bodies making use of existing agency authorities and expertise. However, the PDD also addressed operational concerns. The Directive called for a national capability to detect and respond to cyber attacks while they are in progress. Although not specifically identified in the Directive, the Clinton Administration proposed establishing a **Federal Instruction Detection Network (FIDNET)** that would, together with the **Federal Computer Intrusion Response Capability (FedCIRC)** begun just prior to PDD-63, meet this goal. The Directive explicitly gave the Federal Bureau of Investigation the authority to expand its existing computer crime capabilities into a **National Infrastructure Protection Center (NIPC)**. The Directive called for the NIPC to be the focal point for federal threat assessment, vulnerability analysis, early warning capability, law enforcement investigations, and response coordination. All agencies were required to forward to the NIPC information about threats and actual attacks on their infrastructure as well as attacks made on private sector infrastructures of which they become aware. Presumably, FIDNET[13] and FedCIRC would feed into the NIPC. According to the Directive, the NIPC would be linked electronically to the rest of the federal government and use warning and response expertise located throughout the federal government.. The Directive also made the NIPC the conduit for information sharing with the private sector through equivalent **Information Sharing and Analysis Center(s)** operated by the private sector.

While the FBI was given the lead, the NIPC also includes the Department of Defense, the Intelligence Community, and a representative from all lead agencies. Depending on the level of threat or the character of the intrusion, the NIPC may be placed in direct support of either the Department of Defense or the Intelligence Community.

[13] From the beginning FIDNET generated controversy both inside and outside the government. Privacy concerns, cost and technical feasibility were at issue. By the end of the Clinton Administration, FIDNET as a distributed intrusion detection system feeding into a centralized analysis and warning capability was abandoned. Each agency, however, is allowed and encouraged to use intrusion detection technology to monitor and secure their own systems.

Implementation of PDD-63

Selection of Sector Liaison Officials and Functional Coordinators. The National Strategy for Homeland Security appears to maintain the role of lead agencies as outlined in PDD-63, with the new Department acting as coordinator of their efforts. However, the Strategy does shift liaison responsibilities for some sectors to the new Department, and there remains some discussion about how many sectors for which the new Department would be the primary liaison.[14] The liaison responsibilities outlined in the National Strategy are noted in **Table 2** below.

Table 2. Lead Agencies as Proposed in the National Strategy for Homeland Defense

Department/Agency (PDD-63 liaison)	Sector/Function
Agriculture	Agriculture
	Food
Agriculture	Meat/Poultry
Health and Human Services	All other
Homeland Security (Commerce)	Information and Communications
Treasury	Banking and Finance
EPA	Water
Homeland Security (Transportation)	Transportation
Homeland Security (Federal Emergency Management Agency, Justice, Health and Human Services)	Emergency Services
Health and Human Services	Public Health
	Government
Homeland Security	Continuity of Government
Individual departments and agencies	Continuity of Operations
Energy	Electric Power, Gas, and Oil
Environmental Protection Agency	Chemical Industry and Hazardous Materials
Defense	Defense Industrial Base
Homeland Defense	Postal and Shipping
Interior	National Monuments and Icons

[14] See, *Ridge Says EPA Should Lose Authority to Evaluate Vulnerability of Industrial Facilities,* Inside EPA, June 25, 2002.

Identifying and Selecting Sector Coordinators. The identification of sector coordinators has proceeded with mixed results. Table 3 below shows those individuals or groups that have agreed to act as Coordinators.

Different sectors present different challenges to identifying a coordinator. Some sectors are more diverse than others (e.g. transportation includes rail, air, waterways, and highways; information and communications include computers, software, wire and wireless communications) and raises the issue of how to have all the relevant players represented. Other sectors are fragmented, consisting of small or local entities. Some sectors, such as banking, telecommunications, and energy have more experience than others in working with the federal government and/or working collectively to assure the performance of their systems.

Besides such structural issues are ones related to competition. Inherent in the exercise is asking competitors to cooperate. In some cases it is asking competing industries to cooperate. This cooperation not only raises issues of trust among firms, but also concerns regarding anti-trust rules. Also, having these groups in direct communications with the federal government raises questions about their relationship to the federal government as governed by the Federal Advisory Committee Act (5 USC Appendix) and how the Freedom of Information Act (5 USC 552) applies to them and the information that may be exchanged.

Sector coordinators have been identified for most of the major privately operated sectors: banking and finance, energy, information and communications. In the public sector, EPA early on identified the Association of Metropolitan Water Agency as sector coordinator. In the area of transportation, the Association of American Railroads has been identified as the coordinator for the rail sector. The Department of Transportation would like to also find coordinators for air and water transportation. FEMA has not identified a single coordinator to represent the country's emergency fire service providers. However, through the U.S. Fire Administration, a component of FEMA, they have an established communication network with the nation's fire associations, the 50 State Fire Marshals, and other law enforcement groups. FEMA is also responsible for continuity of government. Again, no single coordinator has been identified, but FEMA had discussed continuity of government issues with state and local governments in the context of the Y2K.[15] Nor has the Department of Health and Human Services identified a central coordinator for the emergency medical community. The Department of Justice, through the NIPC, has helped to create the Emergency Law Enforcement Services (ELES) Forum. The Forum is a group of senior law enforcement executives from state, local, and non-FBI federal agencies.

[15] The New Mexico Critical Infrastructure Assurance Council, an offshoot of the FBI's InfraGard efforts in the state, include the state government and other state and local agencies. The Council is referenced in the *National Plan for Information Systems Protection*. See, **National Critical Infrastructure Plan**, below.

Table 3. Sector Coordinators

Lead Agency	Identified Sector Coordinators
Commerce	A consortium of 3 associations: Information Technology Assn. of America; Telecommunications Industry Assn.; U.S. Telephone Assn.
Treasury	Rhonda McLane - BankAmerica
EPA	Assn. of Metropolitan Water Agencies
Energy	North American Electric Reliability Council and National Petroleum Council
Transportation	Association of American Railroads International Airport Councils of North America (inactive)
Health and Human Services	
FEMA	U.S. Fire Administration
Justice	Emergency Law Enforcement Services Forum

Appointment of the National Infrastructure Assurance Council. The Clinton Administration released an Executive Order (13130) in July, 1999, formally establishing the council. Just prior to leaving office, President Clinton put forward the names of 18 appointees.[16] The Order was rescinded by the Bush Administration before the Council could meet. In Executive Order 13231[17], President Bush establishes a National Infrastructure Advisory Council (with the same acronym, NIAC) whose functions are similar to those of the Clinton Council.

Selection of Agency CIAOs. All agencies made permanent or acting CIAO appointments.

Internal Agency Plans. There has been some confusion about which agencies were required to submit critical infrastructure plans. The PDD-63 directs every agency to develop and implement such a plan. A subsequent Informational Seminar on PDD-63 held on October 13, 1998 identified two tiers of agencies. The first tier included lead agencies and other "primary" agencies like the Central

[16] White House Press Release, dated January 18, 2000.

[17] Executive Order 13231—Critical Infrastructure Protection in the Information Age. Federal Register. Vol. 66. No. 202. October 18, 2001. pp53063-53071. The NIAC is established on page 53069.

Intelligence Agency and Veteran's Affairs. These agencies were held to the 180 day deadline. A second tier of agencies were identified by the National Coordinator and required to submit plans by the end of February, 1999. The "secondary" agencies were Agriculture, Education, Housing and Urban Development, Labor, Interior, General Services Administration, National Aeronautics and Space Administration and the Nuclear Regulatory Commission. All of these "primary" and "secondary" agencies met their initial deadlines for submitting their internal plans for protecting their own critical infrastructures from attacks and for responding to intrusions. The Critical Infrastructure Assurance Office assembled an expert team to review the plans. The plans were assessed in 12 areas including schedule/milestone planning, resource requirements, and knowledge of existing authorities and guidance. The assessment team handed back the initial plans with comments. Agencies were given 90 days to respond to these comments. Of the 22 "primary" and "secondary" agencies that submitted plans, 16 modified and resubmitted them in response to first round comments.

Initially the process of reviewing these agency plans was to continue until all concerns were addressed. Over the summer of 1999, however, review efforts slowed and subsequent reviews were put on hold as the efficacy of the reviews was debated. Some within the CIAO felt that the plans were too general and lacked a clear understanding of what constituted a "critical asset" and the interdependencies of those assets. As a result of that internal debate, the CIAO redirected its resources to institute a new program called Project Matrix. Project Matrix is a three step process by which an agency can identify and assess its most critical assets, identify the dependencies of those assets on other systems, including those beyond the direct control of the agency, and prioritize. CIAO has offered this analysis to 14 agencies, including some not designated as "primary" or "secondary" agencies, such as the Social Security Administration and the Securities and Exchange Commission. Participation by the agencies has been voluntary.

In the meantime, other agencies (i.e. those not designated as primary and secondary) apparently did not develop critical infrastructure plans. In a much later report by the President's Council on Integrity and Efficiency (dated March 21, 2001), the Council, which was charged with reviewing agencies' implementation of PDD-63, stated that there was a misunderstanding as to the applicability of PDD-63 to all agencies. The Council asserted that all agencies were required to develop a critical infrastructure plan and that many had not, because they felt they were no covered by the Directive. Also, the Council found that of the agency plans that had been submitted, many were incomplete, had not identified their mission-critical assets, and that almost none had completed vulnerability assessments.

According to the National Plan released in January 2000 (see below), all "Phase One" and "Phase Two" agencies (presumably this refers to the "primary" and "secondary" agencies mentioned above) were to have completed preliminary vulnerability analyses and to have outlined proposed remedial actions. Again, according to the National Plan, those remedial actions were to be budgeted for and submitted as part of the agencies' FY2001 budgets submissions to the Office of Management and Budget and every year thereafter. However, given the discussion above, the comprehensiveness of these studies and plans are in question.

Neither of the Bush Administration executive orders make reference to these critical infrastructure protection plans of the agencies.

National Critical Infrastructure Plan. The Clinton Administration, after some delay, released Version 1.0 of a National Plan for Information Systems Protection in January 2000.[18] The Plan focused primarily on cyber-related efforts within the federal government. A note in the Executive Summary states that a parallel Critical Physical Infrastructure Protection Plan was to be developed and possibly incorporated in Version 2.0, or later versions.[19] Version 2.0 of the National Plan was to cover the private sector. The Partnership for Critical Infrastructure Protection (see below) has been coordinating the private sector's input to this next edition.

Version 1.0 was divided between government-wide efforts and those unique to the national security community. The Plan (159 pages) will not be summarized here in any detail. See Appendix for a brief synopsis.

The number of National Plans seem to be proliferating. The Bush Administration, through the President's Critical Infrastructure Protection Board (see **Bush Restructuring: Post-September 11** later in this report) has been working on a National Strategy to Secure Cyberspace. This, perhaps, represents Version 2.0 of the Clinton-released Plan. The Office of Homeland Security (see **Bush Restructuring: Post-September 11** later in this report) just released a National Strategy for Homeland Security. Both the National Strategy on Homeland Security and the draft legislation creating the Department of Homeland Security also call for a comprehensive national plan to provide both physical and cyber security for the nation's critical infrastructures. Perhaps this is what was originally envisioned by PDD-63.

Information Sharing and Analysis Center (ISAC). PDD-63 envisaged an ISAC to be the private sector counterpart to the FBI's National Infrastructure Protection Center (NIPC), collecting and sharing incident and response information among its members and facilitating information exchange between government and the private sector. While the Directive conceived of a single center serving the entire private sector, the idea now is that each sector would have its own center. Progress in forming sector ISACs has been mixed.

A number of the nation's largest banks, securities firms, insurance companies and investment companies have joined together in a limited liability corporation to form a banking and finance industry ISAC. The group has contracted with an internet service provider[20] (ISP) to design and operate the ISAC. Individual firms feed raw computer network traffic data to the ISAC. The ISP maintains a database

[18] Defending America's Cyberspace. National Plan for Information Systems Protection. Version 1.0. An Invitation to a Dialogue. The White House. 2000.

[19] Ibid. Executive Summary. p. 13.

[20] The ISP is Global Integrity, a subsidiary of Science Applications International Corp. (SAIC).

of network traffic and analyzes it for suspicious behavior and provides its customers with summary reports. If suspicious behavior is detected, the analysis may be forwarded to the federal government. Anonymity is maintained between participants and outside the ISAC. The ISP will forward to its customers alerts and other information provided by the federal government. The ISAC became operational in October, 1999.

The telecommunications industry has agreed to establish an ISAC through the National Coordinating Center (NCC). The NCC is a government-industry partnership that coordinates responses to disruptions in the National Communications System. Unlike the banking and finance ISAC that uses a third party for centralized monitoring and analysis, each member firm of the NCC will monitor and analyze its own networks. If a firm suspects its network(s) have been breached, it will discuss the incident(s) within the NCC's normal forum. The NCC members will decide whether the suspected behavior is serious enough to report to the appropriate federal authorities. Anonymity will be maintained outside the NCC. Any communication between federal authorities and member firms will take place through the NCC, this includes incident response and requests for additional information[21].

The electric power sector, too, has established a decentralized ISAC through its North American Electricity Reliability Council (NAERC). Much like the NCC, NAERC already monitors and coordinates responses to disruptions in the nation's supply of electricity. It is in this forum that information security issues and incidents will be shared. The National Petroleum Council is still considering setting up an ISAC with its members.

In January, 2001, the information technology industry announced its plans to form an ISAC. Members include 19 major hardware, software, and e-commerce firms, including AT&T, IBM, Cisco, Microsoft, Intel, and Oracle. The ISAC will be overseen by a board made up of members and operated by Internet Security Systems.

The country's water authorities intend to develop an appropriate ISAC model for their sector.

Much like the communications and the electric power sectors, the emergency fire services sector ISAC will be integrated into the responsibilities of an existing organizational body; FEMA's U.S. Fire Administration, headquartered in Emmitsburg, MD. The ISAC will staffed by leading fire experts who will assess NIPC threat intelligence and help prepare warnings for distribution to the nation's fire fighting community. In turn, local fire departments, as first responders in many instances, can provide information through the U.S. Fire Administration that may be helpful to NIPC in its intelligence analysis function.

In addition to these individual sectors setting up or contemplating ISACs, the private sector has formed a **Partnership for Critical Infrastructure Security** to

[21] Federal agencies sit on the NCC, including the NSA. One could assume that knowledge of incidents discussed in the NCC could find its way to federal investigatory authorities without formally being reported.

share information and strategies and to identify interdependencies across sectoral lines. The Partnership is a private sector initiative and has filed as a 501(c)(6) organization. A preliminary meeting was held in December 1999 and five working groups were established (Interdependencies/Vulnerability Assessment, Cross-Sector Information Sharing, Legislation and Policy, Research and Development, and Organization). The working groups meet every other month. The federal government is not officially part of the Partnership, but the CIAO acts as a liaison and has provided administrative support for meetings. Sector Liaison from lead agencies are considered ex officio members. Some entities not yet part of their own industry group (e.g. some hospitals and pharmaceutical firms) or not specifically designated as belonging to a critical infrastructure (the chemical industry) are participating in the Partnership.

Also, besides the efforts of the lead agencies to assist their sectors in considering ISACs, the NIPC offers private sector firms from across all industries a program called **INFRAGARD**. The program includes an Alert Network. Participants in the program agree to supply the FBI with two reports when they suspect an intrusion of their systems has occurred. One report is "sanitized" of sensitive information and the other provides more detailed description of the intrusion. The FBI will help the participant respond to the intrusion. In addition, all participants are sent periodic updates on what is known about recent intrusion techniques. The NIPC is working to set up local INFRAGARD chapters that can work with each other and regional FBI field offices. In January, 2001, the FBI announced it had finished establishing INFRAGARD chapters in each of its 56 field offices.

It should also be noted that the FBI has had since the 1980s a program called the **Key Assets Initiative (KAI)**. The objective of the KAI is to develop a database of information on "key assets" within the jurisdiction of each FBI field office, establish lines of communications with asset owners and operators to improve physical and cyber protection, and to coordinate with other federal, state, and local authorities to ensure their involvement in the protection of those assets. The program was initially begun to allow for contingency planning against physical terrorist attacks. According to testimony by a former Director of the NIPC, the program was "reinvigorated" by the NIPC and expanded to included the cyber dimension.[22]

[22] Testimony by Michael Vatis before the Senate Judiciary Committee, Subcommittee on Technology and Terrorism. Oct. 6, 1999. The above mentioned Washington Post article (Cyber Acts by Al Qaeda Feared, Thursday June 27, 2002) quotes an spokesman for the electric utility industry as suggesting that industry is reluctant to share that information out of concern that it will not be kept confidential.

Restructuring by the Bush Administration

Pre-September 11.

As part of its overall redesign of White House organization and assignment of responsibilities, the in-coming Bush Administration spent the first 8 months reviewing its options for coordinating and overseeing critical infrastructure protection. During this time, the Bush Administration continued to support the activities begun by the Clinton Administration.

The Bush Administration review was influenced by three parallel debates. First, the National Security Council (NSC) underwent a major streamlining. All groups within the Council established during previous Administrations were abolished. Their responsibilities and functions were consolidated into 17 Policy Coordination Committees (PCCs). The activities associated with critical infrastructure protection were assumed by the Counter-Terrorism and National Preparedness PCC. At the time, whether, or to what extent, the NSC should remain the focal point for coordinating critical infrastructure protection (i.e. the National Coordinator came from the NSC) was unclear. Richard Clarke, himself, wrote a memorandum to the incoming Bush Administration that the function should be transferred directly to the White House.[23]

Second, there was a continuing debate about the merits of establishing a government-wide Chief Information Officer (CIO), whose responsibilities would include protection of all federal non-national security-related computer systems and coordination with the private sector on the protection of privately owned computer systems. The Bush Administration announced mid-year its desire not to create a separate federal CIO position, but to recruit a Deputy Director of the Office of Management and Budget that would assume an oversight role of agency CIOs. One of reason's cited for this was a desire to keep agencies responsible for their own computer security.[24]

Third, there was the continuing debate about how best to defend the country against terrorism, in general. Some include in the terrorist threat cyber attacks on critical infrastructure. The U.S. Commission on National Security/21st Century (the Hart-Rudman Commission) proposed a new National Homeland Security Agency. The recommendation built upon the current Federal Emergency Management Agency (FEMA) by adding to it the Coast Guard, the Border Patrol, Customs Service, and other agencies. The Commission recommended that the new organization include a directorate responsible for critical infrastructure protection. While both the Clinton and Bush Administration remained cool to this idea, bills were introduced in Congress to establish such an agency.

[23] Senior NSC Official Pitches Cyber-Security Czar Concept in Memo to Rice. *Inside the Pentagon*. January 11, 2001. p 2-3.

[24] For a discussion of this and the status of federal CIO legislation, see CRS Report RL30914, Federal Chief Information Officer (CIO): Opportunities and Challenges, by Jeffery Siefert.

Post-September 11.

Following the September 11 terrorist attacks President Bush signed two Executive Orders relevant to critical infrastructure protection. E.O. 13228, signed October 8, 2001 established the **Office of Homeland Security**, headed by the **Assistant to the President for Homeland Security**.[25] Its mission is to "develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats and attacks." Among its functions is the coordination of efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks. This includes strengthening measures for protecting energy production, transmission, and distribution; telecommunications; public and privately owned information systems; transportation systems; and, the provision of food and water for human use. Another function of the Office is to coordinate efforts to ensure rapid restoration of these critical infrastructures after a disruption by a terrorist threat or attack.

Finally, the EO also established the **Homeland Security Council**. The Council, made up of the President, Vice-President, Secretaries of Treasury, Defense, Health and Human Services, and Transportation, the Attorney General, the Directors of FEMA, FBI, and CIA and the Assistant to the President for Homeland Security. Other White House and departmental officials could be invited to attend Council meetings.[26] The Council advises and assists the President with respect to all aspects of homeland security. The agenda for those meetings shall be set by the Assistant to President for Homeland Security, at the direction of the President. The Assistant is also the official recorder of Council actions and Presidential decisions.

The second Executive Order (E.O. 13231) signed October 16, 2001, stated that it is U.S. policy "to protect against the disruption of the operation of information systems for critical infrastructure...and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible."[27] This Order also established the **President's Critical Infrastructure Protection Board**. The Board's responsibility is to "recommend policies and coordinate programs for protecting information systems for critical infrastructure..." The Order also established a number of standing committees of the Board that includes Research and Development (chaired by a designee of the Director of the Office of Science and Technology), Incident Response (chaired by the designees of the Attorney General and the Secretary of Defense), and Physical Security (also chaired by designees of the Attorney General and the Secretary of Defense). The Board is directed to propose a National Plan (i.e. the National Plan to Secure Cyberspace, mentioned above) on issues within its purview on a periodic basis, and, in coordination with the Office of Homeland Security, review and make

[25] President Bush selected Tom Ridge to head the new Office.

[26] For more information on the structure of the Homeland Security Council and the Office of Homeland Security, see CRS Report RL31148. *Homeland Security: The Presidential Coordination Office*, by Harold Relyea.

[27] Executive Order 13231—Critical Infrastructure Protection in the Information Age. Federal Register. Vol. 86. No. 202. Oct. 18, 2001.

recommendations on that part of agency budgets that fall within the purview of the Board.

The Board is to be chaired by a **Special Advisor to the President for Cyberspace Security**.[28] The Special Advisor reports to both the Assistant to the President for National Security and the Assistant to the President for Homeland Security. Besides presiding over Board meetings, the Special Advisor may, in consultation with the Board, propose policies and programs to appropriate officials to ensure protection of the nation's information infrastructure and may coordinate with the Director of OMB on issues relating to budgets and the security of computer networks.

Finally, the Order also established the **National Infrastructure Advisory Council**. The Council is to provide advice to the President on the security of information systems for critical infrastructure. The Council's functions include enhancing public-private partnerships, monitoring the development of ISACs, and encouraging the private sector to perform periodic vulnerability assessments of critical information and telecommunication systems.

In many respects, the Bush Administration policy statements regarding critical infrastructure protection are a continuation of PDD-63. The fundamental policy statements are the essentially the same: the protection of infrastructures critical to the people, economy, essential government services, and national security. Also, the goal of the government's efforts are to ensure that any disruption of the services provided by these infrastructures be infrequent, of minimal duration, and manageable. The infrastructures identified as critical are essentially the same. There is to be an interagency group (the Homeland Security Council and the President's Critical Infrastructure Protection Board in EO 13228 and 13231, respectively, replaces the Critical Infrastructure Coordination Group of PDD-63) to develop policies and coordinate activities. Functional areas of concern are similar (i.e. research and development, response coordination, intelligence, etc.). The President shall be advised by a Council made up of private sector executives, academics, and State and local officials. The Critical Infrastructure Assurance Office (CIAO) and the National Infrastructure Protection Center (at the FBI) are left in place, as are the liaison efforts between lead agencies and the private sector and State and local governments, and the structures set up for information sharing.

There are two primary differences, however. First, the Office of Homeland Security has overall authority for coordinating critical infrastructure protection against terrorist threats and attacks. Those responsibilities associated with information systems of critical infrastructures are delegated to the President's Critical Infrastructure Protection Board. Furthermore the Board's responsibilities for protecting the physical assets of the nation's information systems are to be defined by the Assistant to President for National Security and the Assistant to the President for Homeland Security. While PDD-63 focused primarily on cyber security, it gave the National Coordinator responsibility to coordinate the physical and cyber security

[28] President Bush designated Richard Clarke.

for all critical infrastructures. It would appear from the proposed structure of the Department of Homeland Security (see below) that this separation may continue.

Second, the "National Coordinator" is now a Special Advisor to the President rather than a member of the National Security Council staff. However, the Special Advisor still reports to Assistant to President for National Security in addition to the Assistant to the President for Homeland Security. It is not clear what additional authority or influence the new position grants the individual serving as Special Advisor.

Department of Homeland Security.

On June 8, President Bush announced his intention to propose a separate new **Department of Homeland Security** and on June 18, forwarded to Congress draft legislation that would establish this department along the lines proposed by the Hart-Rudman Commission and subsequent bills introduced in Congress (see **Congressional Actions**). The proposed plan does not nullify the above mentioned E.O.s. In fact, the Administration stressed that coordination and advice at the White House level is still needed. However, according to the draft legislation, many of the different agencies and programs within various departments with anti-terrorist functions, would be integrated into the new Department of Homeland Security.

The proposed legislation identifies four primary functional areas that would constitute Divisions within the new Department: **Information Analysis and Infrastructure Protection**; Chemical, Biological, Radiological, and Nuclear Countermeasures; Border and Transportation Security; and Emergency Preparedness and Response. Section 201 of the legislation outlines the responsibilities of the Information Analysis and Infrastructure Protection Division. These are:

- receive and analyze information and intelligence to understand threats and detect potential threats;
- assess vulnerabilities of key resources and critical infrastructures;
- integrate information and intelligence analysis with vulnerability assessments to set protective priorities and support protective measures;
- develop comprehensive national plan for securing key resources and critical infrastructures;
- take or seek to effect necessary measures to protect.

Section 202 of the bill transfers NIPC (except for the Computer Investigations and Operations Section), CIAO, FedCIRC, the **National Infrastructure Simulation and Analysis Center (NISAC)**[29], the Computer Security Division of NIST's

[29] The NISAC was established in The USA Patriots Act (P.L. 107-056), Section 1062. The Center builds upon expertise at Sandia and Los Alamos National Laboratory in modeling (continued...)

Information Technology Laboratory, and the **National Communication System (NCS)**[30] to the new Department.

Section 203 of the bill ensures the Secretary of the new Department shall have access to all threat and vulnerability analyses. Section 204 exempts from the Freedom of Information Act information concerning infrastructure vulnerabilities (and other vulnerabilities) provided voluntarily to the Department by non-federal entities. The exemption follows the information should it leave the Department.

In a more detailed discussion of the reorganization released by the Administration (*The Department Of Homeland Security*, June 2002), an organization chart shows the Information Analysis and Infrastructure Protection Division further divided into an Threat Analysis Section and an Infrastructure Protection Section, with the latter being divided again into **Physical Assets** and **Telecommunications and Cybersecurity**.

According to the document, the Threat Analysis function would fuze and analyze information and intelligence from multiple sources to provide early warning of potential attacks. In this regard the Department is to be a full partner and consumer of all intelligence-gathering agencies, although it will not, itself, become a domestic intelligence agency. The threat analysis and warning function would coordinate and, as appropriate, consolidate federal lines of communications with state and local public safety agencies and with the private sector. The Department will administer the Homeland Security Advisory Systems and be responsible for public alerts.

The document defines critical infrastructure as those assets, systems, and functions vital to our national security, governance, public health and safety, economy, and national morale. It lists the following infrastructures: food, water, agriculture, health systems and emergency services, energy (electrical, nuclear, gas and oil, dams), transportation (air, road, rail, ports, waterways), information and telecommunications, banking and finance, postal and shipping, and national monuments and icons. The infrastructure protection function will be responsible for assessing sector vulnerabilities (in which the NIASC will assist), coordinating the

[29] (...continued)
and simulating infrastructures and the interdependencies between them.

[30] The NCS is not really a single communication system but more a capability that ensures that disparate government agencies can communication with each other in times of emergencies. To make sure this capability exists and to assure that it is available when needed, an interagency group meets regularly to discuss issues and solve problems. The NCS was initially established in 1963 by the Kennedy Administration to ensure communications between military, diplomatic, intelligence, and civilian leaders, following the Cuban Missile Crisis. Those activities were expanded by the Reagan Administration to include emergency preparedness and response, including natural disaster response. The current interagency group includes 22 departments and agencies. The private sector, who own a significant share of the assets needed to ensure the necessary connectivity, is involved through the **National Security Telecommunication Advisory Committee (NSTAC)**. The National Coordinating Center, mentioned earlier in this report, and which serves as the telecommunications ISAC, is an operational entity within the NCS.

national plan, and directing or coordinating protective actions (which would be tiered to correspond to the perceived level of threat). Cybersecurity is singled out as being an especially high priority concern (hence its separation from physical asset protection). According to the document, the remaining agencies being transferred to this division will support the cybersecurity function. It is not clear what capability is available to the new Department to support the physical security function.

In the context of critical infrastructure protection, the proposed legislation basically facilitates a reorganization. Many of the policies, objectives, missions, and responsibilities complement those already established (e.g. vulnerability assessments, national planning, communication between government and private sector, improving protections, and drawing particular attention to cybersecurity). If anything, it adds at least two new players to those responsible for developing, coordinating and implementing policy and action, the Secretary of the Department of Homeland Security and the Under-Secretary for Information Analysis and Infrastructure Protection. It does not create, as yet, and aside from the Department and Division themselves, any new operational entities related to infrastructure protection.

However, the National Strategy for Homeland Security does expand the infrastructures to receive attention. Not only are economic vitality and national security of concern, but also public health and safety and national morale. As a result, agriculture, food, postal and shipping services, the chemical industry, and national monuments and icons are now included in the list of infrastructures that will be assessed.

Other parts of the Administration's proposal represents a major reorganization, Many entities, some with multiple missions, are being transferred or are being split apart, raising issues of how these functions will be reintegrated (including physical relocation), the integrity of functions left behind, and how constituencies will react. However, the proposed transfers associated with infrastructure protection perhaps are less disruptive as others (e.g. Coast Guard, or U.S. Customs). CIAO, FedCIRC, and NIASC are all relatively new organizations, with relatively narrow missions, and will be transferred fully to the new organization. They will likely, initially at least, perform their existing functions.

The disruption associated with transferring parts of NIPC is less clear. The transfer leaves the Computer Investigations and Operations unit within NIPC at the FBI, transferring the Analysis and Warning Section and the Training, Outreach, and Strategy Section. How much synergy was developed between these three sections? The FBI has received some criticism for its management of NIPC. According to a General Accounting Office (GAO) report, the FBI has had trouble recruiting people from other agencies. In the press, the FBI has been accused of being reluctant to share information with other agencies. The GAO report stated that the Threat Analysis and Warning function had not been well-developed (although the GAO noted that the analysis function is a difficult problem). The GAO report also stated that NIPC had provided valuable support to FBI filed investigations. In this reorganization, the part of NIPC most helpful to the FBI field offices will stay at FBI. The part that has experienced some difficulty will be transferred.

Also, it has not been readily transparent the extent to which NIPC has been concerned with the physical protection of critical infrastructure assets. NIPC supposedly has had a role in administering the FBI's Key Asset Initiative. However, the program was primarily implemented through the Field Offices. The National Strategy discusses the protection of key assets as a function of critical infrastructure protection. Key assets are defined as those individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage our nation's morale or confidence. These would include assets such as symbols or historical attractions or individual facilities that deserve special protection because of their destructive potential or their value to the local community. But it is not clear what role, if any, the FBI will continue to play.

Unlike the other agencies to be transferred, the Computer Security Division at NIST's Information Technology Laboratory and the National Communications System (NCS) at the Department of Defense have been established for a longer time. It is not clear what impact separating the Computer Security Division from the rest of NIST's Information Technology Laboratory will have on the Laboratory or the Division. There may synergies established that a physical or budgetary reorganization will sever. The NCS is essentially an interagency organization and assuming that its interagency character (and its close connection to the private sector through the NSTAC) is maintained, the impact of changing Managers (which besides being a Member was DOD's role within NCS) is expected to be minimal. Whether a physical relocation will be called for has not been addressed yet by the Administration. DOD does feel that its other communications and computer organizations with complementary functions benefit by being in close physical proximity. The House Science Committee in its report to the House Select Committee on Homeland Security (see **Congressional Actions**) recommended not moving the Division to the new Department.

Issues

Roles and Responsibilities. One of the issues associated with PDD-63 was whether it duplicated, superseded, or overturned existing information security responsibilities. Although the Directive dealt with infrastructures issues beyond just computer systems and also considered physical protections, its implementation focused on "cyber" threats and vulnerabilities. In this respect, it was an extension of the government's existing efforts in computer security. The Directive sought to use existing authorities and expertise as much as possible in assigning responsibilities. Nevertheless, the Directive did set up new entities that, at least at first glance, assumed responsibilities previously assigned to others.

The Paperwork Reduction Act of 1995 (P.L. 104-13) placed the responsibility for establishing government-wide information resources management policy with the Director of the Office of Management and Budget. Those policies are outlined in OMB Circular A-130. Appendix III of the Circular incorporates responsibilities for computer security as laid out in the Computer Security Act of 1987.[31] The Computer

[31] Appendix III does not apply to information technology that supports certain critical (continued...)

Security Act requires all agencies to inventory their computer systems and to establish security plans commensurate with the sensitivity of information contained on them. Agencies are suppose to submit summaries of their security plans along with their strategic information resources management plan to the Office of Management and Budget (OMB). The agencies are to follow technical, managerial, and administrative guidelines laid out by OMB, the Department of Commerce, the General Services Administration, and the Office of Personnel Management and should include (as detailed in the OMB Circular) incidence response plans, contingencies plans, and awareness and training programs for personnel. The Director of OMB was given the authority by the Computer Security Act to comment on those plans.

Under PDD-63, agencies submitted plans (not dissimilar in content to those called for in the Computer Security Act of 1987 and detailed in OMB Circular A-130 Appendix III) to the CIAO. The Critical Infrastructure Coordination Group assembled an expert review team to review these plans (an "ad hoc" team was set up at CIAO). It was not readily apparent who had the primary role to review and comment of an agency's security plan?[32] Who determined whether an agency's obligation to creating an adequate plan have been met?

It is not yet clear if E.O. 13231 will lead to the same issues. The E.O. specifically reaffirms OMB's role in developing and overseeing the implementation of government-wide information security policy (and the roles of the Secretary of Defense and the Director of Central Intelligence in the case of national security-related systems). The E.O. goes on to reiterate the responsibility of the Director of OMB (or the Assistant to the President for National Security in the case of national security-related systems) to report to the President and the agency head any deficiencies in security practices. The Board is instructed to assist the Director of OMB in this function. However, the E.O. also explicitly allows the Chair (i.e. the Special Advisor to the President), and the Board, to propose policies and programs to "appropriate" officials to ensure the protection of information systems of critical infrastructures. The creation of a new Department of Homeland Security introduces at least one more player into the mix. What role will the Cybersecurity official in the new Department of Homeland Security have in relation to the Special Advisor and the President's Critical Infrastructure Board ?

[31] (...continued)
national security missions as defined in 44 USC 3502(9) and 10 USC 2315. Policy for these national security systems, i.e. telecommunications and information systems containing classified information or used by the intelligence or military community, has been assigned by national security directives to the Department of Defense.

[32] It should be noted that the General Accounting Office has reported that the oversight of agency computer security measures to date has been inadequate. See, U.S. General Accounting Office, Information Security. Weaknesses Continue to Place Critical Federal Operations and Assets at Risk. GAO-01-600T. April 5, 2001.Testimony before the Oversight and Investigations Subcommittee, Committee on Energy and Commerce. House of Representatives.

Incident response is another area where roles and responsibilities are not defined clearly. Among the responsibilities assigned to the Department of Commerce by OMB Circular A-130 Appendix III is the coordination of agency computer incident response activities to promote sharing of incident response information and related vulnerabilities. This function has now migrated over to the General Services Administration which has established a Federal Computer Incident and Emergency Response Capability (FedCIRC). Consistent with OMB Circular A-130, the Government Information Security Reform Act, passed as Title X, Subtitle G in the FY2001 Defense Authorization Act (P.L. 106-398) requires agencies to report incidents to appropriate officials at GSA. But, PDD-63 stated and the National Plan, Version 1.0 reiterated, that the National Infrastructure Protection Center (NIPC) will provide the principal means of facilitating and coordinating the federal government's response to an incident, mitigating attacks, investigating threats, and monitoring reconstitution efforts. Were the lines of authority clearly established between the different organizations many of which are tasked with doing things that sound similar?[33] E.O. 13231 reiterates the NIPC's involvement in incident coordination and crisis response, in coordination with the Board, but makes no specific mention of FedCIRC. Does moving NIPC and FedCIRC into the same department help resolve this issue?

Also, it is not clear to what role the NIPC was to have played in coordinating the response to physical attacks on critical infrastructures. E.O. 13228 grants the Office of Homeland Security the leading role in responding to physical attacks on critical infrastructures other than the physical assets of information systems. E.O. 13228 raises its own issues regarding the relationships between the Office of Homeland Security, FEMA, and the National Security Council.[34] Moving NIPC into the new Department of Homeland Security doesn't really resolve this issue, because the overlap will then be between the Office of Homeland Security and the Department of Homeland Security.

Another area in question is the future role of the CIAO. The CIAO acted as the staff for the National Coordinator under PDD-63. E.O. 13231 makes reference to the continued role of the CIAO in information infrastructure protection, especially in the area of outreach to the private sector and coordination with information sharing centers. It also is directed to provide administrative support to the new NIAC. However, E.O. 13231 also allows the Special Advisor to create yet a different staff within the White House. Furthermore, the E. O. authorizes a staff for the President's Critical Infrastructure Protection Board. How are these three staffs reconciled?

[33] In recent testimony to Congress, the General Accounting Office noted that the mission of the NIPC has not been fully defined, leading to differing interpretations by different agencies. Also, the manpower support from and information sharing with other agencies has not materialized as envisioned. See, General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities*. GAO-01-769, Testimony before the Subcommittee on Technology, Terrorism, and Government Information, Senate Judiciary Committee. May 22, 2001.

[34] See CRS Report RL31148. *Homeland Security*. Op. Cit .pp 7-8.

There was another bureaucratic issued raised by PDD-63. Prior to the Computer Security Act of 1987, the Reagan Administration established the National Telecommunications and Information Systems Security Committee.[35] The Committee consists of 22 civilian and defense agencies. The National Security Agency was named National Manager. The Committee was tasked with setting operating policies governing the nation's telecommunications system, its classified information systems, and "other sensitive information." The Computer Security Act of 1987 was enacted in part out of congressional concern that the Committee might over-classify government-held information[36]. Did PDD-63, and does the Bush Administration's E.O.s, by couching critical infrastructure protection in national security terms and combining DOD and NSA professionals with civilian professionals in operative functions, whether in an interagency entity or in a civilian Department of Homeland Security, blur the distinction between classified and unclassified (or national security and civilian) systems which was a primary focus of the Computer Security Act of 1987?[37]

Costs. An estimate of the amount of money spent by the Federal government on critical infrastructure protection is included in the President's Annual Report to Congress on Combating Terrorism. The Bush Administration estimated that it requested $2.6 billion for critical infrastructure protection for FY2002. This is an estimate based on inputs supplied to OMB from the agencies. According to the report, spending on critical infrastructure protection has been increasing over for the last 4 years. Funding for most critical infrastructure protection activities is located in larger accounts and not readily visible in either agency budgets or in congressional appropriations. The estimate includes both physical and cyber protections. In the previous year's report, critical infrastructure protection activities were broken down further (e.g. system protections, training). The 2001 report does not break activities down further.

Many of the agencies' activities are part of on-going administrative duties. These activities, if not previously done (which appears to be the case in many agencies), will require the reallocation of personnel time and effort, presumably at the expense of other activities or supported by additional resources. The resources required to meet PDD-63 requirements are supposed to be part of the agencies' internal plans. Some of the costs will not be known until after vulnerability assessments are done and remedial actions determined.[38] Also, each agency must develop and implement education and awareness training programs. Agency costs

[35] National Security Decision Directive, NSDD-145. September 17, 1984.

[36] House Report 100-153(I).

[37] This point is made by the Electronic Privacy Information Center in its report, *Critical Infrastructure Protection and the Endangerment of Civil Liberties* (1998) and can be found on the Center's webpage at [http://www.epic.org/security/infowar/epic-cip.html].

[38] The Government Information Security Reform Act (Title X, Subtitle G in the FY2001 Defense Authorization Act, P.L. 106-398) requires agencies to report deficiencies in their information security programs as part of their performance review and to include in their report, how much it will cost to correct the deficiency. This, however, applies only to protection of information systems, and not to other critical assets of the agency.

may not be insignificant. According to OMB, the IRS alone estimated a vulnerability analysis of its systems will cost $58 million.[39] The Plan outlines efforts at the Department of Energy to improve its network security. Total costs were expected to be $80 million ($45 million for operational security measures). There are also those expenditures associated with the PDD-63 initiatives, such as the education and training programs (Federal Cyber Service).

In addition, the Bush Administration has begun assessing the technical, fiscal, and political feasibility of developing a parallel but separate government-only information network (dubbed Govnet). The purpose of the network would be to have increased security without hampering the operations of the commercial network. If the Bush Administration decides to pursue a separate government information network, additional resources would be required.[40]

Potential private sector costs are also unknown at this time.[41] Some sectors are already at the forefront in both physical and computer security and are sufficiently protected or need only marginal investments. Others are not and will have to devote more resources. The ability of certain sectors to raise the necessary capital may be limited, such as metropolitan water authorities which may be limited by regulation, or emergency fire which may function in a small community with a limited resources. Even sectors made up of large well capitalized firms are likely to make additional expenditures only if they can identify a net positive return on investment.

Affecting these business decisions will be issues of risk and liability. As part of its outreach efforts, the CIAO has helped the auditing, accounting, and corporate directors communities identify and present to their memberships the responsibilities governing board of directors and corporate officers have, as part of their fiduciary responsibilities, in managing the risk to their corporation's information assets. The Institute of Internal Auditors, the American Institute of Certified Public Accountants, the Information Systems Audit and Control Association and the National Association of Corporate Directors have formed a consortium and held "summits" around the country in an outreach effort. The main point of their discussion can best be summed up by the following expert from a paper presented at these summits:

> "The consensus opinion from our analysts is that all industries and companies should be equally concerned about information technology security issues because it is an issue that has an enormous potential to negatively impact the valuation of a company's stock...it must be the responsibility of corporate leaders to ensure these threats are actually being addressed on an ongoing basis.

[39] Conversation with OMB officials, 11 February, 1999.

[40] See, "Secure Network Proposal Stirs Debate Among Telecom Companies" in the Oct. 15, 2001 Daily Briefing on the GovExec.com web page: [http://www.govexec.com/dailyfed/1001/101501tj1.htm].

[41] The cyber security market is estimated at $10 billion in products and services (see "Picking the Locks on the Internet Security Market." Redherring.com. July 24, 2001). This probably includes, however, some government expenditures. It also does not include physical security measures.

> At the same time, the investment community must keep the issue front and center of management."[42]

There is also the question of downstream liability, or third party liability. In the denial-of-service attacks that occurred in early 2000, the attacks were launched from "zombie" computers; computers upon which had been placed malicious code that was subsequently activated. What responsibility do the owners of those "zombie" computers have to protect their systems from being used to launch attacks elsewhere? What responsibility do service providers have to protect their customers? According to some, it is only a matter of time before the courts will hear cases on these questions.[43]

Costs to the private sector may also depend on the extent to which the private sector is compelled to protect their critical infrastructure versus their ability to set their own security standards. The current thinking is the private sector should voluntarily join the effort. However, given the events of September 11, the private sector may be compelled politically, if not legally, to increase physical protections. But, what happens if a sector does not take actions the federal government feels are necessary? The National Strategy for Homeland Security stated that private firms will still bear the primary responsibility for addressing public safety risks posed by their industries. The Strategy goes on to state that in some cases, the federal government may have to offer incentives for the private sector to adopt security measures. In other cases, the federal government may need to rely on regulation.

Information Sharing. The information sharing considered necessary for critical infrastructure protection—internal to the federal government, between the federal government and the private sector, and between private firms—raises a number of issues.

In the past, information flow between agencies has been restrained at least three reasons: a natural bureaucratic reluctance to share, technological difficulties associated with compatibility, and legal restraints to prevent the misuse of information for unintended purposes. However, in the wake of September 11, and the apparent lack of information sharing that was exposed in reviewing events leading up to that day, many of these restraints are being reexamined and there appears to be a general consensus to change them. Not to downplay the importance and the difficulties in address these issues, the rest of this section will focus on issues associated with sharing information between the federal government and the private sector.

Since much of what is considered to be critical infrastructure is owned and operated by the private sector, implementing PDD-63 relies to a large extent on the ability of the private sector and the federal government to share information. However, it is unclear how open the private sector and the government will be in

[42] From an paper entitled *Information Security Impacting Securities Valuations*, by A. Marshall Acuff, Jr., Salomon Smith Barney Inc.

[43] See, "IT Security Destined for the Courtroom." Computer World.. May 21,2001. Vol 35. No. 21.

sharing information. The private sector primarily wants from the government information on potential threats which the government may want to protect in order not to compromise sources or investigations. In fact, much of the threat assessment done by the federal government is considered classified. For its part, the government wants specific information on vulnerabilities and incidents which companies may want to protect to prevent adverse publicity or reveal company practices. Success will depend on the ability of each side to demonstrate it can hold in confidence the information exchanged. According to the GAO testimony cited earlier, there is little or no formalized flow of information yet from the private sector to the federal government, in general, or the NIPC specifically.[44]

This issue is made more complex by the question of how the information exchanged will be handled within the context of the Freedom of Information Act (FOIA). The private sector is reluctant to share the kind of information the government wants without an exempting it from public disclosure under the existing FOIA statute. However, the non-government-organizations that actively oppose government secrecy are reluctant to expand the government's ability to to hold more information as classified or sensitive.[45] More recently, the environmental community has become concerned that without careful crafting of any exempting language, firms can shield from disclosure information they would otherwise be obliged to disclose to the public, or worse, be able to prevent the information from being used in any legal proceedings, by claiming it to be related to critical infrastructure protection. This has become a particular issue within the right-to-know community concerned with risks associated with toxic releases from plants using or producing toxic chemicals. The Administration now including the chemical industry as a critical infrastructure.

The National Strategy for Homeland Security makes reference to this issue. The Strategy assigns the Attorney General to convene a panel to propose legal changes necessary to provide reasonable assurance to the private sector that good faith disclosures about vulnerabilities and preparedness do not expose firms to liability, drops in share value or loss of competitive advantage. The Clinton Administration studied this issue as well, but never released an official position.

Finally, the information exchanged between private firms within the context of the Sector Coordinators and the ISACS raises antitrust concerns, as well as concerns about sharing information that might unduly benefit competitors.

Privacy/Civil Liberties? The PPCIP made a number of recommendations that raised concerns within the privacy and civil liberty communities. These included allowing employers to administer polygraph tests to their computer security personnel, and requiring background checks for computer security personnel. The PPCIP also recommended allowing investigators to get a single trap and trace court order to expedite the tracking of hacker communications across jurisdictions, if possible. Another area of concern is the monitoring network traffic in order to detect intrusions. Traffic monitoring has the potential to collect vast amount of information

[44] Op. Cit. General Accounting Office, Critical Infrastructure Protection.

[45] Op. cit. EPIC

on who is doing what on the network. What, if any, of that information should be treated as private and subject to privacy laws? While recognizing a need for some of these actions, the privacy and civil liberty communities have questioned whether proper oversight mechanisms can be instituted to insure against abuse.

The USA Patriot Act (i.e. the anti-terrorism bill passed October 26, 2001 as P.L. 107-56), passed in the wake of the September 11 attacks, contained a number of expansions in government surveillance, investigatory, and prosecutorial authority about which the privacy and civil liberties communities have had concern. Most of these issue are beyond the scope of this report.[46] However, included in the Act is the authority for investigators to seek a single court order to authorize the installation and use of a pen register or a trap and trace device anywhere in the country in order to "record or decode electronic or other impulses to the dialing, routing, addressing, or signaling information used in the processing or transmitting of wire or electronic communications..."[47] The law also defines a "computer trespasser" as one who accesses a "protected computer" without authorization and, thus, has no reasonable expectation to privacy of communications to, through, or from the protected computer.[48] The law goes on to stipulate the conditions under which someone under the color of law may intercept such communications.

The issue of allowing firms to conduct background checks, polygraph tests, and monitor personnel who have access to critical infrastructure facilities or systems lay dormant during the Clinton Administration. The National Strategy for Homeland Security resurrects it. The Strategy tasks the Attorney General to convene a panel with appropriate representatives from federal, state, and local government, in consultation with the private sector, to examine whether employer liability statutes and privacy concerns hinder necessary precautions. It is not clear if the Administration meant to include in the private sector representation labor and civil liberty groups.

Another issue is to what extent will monitoring and responding to cyber attacks permit the government to get involved in the day-to-day operations of private infrastructures? The PCCIP suggested possibly modifying the Defense Production Act (50 USC Appendix, 2061 *et seq*) to provide the federal government with the authority to direct private resources to help reconstitute critical infrastructures suffering from a cyber attack. This authority exists now regarding the supply and distribution of energy and critical materials in an emergency. Suppose that the computer networks managing the nation's railroads were to "go down" for unknown but suspicious reasons. What role would the federal government play in allocating resources and reconstituting rail service?

[46] See CRS Report *RS21051.Terrorism Legislation: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*,by Charles Doyle and *Terrorism and Civil Liberties*, by Charles Doyle in the Legal Issues/Law Enforcement section of the CRS Terrorism Briefing Book.

[47] See Section 216 of P.L. 107-56.

[48] See Section 217 of P.L. 107-56.

In a related matter, the National Strategy for Homeland Security also mentions that the Department of Homeland Security will undertake a study to evaluate mechanisms through which suspicious purchases of dual-use equipment and materials can reported and analyzed. Examples of dual-use equipment and materials included fermenters, aerosol generators, and protective gear. To some extent, this type of monitoring has been going in the area of explosives, fertilizer purchases, etc. The government also maintains a list of equipment that requires export licenses that include some of these same articles. This study would imply the possibility of expanding the monitoring of these transactions.

Congressional Actions

Congress's interest in protecting the nation's critical infrastructure spans its oversight, legislative, and appropriating responsibilities. Prior to September 11, much of the congressional activity regarding critical infrastructure protection focused on oversight. Legislatively, a few bills were introduced relating to critical infrastructure protection. H.R. 1158 would establish a National Homeland Security Agency along the lines recommended by the Hart-Rudman Commission. In a related effort, H.R. 1292, the Homeland Security Strategy Act of 2001 called for the President to develop a Homeland Security Strategy that protects the territory, critical infrastructure, and citizens of the United States from the threat or use of chemical, biological, radiological, nuclear, cyber or conventional weapons. H.R. 1259 would enhance the ability of the National Institute of Standards and Technology to improve computer security (NIST). Among its actions, the bill would authorize NIST, in consultation with other appropriate agencies, to assist agencies in responding to computer intrusions, to perform evaluation and tests of agency security programs and to report the results of those test to Congress, and to establish a computer security fellowship program. H.R. 2435 (similar to H.R. 4246 introduced in the 106th Congress) would exempt information related to cyber security in connection with critical infrastructure protection from FOIA. Its counterpart in the Senate is S. 1456. S. 1407 would support a National Infrastructure Simulation and Analysis Center (this was included in the USA Patriot Act). H.R. 3394 would authorize funding for NSF to support basic research in computer and network security, to establish computer and network security centers, and to support institutions of higher learning in establishing or improving computer and network security programs at all levels. The bill also authorizes funding for NIST to establish a program that would support computer security programs at institutions of higher learning that have entered into partnerships with for-profit entities and to support fellowships at those institutions in computer security.

Since September 11, a number of bills have been introduced to increase physical protections of various infrastructures: H.R. 2060, H.R. 2795, S. 1546 (agroterrorism), S. 1608 (waster water facility security), S. 1593 (R&D related to security at waste water facilities), H.R. 3178, H.R. 3227 (radiological contamination R&D), H.R. 2925 (P.L. 107-69, protection of dams and related facilities), S. 1214 and S. 1215 (port security), H.R. 2983 (security at nuclear facilities), S. 1447 (aviation security). For more information on these and other activities related to the security (primarily physical security) of specific infrastructures, see the Prevention: Security Enhancements section of the CRS Terrorism Briefing Book.

Congress is now taking up the proposed reorganization. H.R. 5005 is the Administration's version in House. The House has appointed a Select Committee on Homeland Security who will be responsible for reporting the bill to the House. A number of House Committees have offered recommendations to the Select Committee. The one primarily affecting Infrastructure Protection was a recommendation by the House Science Committee not to transfer the Computer Security Division from NIST. The Science Committee, along with the Armed Services Committee also suggested moving the Department of Energy's Energy Security and Assurance Program to the new Department. Also, a discussion draft of the Select Committee's mark provided a much more elaborate provision (Subtitle C in Title VII of H.R. 5005) on FOIA exemptions, similar to the bills that have been introduced in the House and Senate.

The Senate Government Affairs Committee is expected to release an amended version of S. 2452, introduced prior to the Administration's proposal, and reported last month. The reported version included a Directorate of Critical Infrastructure that would have many of the same responsibilities included in the other bills.

Appendix

Essentially, the Plan identified 10 “programs” under three broad objectives (see Table 3, below). Each program contained some specific actions to be taken, capabilities to be established, and dates by which these shall be accomplished. Other activities, capabilities, and dates were more general (e.g. during FY2001).

Table A.1. National Plan for Information Systems Protection Version 1.0

Goal: Achieve a critical information systems defense with an initial operating capability by December 2000, and a full operating capability by May 2003...that ensures any interruption or manipulation of these critical functions must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.

Objectives	**Programs**
Prepare and Prevent	ID critical infrastructures and interdependencies and address vulnerabilities
Detect and Respond	Detect attacks and unauthorized intrusions
	Develop robust intelligence and law enforcement capabilities consistent with the law
	Share attack warnings and information in a timely manner
	Create capabilities for response, reconstitution, and recovery
Build Strong Foundations	Enhance research and development in the above mentioned areas
	Train and employ adequate numbers of information security specialists
	Make Americans aware of the need for improved cyber-security
	Adopt legislation and appropriations in support of effort
	At every step of the process ensure full protection of American citizens’ civil liberties, rights to privacy, and rights to protection of proprietary information

For Additional Reading

CRS Report RS21026, *Terrorism and Security: Issue Facing the Water Infrastructure Sector*, by Claudia Copeland and Betsy Cody.

CRS Report RS21050, *Hazardous Materials Transportation: Vulnerability to Terrorists, Federal Activities and Options to Reduce Risks*, by Paul Rothberg.

CRS Report RS20272, *FEMA's Mission: Policy Directives for the Federal Emergency Management Agency*, by Keith Bea.

CRS Report RL30735, *Cyberwarfare*, by Steven Hildreth.

CRS Report RL30861, *Capitol Hill Security: Capabilities and Planning*, by Paul Dwyer and Stephen Stathis.

CRS Report RL31148, *Homeland Security: The Presidential Coordination Office*, by Harold Relyea.

CRS Report RL31150, *Selected Aviation Security Legislation in the Aftermath of the September 11 Attack*, by Robert Kirk.

CRS Report RL31151, *Aviation Security Technology and Procedures: Screening Passengers and Baggage*, by Daniel Morgan.

CRS Report RL31202, *Federal Research and Development for Counter Terrorism: Organization, Funding, and Options*, by Genevieve J. Knezo.

CRS Report RL31465, *Protecting Critical Infrastructure from Terrorist Attack: A Catalog of Selected Federal Assistance Programs*, Coordinated by John Moteff.