Order Code RL30153

CRS Report for Congress
Received through the CRS Web

Critical Infrastructures: Background, Policy, and Implementation

Updated July 15, 2004

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

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 JUL 2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Critical Infrastructures: Background, Policy, and Implementation	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Congressional Research Service,The Library of Congress,101 Independence Ave, SE,Washington,DC,20540-7500**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**14**	

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).

The national security community has been concerned for sometime about the vulnerability of critical infrastructure to both physical and cyber attack. 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, 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 and established the President's Critical Infrastructure Protection Board chaired by a Special Advisor to the President for Cybersecurity (both of which were later abolished by an amending executive order). More recently (December17, 2003), the Bush Administration released Homeland Security Presidential Directive 7, reiterating and expanding upon infrastructure protection policy and responsibilities which remain relatively unchanged through two Administrations.

Congress passed legislation in 2002 creating a Department of Homeland Security, consolidating into a single department a number of offices and agencies responsible for implementing various aspects of homeland security. However, infrastructure protection activities remain spread out between various directorates and agencies within the Department, including the Information Analysis and Infrastructure Protection Directorate and the Transportation Security Administration.

Issues in critical infrastructure protection include how to integrate cyber and physical protection; mechanisms for sharing information between the government, the private sector, and the public; 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. This report will be updated as warranted.

Contents

List of Tables

Critical Infrastructures: Background, Policy, and Implementation

Latest Developments

The House passed its FY2005 appropriation bill for the Department of Homeland Security (H.R. 4567) on June 18. It appropriated $855 million for the Information Analysis and Infrastructure Protection Directorate. The Bush Administration had requested $865 million. The Senate Appropriations Committee reported its appropriation bill (S. 2537) for the Department on June 17. The Committee recommended $876 million for the IA/IP Directorate. For more discussion on the Directorate's budget request and other requests within the Department's overall budget that relate to critical infrastructure protection, see Appendix.

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]

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 threats, primarily to improve

---

[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.

reliability and safety. However, the growing dependency of these systems on information technologies and computer networks has resulted in a new vector by which problems can be introduced.[2] A vector that some in the national security community had felt was not being adequately addressed.

Prior to September 11, critical infrastructure protection was synonymous with cyber security to many people. Initial policies, and implementation of those policies, focused on cyber security and did not focus on physical threats. 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.[3]

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.[4] 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.

---

[2] 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.

[3] 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.

[4] 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.

The PCCIP released its report to President Clinton in October 1997.[5] 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 threat and vulnerability exist.

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

The Commission also proposed a strategy for action:

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

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

Presidential Decision Directive No. 63

Presidential Decision Directive No. 63 (PDD-63)[6] 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

---

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

[6] See *The Clinton's Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63,* White Paper, May 22, 1998. Available at the Federation of American Scientist website: [http://www.fas.org/irp/offdocs/pdd/pdd-63.htm].

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."[7]

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. The list of sectors considered critical has since expanded. 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.

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 was to 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.

The PDD also assigned duties to the **National Coordinator** for Security, Infrastructure Protection, and Counter-terrorism.[8] The National Coordinator reported to the President through the Assistant to the President for National Security Affairs.[9] 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

---

[7] Ibid.

[8] The National Coordinator position was created by Presidential Decision Directive 62, "Combating Terrorism." PDD-62, which was classified, codified and clarified 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.

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

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 two years and updated every two years.

Table 1. Lead Agencies per PDD-63

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 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.

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. These dealt primarily with cyber security. 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 Intrusion Detection Network (FIDNET)** that would, together with the **Federal Computer Intrusion Response Capability (FedCIRC)**, established just prior to PDD-63, meet this goal.[10] 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[11] 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

---

[10] FedCIRC is now called the Federal Computer Incident Response Center.

[11] 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.

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 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 was 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.[12] The Department of Homeland Security has taken over the effort to create a data base of critical assets.

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 eight 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.[13]

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. Shortly after assuming office, the Bush Administration announced its desire

---

[12] Testimony by Michael Vatis before the Senate Judiciary Committee, Subcommittee on Technology and Terrorism. Oct. 6, 1999. This effort was transferred to the Department of Homeland Security.

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

not to create a separate federal CIO position, but to recruit a Deputy Director of the Office of Management and Budget that would assume an oversight role of agency CIOs. One of the reason's cited for this was a desire to keep agencies responsible for their own computer security.[14]

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**.[15] 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 is 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, and the Secretary of Homeland Security. Other White House and departmental officials can

---

[14] 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 Seifert.

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

be invited to attend Council meetings.[16] The Council advises and assists the President with respect to all aspects of homeland security. The agenda for those meetings shall be set by the Assistant to President for Homeland Security, at the direction of the President. The Assistant is also the official recorder of Council actions and Presidential decisions.

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."[17] 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**.[18] 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, 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

---

[16] 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.

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

[18] President Bush designated Richard Clarke.

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.

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 July 2002, the Office of Homeland Security released a ***National Strategy for Homeland Security***. The Strategy covered all government efforts to protect the nation against terrorist attacks of all kinds. It identified 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 reiterated 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 (see below).

On December 17, 2003, the Bush Administration released **Homeland Security Presidential Directive 7 (HSPD-7)**. HSPD essentially updated the policy of the United States and the roles and responsibilities of various agencies in regard to critical infrastructure protection as outlined in previous documents, national strategies, and the Homeland Security Act of 2002 (see below). For example, the Directive reiterated the Secretary of Homeland Security's role in coordinating the overall national effort to protect critical infrastructure. It also reiterated the role of Sector-Specific Agencies (i.e. Lead Agencies)[19] to work with their sectors to identify, prioritize, and coordinate protective measures. The Directive captured the expanded set of assignments of Sector-Specific Agencies made in the *National Strategy for Homeland Security*. The Directive also reiterated the relationship between the Department of Homeland Security and other agencies in certain areas. For example, while the Department of Homeland Security will maintain an cyber security unit, the Directive stated that the Director of the Office of Management remains responsible for overseeing government-wide information security programs and for ensuring the operation of a federal cyber incident response center within the Department of Homeland Security. Also, while the Department of Homeland Security is responsible

[19] This report will continue to use the term "Lead Agency" to refer to the agency assigned to work with a specific sector.

for transportation security, including airline security, the Department of Transportation remains responsible for control of the national air space system.

The only structural change made by the Directive was its establishment of the **Critical Infrastructure Protection Policy Coordinating Committee** which will advise the Homeland Security Council on interagency policy related to physical and cyber infrastructure security.

The Directive made a few other noticeable changes or additions. For example, the Department of Homeland Security was assigned as Lead Agency for the chemical and hazardous materials sector (it had been the Environmental Protection Agency). The Directive also now requires Lead Agencies to report annually to the Secretary of Homeland Security on their efforts in working with the private sector. The Directive also reiterated that all federal agencies must develop plans to protect their own critical infrastructure and submit those plans for approval to the Director of the Office of Management and Budget by July 2004.

The Directive also required that the Secretary of Homeland Security to collaborate with other appropriate federal agencies to develop a program to geospatially map, analyze, and sort critical infrastructure and key resources, and to work with other federal, state, local, and private entities to develop a national indications and warning architecture that can develop a baseline of infrastructure operations and detect potential attacks.

All together, the Bush Administration policy and approach regarding critical infrastructure protection represents a continuation of PDD-63. The fundamental policy statements are essentially the same: the protection of infrastructures critical to the people, economy, essential government services, and national security. National morale has been added to that list. 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 and with an emphasis placed on targets that would result in large numbers of casualties). Finally, the primary effort is directed at working collaboratively and voluntarily with the private sector owners and operators of critical infrastructure to identify critical assets and provide appropriate protection.

Organizationally, there remains an interagency group for coordinating policy across departments and for informing the White House. Certain agencies have been assigned certain sectors with which to work. A Council made up of private sector executives, academics, and State and local officials was established to advise the President. Certain operational units (e.g. the Critical Infrastructure Assurance Office (CIAO) and elements of the National Infrastructure Protection Center (at the FBI)) have been left in place (and later moved to the Department of Homeland Security).

The primary difference, at least initially, was the segregation of cyber security from the physical security mission of the Office of Homeland Security. Dissolution of the President's Critical Infrastructure Protection Board and the transfer of its duties to the Department of Homeland Security would appear to reintegrate the two.

The relationship between physical security and cyber security is discussed in more detail is the Issues section of this report.

Department of Homeland Security

In November 2002, Congress passed the Homeland Security Act (P.L. 107-296), establishing a **Department of Homeland Security (DHS)**. 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 Administration). 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 transferred 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),**[20] other energy security and assurance activities within DOE, and the **National Communication System (NCS).**[21] These agencies and offices shall be integrated within the **Directorate of Information Analysis and Infrastructure Protection (IA/IP)** (one of four operational Directorates established by the act).[22] 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), nor is the Coast Guard, which is responsible for port security. The Directorates shall be headed by someone of Undersecretary rank. Furthermore, the act designated that within the Directorate of Information Analysis and Infrastructure

---

[20] 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.

[21] 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 23 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.

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

Protection, there shall be both an Assistant Secretary for Information Analysis, and an **Assistant Secretary for Infrastructure Protection**.

Among the responsibilities assigned the IA/IP Directorate 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, including **risk assessments** to determine risks posed by particular types of attacks;
- 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).

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, although it has also developed parallel mechanisms to communicate with them. The Bush Administration also 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 as coordinator of their efforts. However, the Strategy did shift liaison responsibilities for some sectors to the new Department. The liaison responsibilities outlined in the National Strategy are noted in **Table 2** below, with the former liaison agency noted in parenthesis. HSPD-7 modified the Strategy's slightly, assigning the chemical sector to the Department instead of the Environmental Protection Agency.

Table 2. Current Lead Agency Assignments

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
Energy	Electric Power
Energy	Oil and Gas
Homeland Security-Transportation Security Administration	Pipelines
Department of Homeland Security (per HSPD-7)	Chemical Industry and Hazardous Materials
Defense	Defense Industrial Base
Homeland Security	Postal and Shipping
Interior	National Monuments and Icons

Identifying and Selecting Sector Coordinators. Different sectors present different challenges to identifying a coordinator. Some sectors are more diverse than others (e.g. transportation includes rail, air, waterways, and highways; information and communications include computers, software, wire and wireless communications) and raises the issue of how to have all the relevant players represented. Other sectors are fragmented, consisting of small or local entities.

Some sectors, such as banking, telecommunications, and energy have more experience than others in working with the federal government and/or working collectively to assure the performance of their systems.

Besides such structural issues are ones related to competition. Inherent in the exercise is asking competitors to cooperate. In some cases it is asking competing industries to cooperate. This cooperation not only raises issues of trust among firms, but also concerns regarding anti-trust rules.

Table 3. Sector Coordinators

Sector	Identified Sector Coordinators
Information and Telecommunications	A consortium of 4 associations: Information Technology Assn. of America; Telecommunications Industry Assn.; U.S. Telephone Assn.; Cellular Telecom. & Internet Assn.
Banking and Finance	Rhonda McLane - BankAmerica
Water	Assn. of Metropolitan Water Agencies
Electricity Oil/Gas	North American Electric Reliability Council National Petroleum Council
Railroads Mass Transit Airports	Association of American Railroads American Public Transportation Assn. Airport Council International-North America
Emergency Fire Services	U.S. Fire Administration
Law Enforcement	Emergency Law Enforcement Services Forum

Table 3 above shows those individuals or groups that have agreed to act as Coordinators. 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. More recently, the American Public Transportation Association was selected to represent commuter transportation systems. The U.S. Fire Administration, a component of FEMA, has an established communication network with the nation's fire associations, the 50 State Fire Marshals, and other law enforcement groups. The Department of Justice, through the NIPC, 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. CIAO is also engaged in outreach activities with state and local government associations including the National Governors Association, the National Association of Counties, the National League of Cities, the National Emergency Management Association,

Public Technology Inc., and th National Association of State Chief Information Officers.

Other sectors have groups that have assumed the role of sector coordinator, although may not have been officially designated as such. For example, the American Chemistry Council and the Food Marketing Institute communicate and coordinate with the federal government and the members of their respective sectors.

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.[23] The Order was rescinded by the Bush Administration before the Council could meet. In Executive Order 13231,[24] 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.[25] The E.O. amending 13231 makes some minor modifications to NIAC. Primarily, the Council now reports to the President through the Secretary of Homeland Security.

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 Directive's 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.

---

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

[24] 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.

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

Initially, the process of reviewing 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 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 Government Accountability Office[26] 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.[27] HSPD-7 reestablished a deadline for agencies to submit a critical infrastructure protection plan to the Director of OMB for approval by July 2004.

As another indication that infrastructure protection and cyber protection are sometimes considered synonymous, the agencies' internal critical infrastructure planning process had 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. HSPD-7 requires agencies to submit agency critical infrastructure protection plans to the Director of OMB, and not to the Secretary of Homeland Security.

National Critical Infrastructure Plan. PDD-63 called for a National Infrastructure Protection Plan that would be informed by sector-level plans and would include an assessment of minimal operating requirements, vulnerabilities,

---

[26] Note: The General Accounting Office has had its name changed legislatively to the Government Accountability Office.

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

remediation plans, reconstitution plans, warning requirements, etc. The National Strategy for Homeland Security, and the Homeland Security Act each have called for the development of a comprehensive national infrastructure protection plan, as well, although without being as specific regarding what that plan should include. HSPD-7 called for a comprehensive National Plan for Critical Infrastructure and Key Resources Protection by the end of 2004.

To date, three National Plans or Strategies have been released. In 2000, the Clinton Administration released Version 1.0 of a *National Plan for Information Systems Protection* in January 2000.[28] 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*.

While these continue to call for assessments of vulnerabilities, risks, identification of critical assets, etc., the plans themselves do not include them. They do include how the federal government is or intends to go about some of these tasks. Some sectors have established guidelines regarding vulnerability assessments, incident reporting procedures, warning procedures, response agreements, etc. When and how the federal government may assist in responding to and reconstituting from an attack are less developed. It is not clear if these national and sectoral plans and guidelines adequately meet the original intent of PDD-63 or the intent for planning by the Homeland Security Act of 2002.

Information Sharing and Analysis Center (ISAC). PDD-63 envisaged a single 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. The idea of a single ISAC evolved into each sector having its own center. Many were conceived originally as concentrating on cyber security issues, and some still function with that emphasis. However, others have incorporated physical security into their missions.

While information sharing mechanisms may exist in many forms, ISACs typically are officially recognized by some kind of agreement between the federal government and the ISAC to share information. Those sectors that have established ISACs have followed two primary models. One model involves ISAC members incorporating in some way and contracting out the ISAC development and operations to a security firm. The banking, information, water, oil and gas, railroad, and mass transit sectors have followed this approach.

---

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

The other model involves utilizing an existing industry or government-industry coordinating group and adding critical infrastructure protection to the mission of that group. The electric power (which uses North American Electricity Reliability Council (NERC)) and the telecommunications sector (which uses the National Coordinating Center (NCC)) follow this model. The emergency fire services sector incorporated ISAC functions into the U.S. Fire Administration (within the Federal Emergency Management Agency)which has interacted with local fire departments for years.

The only sectors that have not yet established ISACs are the Public Health, Emergency Medical Services, and air transport, defense industries. However, that is not to say that information is not being communicated between these sectors and the federal government. It does mean that something identifiable and accepted as an ISAC has yet to be formed.

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

Establishing the Information Analysis and Infrastructure Protection Directorate. The Undersecretary for Information Analysis and Infrastructure Protection was approved by the Senate in June 2003. The Assistant Secretary for Infrastructure Protection was approved in March 2003. The Assistant Secretary for for Information Analysis assumed his duties on November17, 2003.

The organization of the Directorate appears to be in flux. A survey by the DHS Office of Inspector General (IG) of the IA/IP Directorate reported an organization structure dated August 11, 2003, but noted that changes to that structure were under consideration at that time.[29] An organizational chart published by Carroll Publishing, dated November/December 2003 indicates that some of those changes were made. According to this organization chart, there are two divisions under the Assistant Secretary for Information Analysis: Risk Assessment; and Information Management and Requirements. There are three division under the Assistant Secretary for Infrastructure Protection: Infrastructure Coordination; Protective Services; and National Cyber Security. In addition, the Assistant Secretary for Infrastructure Protection has the National Communication System and the Office of Outreach and Partnership reporting to him. In the IG report, in addition to the standard support

---

[29] Department of Homeland Security. Office of the Inspector General. *Survey of the Information Analysis and Infrastructure Protection Directorate.* February 2004.

staff, the Undersecretary for Information Analysis and Infrastructure Protection had an Office of Competitiveness Analysis and Evaluation reporting to him. In addition, the IA/IP Directorate has operational control of the Homeland Security Operations Center.

Congress has expressed concern about the speed with which the Directorate is hiring permanent staff. In its FY2004 budget justification document, the Directorate requested authority for 692 full time equivalent (FTE) positions, an increase of 226 FTE positions above the number of FY2003 positions transferred to the Directorate. However, most of the funding requested by the Directorate was devoted to advisory and assistance services, purchases of goods and services from government accounts, and other services. Congress authorized a total of 729 FTE positions. In its FY2005 budget request, the Directorate requested an additional 8 FTEs, but IA/IP budgeted zero dollars for permanent staff outside its administration and management account. However, during the a House Appropriations Subcommittee on Homeland Security hearing on April 1, 2004, the Undersecretary for IA/IP stated that the Directorate had hired 299 employees and had developed a plan to hire 40 new employees per month. In its FY2005 appropriations bill, the House added authorized another 132 FTE positions (see Appendix).

Vulnerability Assessments, Risk Assessments, and Prioritizing Protective Measures. Among the activities assigned to the Information Analysis and Infrastructure Protection Directorate by the Homeland Security Act of 2002 are:

1. 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;
2. carry out comprehensive assessments of the vulnerabilities of key resources and critical infrastructure, of the United States including risk assessments to determine risks posed by particular types of attacks;
3. integrate relevant information, analyses, and vulnerability assessments in order to identify priorities for protective and support measures.

Furthermore, according to the National Strategy for the Physical Protection, the Department of Homeland Security will: a) in collaboration with other key stakeholders, develop a uniform methodology for identifying facilities, systems, and functions with national-level criticality to help establish protection priorities; b) build a comprehensive database to catalog these critical facilities, systems, and functions, and c) maintain an comprehensive, up-to-date assessment of vulnerabilities and preparedness across critical sectors.

In his testimony before the House Appropriations Committee in April, the Undersecretary for IA/IP stated that Directorate had assembled a list of 28,000 critical infrastructure assets and that it planned to conduct vulnerability assessments on 1700 of those judged to be of highest priority. Based on further testimony, budget

documents, and DHS's recent strategic plan,[30] a priority asset is one that could be "catastrophically exploited."

It is not clear from the testimony how the list of 28,000 was developed. States and certain urban areas have identified critical assets as part of their applications for State Homeland Security Grants and the Urban Areas Security Initiatives Grants. Also, firms in some sectors have been active in performing vulnerability assessments and prioritizing corrective actions. Some are required by law to do so (e.g. drinking water, ports). The Department has proposed regulations governing the voluntary submission of these assessments as critical infrastructure information (see, Information Sharing in the Issues section below). The Directorate, too, has researched various sector-oriented databases.

In his testimony to the House Appropriations Committee, the Undersecretary stated that 377 chemical plants were included in the 1700 priority sites. The IA/IP is also working with the Transportation Security Administration and the railroads to assess vulnerabilities of the transportation of hazardous materials, and with the Nuclear Regulatory Commission to assess the vulnerability of nuclear plants and the transportation of nuclear materials. It is not clear from the testimony if critical rail sites or nuclear plants are included in the 1700 priority sites. Nor is its clear how many of the 1700 priority assets have had their vulnerability assessed. According to the Senate Appropriation Committee's report for its FY2005 DHS appropriation, the vulnerability of 150 priority sites have been assessed so far. The report also stated that the Committee expects another 400 to be assessed in FY2005.

After assessing the priority sites, the Protection Services Division works with the stakeholders to develop protections plans. These plans focus on working with state and local officials to provide security "outside" the fence, creating buffer zones.

Issues

Cyber vs. Physical Vulnerabilities and Protection. 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.

E.O. 13228 and E.O. 13231, both released in October 2001, split the responsibilities for physical protection and cyber protection of the nation's critical

---

[30] Department of Homeland Security. Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan. 2004. See, objective 1.2, p. 11.

infrastructure. 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 were 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 had some in the cyber security community concerned that cyber security would be buried too deep within the organization and not receive the special attention they think it requires.[31]

The Department announced the formation of a National Cyber Security Division (NCSD), reporting to the Assistant Secretary for Infrastructure Protection. The Division integrates many of the resources and activities transferred over to the Directorate from other agencies (i.e. CIAO, NIPC, FedCIRC, and NCS). Administration officials take the position that one cannot fully dissociate cyber security from physical security when assessing vulnerabilities and taking protective actions. The Administration states that the Cyber Security Division works closely with other Directorate activities that identify critical assets, assess their vulnerabilities, and in developing protection strategies.

Is cyber security a special case of infrastructure protection, or is it just one of a number of threat vectors? Some have said that the extent to which computer networks have permeated other infrastructures make it different. However, electricity and energy can make similar claims, and there is a mutual interdependence among all the infrastructures. Cyber attacks, however, are different from physical attacks since they can be launched from anywhere in the world and be routed through numerous intermediate computers. Cyber attacks require a different skill set to counter.

While differences in the threat may point to the need for a separate focus on cyber security, it also expands the threat envelope that the Department must monitor.

---

[31] 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.

Cyber security, as it has been discussed nationally, goes beyond the threat posed by terrorists and includes threats posed by criminals and hackers. The latter are already attacking the information infrastructure or using it to steal information and extort money. Attacks by terrorist groups (or at least by politically motivated groups) have been limited and fairly targeted. Motivation and the desired impact are likely to be different between terrorists and criminals or hackers. Could this require a different allocation of, or perhaps result in competition for, intelligence resources?

What is Critical and Needs Protection and How Do We Decide? The term critical infrastructure has been broadly defined in most of the official documents mentioned in this report. The definition has changed somewhat over time.[32] 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.

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.

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. Nor has a methodology been described for setting priorities.

Typically, risk is considered a function of threat, vulnerability, and impact. How the Directorate plans to assess this raises many questions. How will threat be characterized? Will specific modes of attack be considered? Will more than one

---

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

threat scenario be considered? Will these differ depending on sector or asset? How will intent, capability, and target value to the attacker be integrated into the analysis? How will vulnerability be characterized? How will impact be characterized? How will loss of life be valued and compared with economic impact or national morale? How iterative will the analysis be (recognizing that taking protective action in one area may change the target value and vulnerability of other assets)? How will uncertainty be handled in the analysis? How will the Directorate reconcile any differences in criticality and priorities based on a national-level analysis with those based on more parochial analyses by the private sector or states and localities?

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*.[33] According to the 2003 report, funding for Critical Infrastructure Protection was estimated at $13.2 billion for FY2003 and the Administration request for FY2004 was $12.2 billion (see Table A.1. in the **Appendix**).

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. According to GAO, improving security in the 22 largest mass transit systems would cost over $700 million.[34] In testimony before the House Transportation and Infrastructure's Subcommittee on Water Resources and the Environment (November 3, 2003), the Executive Vice President of the American Association of Port Authorities, federal security requirements at the nation's ports will cost over $5 billion over the next 10 years.[35] While some transit systems and ports are privately owned and operated, many are owned and operated by local or regional government or semi-government entities.

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 PATRIOT 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 State and Local Government

---

[33] 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. Also, OMB has continued to refine the criteria used by agencies to determine how much they spend. While the most recent report goes back and estimates figures based on the latest criteria, older report figures cannot be considered comparable.

[34] Government Accountability Office, *Mass Transit*, GAO–03-263. December 2002.

[35] This testimony did reveal how that figure was determined.

Coordination and Preparedness (OSLGCP).[36] The grant will support, among many other items, the purchase of equipment, including equipment used for enhancing the physical protection of critical infrastructure. Funding for this and grants related to critical infrastructure protection are discussed in the Appendix. For more information on this and other grant programs related to homeland security, see CRS Report RL31490, *Homeland Security: State and Local Preparedness Issues*.

Potential private sector costs are unknown at this time.[37] 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.

Issues of liability may also determine private sector costs. The airline industry was protected after September 11. It is not clear if this would continue in any future attacks. In the case of computer security, there is also the potential for 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.[38]

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

---

[36] This grant program was initially manged by the Office of Domestic Preparedness, which was transferred from the Department of Justice to DHS. The ODP is now merged with the Office of State and Local Government Coordination to form the Office of State and Local Government Coordination and Preparedness (OSLGCP). The OSLGCP now manages the State Homeland Security Grants, the Urban Areas Security Grants, and the Port Security Grants, formerly managed by the Transportation Security Administration.

[37] The cyber security market alone 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.

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

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.

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.

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:

- 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. 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.[39] 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.

On April 15, 2003, the Department of Homeland Security released draft procedures for receiving, marking, and handling of critical infrastructure information,[40] implementing the provisions stated above. The proposed rule states that the Secretary of Homeland Security shall name the Undersecretary of Information Analysis and Infrastructure Protection (IA/IP) as the senior official responsible for directing and administering a Critical Infrastructure Information (CII) Program. The Undersecretary is to appoint a CII Program Manager. Only the CII Program Manager may acknowledge the receipt of, validate, and mark information received as CII. Such information may be submitted directly to CII Program Manager or it may be forwarded to the CII Program Manager by other agencies. While the submitter of the information may designate it as CII, it is up to the CII

---

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

[40] Procedures for Handling Critical Infrastructure Information. Federal Register. Vol. 68. No. 72. pp.18524-18529.

Program Manager to validate it as such. The information, however, shall be protected, until the Manager has had a chance to rule. The Manager has 30 days to inform the submitter that the information does not meet the standards for CII. These standards, however, are not defined beyond the relatively broad definition of CII provided in the act. Furthermore, if the CII Program Manager finds that the information was submitted in bad faith, the Manager is not required to notify the submitter that the information does not qualify.

The draft procedures states that these procedures do not apply to or affect any requirement pertaining to information that must be submitted to a federal agency or pertaining to the obligation of any federal agency to disclose such information under the Freedom of Information Act. The procedure goes on to state that information required to be submitted to satisfy a provision of law may not be marked as CII by the submitter, the Department of Homeland Security, or any other federal agency.

Also, while the act specifies penalties associated with unauthorized disclosure of this information by federal employees, the draft procedures specifies "whistle-blowing" disclosures that are exempt from these penalties.

The draft provisions, in some ways, address some of the concerns expressed by those who opposed this provision of the act, but also raises some more questions. For example, while the procedures allow entities to submit information they think is CII to the CII Program Manager indirectly through other officials or agencies, the information is not validated as CII until the Manager designates as such. However, as pointed out by critics[41], the presumption is that the information shall be protected until the Manager makes such a ruling. There is no time frame for the Manager to receive the information or to make a ruling. However, the Manager has 30 days to inform the submitter that the information does not qualify as CII. Will the Manager have the time and resources to validate the amount of information coming in?

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 possible. Another area of concern is the monitoring network traffic in order to detect

---

[41] See, DHS Broadens CII in Proposed Rule. OMB Watch, published April 21, 2003. [http://www.ombwatch.org/article/articleprint/1475]. This site was last viewed Jan. 6, 2003.

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.[42] 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..."[43] 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.[44] 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 resurrected it. The Strategy tasked 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 mentioned exploring the possibility of establishing national standards by which to check the backgrounds of personnel with access to critical infrastructures. And, the Transportation Security Administration is planning to develop a certification program for all transportation workers with access to critical infrastructure.

Another issue is to what extent will monitoring and responding to cyber attacks (or any kind of attack against critical assets) 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

---

[42] 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.

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

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

provide the federal government with the authority to direct private resources to help reconstitute critical infrastructures suffering from a cyber attack. This authority exists now regarding the supply and distribution of energy and critical materials in an emergency. Suppose that the computer networks managing the nation's railroads were to "go down" for unknown but suspicious reasons. What role would the federal government play in allocating resources and reconstituting rail service?

Congressional Action

Congressional 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, notwithstanding any restructuring of committee jurisdictions. 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. 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.

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).

Prior to September 11, Congress had not had to appropriate large amounts of resources to infrastructure protection. For the most part appropriations had been directed at protecting critical federal assets. Since September 11, Congress has provided grant money for states and some sectors to help protect infrastructures in their jurisdictions. 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. For a discussion of Congressional action on FY2005 appropriations, see the **Appendix**.

For Additional Reading

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

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

CRS Report RL32189, *Terrorism and Security: Issue Facing the Water Infrastructure Sector*, by Claudia Copeland and Betsy Cody.

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 RL31990, *Pipeline Security: An Overview of Federal Activities and Current Policy Issues*, by Paul Parfomak.

CRS Report RL31873, *Homeland Security: Banking and Financial Infrastructure Continuity*, by William Jackson.

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

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

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

Appendix

Federal Funding for Critical Infrastructure Protection

Table A.1. Critical Infrastructure Protection Funding by Department

($ in millions)

Department	FY02 enacted	ERF**	FY03 enacted	FY03 Sup	FY04 Request
Agriculture	163.6	248.7	196.7	110.0	244.1
Commerce	23.6	16.9	31.3		46.1
Defense	4076.0	708.0	8545.0		6467.0
Energy	953.3	135.7	1130.6	77.5	1272.4
HHS	147.7	59.3	181.6		182.3
Homeland Security	977.7	186.0	1384.7	240.3	1877.4
HUD	1.0		2.0		2.0
Interior	11.1	92.6	106.7	25.0	110.6
Justice	208.2	128.9	368.7	32.6	502.9
Labor	65.9	5.9	64.2		63.0
State	12.2	1.6	32.9	1.4	31.8
Transportation	88.2	48.0	128.0		179.3
Treasury	23.1	10.0	21.9		27.0
Veterans Affairs	27.8	2.0	90.0		128.1
Corps of Engineers		100.0	36.0	39.0	104.0
District of Columbia		26.0			
EPA	8.7	135.7	44.9		86.8
FCC			1.0		1.0
GSA	45.5	51.0	92.8		93.6
Holocaust Museum	7.0		8.0		8.0
NASA	114.0	109.0	163.0		170.0
Nat'l Archives	7.0	3.0	11.0		12.0
NSF	231.0	19.6	257.6		280.5
NRC	6.5	36.4	35.3		41.1
OPM	1.8		3.0		2.5
Postal Service		406.5			
Smithsonian	62.5	27.8	82.8		80.1
Social Security	113.0	8.0	132.0		143.0
Grand Total	7376.4	2566.6	13151.7	525.8	12156.6

Source: OMB, 2003 Report to Congress on Combating Terrorism, September 2003.**ERF is the Emergency Response Fund. Table does not include National Capital Planning Commission.

The Infrastructure Analysis and Infrastructure Protection Directorate's FY2005 Budget and Related Items

The following is a brief discussion of the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate's FY2005 budget request and subsequent Congressional action. This discussion also identifies other areas within the Department's budget that relate to critical infrastructure protection.

The Administration requested $865 million in FY2005 for activities within the Information Analysis and Infrastructure Protection Directorate, about $30 million above the Directorate's estimated FY2004's budget. The $30 million increase includes a request for $22.9 million in new funds for three new initiatives. In addition, the requests 8 new FTE positions. The balance of the increase maintains current level of services. The Directorates's request for new initiatives include renovations and upgrades to the current Homeland Security Operations Center; funding for cyber security exercises; and, the establishment of a National Biosurveillance Group that would integrate and analyze data from dissparate biosurveillance programs run by DHS and other agencies.

Table A.2 Requested Increases in FY2005 Budget for New Initiatives Within the Information Analysis and Infrastructure Protection Directorate

($ in millions)

New Initiatives	Requested Increase
Renovations and upgrades to current Homeland Security Operations Center	+10.0
Cybersecurity exercises	+1.3 (+1.9)*
Biosurveillance (National Biosurveillance Group)	+11.6(+11.0)*

* The Directorate's budget justification document reports two different figures.

The proposed budget supports two accounts: Management and Administration, which includes the Homeland Security Operations Center; and Assessments and Evaluations, which includes 8 program areas (see **Table A.3**) A short description of these 8 program areas, taken from the Directorate's budget justification document, follows.

Threat Determination and Assessment: This program is designed to detect and identify the terrorist threat. Funding is targeted at increasing the Directorate's technical competencies. These technical capabilities are to be used to: model terrorist organizations; baseline terrorist capabilities; expand collaboration and fusion of data; and coordinate analysis with other intelligence communities (the Terrorist Threat Integration Center (TTIC), et al.). The drop in funding between FY2004 and FY2005 reflects the Administration's proposal to centrally fund the Terrorist Integration Center and other interagency intelligence efforts. Therefore, the IA/IP FY2005 budget request does not support the TTIC directly as did the FY2004 budget.

Information and Warning Advisories: This program supports three activities. Tactical Indications and Warning Analysis/Warning Advisory Preparation and Issuance requests information from others in the intelligence community and develops the tools and technologies needed to interpret, integrate, and catalog indicators, warnings, and actual events and to provide the Department and national leadership with situational awareness. Information Requirements Management supports the technologies needed to search diverse databases to identify, distill, and acquire useful information, to coordinate information requests from other part of DHS and elsewhere, and to make that information accessible as appropriate. Integrated Physical and Cyber Infrastructure Monitoring and Coordination coordinate incident response, mitigation, restoration and prioritization across critical sectors. The $4 million decrease in funding between FY2005 and FY2004 reflects the transfer of that amount to the Homeland Security Operations Center program, in an effort to consolidate the Centers funding. This transfer is in addition to the $10 million additional funds requested for renovations and upgrades to the Center.

Infrastructure Vulnerability and Risk Assessment: FY2005 funds were requested in three areas: support for a comprehensive risk assessment on a national scale; development of tools and databases to better understand interdependencies among sectors and to facilitate access to many types of information from many types of sources; coordination and direction of the development of a national database on the risks (i.e. probability of attack and associated consequences) for specific assets. The reduction in this year's budget request reflects, again, the elimination of direct IA/IP support for the TTIC and other interagency intelligence efforts.

Remediation and Protective Actions: The largest program area of the Directorate, Remediation and Protective Actions activities include identifying which assets are most critical, conducting and coordinating specialized vulnerability assessments on the highest priority assets, working with asset owners and state and local officials to implement protective measures, and working with NIST to develop an objective set of performance measures to assess the effectiveness of the protective measures taken. This program area also includes activities of the National Computer Security Division within IA/IP which include developing a Global Early Warning Information System to monitor the internet worldwide, completing the warning and information network to support crisis management during cyber and physical attacks, creating a national cyber vulnerability reduction program, and supporting cyber security awareness and training programs.

The National Communication System: The National Communication System (NCS) is a set of assets that allow for national security and emergency preparedness communication between government agencies with missions in those areas and national leadership. An interagency Committee of Principals acts as the forum for coordinating and planning the availability of assets. The Committee interacts with industry through the President's National Security Telecommunications Advisory Committee (NSTAC). The NCS includes the National Coordination Center (NCC), which is the operational center used to restore and reconstitute national security and emergency preparedness services in necessary. The Homeland Security Act of 2002 passed the responsibility for Executive Agent of the NCS from the Secretary of Defense to the Secretary of Homeland Security. FY2005 funding maintains current level of services.

Competitive Analysis and Evaluation: This program essentially evaluates the processes and products of the IA/IP Directorate. It also supports "red teams" that emulate terrorist organizations, strategy and tactics and interagency exercises and games that test protective strategies and measures.

National Planning and Strategies: This program area monitors the implementation of the various strategies that have been released.

Outreach and Partnerships: This program area supports the communication and coordination of effort with the private sector, state and local governments, academia, and foreign states. This program continues and expands activities initiated by the Critical Infrastructure Assurance Office, including acting as the Lead Agency contact with the Information and Telecommunications Sector.

In addition to the IA/IP budget request, the Transportation Security Administration, part of the Border and Transportation Directorate requested $5.3 billion, most of which is targeted at aviation security. Included in the $5.3 billion request is $146 million for the Transportation Security Enterprise program to address security in other transportation modes. The Coast Guard is requesting $102 million to implement Maritime and Transportation Security Act requirements, including reviewing and approving vessel and facility security plans. Of the $1.2 billion being requested for the Urban Area Security Initiative grants, $200 million is being requested to supoort infrastructure-related activities. Also, within the Threat, Vulnerability, Testing and Assessment portfolio of the Science and Technology Directorate, $18 million is targeted at cyber security and another $6 million targeted at critical infrastructure protection.

The House passed its appropriation for the Department of Homeland Security (H.R. 4567, H.Rept. 108-541) on June 18, 2004. The House stated it was "very dissatisfied" with the structure of IA/IP Directorate's budget request and restructured it to "better reflect program operations..." As a consequence, the House appropriated funds based on a slightly expanded list of budget activities as shown in Table A.4. The House appropriated $854 million for IA/IP, about $10 million less that the request. The House fully funded the 3 new initiatives (although it transferred the Homeland Security Operations Center activity to the Evaluations and Assessments account). Within the Management and Administration account, the House added half-year funding for an additional 12 Protective Security Advisors and 120 Protective Security Team positions. The Administration had requested funding for 56 Advisor positions, one in each FBI field office. The House added 12 extra advisor positions to be assigned to those field offices with greater concentrations of critical infrastructures. The additional team positions would increase team size from 8 teams of 5 (as requested) to 8 teams of 20. While expanding Protective Security Field Operations presence, the House voted not to provide the $20 million requested to construct of 4 to 8 Protective Security Centers, as requested. Those funds were redirected to security planning and vulnerability reduction activities. The House also provided $3.9 million for the Competitive Analysis and Evaluation activity, $15 million less than what was requested, stating it received insufficient information to justify the requested level of funding.

In addition to the House appropriations for the IA/IP Directorate, the House appropriated the following for other infrastructure related programs within the

Department: $125 million for port security grants (an increase $79 million above the request); $1 billion for Urban Areas Security Initiative Grants ($300 million below the request), of which $100 million was set aside for rail security; $10 million for intercity bus security grants and another $11 million for rail security through Transportation Security Administration accounts; $27 million for critical infrastructure protection research within the Science and Technology Directorate[45]; and $18 million for cyber security research, also in the Science and Technology Directorate.

The House also combined the Office of State and Local Government Coordination and the Office of Domestic Preparedness (ODP) into the Office of State and Local Government Coordination and Preparedness (OSLGCP). The OSLGCP will now administer the formula based state grants, the Urban Areas Security Initiative Grants, and the TSA's port security grants (the intercity bus security grants and the rail grants will remain with TSA). The House did not appropriate funds for a separate critical infrastructure grant within the Urban Areas Security Initiatives Grant Program.

The Senate Appropriations Committee reported its DHS appropriation bill (S. 2537, S.Rept. 108-280). The Committee recommended $876 million for the IA/IP Directorate. As did the House, the Committee fully supported the new initiatives of the Directorate. The Committee also adopted the same list of budget activities as the House. The Committee recommended $20 million extra for Partnership and Outreach to develop a database for the Critical Infrastructure Information Program, and increased Protective Actions by $2 million. The Committee recommended cutting the Critical Infrastructure Identification and Evaluation request by $13 million. The Committee gave no reason for the reduction in its report.

The Senate Appropriations Committee appropriated $1.2 billion for the Urban Areas Security Initiative Grants (setting aside $150 million each for port security grants and rail security grants and $10 million for bus security and $15 million for trucking). In addition, the Committee recommended $15 million for rail security through the TSA.

[45] Research to defend commercial aircraft from shoulder-fired missiles was funded in a separate budget activity.

Table A.3 Appropriations for the Information Analysis and Infrastructure Protection Directorate

($ in millions)

Budget Activity/Program Area	FY2004 Apprn. P.L. 108-90 (H.Rpt.108-280)	FY2005 Request
Assessments and Evaluations		
Threat Determination and Assessment	28.4	21.9
Information and Warning Advisories	52.3	59.8
Infrastructure Vulnerability and Risk Assessment	84.2	71.1
Remediation and Protective Action	345.1	345.7
National Communication System	141.0	140.8
Competitive Analysis and Evaluation	18.9	18.9
National Plans and Strategies	3.5	3.5
Outreach and Partnerships	40.9	40.8
Management and Administration[1]		162.1
Salaries and Expenses	125.0	
Total	839.3	864.6

1. Includes funding for the Office of the Under Secretary IA/IP, other salaries and expenses, and the Homeland Security Operations Center.

Budget Activity/Program Area	FY2005 Request	House Apprn. H.R. 4567 (HRpt 108-541)	Senate Apprn. S. 2537 (SRpt 108-280)
Assessments and Evaluations			
Threat Determination and Assessment	21.9	21.9	21.9
Critical Infrastructure Identification and Evaluation	77.9	77.9	64.7
Infrastructure Vulnerability and Risk Assessment	71.1	71.1	71.1
Protective Actions	191.6	191.6	193.7
National Security and Emergency Preparedness Telecommunications	140.8	140.8	140.8
Competitive Analysis and Evaluation	18.9	3.9	18.9
Biosurviellance	11.0	11.0	11.0
Cyber Security	67.4	67.4	67.4
National Infrastructure Simulation and Analysis Center	16.0	16.0	23.1
Homeland Security Operations Center		35.0	
Evaluation and Studies	14.4	14.4	14.4
Critical Infrastructure Outreach and Partnerships	71.6	71.6	91.6
Management and Administration			
Other Salaries and Expenses	107.7	103.3	116.2
Protective Security Field Operations	13.4	22.9	(included in above activity)
Office of the Secretary	5.9	5.9	5.9
Homeland Security Operations Center	35.0		35.0
Total	864.6	854.6	875.6