Order Code RL30153

Report for Congress

Received through the CRS Web

Critical Infrastructures: Background, Policy, and Implementation

Updated April 9, 2003

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

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). However, given the physical damage caused by the September 11 attacks and the subsequent impact on the communications, finance, and transportation services, physical protections of critical infrastructures is receiving greater attention.

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, 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 assumed continuation of many PDD-63 activities. E.O. 13231, which also established the President's Critical Infrastructure Protection Board, whose mission was to "recommend and coordinate programs for protecting information systems for critical infrastructures," was amended in February 2003. While retaining the same policy-related statements, the Board was eliminated.

On November 22, 2002, Congress passed legislation creating a Department of Homeland Security. The Department consolidates into a single department a number of offices and agencies responsible for implementing various aspects of homeland security. One of the directorates created by the legislation is responsible for Information Analysis and Infrastructure Protection.

Issues include whether to segregate cyber protection from physical protection organizationally, mechanisms for sharing information shared between the government and the private sector, costs, the need to set priorities, and whether or not the federal government will need to employ more direct incentives to achieve an adequate level of protection by the private sector and states, and privacy versus protection. This report will be updated as warranted.

Contents

List of Tables

Critical Infrastructures: Background, Policy, and Implementation

Latest Developments

The President's Critical Infrastructure Protection Board released the final version of the National Strategy to Secure Cyberspace in February 2003. The Strategy could be considered Version 2.0 of an earlier National Plan for Information Systems Protection released by the Clinton Administration in 2000. The Bush Strategy reflects input from the private sector and state and local governments and makes recommendations for actions that those sectors, as well as all stakeholders, may wish to take to help secure their share of the nation's information infrastructure.

Also in February 2003, the Office of Homeland Security released the National Strategy for The Physical Protection of Critical Infrastructures and Key Assets. This strategy complements the strategies aimed at protecting the nation's information infrastructure and is a key element of the nation's overall Homeland Security Strategy released in July 2002. For more discussion of both of the strategies, see the **Appendix**.

Also, on February 28, the Bush Administration released Executive Order 13286, which amended Executive Order 13231 and effectively eliminated the President's Critical Infrastructure Board and the position of Special Advisor to the President for Cyberspace Security. The duties of the Board and the Special Advisor were subsumed by the Department of Homeland Security and the Homeland Security Council.

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. 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 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.

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. To date, the ability to detect and deter unauthorized access to computer systems is limited. 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.[4]

Prior to September 11, critical infrastructure protection was synonymous with cyber security to many people. Initial policies, and implementation of those policies,

---

[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. More recently, the so-called Slammer worm, which attacked a known vulnerability in Microsoft's SQL Server Service, and resulted in tying up infected servers, led to disruptions in ATM machines, airline online ticketing systems, and newspaper publishing. See *http://www.washingtonpost.com/wp-dyn/articles /A46928-2003Jan26.html.*

[4] The Director of the Central Intelligence Agency testified before the Senate Committee on 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.

focused on cyber security. 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.[5] This report provides an historical background and tracks the evolution of such an overall policy and its implementation. 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.[6] 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.[7] 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.

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

---

[5] 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.

[6] Executive Order 13010.Critical Infrastructure Protection. Federal Register. Vol 61. No. 138. July 17, 1996. pp. 3747-3750. Concern about the security of the nation's information infrastructure and the nation's dependence on it preceded the establishment of the Commission.

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

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)[8] 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."[9]

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.[10] In addition, the PDD identified four activities where the federal government controls the critical infrastructure: internal security and federal law enforcement; foreign intelligence; foreign affairs; and national defense.

---

[8] 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].

[9] Ibid.

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

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**. Each of the activities performed primarily by the federal government also were assigned a lead agency who was to 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 also assigned duties to the **National Coordinator** for Security, Infrastructure Protection, and Counter-terrorism.[11] The National Coordinator reported to the President through the Assistant to the President for National Security

[11] The National Coordinator position was created by Presidential Decision Directive 62, "Combating Terrorism." PDD-62, which is classified, codifies and clarifies the roles and missions of various agencies engaged in counter-terrorism activities. The Office of the National Coordinator was established to integrate and coordinate these activities. The White House released a fact sheet on PDD-62 on May 22, 1998.

Affairs.[12] Among his many duties outlined in PDD-63, 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 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 was 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 supported the National Coordinator's efforts to integrate the sectoral plans into a National Plan, supported individual agencies in developing their internal plans, helped coordinate a national education and awareness programs, and provided 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

---

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

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 an equivalent **Information Sharing and Analysis Center(s)** operated by the private sector, which PDD-63 encouraged the private sector to establish.

While the FBI was given the lead, the NIPC also included 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 was to have been placed in direct support of either the Department of Defense or the Intelligence Community.

Quite independent of PDD-63 in its origin, but clearly complimentary in its purpose, the FBI offers a program called **INFRAGARD** to private sector firms. 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 FBI has set up local INFRAGARD chapters that can work with each other and regional FBI field offices. In January, 2001, the

---

[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.

FBI announced it had finished establishing INFRAGARD chapters in each of its 56 field offices. Rather than sector-oriented, INFRAGARD is geographically-oriented.

It should also be noted that the FBI 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.[14]

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.[15]

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

---

[14] Testimony by Michael Vatis before the Senate Judiciary Committee, Subcommittee on Technology and Terrorism. Oct. 6, 1999. This programs has since been transferred to the Department of Homeland Security.

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

of the reason's cited for this was a desire to keep agencies responsible for their own computer security.[16]

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. As discussed below, the Bush Administration changed its position in June 2002, and proposed a new department along the lines of that proposed by the Hart/Rudman Commission and Congress.

Post-September 11. Soon after the September 11 terrorist attacks, President Bush signed two Executive Orders relevant to critical infrastructure protection. These have since been amended to reflect changes brought about by the establishment of the Department of Homeland Security (see below). The following is brief discussion of the original E.O.s and how they have changed.

E.O. 13228, signed October 8, 2001 established the **Office of Homeland Security**, headed by the **Assistant to the President for Homeland Security**.[17] 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.

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.[18] 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

---

[16] 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.

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

[18] 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.

Homeland Security, at the direction of the President. The Assistant is also the official recorder of Council actions and Presidential decisions.

In January and February 2003, this E.O. was amended (by Executive Orders 13284 and 13286, respectively). The Office of Homeland Security, the Assistant to the President, and the Homeland Security Council were all retained. However, the Secretary of Homeland Security was added to the Council. The duties of the Assistant to the President for Homeland Security remain the same, recognizing the statutory duties assigned to the Secretary of Homeland Security as a result of the Homeland Security Act of 2002 (see below).

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."[19] This Order also established the **President's Critical Infrastructure Protection Board**. The Board's responsibility was 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 was directed to propose a National Plan on issues within its purview on a periodic basis, and, in coordination with the Office of Homeland Security, review and make recommendations on that part of agency budgets that fall within the purview of the Board.

The Board was chaired by a **Special Advisor to the President for Cyberspace Security**.[20] The Special Advisor reported 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, was to propose policies and programs to appropriate officials to ensure protection of the nation's information infrastructure and to coordinate with the Director of OMB on issues relating to budgets and the security of computer networks.

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.

---

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

[20] President Bush designated Richard Clarke.

Subsequent amendments to this E.O. (by E.O. 13286) abolished the President's Board and the position of Special Advisor. The Advisory Council was retained, but now reports to the President through the Secretary of Homeland Security.

In many respects, the Bush Administration policy and approach regarding critical infrastructure protection represents a continuation of PDD-63. The fundamental policy statements were the essentially the same: the protection of infrastructures critical to the people, economy, essential government services, and national security. Also, the stated goal of the government's efforts is to ensure that any disruption of the services provided by these infrastructures be infrequent, of minimal duration, and manageable. The infrastructures identified as critical were essentially the same (although expanded). A Council made up of private sector executives, academics, and State and local officials was established to advise the President. The Critical Infrastructure Assurance Office (CIAO) and the National Infrastructure Protection Center (at the FBI) were left in place (and later moved to the Department of Homeland Security), as were the liaison efforts between lead agencies and the private sector and State and local governments, and the structures set up for information sharing.

The primary difference, at first at least, was the segregation of cyber security from the rest of the critical infrastructure protection function. As stated, earlier, prior to September 11, the focus of critical infrastructure protection was cyber security. Following September 11, physical security became more of and issue, and cyber security now appears to be integrated into an overall critical infrastructure protection organizational structure.

National Strategy for Homeland Security. In July 2002, the Office of Homeland Security released a *National Strategy for Homeland Security.* The Strategy covers all government efforts to protect the nation against terrorist attacks of all kinds. It identifies protecting the nation's critical infrastructures and key assets (a new term, different as implied above by the FBI's key asset program) as one of six critical mission areas. The Strategy expanded upon the list of infrastructure considered to be critical to include the chemical industry, postal and shipping services, and the defense industrial base. It also introduced a new class of assets, called key assets, which are potential targets whose destruction may not endanger vital systems, but could create local disaster or profoundly affect national morale. Such assets could include schools, court houses, individual bridges, or state and national monuments.

The Strategy reiterates many of the same policy-related activities as mentioned above: working with the private sector and other non-federal entities, naming those agencies that should act as liaison with the private sector, assessing vulnerabilities, and developing a national plan to deal with those vulnerabilities. The Strategy did not create any new organizations, but assumed that a Department of Homeland Security would be established.

Department of Homeland Security

On November 22, Congress passed the Homeland Security Act (P.L. 107-296), establishing a **Department of Homeland Security**. The Act assigned to the new

Department the mission of preventing terrorist attacks, reducing the vulnerability of the nation to such attacks, and responding rapidly should such and attack occur. The Act essentially consolidated within one department a number of agencies that have had, as part of their mission, homeland security-like functions (e.g. Border Patrol, Customs, Transportation Security Agency). The full impact of the Act is beyond the scope of this report. The following discussion focuses on those provisions relating to critical infrastructure protection.

In regard to critical infrastructure protection the Act transfered the following agencies and offices to the new department: the NIPC (except for the Computer Investigations and Operations Section), CIAO, FedCIRC, the **National Simulation and Analysis Center (NISAC),**[21] other energy security and assurance activities within DOE, and the **National Communication System (NCS).**[22] These agencies and offices shall be integrated within the **Directorate of Information Analysis and Infrastructure Protection** (one of four Directorates established by the Act).[23] Notably, the Transportation Security Administration (TSA), who is responsible for securing all modes of the nation's transportation system, is not part of this Directorate (it has been placed within the Border and Transportation Security Directorate). The Directorates shall be headed by someone of Undersecretary rank. Furthermore, the Act designated that within the Directorate of Information Analysis and Infrastructure Protection, there shall be both an Assistant Secretary for Information Analysis, and an **Assistant Secretary for Infrastructure Protection**.[24]

---

[21] The NISAC was established in the USA PATRIOT Act (P.L. 107-56), Section 1062. The Center builds upon expertise at Sandia National Laboratory and Los Alamos National Laboratory in modeling and simulating infrastructures (namely energy infrastructures) and the interdependencies between them.

[22] The NCS is not 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 later in this report, and which serves as the telecommunications ISAC, is an operational entity within the NCS.

[23] The other directorates included: **Science and Technology**, **Border and Transportation Security** and **Emergency Preparedness and Response**.

[24] In a more detailed discussion of the Administration's original reorganization proposal (*The Department Of Homeland Security*, June 2002), the Administration provided an organization chart showing what it then called 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. How this Directorate eventually gets organized remains to be seen.

Among the responsibilities assigned the Directorate of Information Analysis and Infrastructure Protection were:

- to access, receive, analyze, and integrate information from a variety of sources in order to identify and assess the nature and scope of the terrorist threat;
- to carry out comprehensive assessments of the vulnerabilities of key resources and critical infrastructure of the United States;
- to integrate relevant information, analyses, and vulnerability assessments in order to identify priorities for protective and support measures;
- to develop a comprehensive national plan for securing key resources and critical infrastructures;
- to administer the Homeland Security Advisory System;
- to work with the intelligence community to establish collection priorities; and,
- to establish a secure communication system for receiving and disseminating information.

In addition, the Act provided a number of protections for certain information (defined as critical infrastructure information) that non-federal entities, especially private firms or ISACs formed by the private sector, voluntarily provide the Department. Those protections included exempting it from the Freedom of Information Act, precluding the information from being used in any civil action, exempting it from any agency rules regarding ex parte communication, and exempting it from requirements of the Federal Advisory Committee Act.

The Act basically built upon existing policy and activities. Many of the policies, objectives, missions, and responsibilities complement those already established (e.g. vulnerability assessments, national planning, communication between government and private sector, and improving protections).

The Act represented a major reorganization. Many entities, some with multiple missions, were transferred or were 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 transfers associated with infrastructure protection perhaps were less disruptive as others (such as Coast Guard, or U.S. Customs). CIAO, FedCIRC, and NIASC are all relatively new organizations, with relatively narrow missions, and were transferred fully to the new organization. While they are not likely to maintain their current identities as separate offices, the functions they have been performing are likely to continue.

The NIPC, however, was not transferred intact. The transfer leaves the Computer Investigations and Operations unit within NIPC at the FBI, while moving the Analysis and Warning Section and the Training, Outreach, and Strategy Section function to the Department. The FBI had received some criticism for its management of NIPC. In the press, the FBI had been accused of being reluctant to share information with other agencies. According to a General Accounting Office (GAO) report, the FBI had trouble recruiting people from 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, through its Investigations and Operations unit, had provided valuable support to FBI field investigations.

Although not specified in Homeland Security Act legislation, the NIPC's role in managing the FBI's Key Asset Initiative was also transferred to the Department of Homeland Security. The program had been implemented primarily through FBI Field Offices. The Department of Homeland Security will take over and standardized the information collection process and management of the database.

Splitting the functions of the NIPC should not have an adverse impact on the FBI. The Investigations function left behind has been a traditional mission area for the FBI, while those transferred represented relatively new missions. From the Department of Homeland Security's perspective, however, the transfer of functions came without the transfer of many human resources which will have to be reconstituted.[25]

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 from DOD to the Department of Homeland Security (which is the immediate impact of the transfer) 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.

Policy Implementation

There is an element of continuity in the policies and activities undertaken by the Clinton and Bush Administrations. For example, the Bush Administration maintains the effort to communicate with infrastructure operators through ISACs, and, although it made some changes to accommodate the existence of the Department of Homeland Security, maintains certain lead agencies as the main liaison with certain sectors. The following discusses the implementation of major elements of PDD-63 and the Bush Administration's policy as policy and action continue to evolve.

Lead Agencies and Selection of Sector Liaison Officials and Functional Coordinators. The National Strategy for Homeland Security, released by the Bush Administration in July 2002, maintained the role of lead agencies as outlined in PDD-63, with the then proposed Department of Homeland Security acting

---

[25] Testimony of Michael Vatis before the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, April 8, 2003. Vatis's testimony notes that while the transfer of the NIPC functions involved the transfer of over 300 positions, only 10 to 20 people actually transferred. What is not clear is if the number of positions transferred from NIPC include the Investigations people that stayed at FBI. If so, then the loss in analytical capacity may not be as great as it sounds. In any event, in its budget justification, the Directorate for Information Analysis and Infrastructure Protection is asking for funds to fill 226 positions for intelligence and analysis and vulnerability assessments.

as coordinator of their efforts. However, the Strategy did shift liaison responsibilities for some sectors to the new Department.[26] 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

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

[26] There was some debate on how many sectors should be transferred to the new department. See, *Ridge Says EPA Should Lose Authority to Evaluate Vulnerability of Industrial Facilities*, Inside EPA, June 25, 2002.

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.

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.[27] 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.

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.[28] The Order was rescinded by the Bush Administration before the Council could meet. In Executive Order 13231,[29] President Bush established a National Infrastructure Advisory Council (with the same acronym, NIAC) whose functions are similar to those of the Clinton Council. On September 18, 2002, President Bush announced his appointment of 24 individuals to serve on Council.[30] The E.O. amending 13231 makes some minor modifications to NIAC.

---

[27] 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 was referenced in the *National Plan for Information Systems Protection*. See, **National Critical Infrastructure Plan**, below.

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

[29] 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.

[30] See White House Press Release, September 18, 2002.

Primarily, the Council now reports to the President through the Secretary of Homeland Security

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

Internal Agency Plans. There had been some confusion about which agencies were required to submit critical infrastructure plans. PDD-63 directed 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 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 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. Project Matrix continues.

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 not 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. Two years later, the General Accounting Office reported that four of the agencies they reviewed for the House Committee on Energy and Commerce (HHS, Energy, Commerce, and EPA) had still not yet identified their critical assets and operational dependencies, nor have they set any deadlines for doing so.[31]

According to the National Plan for Information Systems Protection, 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 have been budgeted for and submitted as part of the agencies' FY2001 budgets submissions to the Office of Management and Budget and every year thereafter.

As another indication that infrastructure protection and cyber protection are sometimes considered synonymous, the agencies' internal critical infrastructure planning process has been melded with the agencies' computer security planning process (as reauthorized by the Federal Information Security Management Act of 2002, included in Title III of E-Government Act of 2002, P.L. 107-347) and their continuity of operations planning.

---

[31] U.S. General Accounting Office, Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors. Report to the Committee on Energy and Commerce, House of Representatives. GAO-03-233. February 2003. pp4-5.

National Critical Infrastructure Plan. PDD-63, the National Strategy for Homeland Security, and the Homeland Security Act each have called for the development of a comprehensive national infrastructure protection plan. However, reflecting the initial emphasis on addressing vulnerabilities associated with information networks, the first two national strategies focused primarily on protecting information systems. In 2000, the Clinton Administration released Version 1.0 of a *National Plan for Information Systems Protection* in January 2000.[32] The Plan focused primarily on cyber-related efforts within the federal government. In September 2002, the Bush Administration, through the President's Critical Infrastructure Protection Board, released a draft of *The National Strategy to Secure Cyberspace*. The latter was released in its final form in February 2003, and could be considered Version 2.0 of the Clinton-released Plan. It addressed all stakeholders in the nation's information infrastructure, from home users to the international community, and included input from the private sector, the academic community, and state and local governments. Also in February 2003, the Office of Homeland Security released the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. A short synopsis of the two Strategies released in 2003 is given in the Appendix. The Department of Homeland Security plays a predominant role in implementing both of these strategies.

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 evolved into each sector having 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 to form a banking and finance industry ISAC. The group has contracted with an internet service provider[33] (ISP) to design and operate the ISAC. Individual firms feed raw computer network traffic data to the ISAC. The ISP maintains a database 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 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

---

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

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

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.[34]

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 oil and gas industry established a separate ISAC in 2001, choosing a model more like the banking and finance sector (i.e. managed by Global Integrity).

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, with help from an EPA grant, officially launched the WaterISAC in December 2002. The ISAC is run by a Board of water utility managers appointed by 8 national drinking water and waste water associations.

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.

As well as those mentioned above, a number of other sectors, not originally included in PDD-63, but subsequently mentioned by the Bush Administration as infrastructures in need of protection to counter-terrorism, have formed ISACs. These include the food and chemical industries.

In addition to these individual sectors setting up or contemplating ISACs, the private sector, in December 1999, formed a **Partnership for Critical Infrastructure Security** to share information and strategies and to identify interdependencies across sectoral lines. The Partnership is a private sector initiative. Five working groups were established (Interdependencies/Vulnerability Assessment, Cross-Sector Information Sharing, Legislation and Policy, Research and Development, and Organization). The federal government is not officially part of the Partnership, but

---

[34] 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.

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. The Partnership helped coordinate the private sector's input to the National Strategy to Secure Cyberspace.

Issues

Cyber vs. Physical Vulnerabilities and Protection. The issue is not cyber protection or physical protection of the nation's critical infrastructure. The issue that has arisen recently is how best to organize to ensure that both are adequately covered. Both the President's Commission on Critical Infrastructure Protection and PDD-63 addressed both the physical and cyber vulnerabilities of the nation's critical infrastructures. However, in the recommendations made, the organizational structures developed, and the early planning required, emphasis was given to cyber vulnerabilities and protection. This was because, at the time, there was a consensus that the cyber area was a new vector of vulnerability and one that was not being adequately addressed. Many spoke of critical infrastructure protection and cyber protection synonymously. While physical threats and protections were not dismissed, it was stated that these were better understood and processes already in place to address them. This changed after September 11, 2001, when the physical threat of and vulnerability to physical attacks was made apparent.

In E.O. 13228 and E.O. 13231, both released in October 2001, the responsibilities for physical protection and cyber protection of the nation's critical infrastructure was split. The Office of Homeland Security, the Assistant to the President for Homeland Security, and the Homeland Security Council were given responsibility for physical protection. The President's Board on Critical Infrastructure Protection and the Assistant to the President for Cybersecurity was given cyber protection (including the physical protection of information network assets). Each developed a National Strategy to cover their area of responsibility.

When the Bush Administration decided to support the establishment of a Department of Homeland Security, in June 2002, it retained this split organizationally by proposing that the office responsible for Infrastructure Protection be further divided with someone responsible for Physical Assets and someone responsible for Telecommunications and Cybersecurity. The National Strategy for Homeland Security, released in July 2002, stated that "securing cyberspace poses unique challenges..." and that "the Department of Homeland Security will place an especially high priority on protecting our cyber infrastructure."

However, in February 2003, while working to stand up the Department of Homeland Security, the Bush Administration released E.O. 13286, which amended E.O. 13231 and effectively abolished both the President's Board on Critical Infrastructure and the position of Assistant to the President for Cybersecurity. This has some in the cyber security realm concerned that cyber security will be absorbed within the effort to provide physical protections for the nation's critical infrastructure

and not receive the special attention they think it requires.[35] It is not yet clear how the Department's Directorate of Information Analysis and Infrastructure Protection will eventually be structured.

What is Critical and Needs Protection and How Do We Decide? The term critical infrastructure has been defined in most of the official documents mentioned in this report. The definition has changed somewhat over time.[36] The USA PATRIOT Act provided the following definition:

> The term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters.

The list of infrastructures that have been selected as fitting this definition has grown as well, from seven in the Commission report to thirteen (where it has currently stabilized) in the National Strategy for Homeland Security. These thirteen are

- Agriculture
- Food
- Water
- Public Health
- Emergency Services
- Government
- Defense Industrial Base
- Energy
- Transportation
- Banking and Finance
- Chemicals and Hazardous Materials
- Postal and Shipping

In addition, the National Strategy for Homeland Security raised the issues of key assets and national morale. Key assets are those "whose destruction would not endanger vital systems, but could create local disaster or profoundly damage our Nation's morale." These could include prominent national, state, or local monuments and icons. These could also include nuclear power plants or other "localized" facilities that deserve protection because of their destructive potential or their value to the local community.

The National Strategy for Homeland Security also commits the federal government to work closely with state and local governments to develop and apply compatible approaches to ensure protection for critical assets...at all levels of society. For example, schools, courthouses, and bridges are critical to the communities they serve.

---

[35] Testimony of Michael Vatis before the Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. April 8, 2003. See page 4 of his testimony.

[36] For a discussion of how the definition has changed slightly over time, see CRS Report RL31556, *Critical Infrastructures: What Makes An Infrastructure Critical?*.

However, it is not practical to try and protect all of these assets to the same degree. So how will priorities be set and protective measures allocated? According to the National Strategy for Homeland Security, a consistent methodology will be developed and applied to focus the federal government's efforts. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets makes mention of developing a uniform methodology for identifying facilities, systems and functions with national-level criticality to help establish federal, state, local, and private sector protection priorities. Such a methodology has not yet been articulated (although the Office of Management and Budget does apply criteria in its combating terrorism budget analysis, see below).

How Much Will It Cost and Who Pays? An estimate of the amount of money the Federal government spends on critical infrastructure protection is included in the President's *Annual Report to Congress on Combating Terrorism*.[37] Funding for Critical Infrastructure Protection was estimated at $3.2 billion for FY2002 and the Administration request for FY2003 was $3.9 billion (see Table A.1. in the **Appendix**). Most of this is associated with cyber security within the federal government. It also includes funding of research and development, training (e.g. Scholarship for Service)[38], outreach, etc.

The report makes a distinction between critical infrastructure protection and other infrastructure-related protection that may be confusing. The Report aggregates funds for three different *programs*—Combating Terrorism, Critical Infrastructure Protection, and Continuity of Operations. The Combating Terrorism program includes activities in 5 categories/mission areas, two of which are physical security of government facilities and workers, and physical protection of the national populace and national infrastructure. OMB does not consider the activities supported in these latter two categories as critical infrastructure protection, although the description of the activities might imply that it should. For example, included in the physical protection of the national populace and infrastructure category are activities taken to help protect banking and finance, water, telecommunications, transportation, and energy production and distribution. Much of what is spent on new airport security is aggregated in this category. So, too, according to the report, are activities by the Department of Energy to protect the supply and transmission of all forms of energy. The distinction between these activities and critical infrastructure protection is that to be considered as a critical infrastructure protection activity, the asset being protected must be critical at the national level (i.e. incapacitation would require restoration within 72 hours, disruption would have serious consequences on critical government operations and/or society's quality of life, or outage would interrupt

---

[37] OMB aggregates these numbers based on input from relevant agencies. In most cases, activities associated with critical infrastructure protection are funded as part of larger accounts and are not readily visible in either agency budgets or in congressional appropriations.

[38] Scholarship for Service is a program initiated during the Clinton Administration to support the development of computer security expertise within the federal government. Funds are made available to institutions of higher learning to develop computer security programs and to support students, who pledge to work a stint in the federal government. The program also supports continuing education for federal workers in computer security.

information flows or service provision essential to government operations or the public at large). A public telephone switch or the electric power grid would be considered critical.[39] An inventory control system would not. The provision of fences or surveillance cameras at tunnels or bridges, or at nuclear power plants, would apparently fall within the physical protection category of Combating Terrorism. According to the FY2002 report, funding for the Combating Terrorism activities related to the physical protection of the government and national populace totaled $9.6 billion in FY2002 and the request for FY2003 was $14. 6 billion.

It is not known how much money states and localities are spending on what they consider to be critical infrastructure protection. According to the National Strategy on Homeland Security, the National Governors Association estimated that states had spent $6 billion between September 11, 2001 and the end of 2002 on all homeland security-related activities. States have made it clear that their budgets, especially in the current economic environment, make these expenditures difficult. The National Strategy for Homeland Security and the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets recognize that while the federal government must focus on protecting assets that have a national importance, states may need help in protecting their assets as well. Much of the federal assistance to states so far have been for preparedness activities focused mostly on first responders and dealing with weapons of mass destruction. The USA PARTIOT Act established a federal grant program specifically for this purpose. The grant program, called the State Homeland Security Grant Program is managed by the Office for Domestic Preparedness (now part of the Department of Homeland Security). The grant will support, among many other items, the purchase of equipment, including equipment used for enhancing the physical protection of critical infrastructure.

Potential private sector costs are unknown at this time.[40] 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

---

[39] The report mentions that the government's Critical Infrastructure Program (CIP) focuses on information infrastructure and the physical assets that support it. The implication is that the CIP activities counted in the report also focus on the protection of the information infrastructure. However, an OMB official has clarified (per phone conversation, November 7, 2002) that the CIP also includes the protection of assets other than information assets.

[40] 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.

responsibilities governing board of directors and corporate officers have, as part of their fiduciary responsibilities, to manage 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. At the same time, the investment community must keep the issue front and center of management."[41]

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.[42]

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

---

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

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

In the past, information flow between agencies has been restrained for 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, given 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. Some changes have been as a result of the USA PATRIOT Act (including easing the restrictions limiting the sharing of information between national law enforcement agencies and those agencies tasked with gaining intelligence of foreign agents). The legislation establishing the Department of Homeland Security also authorizes efforts to improve the ability of agencies within the federal government to share information.

Since much of what is considered to be critical infrastructure is owned and operated by the private sector, critical infrastructure protection 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 sharing information. The private sector primarily wants from the government information on specific 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 revealing 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.[43]

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.

The Homeland Security Act protects information, defined as critical infrastructure information, voluntarily provided the Department of Homeland Security not only from FOIA, but also prohibits from being used in any civil action against the provider, exempts from any agency rules regarding ex parte communications, and exempts it from following under the requirements of the Federal Advisory Committee Act. It only can be shared with other entities in fulfillment of their responsibilities in homeland security, and any unauthorized disclosure by a federal government official can lead to imprisonment. Also, these disclosure rules take precedent over any State rules.

The Act defines critical infrastructure information to include:

---

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

- actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure by either physical or computer-based attack that violates federal or state law, harms interstate commerce, or threatens public health and safety;
- the ability of critical infrastructures to resist such attacks;
- any planned or past operational problem or solution regarding critical infrastructure including repair, recovery, reconstruction, insurance, or continuity to the extent it relates to such interference, compromise, or incapacitation.

The submittal is considered voluntary if it was done in the absence of an agency's exercise of legal authority to compel access to or submission of such information.

The FOIA exemption is not without its critics. 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.[44] These critics feel that language agreed upon in the final legislation is too broad (covers too much material and offers too many protections) and is unnecessary given current restrictions on the disclosure of information contained in the FOIA statute and case law. More recently, the environmental community has become concerned that the language could allow firms to 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, which are now being considered as a critical infrastructure.[45] It is not clear if this is the case, since the Act also states that other agencies or third parties may receive similar information by other lawful means and may use it any appropriate legal manner.

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

There is also a technical dimension to all of this information sharing that is suppose to occur. Once collected, the information is stored in different databases, utilizing different technologies. Integrating these databases while controlling access will not be a trivial technical and managerial task.

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

---

[44] Op. cit. EPIC

[45] For more discussion of these issues, see CRS Report, RL31547, *Critical Infrastructure Information Disclosure and Homeland Security*, by John D. Moteff and Gina Stevens.

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 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, some of the provisions impact directly the ability to track, in real time or after the fact, computer hackers. This includes provisions giving investigators the authority 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. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets also mentions exploring the possibility of establishing national standards by which to check the backgrounds of personnel with access to critical infrastructures.

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

---

[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.

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?

In a related matter, the National Strategy for Homeland Security and the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets 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 Action

Congress' interest in protecting the nation's critical infrastructure spans its oversight, legislative, and appropriating responsibilities. Because the scope of critical infrastructure protection extends across many committee jurisdictions, many hearings, bills, and appropriations have dealt with only certain elements of the issue. Since much of the nation's infrastructure is owned or operated by the private sector, much of its activity has focused on oversight of the governments efforts to coordinate with the private sector.

After September 11, Congress passed legislation that touched upon some elements of critical infrastructure. For example, it clarified the monetary threshold that triggers prosecution for computer crimes and increases penalties for those crimes. Congress also gave more flexibility to investigators to track computer hackers, and in those cases where the federal government has some authority, provided for increased protections (e.g. drinking water, nuclear power plants, ports).

Also, because much of the infrastructure is owned and operated by the private sector, Congress has not had to appropriate large amounts of resources to infrastructure protection to date. For the most part appropriations are directed at protecting critical federal assets. The FY2003 Consolidate Appropriations Resolutions (P.L. 108-7) included grant money for states to help protect infrastructures in their jurisdictions. There have also been appropriations directed at improving the nation's expertise in computer security. At some point Congress may have to consider whether the private sector, or other non-federal entities, require more than market incentives to affect an appropriate level of protection.

The 108th Congress, exercising its oversight responsibility to monitor the establishment of the new Department of Homeland Security, could use the two National Strategies released in February as a roadmap for overseeing federal efforts in critical infrastructure protection.

For Additional Reading

CRS Report RL31556, *Critical Infrastructures: What Makes an Infrastructure Critical?*, by John Moteff, Claudia Copeland, and John Fischer

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

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

CRS Report RL31466, *Homeland Security Department:U.S. Department of Agriculture Issues*, by Jean Rawson.

CRS Report RL31530, *Chemical Plant Security*, by Linda-Jo Schierow.

CRS Report RL31542, *Homeland Security–Reducing the Vulnerability of Public and Private Information Infrastructures to Terrorism: An Overview*, by Jeffrey Seifert.

CRS Report RS21131, *Nuclear Power Plants: Vulnerability to Terrorist Attack*, by Carl Behrens.

CRS Report RL31534, *Critical Infrastructure Remote Control Systems and the Terrorist Threat*, by Dana Shea (Consultant).

CRS Report RL31294, *Safeguarding the Nation's Drinking Water: EPA and Congressional Actions*, by Mary Tiemann.

CRS Report RL31375, *Meeting Public Spectrum Needs*, by Linda Moore.

CRS Electronic Briefing Book, *Terrorism*, "Electric Utility Infrastructure," by Amy Abel and Mark Holt.

CRS Report RL31787, *Information Warfare and Cyberwar: Capabilities and Related Policy Issues*, by Clay Wilson.

CRS Report RL31733, *Port and Maritime Security: Background and Issue for Congress*, by John Fritelli.

CRS Electronic Briefing Book, *Terrorism*, "Aviation Security," by Bartholomew Elias and Daniel Morgan.

Appendix

Federal Funding for Critical Infrastructure Protection

Table A.1. Critical Infrastructure Protection Funding by Department

(millions$)

Department	FY98 actual	FY99 actual	FY00 actual	FY01 actual	FY02 enacted	ERF**	FY03 request
Agriculture	5.20	9.90	8.20	21.22	49.01	90.08	12.78
Commerce	9.10	21.81	14.40	27.94	30.10	10.25	50.69
Education	3.59	4.45	6.70				
Energy	3.80	11.90	28.10	48.41	46.25	0.00	71.79
EOP	0.05	0.58	0.48	0.16	1.80	123.00	42.50
EPA	0.00	0.24	0.70	2.15	3.35	121.00	41.67
FEMA	0.00	0.00	0.40	1.55	1.47	0.00	1.47
GSA	0.00	3.00	1.00	7.98	13.48	0.00	19.58
HHS	37.00	44.50	69.60	84.34	96.75	0.00	87.19
Interior	1.29	1.60	2.10	2.60	3.79	0.00	0.38
Justice	25.80	55.30	42.20	72.29	80.41	73.83	153.87
Labor	3.80	5.40	7.90	13.37	16.58	5.88	23.80
NASA	40.00	42.00	66.00	116.00	112.00	108.50	133.00
NSF*	19.15	21.42	26.65	205.15	209.69	0.00	203.73
National Security	926.40	1217.70	1404.10	1824.13	2254.49	514.27	2343.38
NRC	0.00	0.20	0.00				
OPM	0.00	0.00	0.90	0.85	0.00	0.00	0.00
Social Security	60.70	57.10	48.90	73.83	105.60	7.50	129.16
State	6.00	19.00	40.00				
Transportation	21.50	24.40	44.50	78.24	89.44	107.70	487.85
Treasury	31.50	50.10	47.40	55.45	34.95	16.19	42.72
Corps of Engineers				0.00	0.00	138.60	65.00
Veterans Affairs	0.00	0.00	2.00	17.54	23.02	0.00	28.58
Grand Total	1194.88	1590.60	1862.23	2653.20	3172.18	1316.80	3939.14

Sources: For FY2001 - FY2003 request, OMB, Annual Report to Congress on Combating Terrorism, June 24, 2002. For FY1998-FY2000, OMB, Annual Report to Congress on Combating Terrorism, July 2001. *NSF figures for FY1998-FY2000 come from May 2000 report.**ERF is the Emergency Response Fund, the supplemental passed after 9/11.

National Strategy to Secure Cyberspace

This Strategy identified five priority areas:

- National Cyberspace Security Response System
- National Cyberspace Security Threat and Vulnerability Program
- National Cyberspace Security Awareness and Training Program
- Securing Government's Cyberspace
- National Security and International Cyberspace Security Cooperation

Within each of these priorities are a set of actions or recommendations for action. A few of these are highlighted below.

National Cyberspace Security Response System: Such a system would be an informal collaborative network of public and private organizations that would detect potentially damaging activity in cyberspace, analyze exploits and warn potential victims, coordinate a national response if necessary, and restore essential services. The Strategy uses the air defense system over North America as an analogy. Participants in such a system would include existing government and private computer incident response teams, private information sharing and analysis centers, and state and local entities. To some extent this capability exists in bits and pieces all over the country, and works informally relatively well when vulnerabilities are found and incidents occur. What is lacking most is a strategic view of the Internet as a whole and a plan for determining when a cyber attack reaches a level that threatens national or economic security and how to respond to such an attack. The Department of Homeland Security has been given the lead to coordinate efforts to establish such a capability.

National Cybersecurity Threat and Vulnerability Awareness Program: This priority area envisions a number of activities to ensure that information on threat and vulnerabilities is widely disseminated and that those threats and vulnerabilities be reduced.

In regard to facilitating a broad dissemination of information, the Strategy recommends that the government, academia, and the private sector work together to make it easier for all users of cyberspace, whether a home user, a large conglomerate, or a federal agency, to stay abreast of and take action to protect against known vulnerabilities in software. Most cyber attacks exploit known vulnerabilities for which "patches" exist. However, to stay abreast of and employ these "patches," some of which may affect the function of an individual computer system, is difficult job. Failure to fix vulnerabilities can have an impact beyond the individual system since the "affected" computers can be used to launch attacks on other computers. In addition to recommending that the federal government and the private sector work together to establish a one-stop clearinghouse for identifying vulnerabilities and patches, the Strategy also recommends that the government and the private work together to find ways to encourage software and computer vendors to improve the security of their products.

To reduce the threat, the Strategy recommends improving the forensic capabilities of both federal and state/local investigators and makes the Office of

Science and Technology Policy responsible, with support from the Department of Homeland Security, for developing a cybersecurity research and development agenda.

National Cyberspace Security Awareness and Training Program: The Strategy envisions the Department of Homeland Security going beyond current efforts at cybersecurity awareness and working with the Department of Education and other agencies to develop a cybersecurity curriculum for primary and secondary school students. The Strategy also calls for building upon existing education and training programs such as the Cyber Corps Scholarship for Service program, the new programs initiated under the Cyber Security Research and Development Act (both managed by the National Science Foundation), and the National Security Agency's Centers of Excellence in Information Security. The Strategy also encourages the development of certification programs for cybersecurity specialists that will be broadly accepted in the public and private sector.

Securing Government's Cyberspace: The Strategy recommends a number of activities where the federal and state governments can improve their cybersecurity. These include increased use of automated security assessment and security policy enforcement tools, strong access control and authentication tools, and systems that check for unauthorized connections to networks. Federal agencies are bound by statute to secure their cyberspace. Most recently, the E-Government Act of 2002 (P.L. 107-347) included the Federal Information Security Management Act of 2003 (Title III), which states that federal agencies must have cybersecurity plans, that these plans must regularly reviewed, audited, and updated.

National Security and International Cyberspace Security Cooperation: The Strategy calls for the ability to quickly determine the source of a cyber attack that threatens the nation's security. It also reserves the right of the United States to respond to threatening attacks in ways that go beyond law enforcement. In the area of international cooperation, the Strategy recommends that nations sign on to the Council of Europe's Convention on Cybercrime, which commits signatories to cooperate with each other in investigating and prosecuting cybercrimes. It also calls for a Safe Cyber Zone between Mexico, the U.S. and Canada. It also calls for countries to appoint central points-of-contact to work with their counterparts in other countries. It also calls for the establishment of an international network of incident response teams.

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

This Strategy gives a strategic overview of how the federal government plans to address critical infrastructure protection. It acknowledges that the primary responsibility for protecting critical infrastructure lies with the owners and operators, whether they are the federal government, the private sector, or state and local entities. In addition to protecting its own infrastructure, the federal government will also assume the responsibility for cooperating and coordinating the overall effort. In this regard, the Strategy identified five areas that cut across all infrastructures and for which a national approach seems appropriate. Those five areas are

- Planning and Resource Allocation

- Information Sharing and Indications and Warnings
- Personnel Surety, Building Human Capital, and Awareness
- Technology and Research and Development
- Modeling, Simulation, and Analysis

Within each of these are set of initiatives that have been identified. A few of these are highlighted below.

Planning and Resource Allocation: This includes an initiative to develop a uniform methodology for identifying assets that are critical at a national-level. This will help all stakeholders to set priorities and allocate their resources in a cost-effective manner. Such a uniform methodology would also help states and the private sector make a case for federal assistance when their own resources are not adequate or market forces do not support additional protection efforts. The federal government will also maintain a comprehensive up-to-date assessment of vulnerabilities and preparedness across critical sectors. This will include an integrated geospatial database of critical and key assets.

Information Sharing and Indications and Warning: The Department of Homeland Security is to act as a major conduit of information. The Department is tasked with defining protection-related information sharing requirements and establishing effective and efficient information sharing processes that preserve confidentiality or classification. Another initiative is directed at finding ways to integrate threat information from state and local law enforcement entities and the private sector with that from the intelligence community, and then disseminate the integrated threat information to all stakeholders. The Department of Homeland Security is also tasked with refining the Homeland Security Alert System.

Personnel Surety, Building Human Capital, and Awareness: Initiatives in this area include coordinating a task force to explore the possibility of developing national standards for background checks, screenings, etc. for occupants of critical job categories. Similarly, the federal government will explore standards for certifying companies to do such background checks. The government will also explore establishing a certification regime or model security training program to train private security officers.

Technology and Research and Development: The Department of Homeland Security will coordinate with other agencies to support the development of security related technologies. These include communications equipment that allow for interoperability, techniques for verifying and authenticating peoples' identities, and improved technologies for surveillance, monitoring, and detection of chemical, biological, and radiological substances.

Modeling, Simulation and Analysis: The Department of Homeland Security will study ways to integrate modeling, simulation and analysis, of infrastructure behavior. These models, etc. should examine interdependencies and economic impacts of terrorist attacks. Models should also be developed for the Alert system to improve its effectiveness. Models should also examine the interaction between physical and cyber systems.