

Critical Infrastructures: Background, Policy, and Implementation

John D. Moteff
Specialist in Science and Technology Policy

July 11, 2011

GalleryWatch.com
http://www.crsdocuments.com
Penny Hill Press

Congressional Research Service
7-5700
www.crs.gov
RL30153

CRS Report for Congress
Prepared for Members and Committees of Congress

c11173008

Summary

The nation's health, wealth, and security rely on the production and distribution of certain goods and services. The array of physical assets, functions, and systems 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 some time 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 protection of critical infrastructures has received increased attention.

Following the events of September 11, the Bush Administration released Executive Order 13228, signed October 8, 2001, establishing the Office of Homeland Security and the Homeland Security Council. In November 2002, Congress passed legislation creating a Department of Homeland Security. Among its responsibilities is overall coordination of critical infrastructure protection activities. In December 2003, the Bush Administration released Homeland Security Presidential Directive 7, reiterating and expanding upon infrastructure protection policy and responsibilities. In June 2006, the Bush Administration released a National Infrastructure Protection Plan. This Plan presents the process by which the Department of Homeland Security intends to identify those specific assets most critical to the United States, across all sectors, based on the risk associated with their loss to attack or natural disaster, and then to prioritize activities aimed at maximizing the reduction of those risks for a given investment. In 2009, the Obama Administration released an updated version of the Plan. For the most part, the Obama Administration continues to follow the basic organizational structures and strategy of prior adminstrations.

This report discusses in more detail the evolution of a national critical infrastructure policy and the institutional structures established to implement it. The report highlights five issues of Congressional concern: identifying critical assets; assessing vulnerabilities and risks; allocating resources; information sharing; and regulation. This report will be updated.

Contents

Latest Update Information 1
Introduction 1
Federal Critical Infrastructure Protection Policy: In Brief 2
The President's Commission on Critical Infrastructure Protection 3
Presidential Decision Directive No. 63 4
Restructuring by the Bush Administration 7
  Pre-September 11 7
  Post-September 11 8
The Obama Administration 12
Department of Homeland Security 13
  Initial Establishment 13
  Second Stage Review Reorganization 14
  Post-Katrina Emergency Management Reform Act of 2006 15
Policy Implementation 16
  Government—Sector Coordination 16
  Appointment of the National Infrastructure Advisory Council 19
  Internal Agency Plans 19
  National Critical Infrastructure Plan 21
  Information Sharing and Analysis Center (ISAC) 23
  Identifying Critical Assets, Assessing Vulnerability and Risk, and Prioritizing Protective Measures 24
Issues and Discussion 26
  Identifying Critical Assets, Functions, and Systems 26
  Assessing Vulnerabilities and Risk 27
  Allocating Resources 28
  Information Sharing 29
  Regulation 31

Tables

Table 1. Lead Agencies per PDD-63 5
Table 2. Current Lead Agency Assignments 17
Table 3. Performance Measures for the Infrastructure Protection and Risk Management Program 28
Table A-1. Funding for Protecting the American People, Our Critical Infrastructure, and Key Resources by Department (*Funding for Critical Infrastructure and Key Resources Protection*) 35
Table A-2. Funding for the Infrastructure Protection and Information Security Program 37

Appendixes

Appendix. Funding for Critical Infrastructure 33

Contacts

Author Contact Information 38

GalleryWatch.com
http://www.crsdocuments.com
Penny Hill Press

Latest Update Information

This update includes the President's FY2012 budget request for activities related to critical infrastructure protection (see **Appendix**) and the Obama Administration's legislative proposal requiring owners and operators of selected critical infrastructure assets to develop cybersecurity plans (see "The Obama Administration").

Introduction

Certain socioeconomic 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, functions, information, people, and systems forming what has been called the nation's critical infrastructures. These infrastructures have grown complex and interconnected, meaning that a disruption in one may lead to disruptions in others.[2]

Disruptions can be caused by any number of factors: poor design, operator error, physical destruction due to natural causes, (earthquakes, lightning 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 reliability and safety. However, the terrorist attacks of September 11, and the subsequent anthrax attacks, demonstrated the need to reexamine protections in light of the terrorist threat, as part of an overall critical infrastructure protection policy.[3]

This report provides an historical background and tracks the evolution of such an overall policy and its implementation. However, specific protections associated with individual infrastructures is beyond the scope of this report. For CRS products related to specific infrastructure protection efforts, the reader is encouraged to visit the Homeland Security Current Legislative Issues webpage and look at the Critical Infrastructure Security link.

[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.

[2] The electricity blackout in August 2003 in the United States and Canada illustrated the interdependencies between electricity and other elements of the energy market such as oil refining and pipelines, as well as communications, drinking water supplies, etc.

[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.

Federal Critical Infrastructure Protection Policy: In Brief

As discussed further below, a number of federal executive documents and federal legislation lay out a basic policy and strategy for protecting the nation's critical infrastructure. To summarize, it is the policy of the United States to enhance the protection of the nation's critical infrastructure. Critical infrastructure has been defined as those systems and assets, the destruction or incapacity of which would:

- cause catastrophic health effects or mass casualties comparable to those from the use of weapons of mass destruction,
- impair Federal departments and agencies' abilities to perform essential missions or ensure the public's health and safety,
- undermine State and local government capacities to maintain order and deliver minimum essential public services,
- damage the private sector's capability to ensure the orderly functioning of the economy,
- have a negative effect on the economy through the cascading disruption of other critical infrastructure,
- or undermine the public's morale and confidence in our national economic and political institutions.[4]

The federal government will work with states, localities, and the owners and operators of critical infrastructure (in both the private and public sector) to identify those specific assets and systems that constitute the nation's critical infrastructure. Together, these entities will assess those assets' vulnerabilities to the threats facing the nation (natural or manmade, i.e., all hazards), determine the level of risk associated with possible attacks or the impacts of natural events on those assets, and identify and prioritize a set of measures that can be taken to reduce those risks. Primary responsibility for protection, response, and recovery lies with the owners and operators.[5] However, the federal government holds open the possibility of intervening in those areas where owners and operators are unable (or unwilling) to provide what it, the federal government, may assess to be adequate protection or response.[6]

[4] White House, Homeland Security Presidential Directive Number 7, *Critical Infrastructure Identification, Prioritization, and Protection.* Released December 17, 2003. A more general definition is given in statute (P.L. 107-71, Sec. 1016): "systems and assets, 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."

[5] See White House. Office of Homeland Security. *National Strategy for Homeland Security*, p. 33, "Private firms bear primary and substantial responsibility for addressing the public safety risks posed by their industries."

[6] Op. cit., p. 33, "The plan will describe how to use all available policy instruments to raise the security of America's critical infrastructure and key assets to a prudent level.... In some cases the Department may seek legislation to create incentives for the private sector to adopt security measures.... In some cases, the federal government will need to rely on regulation."

The reader who is not interested in the evolution of this policy and the organizational structures that have evolved to implement it can proceed to the "Policy Implementation" and/or "Issues and Discussion" sections of this report.

The President's Commission on Critical Infrastructure Protection

This report takes as its starting point the establishment of the President's Commission on Critical Infrastructure Protection (PCCIP) in July 1996.[7] Its tasks were to: report to the President the scope and nature of the vulnerabilities and threats to the nation's critical infrastructures (focusing primarily on cyber threats);[8] recommend a comprehensive national policy and implementation plan for protecting critical infrastructures; determine legal and policy issues raised by proposals to increase protections; and propose statutory and regulatory changes necessary to effect recommendations.

The PCCIP released its report to President Clinton in October 1997.[9] 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;

[7] 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.

[8] Given the growing dependence and interconnectedness of the nation's infrastructure on computer networks, there was concern that computers and computer networks presented a new vulnerability and one that was not receiving adequate attention.

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

- 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)[10] set as a national goal the ability to protect the nation's critical infrastructure from intentional attacks (both physical and cyber) by the year 2003. According to the PDD, any interruptions in the ability of these infrastructures to provide their goods and services must be "brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States."[11]

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. 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.

[10] 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 Scientists website: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

[11] Ibid.

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 Internal Security[a]
Director of Central Intelligence	Intelligence[a]
State	Foreign Affairs[a]
Defense	National Defense[a]

a. These are the functions identified by PDD-63 as being primarily under federal control.

The PDD also assigned duties to the **National Coordinator** for Security, Infrastructure Protection, and Counter-terrorism.[12] The National Coordinator reported to the President through the Assistant to the President for National Security Affairs.[13] Among his many duties outlined in PDD-63, the National Coordinator chaired the **Critical Infrastructure Coordination Group**. This Group was the primary interagency working group for developing and implementing policy and for coordinating the federal government's own internal security measures. The Group included high level representatives from the lead agencies (including the Sector Liaisons), the National Economic Council, and all other relevant agencies.

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

The PDD set up a **National Infrastructure Assurance Council**. The Council was to be a panel that included private operators of infrastructure assets and officials from state and local

[12] 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.

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

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 national education and awareness programs, and provided legislative and public affairs support. Coordinating the development of and maintaining the National Plan is now part of the Department of Homeland Security Infrastructure Protection and Information Security (IPIS) program.

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. The Directive explicitly gave the Federal Bureau of Investigation the authority to expand its 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[14] and FedCIRC would feed into the NIPC. According to the Directive, the NIPC would be linked

[14] FIDNET initially 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. A comparable capability has been developed, called the EINSTEIN Program, that addressed the privacy concerns of FIDNET. Under EINSTEIN, participating agencies retain complete control of network data in strict accordance with Federal laws and polices. Agencies gather and subsequently share security data directly with DHS, based on reporting requirements established by the Office of Management and Budget. In turn, DHS prepares a strategic, cross-agency assessment, which is then shared back with all federal civilian agencies. As part of a broader cyber security initiative aimed at better securing federal information systems, the EINSTEIN program has expanded to include all federal agencies and to use improved sensors to monitor network traffic on federal systems. The current phase of the program, EINSTEIN III, would monitor federal network traffic from sensors placed on internet service provider networks servicing federal agencies. These new sensors would also provide the capability to counter intrusion attempts (i.e. intrusion prevention). Notwithstanding the results of privacy impact statements, the involvement of the National Security Agency in developing and implementing the EINSTEIN technology has resurrected privacy concerns.

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. These functions have been transferred to and greatly expanded upon at the Department of Homeland Security. The **U.S. Computer Emergency Response Team (U.S. CERT)** now handles the computer security incidents occurring on non-national security federal systems and the **National Operations Center (NOC)** provides all hazard situation awareness.

Quite independent of PDD-63 in its origin, but clearly complimentary in its purpose, the FBI established a program called **INFRAGARD** to interact with private sector firms. The program facilitates information exchange between FBI field offices and the surrounding business communities. Its initial focus was network security. After September 11, its focus included both cyber and physical security. INFRAGARD is geographically oriented rather than sector-oriented. Each FBI field office has a Special Agent Coordinator who gathers interested companies of various sizes from all industries to form a chapter. Any company can join INFRAGARD. Local executive boards govern and share information within the membership. Chapters hold regular meetings to discuss issues, threats, and other matters that impact their companies. Chapters may also engage in contingency planning for using alternative systems in the event of a successful large scale attack on the information infrastructure. The program was transferred to the NIPC, before it was absorbed by the Department of Homeland Security. The program is now managed by the FBI's Cyber Division.[15]

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 include the cyber dimension.[16] The Department of Homeland Security is now responsible for creating 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 incoming 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 infrastructure protection activities begun by the Clinton Administration.

[15] For more information on INFRAGARD, see http://www.infragard.net.

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

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 advocating that the function be transferred directly to the White House.[17]

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 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 reasons cited for this was a desire to keep agencies responsible for their own computer security.[18]

Third, there was the continuing debate about how best to defend the country against terrorism, in general. 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 a 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**.[19] 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 was the coordination of efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks. This included strengthening measures for protecting energy production, transmission, and distribution;

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

[18] For a discussion of the debate surrounding this issue at the time, see CRS Report RL30914, *Federal Chief Information Officer (CIO): Opportunities and Challenges*, by Jeffrey W. Seifert.

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

telecommunications; public and privately owned information systems; transportation systems; and, the provision of food and water for human use. Another function of the Office was to coordinate efforts to ensure rapid restoration of these critical infrastructures after a disruption by a terrorist threat or attack. Many of the functions of the Office of Homeland Security were transferred to the Department of Homeland Security when the latter was established (see below).[20]

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. The EO was later amended to add the Secretary of Homeland Security. Other White House and departmental officials can be invited to attend Council meetings.[21] 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.[22]

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 remained 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."[23] This Order also established the **President's Critical Infrastructure Protection Board**. The Board, consisting of federal officials, was authorized to "recommend policies and coordinate programs for protecting information systems for critical infrastructure." The Board also 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**.[24] 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

[20] Some of the staff of the Office of Homeland Security migrated to the Homeland Security Council. For a discussion of budget issues surrounding this, see, CRS Report RS22840, *Organizing for Homeland Security: The Homeland Security Council Reconsidered*, by Harold C. Relyea.

[21] For more information on how the Homeland Security Council and the Office of Homeland Security were structured, see CRS Report RL31148, *Homeland Security: The Presidential Coordination Office*, by Harold C. Relyea.

[22] In February 2009, President Obama ordered a review of the White House's organization for homeland security and counterterrorism. In May 2009 he directed that the staff of the two organizations be merged, but retained the independence of the two Councils. See discussion below.

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

[24] President Bush designated Richard Clarke.

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 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 sectors considered to possess critical infrastructure to include public health, the chemical industry and hazardous materials, postal and shipping, the defense industrial base, and agriculture and food. The *Strategy* also added continuity of government and continuity of operations to the list, although it is difficult to see how the latter would be a considered sector. It also combined emergency fire service, emergency law enforcement, and emergency medicine as emergency services. And, it dropped those functions that primarily belonged to the federal governments (e.g., defense, intelligence, law enforcement). It also reassigned some of the sectors to different agencies, including making the then proposed Department of Homeland Security lead agency for a number of sectors—postal and shipping services, and the defense industrial base. It also introduced a new class of assets, called key assets, which was defined as potential targets whose destruction may not endanger vital systems, but could create a local disaster or profoundly affect national morale. Such assets were defined later to include national monuments and other historic attractions, dams, nuclear facilities, and large commercial centers, including office buildings and sport stadiums, where large numbers of people congregate to conduct business, personal transactions, or enjoy recreational activities.[25]

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 also mentioned the need to set priorities, acknowledging that not all assets are equally critical, and that the costs associated with protecting assets must be balanced against the benefits of increased security according to the threat. The Strategy did not create any new organizations, but assumed that a Department of Homeland Security would be established (see below). The Strategy was updated in October 2007.[26] With the exception of a somewhat greater recognition of the role improving resilience can play in reducing the nation's risk, the strategy related to critical infrastructure saw little change.

[25] The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. February 2003. p. 71.

[26] Homeland Security Council. *National Strategy for Homeland Security*. October 2007.

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)[27] to work with their sectors to identify, prioritize, and coordinate protective measures. The Directive captured the expanded set of critical infrastructures and key assets and Sector-Specific Agencies assignments 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 a 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 for transportation security, including airline security, the Department of Transportation remains responsible for control of the national air space system.

The only organizational change made by the Directive was the establishment of the **Critical Infrastructure Protection Policy Coordinating Committee** to 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 required 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 Bush Administration policy and approach regarding critical infrastructure protection can be described as an evolutionary expansion of the policies and approaches laid out in PDD-63. The fundamental policy statements were essentially the same: the protection of infrastructures critical to the people, economy, essential government services, and national security. National morale was 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 was 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 remained an interagency group for coordinating policy across departments and for informing the White House (Homeland Security Council, supported by the Critical Infrastructure Protection Coordinating Committee). Certain agencies were assigned certain sectors with which to work. Sectors were asked to organize themselves to assist in coordination of

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

effort and information sharing. 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)) were initially left in place, though later moved to and restructured within the Department of Homeland Security (DHS), where, now, the Undersecretary for National Protection and Programs is responsible for coordinating the implementation of policies and programs (see below). However, DHS takes a much more active role in identifying critical assets, assessing vulnerabilities, and recommending and supporting protective measures than did these earlier operational units. Also, the manpower and resources devoted to these activities have greatly increased.

One major difference between PDD-63 and the Bush Administration's efforts was a shift in focus. PDD-63 focused on cybersecurity. While the post-September 11 effort is still concerned with cybersecurity, its focus on physical threats, especially those that might cause mass casualties, is greater than the pre-September 11 effort. This led to some debate and organizational instability initially. The early executive orders discussed above segregated cyber security from the physical security mission with the formation of the Office of Homeland Security and the President's Critical Infrastructure Protection Board. Dissolution of the Board and the subsequent establishment of the Critical Infrastructure Protection Policy Coordinating Committee, responsible for advising the Homeland Security Council on both physical and cyber security issues, appears to have reunited these two concerns within a single White House group.[28]

The Obama Administration

The Obama Administration has, to date, kept in place much of the policy and organization of the Bush Administration. In February 2009, President Obama ordered a review of the homeland security and counterterrorism structures within the White House (**Presidential Security Directive 1**).[29] Debate centered on the merging of the Homeland Security Council and the National Security Council. In May, the President directed that the staff of the two councils be merged into the National Security Staff, while retaining the independence of the two councils.[30] President Obama also ordered a review of the federal government's policies and activities on cyber security.[31] The results of that review were released on May 29, 2009.[32] One result of the cyber security policy

[28] Computer security advocates have sought to highlight cyber security issues by maintaining a separate organization high within the bureaucracy. There now exists both an Assistant Secretary for Cyber Security and Telecommunications and an Assistant Secretary for Infrastructure Protection, both reporting to the Undersecretary for National Protection and Programs. While the latter is concerned with both physical and cyber security issues, the former is focused on cyber security issues.

[29] Presidential Security Directive 1. *Organizing for Homeland Security and Counterterrorism*. Feb. 23, 2009. See http://www.fas.org/irp/offdocs/psd/psd-1.pdf. As part of this reorganization, a Resilience Directorate was established that includes in its portfolio critical infrastructure protection and resilience.

[30] White House, "Statement by the President on the White House Organization for Homeland Security and Counterterrorism," press release, May 26, 2009, http://www.whitehouse.gov/the_press_office/Statement-by-the-President-on-the-White-House-Organization-for-Homeland-Security-and-Counterterrorism.

[31] White House, "President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review," press release, February 9, 2009, http://www.whitehouse.gov/the_press_office/AdvisorsToConductImmediateCyberSecurityReview.

[32] White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

review was to recommend the appointment of a White House official to coordinate cyber security policies and activities across the federal government. The recommendation and subsequent appointment reestablished a cyber security coordinating function within the White House.[33]

In May 2011, the Obama Administration released proposed legislation aimed to strengthen cybersecurity.[34] Among the provisions was a proposed regulatory framework to enhance the cybersecurity at those infrastructures sites considered by the Secretary of Homeland Security to be critical to the nation. Owners and operators of designated infrastructure assets would be required to develop cybersecurity plans, have those plans evaluated by accredited outside evaluators, and to report to the Securities and Exchange Commission. Congress is considering elements of this proposal in their own pending cybersecurity legislation.

Department of Homeland Security

Initial Establishment

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 an attack occur. The act essentially consolidated within one department a number of agencies that had, as part of their missions, homeland security-like functions (e.g., Border Patrol, Customs, Transportation Security Administration). 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),**[35] other energy security and assurance activities within DOE, and the **National Communication System (NCS).**[36] These agencies and offices were integrated within the Directorate of Information Analysis and Infrastructure Protection (IA/IP) (one of four operational Directorates established by

[33] President Obama named Howard Schmidt to this position, who had served briefly as President Bush's Special Advisor on Cybersecurity before that position was abolished. See http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator.

[34] *The Administration Unveils Its Cybersecurity Legislative Proposal*. See http://www.whitehouse.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal.

[35] 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 and the interdependencies between them.

[36] 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, which 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.

the act).[37] Notably, the Transportation Security Administration (TSA), which is responsible for securing all modes of the nation's transportation system, was not made part of this Directorate (it was placed within the Border and Transportation Security Directorate); nor was the Coast Guard, which is responsible for port security. The act assigned the rank of Undersecretary to the head of each Directorate. Furthermore, the act designated that within the Directorate of Information Analysis and Infrastructure Protection, there were to 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).

Second Stage Review Reorganization

Secretary Chertoff (the second Secretary of Homeland Security), as one of his Second Stage Review recommendations, proposed restructuring the IA/IP Directorate and renaming it the **Directorate of Preparedness**. The IA function was merged into a new **Office of Intelligence and Analysis**. The IP function, with the same missions as outlined in the Homeland Security Act,

[37] As the result of reorganizations, the IA/IP Directorate no longer exists. The infrastructure protection activities originally given to the IA/IP Directorate are now performed by the National Protection and Programs Directorate. See below.

remained, but was joined by other existing and new entities. The renamed Directorate included elements from Office of State and Local Government Coordination and Preparedness, including its principal grant-making functions and some of the preparedness functions of the Federal Emergency Management Agency (FEMA). A new position of Chief Medical Officer was created within the Directorate and the U.S. Fire Administration and the Office of National Capital Region Coordination were transferred into the Directorate. In addition, the restructuring called for an **Assistant Secretary for Cyber Security and Telecommunications** (a position sought by many within the cyber security community following the termination of the position of Special Advisor to the President for Cyberspace Security) and an Assistant Secretary for Infrastructure Protection.

According to the DHS press release, the mission of the restructured Directorate was to "facilitate grants and oversee nationwide preparedness efforts supporting first responder training, citizen awareness, public health, infrastructure and cyber security, and [to] ensure proper steps are taken to protect high-risk targets."

Other recommendations resulting from the review that impacted infrastructure protection included moving the Homeland Security Operations Center, now called the National Operations Center, out of the old IA/IP Directorate and placing it within a new Office of Operations Coordination; and, a new Directorate of Policy, which is described as serving as the primary Department-wide coordinator of policies, regulations, and other initiatives. The conference committee report on the Department's FY2006 appropriations (H.Rept. 109-241) approved these changes.[38]

Post-Katrina Emergency Management Reform Act of 2006

The Post-Katrina Emergency Management Reform Act of 2006 (referred hereon as the Post-Katrina Act) was passed as Title VI of the Department of Homeland Security Appropriations Act, 2007 (P.L. 109-295). The Post-Katrina Act reunited the Department's preparedness activities with its response and recovery activities within a restructured Federal Emergency Management Agency (FEMA). The Post-Katrina Act explicitly preserved the restructured FEMA as a distinct entity within the Department. The Post-Katrina Act also transferred the Preparedness Directorate's Office of Grants and Training to the restructured FEMA. The Post-Katrina Act left the remaining activities, including those associated with the Office of the Chief Medical Officer and the critical infrastructure protection activities associated with the Assistant Secretary of Infrastructure Protection and the Assistant Secretary for Cyber Security and Telecommunications, in the Preparedness Directorate. The Post-Katrina Act also established the **Office of Emergency Communications** and required that it report to the Assistant Secretary for Cyber Security and Telecommunications. The Office of Emergency Communications has within its responsibilities a number of activities associated with assisting interoperable communications among first responders.

On January 18, 2007, Secretary Chertoff submitted to Congress a description of the Department's reorganization pursuant to the Post-Katrina Act, and additional changes made pursuant to the Secretary's authority provided in the Homeland Security Act (P.L. 107-296, Section 872). Under this latter authority, the Secretary renamed the Preparedness Directorate the **National Protection and Programs Directorate** (NPPD), still to be headed by someone of Undersecretary rank. The

[38] See report language, H.Rept. 109-241, accompanying H.R. 2360, September 2005, p. 29.

NPPD includes the Office of the Undersecretary, the Office of Cybersecurity and Communications (including the new Office of Emergency Communications), the Office of Infrastructure Protection, the Office of Risk Management and Analysis (formerly a division of the Office of Infrastructure Protection), and the Office of Intergovernmental Programs. In addition, the Secretary moved the U.S.-VISIT program into the NPPD.[39]

The Secretary also, pursuant to his Section 872 authority, transferred the Chief Medical Officer to head a new Office of Health Affairs. This new Office reports to the Secretary through the Deputy Secretary. This reorganization consolidated activities associated with the Department's bio-defense efforts, including the transfer of the Biosurveillance program, formerly part of the Infrastructure Protection and Information Security (IPIS) Program (see **Appendix**). Except for the transfer of the Biosurveillance program, the IPIS program, which represents the core of the Department's effort to coordinate the nation's critical infrastructure protection activities, remained in the National Protection and Programs Directorate.

Policy Implementation

Government—Sector Coordination

The number and breakdown of sectors and lead, or sector specific agencies, have expanded and changed since the assignments made by PDD-63 (see **Table 1**). As mentioned above, the Bush Administration has expanded the number of sectors considered to possess critical infrastructure and made some changes in assignments.

In March 2008, DHS announced that it was designating what would be an 18th critical infrastructure sector, Critical Manufacturing.[40] The sector includes certain sub-groups from the primary metal, machinery, electrical equipment, and transportation equipment manufacturing industries.[41] The designation was made by the Secretary by authority granted him in HSPD-7, and represents the first exercise of that authority. **Table 2**, below, shows the current list of sectors and their lead agencies.

PDD-63 called for the selection, by each Lead Agency, of a Sector Liaison Official (representing the Lead Agency) and a Sector Coordinator (representing the owners/operators of each sector). While most agencies quickly identified their Sector Liaison Official, it took more time to identify Sector Coordinators. Different sectors present different challenges for coordination. 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 raise 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,

[39] U.S.-VISIT is the Department's effort to verify the identity of people entering and exiting the United States.

[40] Department of Homeland Security. Designation of the National Infrastructure Protection Plan Critical Manufacturing Sector. *Federal Register*. Vol 73, No. 84. April 30, 2008. pp23476-23478.

[41] These include iron and steel, ferro alloys, alumina and aluminum, and other non-ferrous metal production; engine, turbine, and power transmission equipment; and, motor vehicle, aerospace products, railroad rolling stock, and other transportation equipment.

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.

Table 2. Current Lead Agency Assignments

Department/Agency	Sector/Subsector
Agriculture	Agriculture
	Food
Agriculture	Meat/Poultry
Health and Human Services	All other
Treasury	Banking and Finance
EPA	Drinking Water and Water Treatment Systems
Health and Human Services	Public Health and Healthcare
Defense	Defense Industrial Base
Interior	National Monuments and Icons
Energy	Energy[a]
Homeland Security	Transportation Systems[b]
Homeland Security	Postal and Shipping
Homeland Security	Information Technology
Homeland Security	Communications
Homeland Security	Commercial Nuclear Reactors, Materials, and Waste
Homeland Security	Chemical
Homeland Security	Emergency Services
Homeland Security	Dams
Homeland Security	Commercial Facilities
Homeland Security	Government Facilities
Homeland Security[c]	Critical Manufacturing

a. While noted here as a single sector, in practice it is represented by two relatively separate sectors: electric power (except for nuclear power facilities); and the production, refining, and some distribution of oil and gas. The Department of Energy is the lead agency for both. However, the Department of Homeland Security (through the Transportation Security Administration) is the lead agency for the distribution of oil and gas via pipelines. Nuclear power is considered its own sector.

b. While noted here as a single sector, Transportation includes all modes of transportation: rail, mass transit (rail and bus), air, maritime, highways, pipelines, etc. The Transportation Security Administration within the Department of Homeland Security, in collaboration with the Department of Transportation, is the lead agency for all but the maritime subsector, for which the Coast Guard, also within the Department of Homeland Security, acts as lead agency.

c. According to the Federal Register announcement, the Department of Homeland Security will act as the interim Lead Agency.

In addition to 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.

Over time, Sector Coordinators were selected for most of the sectors identified under PDD-63. Typically, a representative from a relevant trade organizations was chosen to act as sector coordinator. For example, the Environmental Protection Agency selected the Executive Director of the Association of Metropolitan Water Agencies to act as Sector Coordinator for the water sector. In the case of the law enforcement sector (no longer identified as a separate sector), the National Infrastructure Protection Center helped create a Emergency Law Enforcement Services Forum, consisting of senior state, local, and non-FBI law enforcement officials. In the case of banking and finance, the Sector Coordinator was chosen from a major banking/finance institution, who doubled as the Chairperson of the Financial Services Sector Coordinating Council, an organization specifically set up by the industry to coordinate critical infrastructure protection activities with the federal government.

In December 1999, a number of the sectors formed a **Partnership for Critical Infrastructure Security** to share information and strategies and to identify interdependencies across sectoral lines. The Partnership was a private sector initiative. The federal government was not officially part of the Partnership, but the Department of Homeland Security (and CIAO before that) acted as a liaison and provided administrative support for meetings. Sector Liaisons from lead agencies were considered ex officio members. The Partnership helped coordinate its members input to a number of the national strategies released to date and were to provide input into the National Plan called for in PDD-63.

While initially working with this organizational structure, the Bush Administration promoted a new Critical Infrastructure Protection Partnership Model. Resembling the Financial Services Sector Coordinating Council approach, this newer Model expanded the sector liaison and sector coordinator model of PDD-63 into **Government Coordinating Councils** and **Sector Coordinating Councils** for each sector. The primary objective was to expand both owner/operator and government representation within all sectors. For example, the Water Sector Coordinating Council expanded to include two owner/operator representatives, along with one non-voting association staff, from each of the following participating organizations: the Association of Metropolitan Water Agencies, the American Water Works Association, the American Water Works Association Research Foundation, the National Association of Clean Water Agencies, the National Association of Water Companies, the National Rural Water Association, the Water Environment Federation, and the Water Environment Research Foundation. The Water Government Coordinating Council is chaired by the Environmental Protection Agency, the Lead Agency, but also includes the Department of Homeland Security, the Food and Drug Administration, the Department of Interior, and the Center for Disease Control. Government Coordinating Councils can also include state, local, and tribal government entities. The Sector Coordinating Councils are to establish their own organizational structures and leadership and act independently from the federal government. Also, under this model, the Partnership for Critical Infrastructure Security has been designated the **Private Sector Cross-Sector Council**. The Sector Coordinating Councils are to provide input into both the National Infrastructure Protection Plan and the individual Sector Specific Plans (see below). Many of the issues governing the progress made in identifying and working with the sector coordinators model of PDD-63 continue with the sector coordinating councils.[42]

[42] See U.S. Congress. General Accountability Office. *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*. GAO-07-39. October 2006.

In March 2006, the Department of Homeland Security used its authority under the Homeland Security Act (P.L. 107-296, Section 871) to form advisory committees that are exempt from the Federal Advisory Committee Act (P.L. 92-463) to establish the **Critical Infrastructure Partnership Advisory Council (CIPAC)**.[43] The Federal Advisory Committee Act requires advisory committees generally to meet in open session and make written materials available to the public. The purpose of waiving this act for the CIPAC is to facilitate more open discussion between the sector coordinating councils and the government coordinating councils (if not with the public). DHS acts as the Executive Secretariat. Members include owner/operators that are members of their respective sector coordinating councils or belong to an association that is a member of the coordinating council. Members also include federal, state, local, and tribal government entities that belong to their respective government coordinating councils. While the CIPAC is exempt from the Federal Advisory Committee Act, DHS stated in its public notice that it will make meeting dates and appropriate agendas available. There is a CIPAC webpage on the DHS website.[44]

Appointment of the National Infrastructure Advisory Council

The Clinton Administration released an Executive Order (13130) in July, 1999, formally establishing the National Infrastructure Assurance Council. Just prior to leaving office, President Clinton put forward the names of 18 appointees.[45] The Order was rescinded by the Bush Administration before the Council could meet. In Executive Order 13231,[46] President Bush established a National Infrastructure Advisory Council (with the same acronym, NIAC) whose functions were similar to those of the Clinton Council. On September 18, 2002, President Bush announced his appointment of 24 individuals to serve on Council.[47] 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.[48]

Internal Agency Plans

There had been some confusion about which agencies were required by PDD-63 to submit critical infrastructure plans. The Directive required 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

[43] See *Federal Register*. Vol. 71 No. 57. pp. 14930-14933. March 24, 2006.

[44] See http://www.dhs.gov/xprevprot/committees/editorial_0843.shtm.

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

[46] Executive Order 13231—Critical Infrastructure Protection in the Information Age. Federal Register. Vol. 66. No. 202. October 18, 2001. pp. 53063-53071. The NIAC is established on page 53069.

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

[48] The current membership and activities of the National Infrastructure Advisory Council can be found on the DHS website. See http://www.dhs.gov/xprevprot/committees/editorial_0353.shtm.

plans for protecting their own critical infrastructures from attacks and for responding to intrusions. The Critical Infrastructure Assurance Office (CIAO) assembled an expert team to review the plans. The plans were assessed in 12 areas including schedule/milestone planning, resource requirements, and knowledge of existing authorities and guidance. The assessment team handed back the initial plans with comments. Agencies were given 90 days to respond to these comments. Of the 22 "primary" and "secondary" agencies that submitted plans, 16 modified and resubmitted them in response to first round comments.

Initially, the process of reviewing 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 was voluntary.[49]

In the meantime, other agencies (i.e., those not designated as primary or 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[50] 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.[51]

HSPD-7 reestablished a deadline for agencies to submit critical infrastructure protection plans to the Director of OMB for approval by July 2004. The Director of OMB provided guidance on how agencies should meet their requirement (Memorandum M-04-15, June 17, 2004). The memorandum stated that plans for the physical protection of assets would be subject to interagency review coordinated by the Department of Homeland Security, with DHS providing a written evaluation of each agency's plans within 120 days. Agency cyber security plans would be reviewed by OMB, as part of the requirements associated with the Federal Information Security Management Act of 2002, included as Title III of E-Government Act of 2002 (P.L. 107-347). These plans are to provide information to be included in the National Infrastructure Protection

[49] The use of Project Matrix's methodology continues under HSPD-7.

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

[51] 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. pp. 4-5.

Plan (see below). DHS and OMB have not been willing to provide CRS with the status of these reports.

National Critical Infrastructure Plan

PDD-63 called for a National Infrastructure Assurance Plan that would be informed by sector-level plans and would include an assessment of minimal operating requirements, vulnerabilities, 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 specifying deadlines and 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. According to HSPD-7, the National Plan should include (a) a strategy to identify, prioritize, and coordinate the protection of critical infrastructure and key resources, including how the Department will work with other stakeholders; (b) a summary of activities to be undertaken in order to carry out the strategy; (c) a summary of initiatives for sharing critical infrastructure information and threat warnings with other stakeholders; and (d) coordination with other federal emergency management activities.

In January 2000, the Clinton Administration released Version 1.0 of a *National Plan for Information Systems Protection*.[52] In keeping with the original focus of PDD-63, the Plan focused primarily on cyber-related efforts within the federal government. The Bush Administration, through the President's Critical Infrastructure Protection Board, released *The National Strategy to Secure Cyberspace* in February 2003, which 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*. This strategy took a broad perspective of the issues and needs associated with organizing the nation's efforts to protect its critical infrastructure; identifying roles and responsibilities, actions that need to be taken, and guiding principles.

The Department of Homeland Security missed the December 2004 deadline for releasing the National Infrastructure Protection Plan called for in HSPD-7. It did publish an Interim National Infrastructure Protection Plan in February 2005. According to media reports, some in the private sector complained they were not adequately consulted.[53] The Department subsequently released for public comment a "draft" National Infrastructure Protection Plan in November 2005.[54] A final version of the National Infrastructure Protection Plan (NIPP) was approved June 30, 2006. The NIPP was revised in early 2009 to reflect the evolution and maturation of the process, including

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

[53] See "Still Waiting: Plan to Protect Critical Infrastructure Overdue from DHS," Congressional Quarterly. Homeland Security-Transportation & Infrastructure Newsletter, January 28, 2005. The Newsletter is electronic and available by subscription only. See http://homeland.cq.com/hs/display.do?dockey=/cqonline/prod/data/docs/html/hsnews/109/hsnews109-000001507251.html@allnews&metapub=HSNEWS&seqNum=827&searchIndex=1.

[54] See *Federal Register*, vol. 70, no. 212, November 3, 2005, pp. 66840-66841.

expanded integration of all-hazard and resiliency concepts.[55] The changes do not appear to represent major shifts in policy or programs.

The NIPP identifies and integrates specific processes by which an integrated national risk management effort can proceed. For example, it defines and seeks to standardize, across all sectors, the process for identifying and selecting assets for further analysis, identifying threats and conducting threat assessments, assessing vulnerabilities to those threats, analyzing consequences, determining risks, identifying potential risk mitigation activities, and prioritizing those activities based on cost-effectiveness.[56] The NIPP also calls for implementation plans for these risk reduction activities, with timelines and responsibilities identified, and tied to resources. Each lead agency is to work with its sector to generate **Sector Specific Plans**, utilizing the processes outlined in the NIPP. DHS will then use these same processes to integrate the sector specific plans into a national plan that identifies those assets and risk reduction plans that require national level attention because of the risk the incapacitation of those assets pose to the nation as a whole.[57]

According to the NIPP, Sector Specific Plans (SSPs) were due 180 days after release of the NIPP (i.e., the end of 2006). Apparently, all 17 sectors met that deadline. However, they went through a DHS review process before being released in May 2007. Of the 17 plans submitted, 7 were made available to the public, the rest were designated For Official Use Only.[58] The Government Accountability Office (GAO) reviewed 9 of the SSPs and found that while all complied, more or less, with the NIPP process, some plans were more developed and comprehensive than others.[59] As a result, GAO was unable to assess how far along each sector actually is in identifying assets, setting priorities, and protecting key assets. DHS views these SSPs as a first step in the process, and plans to review the sectors' annual progress reports, as required by HSPD-7.

It should be noted, that some sectors and agencies have performed already some or all of these risk management steps using various techniques and processes. The NIPP requires that each sector and lead agency ensure that previous work meets the basic requirements associated with the processes described in the NIPP.

Distinguishing between a strategy and plan, and whether these documents yet fulfill the requirement for the comprehensive national plan called for in the Homeland Security Act, is beyond the scope of this report. However, each succeeding document does appear to refine further some goal, objective, or initiative discussed in preceding documents.

---

[55] The 2009 version of the NIPP can be found at http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.

[56] For a discussion of a basic risk management process in a critical infrastructure context, see CRS Report RL32561, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*, by John D. Moteff.

[57] The Homeland Infrastructure Threat and Risk Center (HITRAC), a joint effort by the Office of Infrastructure Protection and the Office of Intelligence and Analysis, through its Strategic Homeland Infrastructure Risk Assessment (SHIRA) program prioritizes the risk across all sectors to produce an annual National Critical Infrastructure and Key Resources Risk Profile.

[58] See http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm#2 for a short discussion and to access those SSPs that are not designated as For Official Use Only.

[59] Government Accountability Office. *Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve*. GAO-07-706R. July 10, 2007.

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, analyzing, 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. ISACs differ somewhat from sector coordinating councils in that ISACs were to be 24/7/365 operations, where incidents experienced by owner/operators, as well as threat information from the government, could be reported, analyzed, and shared. 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.

ISACs were formed around two primary models. One model involved ISAC members legally incorporating and establishing either their own ISAC operations or contracting operations out to a security firm. The banking, information, water, oil and gas, railroad, and mass transit sectors followed this approach.

The other model involved 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]) followed this model. The emergency fire services sector incorporated ISAC functions into the existing operations of the U.S. Fire Administration, which has interacted with local fire departments for years.

Different federal financial support models were developed for ISACs, too. In some cases, ISACs received start up funding from their Lead Agency (e.g., drinking water received funding from EPA). In some cases, that support continues, in some cases the support has not continued (e.g., DOE no longer supports the energy ISAC). Other ISACs have always been self-supporting. The individual ISACs have formed a group called the ISAC Council.[60] Their formation and function experience some of the same variation as the coordinating councils, for some of the same reasons.

While PDD-63 envisioned ISACs to be a primary conduit for exchanging critical infrastructure information between the federal government and specific sectors, the Department of Homeland Security has developed a number of other information sharing systems and mechanism. In addition to the Sector Coordinating Councils discussed above, **US-CERT** (the U.S. Computer Emergency Readiness Team, which took over many of the NIPC functions) publishes information on the latest computer-related vulnerabilities and threats and information on how to respond to a specific incident. U.S.-CERT also accepts incidents reports. It also manages the **National Cyber Alert System**, to which any organization or individual can subscribe. The Department also has developed a **Homeland Security Information Network (HSIN)**. HSIN initially served as the primary communication network for communicating and analyzing threat information between government law enforcement agencies at the federal, state, and local levels. The HSIN now provides real-time connectivity between all 50 states, 5 territories, and 50 urban areas and the National Operations Center at DHS. The HSIN is being expanded to include each critical infrastructure sector (dubbed HSIN-CI) as part of the Critical Infrastructure Protection Partnership Model (i.e., through each sector and government coordinating council).

[60] See http://www.isaccouncil.org.

Shortly after September 11, 2001, the Department established what is now called the Infrastructure Protection **Executive Notification Service (ENS)**, which connects DHS directly with the Chief Executive Officers of major industrial firms. The ENS is used to alert partners to infrastructure incidents, to disseminate warning products, and to conduct teleconferences. The Department is also responsible for operating the **Critical Infrastructure Warning Network (CWIN)**, which provides secure communications between DHS and other federal, state, and local agencies, the private sector, and international agencies. CWIN does not rely on the Public Switch Network or the internet.[61]

Identifying Critical Assets, Assessing Vulnerability and Risk, and Prioritizing Protective Measures

Among the activities assigned to the Information Analysis and Infrastructure Protection Directorate by the Homeland Security Act of 2002 were:

- 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;
- 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;
- 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 of Critical Infrastructures and Key Assets*, the Department of Homeland Security: (a) "in collaboration with other key stakeholders, will develop a uniform methodology for identifying facilities, systems, and functions with national-level criticality to help establish protection priorities;" (b) "will build a comprehensive database to catalog these critical facilities, systems, and functions;" and (c) "will also maintain a comprehensive, up-to-date assessment of vulnerabilities and preparedness across critical sectors." Furthermore, these efforts "will help guide near-term protective actions and provide a basis for long-term leadership focus and informed resource investment."

Following September 11, 2001, owners/operators of critical infrastructure assets, to varying degrees, began identifying critical assets, assessing their vulnerabilities to attack, and developed security plans or beefed up protections. For example, the Federal Transit Authority assessed the vulnerabilities of the nation's largest mass transit systems. The freight rail companies developed additional security measures to coincide with the level of threat identified by DHS's color-coded National Alert System. Drinking water authorities, through the Public Health Security and Bioterrorism Preparedness Act (P.L. 107-188), were required to conduct vulnerability assessments and to develop security plans based on those assessments. Port facilities and maritime vessels were required by the Maritime Transportation Security Act (P.L. 107-295) to do the same. The American Petroleum Institute, the North American Electric Reliability Council, and other industry associations offered guidance to their respective members on how to conduct vulnerability assessments and to manage their risk from possible attack. However, DHS's ability

[61] The President's FY2011 budget request for the National Protection and Programs Directorate proposed terminating NPPD's operation of CWIN.

to coordinate this activity developed more slowly, and its ability to develop a uniform methodology that would allow it to generate a set of national priorities awaited the release of its NIPP, described above.

Nevertheless, during this same time, DHS has engaged in at least two other sets of activities that have, also to varying degrees, identified critical assets, assessed their vulnerabilities, and provided assistance to increase protection of these sites.

Shortly before the beginning of Operation Iraqi Freedom in 2003, as part of Operation Liberty Shield[62], what was then called the Protective Services Division of the newly formed Information Analysis and Infrastructure Protection Directorate, identified a list of 160 assets or sites, including chemical and hazardous materials sites, nuclear power plants, energy facilities, business and finance centers, and more, that it considered critical to the nation based on their vulnerability to attack and potential consequences. During the course of the year, that list grew to 1,849 assets or sites.[63]

According to testimony before the House Appropriations Committee on April 1, 2004, then-Undersecretary for Information Analysis and Infrastructure Protection Frank Libutti, made reference to 1700 sites identified by DHS as being high-priority sites.[64] According to the testimony, DHS intended to visit each of these sites to assess their vulnerabilities to various forms of attack and to meet with local law enforcement officials to assist them in developing **Buffer Zone Protection Plans (BZPPs)**. BZPPs focus on protections that can be taken "outside the fence," including how to identify threatening surveillance, patrolling techniques, and how to assert command and control if an incident should occur. DHS has provided training and technical assistance to help state and local law enforcement entities develop their own BZPPs. The BZPP activity is now integrated into the State and Local Grants Program. In addition to these "outside the fence" activities, DHS has conducted **Site Assistance Visits (SAVs)** at selected sites, on a voluntary basis, to discuss with owners and operators vulnerabilities and protective measures that can be taken "inside the fence." SAVs form an integral part of the "**comprehensive reviews (CRs)**" which DHS is performing on both nuclear power facilities and high-priority chemical facilities. Beginning in FY2009, through a **Regional Resiliency Assessment Program,** DHS expanded its vulnerability assessments to consider clusters of critical infrastructures and key resources within a region.

In addition to its selection of high-priority sites and subsequent site visits, vulnerability assessments, and buffer zone protection plans, DHS, through the Federal Emergency Management Agency's (FEMA's) Grants Program Directorate, also has been supporting infrastructure protection at the state and local level through its State and Local Grant Programs. Specific grant programs include the State Homeland Security Formula-based Grants, the Urban Area Security Initiative (UASI) Grants (both of which primarily support first responder needs, but include certain infrastructure protection expenditures), Port Security Grants, Rail and Transit Security Grants, Intercity Bus Security Grants, and Highway (Trucking) Security Grants. The Buffer Zone Protection Plan grants have been added to this set of programs. Before receiving

[62] Operation Liberty Shield was a comprehensive national plan to protect the homeland during operations in Iraq.

[63] See, Department of Homeland Security. Office of the Inspector General. *Progress in Developing the National Asset Database.* OIG-06-04. June 2006.

[64] According to the Department's Inspector General report, these 1,700 assets refer to the 1,849 assets identified in its research.

funds, grants recipients must identify specific critical infrastructure assets, conduct threat and vulnerabilities assessments, and develop a plan for how they intend to use grant funds to reduce those vulnerabilities through eligible expenditures.[65]

Issues and Discussion

Congressional interest in critical infrastructure protection is focused, principally, on reviewing the progress and effectiveness of DHS's efforts.

Identifying Critical Assets, Functions, and Systems

There has been some debate about the progress and effectiveness of DHS's efforts at identifying high-priority assets. For example, when developing the initial list of priority sites during Operation Liberty Shield, certain utility operators, when presented a list of what DHS considered to be critical electric power assets, noticed that some of the entries were not currently in use.[66] According to the DHS Inspector General, DHS itself determined that its early list of priority sites was unreliable.[67]

Over time, according to the DHS Inspector General, this initial priority list evolved into what became the **National Asset Database**, which, as of January 2006, contained over 77,000 entries. While DHS apparently made progress on the reliability of the information contained in the Database, it continued to draw criticism for including thousands of assets that many believe have more local importance than national importance. There is some confusion as to what the National Asset Database is meant to be. Critics of the Database assume it is a continuation of DHS's list of high-priority sites. DHS asserts that it is an inventory of assets, from which critical assets may be drawn.[68] Perhaps in response to these criticisms, the National Asset Database has evolved first into the **Infrastructure Data Warehouse**, then into the **Infrastructure Information Collection Project**.

In his response to the Inspector General's report, the then-Undersecretary for Preparedness stated that DHS does not intend to have one definitive prioritized list of critical assets. He further stated that it would not be possible or useful to develop one.[69] However, the then-Assistant Secretary for Infrastructure Protections stated that DHS does maintain a list of roughly 600 high-priority sites, which it uses to focus DHS operations, resource allocation and grants.[70]

---

[65] For more information on the grant programs, see CRS Report R40246, *Department of Homeland Security Assistance to States and Localities: A Summary and Issues for the 111th Congress*, by Shawn Reese; and CRS Report R40632, *FY2010 Department of Homeland Security Assistance to States and Localities*, by Shawn Reese.

[66] Based on personal communication with industry official, September 29, 2003.

[67] Department of Homeland Security. Office of the Inspector General. *Progress in Developing the National Asset Database*. Op. cit., p. 16.

[68] For more discussion of the issues associated with the National Asset Database see, CRS Report RL33648, *Critical Infrastructure: The National Asset Database*, by John D. Moteff.

[69] Department of Homeland Security. Office of the Inspector General. *Progress in Developing the National Asset Database*. Op. cit., p. 31.

[70] *USA Today*. "Database is Just the 1st Step," by Robert Stephan. July 21, 2006. p. 8A.

The number of assets making onto this high-priority list has apparently grown.[71] Implementation of the National Infrastructure Protection Plan (NIPP) is suppose to contribute to the identification of assets that are most critical to the nation. The Assistant Secretary for Infrastructure Protection approves the lists annually. Also, the FY2009 IPIS budget justification document mentioned the intention to begin conducting High-Risk Infrastructure Cluster vulnerability assessments (now referred to as the Regional Resiliency Assessment Program). These assessments would focus on multiple sites that might collectively be affected by a single event. These clusters are identified through the Urban Area Security Initiative program.

In June 2009, the DHS Inspector General's Office released a follow-up report on DHS's efforts to identify critical infrastructure assets.[72] In summary, the report found that the effort to develop the Infrastructure Data Warehouse was proceeding slowly. The report also found that while opportunities for improvement exist, DHS's effort to identify high-priority sites was well conceived and maturing.

Assessing Vulnerabilities and Risk

Assuming DHS does maintain a list of high-priority assets, it is not clear how many of these have been visited, had their vulnerability and risk assessed, or have had buffer zone protection plans or other protective measures developed and implemented to-date. Directorate budget requests report some figures, but the reporting is not consistent nor standardized from year to year. Also, reference to high-priority sites in earlier years may not refer to the same list of high-priority sites currently under consideration. The FY2011 budget request stated that 450 vulnerability assessments would be accomplished in FY2010.

DHS's Annual Performance Reports offer a different view of the progress made in assessing vulnerabilities and risk and subsequent action. DHS's Annual Performance Report matches specific programs with specific performance metrics. However, as with the budget justifications, reporting and the metrics identified in the Annual Performance Reports have varied over the years. DHS's FY2008-FY2010 Annual Performance Report identified three performance metrics by which it measures progress of the Infrastructure Protection Program (apparently referring to the non-cyber and non-communications related activities of the Infrastructure Protection and Information Security Program in the budget). These were: the percentage of critical infrastructure and key resource sector specific protection implementation actions on track (apparently referring to actions identified in the individual Sector Specific Plans); the percent of high-priority critical infrastructure and key resources where a vulnerability assessment has been conducted and enhancements(s) have been implemented; and percent of inspected high-risk chemical facilities in compliance with risk based performance standards. The targets and actual percentages for each of these measures are listed in **Table 3** below.

[71] In testimony before the Senate Ad Hoc Subcommittee on State, Local, and Private Sector Preparedness and Integration, Senate Committee on Homeland Security and Governmental Affairs, July 12, 2007, the Assistant Secretary stated that this list has grown to about 2,500 assets. The list is divided into Tier 1 (most critical), and Tier 2 (significantly critical) sites, based on analysis conducted by the Office of Infrastructure Protection.

[72] Department of Homeland Security. Office of the Inspector General. Efforts to Identify Critical Infrastructure Assets and Systems. OIG-09-86. June 2009.

Table 3. Performance Measures for the Infrastructure Protection and Risk Management Program

Measure		FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010
Percent of critical infrastructure and key resource sector specific implementation actions on track	target	-	-	-	90%	90%	90%
	actual	-	-	-	93%		
Percent of high-priority critical infrastructure and key resources where a vulnerability assessment has been conducted and enhancement(s) have been implemented	target	-	-	-	95%	95%	95%
	actual	-	-	-	100%		
Percent of inspected high-risk chemical facilities in compliance with risk based performance standards	target	-	-	-	75%	85%	70%
	actual	-	-	-	0%[a]		

Source: Department of Homeland Security. Department of Homeland Security Annual Performance Report: FY2008-FY2010.

a. The compliance program has not yet commenced.

Allocating Resources

It is a matter of policy, as articulated in the documents discussed above, that federal resources should focus on those critical infrastructure assets that, if attacked, pose the greatest risks to the nation.

Risk, in the context of critical infrastructure and terrorism, can be defined as the potential consequences associated with a particular kind of attack or event against a particular target, discounted by the likelihood that such an attack or event will occur (threat) and the likelihood that the target will sustain a certain degree of damage (vulnerability). Threat includes not only the identification of specific adversaries, but also their intentions and capabilities (both current and future). Consequences include lives and property lost, short term financial costs, longer term economic costs, environmental costs, etc. Given this definition, risk is not threat, nor vulnerability to a threat, nor the estimated consequences associated with a specific attack, but some integration of the three.[73]

According to the NIPP, the allocation of resources is to be a two step process. First, those critical assets which pose the greatest risk to the nation if attacked (i.e., those assets that score highest when integrating threat, vulnerability, and consequences) are to be given the highest priority. The second step is to identify and support those protective measures that are likely to provide the greatest risk reduction for any given investment.

Federal resources are spent in a number of ways, including agencies' internal budgets for operations and programs, grants to states and localities, and research and development funding for universities and industry. The most publicized debates on the allocation of federal resources

[73] Note, that in many cases these factors may not be independent. In other words, the likelihood that a particular asset may be attacked may increase if it is perceived to have a high vulnerability and/or the consequences of the attack are great. For more discussion of how risks can be assessed and its implications for decision making, see CRS Report RL32561, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*, by John D. Moteff.

focuses primarily on grants to states and localities. The formula-based State Homeland Security Grants, mentioned above, has been criticized by some for allocating more dollars per capita to states that some perceive as having lower risks than other states. Congress has been at odds on if, or how, to modify the allocation of those funds. The other grant programs mentioned above (i.e., Urban Area Security Initiative grants and the sector specific grants) are discretionary. According to DHS, allocation of these funds are based on a calculation not only of risk, but also on need. With the allocation of FY2006 Urban Area Security Initiative grants, some cities which perceived themselves as having greater risk (or at least being more at threat or could suffer greater losses) received less funding than they did the previous year, while other cities perceived as having lower risks saw their funds increased. DHS stated that one reason for this was the way it determined the unmet needs of the area and the programs proposed by the areas to address those needs. Faced with criticism from those cities and states that received a drop in funds, DHS stated it would rework its grant review process.[74] In addition, Congress requested that the Government Accountability Office review the validity, relevance, reliability, timeliness and availability of the risk factors used by DHS in its discretionary grant programs.[75] Meanwhile, Congress continues to set its own priorities by specifying the amount of funds that go to each of these grant programs.

Also, it is not clear to what extent the NIPP process influences the allocation of resources to states and localities. DHS states that information contained in its list of high-priority sites is reviewed when making these grant allocation decisions. However, these grant programs are managed by FEMA which apparently assesses risks independent of the NIPP. Similarly, port security grants, while managed by FEMA, are influenced largely by the review of vulnerability assessments and security plans performed by the Coast Guard.

Information Sharing

Information sharing in the context of homeland security encompasses a very complex network of proposed connections. There is information sharing between federal agencies, especially between intelligence agencies, and between intelligence and law enforcement agencies. There is information sharing between federal agencies and their state and local counterparts. There is information sharing between federal, state, and local agencies and the private sector. There is information sharing within and between the private sectors. And there is information sharing between all of these entities and the public. A multitude of mechanisms have been established to facilitate all of this information sharing. While the multitude of mechanism may cause some concern about inefficiencies, a highly connected, in some cases redundant, network may not be a bad thing. A primary concern is if these mechanisms are being used and are effective.

In the past, information flow between all of these stakeholders has been restrained, or non-existent, for at least three reasons: a natural bureaucratic reluctance to share information, 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,

[74] DHS's solution was to establish multiple tiers, with urban areas competing for funds within their tier. Tier 1 urban areas are those considered to have a greater likelihood of being targeted or have a large number of probable targets (including number of people).

[75] For a detailed discussion of the risk assessment process used to allocate grant funds to urban areas, see CRS Report RL33858, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, by Todd Masse, Siobhan O'Neil, and John Rollins.

many of these restraints are being reexamined and there appears to be a general consensus to change them. Some changes have resulted from the USA PATRIOT Act (including easing the restrictions on 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 between themselves and other entities at the state and local level. The Intelligence Reform and Terrorism Prevention Act (P.L. 108-458) reorganized the entire intelligence community, in part to improve the level of communication and coordination between the various intelligence organizations.[76] The legislation also required the President to establish an **information sharing environment (ISE)** for the sharing of terrorism information among all appropriate federal, state, local, and tribal entities, and the private sector.

While the federal government is trying to increase the amount of information shared among appropriate stakeholders, it is also trying to maintain a tight control (short of classification) on who gets to see what information. A variety of designations have been given to information the federal government wishes to control (critical infrastructure information [see below], homeland security information, terrorism information, sensitive security information). A catch-all term for these and other designations of controlled information is "**sensitive but unclassified**."

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 have been in sharing information. The private sector primarily wants from 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 to keep confidential company practices. The private sector, too, is concerned about whether providing this information might lead to future regulatory action or other liabilities. Successful information sharing will depend on the ability of each side to demonstrate it can hold in confidence the information exchanged.

Sharing information between government and the private sector is made more complex by the question of how the information will be handled within the context of the Freedom of Information Act (FOIA). In particular, the private sector is reluctant to share the kind of information the government wants without it being exempt from public disclosure under the existing FOIA statute. The Homeland Security Act (P.L. 107-296, Sec. 214) exempts information defined as **critical infrastructure information** from FOIA (as well as providing other protections). Similar FOIA exemptions are offered in other legislation. For example, the Public Health Security and Bioterrorism Preparedness Act (P.L. 107-188, Sec. 401, see below) exempts certain security-related information from FOIA. Even with these protections in statute, it is uncertain how much information on assets, vulnerabilities, incidents, etc. is being shared with DHS, or how useful it is.[77]

---

[76] See also CRS Report RL32366, *Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6*, by William J. Krouse.

[77] In February 2005, DHS acknowledged the receipt of 29 submissions of CII documents, 22 of which were approved as CII by DHS. See *DHS Finally Speaks on CII* at http://www.ombwatch.org/article/articleprint/2683/-1/321. In previously cited testimony (before the Senate Ad Hoc Subcommittee on State, Local, and Private Sector Preparedness (continued...)

The FOIA exemptions for critical infrastructure information (CII) and other types of sensitive but unclassified information is not without its critics. The non-government-organizations that actively oppose government secrecy are reluctant to expand the government's ability to hold more information as classified or sensitive. These critics, and others, feel that the protections offered to CII and other types of sensitive but unclassified information is too broad and believe that controls are stifling public debate and oversight, as well as impeding technological advances that could benefit both security and the economy.[78]

Regulation

As a general statement of policy, owners and operators of critical infrastructure are to work with the federal government on a voluntary basis. Sharing information with the federal government about vulnerability assessments, risk assessments, and the taking of additional protective actions is meant to be voluntary.

However, the degree to which some of the activities are mandated varies across sectors. In some cases, sectors are quite regulated. Nuclear power plants must meet very specific standards for assessing their vulnerabilities to very specific types of attacks and to take the necessary actions to address those vulnerabilities. The Nuclear Regulatory Commission enforces these regulations. The Maritime Transportation Security Act (P.L. 107-295) requires facilities at ports, and certain vessels, to conduct vulnerability assessments and to develop and implement security plans (including naming a security officer who is responsible for developing and implementing these plans). The vulnerability assessments and security plans are reviewed by the Coast Guard. The Public Health Security and Bioterrorism Preparedness Act (P.L. 107-188) requires community drinking water systems to conduct vulnerability assessments and to incorporate the results of those assessments into their emergency response plans. The vulnerability assessments must be submitted to the Environmental Protection Agency (EPA). The EPA must also receive certification that the emergency response plans have been appropriately modified to reflect the vulnerability assessments. This same Act also amended the Federal Food, Drug, and Cosmetic Act to require all facilities engaged in manufacturing, processing, packing, or holding food for consumption to register with the Department of Health and Human Services. In addition, the Food and Drug Act was amended to require regulations specifying the types of information these facilities needed to keep on record for a specified amount of time to assist the Secretary in determining if a food product has been adulterated and represents a public health problem. The FY2006 DHS appropriation bill (P.L. 109-295, Sec. 550), authorized the Secretary of Homeland Security to issue interim final regulations requiring vulnerability assessments and security plans for certain chemical facilities, except those covered by the Maritime Transportation and Security Act, other relevant acts affecting drinking water authorities, or those operated by the Department of Energy, the Department of Defense, or the Nuclear Regulatory Commission.

(...continued)

and Integration, July 12, 2007), the Assistant Secretary for Infrastructure Protection stated that since the final rule governing implementation of the CII program was released, DHS has received about 5,400 submissions.

[78] For a discussion of sensitive but unclassified information—not only science and technology information, but other types of information held by, or given to, the federal government—see CRS Report RL33303, *"Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information*, by Genevieve J. Knezo.

At the other end of the spectrum are sectors such as information and telecommunication, oil and gas, and commercial (i.e., malls and office buildings) where similar activities (i.e., vulnerability assessments, etc.) are encouraged but not mandated.

As mentioned above, the Obama Administration has proposed that owners and operators of sites or facilities that are deemed critical to the nation by the Secretary of Homeland Security be required to develop cybersecurity plans.

GalleryWatch.com
http://www.crsdocuments.com
Penny Hill Press

Appendix. Funding for Critical Infrastructure

Federal Funding for Critical Infrastructure Protection

It is difficult to determine how much funding the federal government devotes to the protection of critical infrastructure. The Homeland Security Act requires the President's Budget to include a budget analysis of homeland security activities across the federal government. This analysis appears in Chapter 3 of the Analytical Perspectives volume of the President's Budget.[79] However, the FY2010 budget request made a change in the way homeland security activities are accounted for, making the estimate of how much is spent on critical infrastructure less clear.

During the Bush Administration, OMB defined six categories of homeland security activities that paralleled the mission areas defined in the *National Strategy for Homeland Security.* These were: intelligence and warning; border and transportation security; domestic counter-terrorism; critical infrastructure and key asset protection; defending against catastrophic events; and emergency preparedness and response. The "critical infrastructure and key resources protection" category included funding spent by agencies to protect their own critical infrastructure. It also included funds that agencies may have spent working with states, local governments, and private owners/operators to reduce their respective vulnerabilities. DHS activities included both of these, as well as activities associated with coordinating the national effort.

Other mission areas included activities that could also be considered part of the effort to protect critical infrastructure. For instance, the intelligence and warning mission area includes threat analysis, risk analysis, and the sharing of that information with other stakeholders, including states, localities, and the private sector, each of which factor into critical infrastructure protection. Border and transportation security includes activities associated with protecting airports, sea ports, and other transportation modes. Therefore, previous estimates for "critical infrastructure and key resources protection" probably represented a minimum estimate of the total amount of federal funding spent on critical infrastructure protection.

For FY2010, OMB reformulated the categories for tracking homeland security activity, combining them into three new categories: prevent and disrupt terrorist attacks; protect the American people, our critical infrastructure, and key resources; and respond to and recover from incidents. As a result, it is not possible to compare the FY2010 figures with those from prior budgets. The category "protect the American people, our critical infrastructure, and key resources" now includes more activities than were counted in the "critical infrastructure and key resources protection" category in FY2009 and before. These additional activities include ones that were previously counted in the "defending against catastrophic events" category. The latter represents a significant addition in funding, and includes activities meant to protect the general population. The FY2010 budget recalculated homeland security funding broken down by these three new categories for the last two fiscal years (FY2008 and FY2009) in addition to the FY2010

[79] In many cases, funding for homeland security (and critical infrastructure protection) is buried within a number of different accounts, activities, programs, and projects. It is not possible to track budget requests or Congressional appropriations in each of these mission areas to this level of detail. Agencies may not know themselves until they allocate their appropriations. However, once appropriations are allocated, agencies must report homeland security-related allocations down to the budget account level. OMB provides a breakdown of funding to this level in supplemental documentation to the budget. See http://www.whitehouse.gov/omb/budget/fy2010/assets/homeland.pdf.

request. **Table A-1** below shows the funding figures for the "protecting the American people, our critical infrastructure, and key resources" category. The table also includes the FY2008 figures for the "critical infrastructure and key resources protection" category taken from the FY2009 budget request for comparison. The FY2008 numbers in the new category taken from the FY2010 budget request are substantially higher. Since this report does not cover many of the activities associated with defending against catastrophic events, the OMB accounting is no longer representative of the activities covered in this report.

GalleryWatch.com
http://www.crsdocuments.com

Table A-1. Funding for Protecting the American People, Our Critical Infrastructure, and Key Resources by Department (*Funding for Critical Infrastructure and Key Resources Protection*)

($ in millions)

Department	*(FY2008 enacted[a]*	FY2008 enacted	*(FY2008 supplemental[a]*	FY2008 supplemental	FY2009 enacted	FY2009 supplemental	FY2010 request
Agriculture	*64*	255			269		311
Commerce		158			203	11	210
Defense	*11,966*	16,881		658	18,853	365	18,760
Energy	*1,607*	1,667			1,722		1,786
HHS	*180*	2,201			2,511	50	3,861
Homeland Security	*3,036*	4,893			5,361	500	3,971
Justice	*493*	459	*16*	18	666	3	630
Veterans Affairs	*222*	236			228		271
NASA	*194*	205			222		220
NSF	*350*	365		1	377	29	386
Social Security	*215*	173			213		228
Other Agencies	*602*	681		8	735	69	747
Grand Total[b]	*19,096)*	28,173	*16)*	685	31,360	1,027	31,380

Source: OMB, Budget of the U.S. Government, FY2009 Analytical Perspectives. Cross-Cutting Programs. Chapter 3. Homeland Security Funding Analysis. p. 27. FY2006 figures taken from FY2008 Analytical Perspectives.

a. Funding for the Critical Infrastructure and Key Resources Protection category per FY2009 request. FY2010 request no longer uses this category.

b. Numbers may not add due to rounding.

FY2011 DHS Budget Request and Prior Year Appropriations for Infrastructure Protection and Information Security Program and Other Relevant DHS Budget Activities

Just as it is difficult to account for all the federal activities associated with critical infrastructure protection in the federal government, it is also difficult to track the critical infrastructure protection activities within the Department of Homeland Security. Funding for activities related to critical infrastructure protection is found in numerous places within the Department, including the National Protection and Programs Directorate, the Transportation Security Administration, the Coast Guard, Secret Service, the Science and Technology Directorate, FEMA, and U.S. Customs and Border Protection. However, much of the funding for the organizations and activities discussed in the body of this report can be found in the Infrastructure Protection and Information Security (IPIS) Program. See **Table A-2**, below.[80]

IPIS

The Infrastructure Protection and Information Security Program (IPIS) supports the activities of the Office of Infrastructure Protection (OIP), and the Office of Cybersecurity and Communications. The latter includes the National Cyber Security Division (NCSD), the National Communication System (NCS), and the Office of Emergency Communications (OEC). OIP coordinates the national effort to reduce the risks associated with the loss or damage to the nation's critical infrastructure due to terrorist attack or natural events. This effort is a cooperative one between the federal government; state, local, and tribal governments; and the private sector, to identify critical elements of the nation's infrastructure, their vulnerabilities, the potential consequences of their loss or damage, and ways to mitigate those losses. The NCSD performs a similar function, but specifically focuses on the nation's information networks. The NCS also performs a similar function, but specifically focuses on the nation's communication systems, in particular the communications systems and programs that ensure the President can communicate with selected federal agencies, state, local, and tribal governments, and certain private sector entities during times of national emergencies. The OEC is responsible for promoting the ability of state, local and federal emergency response providers to communicate with each other during an emergency through the development and distribution of interoperable communication equipment. Funding is aligned with this organizational structure and provided in a set of program/project activities (PPAs) as noted in the table below.

DHS requested approximately $936 million for IPIS in FY2012, about $96 million above what Congress eventually appropriated for FY2011.

The request for the Infrastructure Protection (IP) PPA included increases for additional Protective Security Advisors to be placed in state and local fusion. The increase in advisors was offset by a decrease in the number of Infrastructure Sector Analysis studies that would be conducted.

Much of the increase in the IPIS program was directed to U.S. CERT operations. This included an increase of $57 million to support the increased analysis needs of the current EINSTEIN program

[80] The IPIS budget activity supports many of the same (though slightly restructured) infrastructure protection activities that have evolved from the days of the "old" Information Analysis and Infrastructure Protection Directorate.

and to support continued expansion of that program. It also included an increase of $22 million to support DHS's expanded role in monitoring and enforcing compliance by federal agencies with the Federal Information Security and Management Act (FISMA) requirements. There was also $9 million added for a new program to support DHS's role in executing the National Initiative in Cybersecurity Education.[81]

The FY2012 budget request for the NCS and OEC essentially maintains base level activities.

Table A-2. Funding for the Infrastructure Protection and Information Security Program

(budget authority in millions of dollars)

Program Project Activity	FY2009 Enacted	FY2010 Enacted	FY2011 Enacted	FY2012 Request
IP	**314**	**347**	**n/a**	**322**
Identification and Analysis	87	91		84
Coordination and Information Sharing	56	60		48
Mitigation Programs	171	197		190
NCSD	**314**	**397**	**n/a**	**439**
US-CERT	255	324		391
Strategic Initiatives	49	64		65
Outreach and Programs	9	9		7
NCS (NS/EP)	**141**	**110**	**n/a**	**107**
Priority Telecom Service	59	57		57
Programs to Study and Enhance Telecom	15	17		13
Critical Infrastructure Protection	11	11		11
Next Generation Networks	50	25		25
Nat'l Command and Coordination Capability	6	0		
OEC	**38**	**45**	**n/a**	**43**
Total	**807**	**899**	**840**	**936**

Source: CRS Analysis of the *FY2011 DHS Congressional Budget Justifications.*.

Notes: Tables may not add due to rounding. IP=Infrastructure Protection; NCSD=National Cyber Security Division; NCS=National Communications System; OEC=Office of Emergency Communications.

Other Infrastructure Related Programs

In addition to the IPIS program within the National Protection and Programs Directorate, other areas in DHS support infrastructure protection. A major component of support for critical infrastructure protection within the Department are the grant programs in the Federal Emergency

[81] See, http://csrc.nist.gov/nice/aboutUs.htm.

Management Agency (FEMA); in particular, the State and Regional Preparedness Program and the Metropolitan Statistical Area Preparedness Program. The former includes the State Homeland Security grants and the latter include the Urban Areas Security Initiative, Buffer Zone Protection Plans (BZZP), port security, and rail and transit grants. The State Homeland Security grants and the Urban Areas Security Initiative grants primarily support first responder capabilities, but funding can also be spent on critical infrastructure protection expenses (such as the purchase of cameras, sensors, etc.). The BZPPs, port security, and rail and transit security grants focus primarily on protecting infrastructure assets. For FY2012, the Administration requested $1 billion for State Homeland Security Grants, $920 million for the Urban Area Security Initiative, $300 million each for ports and rail and transit, and $50 million for buffer zone protection.

The Transportation Security Administration (TSA) is responsible for overseeing the security of the nation's transportation sectors (as directed by the Aviation and Transportation Security Act, P.L. 107-71). The Administration's total budget request for FY2011 was $7.9 billion (excluding offsetting receipts and capital fund accounts). Aviation security consumes a large fraction of the TSA budget, including support for: passenger and baggage screening; the purchase, installation, and operation of explosive detection equipment; and airport perimeter security; air marshals; crew vetting; etc. TSA also receives funds for surface transportation security and security-related support activities. For more information on issues associated with transportation security, see CRS Report RL33512, *Transportation Security: Issues for the 112th Congress*, by David Randall Peterman, Bart Elias, and John Frittelli

The Science and Technology Directorate budget supports research and development in a number of areas relevant to critical infrastructure protection. This includes research and development in cyber security, risk analysis, explosive detection, blast protection, modeling and simulation, safe cargo containers, and more. The Directorate also works with the Office of Infrastructure Protection to develop and maintain a National Critical Infrastructure Protection R&D Plan. It is difficult to determine how much funding is devoted overall to critical infrastructure protection-related research, given the budget structure of the programs.

Author Contact Information

John D. Moteff
Specialist in Science and Technology Policy
jmoteff@crs.loc.gov, 7-1435