Order Code RL30153



# Critical Infrastructures: Background, Policy, and Implementation

**Updated April 18, 2006**

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

# Critical Infrastructures: Background, Policy and Implementation


## Summary

The nation's health, wealth, and security rely on the production and distribution of certain goods and services. The array of physical assets, processes and organizations across which these goods and services move are called critical infrastructures (e.g., electricity, the power plants that generate it, and the electric grid upon which it is distributed).

The national security community has been concerned for sometime about the vulnerability of critical infrastructure to both physical and cyber attack. In May 1998, President Clinton released Presidential Decision Directive No. 63. The Directive set up groups within the federal government to develop and implement plans that would protect government-operated infrastructures and called for a dialogue between government and the private sector to develop a National Infrastructure Assurance Plan that would protect all of the nation's critical infrastructures by the year 2003. While the Directive called for both physical and cyber protection from both man-made and natural events, implementation focused on cyber protection against man-made cyber events (i.e. computer hackers). However, given the physical damage caused by the September 11 attacks, physical protections of critical infrastructures has received increased attention.

Following the events of September 11, the Bush Administration released Executive Orders 13228, signed October 8, 2001, establishing the Office of Homeland Security. Among its duties, the Office shall "coordinate efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks." 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.

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 three issues of Congressional concern: allocating resources based on risk; information sharing; and, regulation. This report will be updated as warranted.

## Contents



## List of Tables

# Critical Infrastructures: Background, Policy, and Implementation

## Latest Developments

The proposed purchase by Dubai Ports World (a government owned corporation of the United Arab Emirates) of several U.S. port facilities from a British firm, which currently operates those facilities, sparked a national debate. Among the questions raised was, "what impact might the foreign ownership of certain assets associated with critical infrastructure have on homeland security?" Various Members of Congress responded to the proposed purchase with a wide range of legislative proposals. Some focus specifically on the proposed deal (from which Dubai Ports World has since retreated), some would place new restrictions on the ownership of U.S. port facilities. Other legislative proposals seek to amend the process by which the deal was reviewed and initially approved.

The current review process for such purchases, implemented under authority of the Exon-Florio provision of the Defense Production Act (50 U.S.C., App. 2170), authorizes the President to block proposed or pending acquisitions "by or with foreign persons which could result in foreign control of persons engaged in interstate commerce in the United States...so that such control will not threaten to impair the national security." As initially conceived , the provision addressed concerns that the rise in foreign ownership of certain domestic industrial assets could force the Department of Defense to rely on foreign-owned businesses to provide critical defense expertise, products, and technology. Of additional concern was the potential export by foreign-owned businesses of critical defense expertise, technologies, or products to certain other countries or entities. Some of the legislative proposals "broaden" coverage of Exon-Florio to include the purchase of assets associated with critical infrastructure. As currently written, Exon-Florio covers persons engaged in interstate commerce. While this covers a broad range of "persons," extending beyond those that might be part of the nation's critical infrastructure, not all critical infrastructure assets necessarily engage in interstate commerce (perhaps, for example, some water utilities) or may not be particularly associated with the supply of defense expertise, products, or technologies. Tracking of this issue and the progress of these bills is beyond the scope of this report. For a review and discussion of these bills, the reader is referred to CRS Report RL33312, *The Exon-Florio Test for Foreign Investment*, by James K. Jackson.

## 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, processes, information, and organizations 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, lightening strikes, etc.) or physical destruction due to intentional human actions (theft, arson, terrorist attack, etc.). Over the years, operators of these infrastructures have taken measures to guard against, and to quickly respond to, many of these threats, primarily to improve 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.

## 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:

---

[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.

- 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, determine the level of risk associated with possible attacks on those assets, and consider and prioritize a set of protection 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]

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** sections of this report.

---

[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 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;

---

[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.

- develop a real-time capability of attack warning;
- establish and promote a comprehensive awareness and education program;
- streamline and clarify elements of the legal structure to support assurance measures (including clearing jurisdictional barriers to pursuing hackers electronically); and,
- expand research and development in technologies and techniques, especially technologies that allow for greater detection of intrusions.

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

## Presidential Decision Directive No. 63

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

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

## 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 |
| Director of Central Intelligence | **Intelligence |
| State | **Foreign Affairs |
| Defense | **National Defense |

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

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

---

[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.

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 government officials and relevant federal agencies. The Council was to meet periodically and provide reports to the President as appropriate. The National Coordinator was to act as the Executive Director of the Council.

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

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

Most of the Directive established policy-making and oversight bodies making use of existing agency authorities and expertise. However, the PDD also addressed operational concerns. These dealt primarily with cyber security. The Directive called for a national capability to detect and respond to cyber attacks while they are in progress. Although not specifically identified in the Directive, the Clinton Administration proposed establishing a **Federal Intrusion Detection Network (FIDNET)** that would, together with the **Federal Computer Intrusion Response Capability (FedCIRC)**, established just prior to PDD-63, meet this goal.[14] The Directive explicitly gave the Federal Bureau of Investigation the authority to expand its existing computer crime capabilities into a **National Infrastructure Protection Center (NIPC)**. The Directive called for the NIPC to be the focal point for federal threat assessment, vulnerability analysis, early warning capability, law enforcement investigations, and response coordination. All agencies were required to forward to the NIPC information about threats and actual attacks on their infrastructure as well as attacks made on private sector infrastructures of which they become aware. Presumably, FIDNET[15] and FedCIRC would feed into the NIPC. According to the

---

[14] FedCIRC was renamed the Federal Computer Incident Response Center and has since been absorbed into the Department of Homeland Security's National Cyber Security Division.

[15] From the beginning FIDNET generated controversy both inside and outside the (continued...)

Directive, the NIPC would be linked electronically to the rest of the federal government and use warning and response expertise located throughout the federal government. The Directive also made the NIPC the conduit for information sharing with the private sector through an equivalent **Information Sharing and Analysis Center(s)** operated by the private sector, which PDD-63 encouraged the private sector to establish.

While the FBI was given the lead, the NIPC also included the Department of Defense, the Intelligence Community, and a representative from all lead agencies. Depending on the level of threat or the character of the intrusion, the NIPC was to have been placed in direct support of either the Department of Defense or the Intelligence Community. With the formation of the Department of Homeland Security, the NIPC has dissolved away. The **U.S. Computer Emergency Response Team (U.S. CERT)** and the **Homeland Security Operations Center (HSOC)**, discussed later in this report, perform similar tasks today.

Quite independent of PDD-63 in its origin, but clearly complimentary in its purpose, the FBI offers a program called **INFRAGARD** to private sector firms. The program includes an Alert Network. Participants in the program agree to supply the FBI with two reports when they suspect an intrusion of their systems has occurred. One report is "sanitized" of sensitive information and the other provides more detailed description of the intrusion. The FBI will help the participant respond to the intrusion. In addition, all participants are sent periodic updates on what is known about recent intrusion techniques. The FBI has set up local INFRAGARD chapters that can work with each other and regional FBI field offices. In January, 2001, the FBI announced it had finished establishing INFRAGARD chapters in each of its 56 field offices. Rather than sector-oriented, INFRAGARD is geographically-oriented.

It should also be noted that the FBI had, since the 1980s, a program called the **Key Assets Initiative (KAI)**. The objective of the KAI was to develop a database of information on "key assets" within the jurisdiction of each FBI field office, establish lines of communications with asset owners and operators to improve physical and cyber protection, and to coordinate with other federal, state, and local authorities to ensure their involvement in the protection of those assets. The program was initially begun to allow for contingency planning against physical terrorist attacks. According to testimony by a former Director of the NIPC, the program was "reinvigorated" by the NIPC and expanded to include the cyber dimension.[16] The Department of Homeland Security has been given the responsibility to create a data base of critical assets.

---

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

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

## Restructuring by the Bush Administration

**Pre-September 11.** As part of its overall redesign of White House organization and assignment of responsibilities, the in-coming Bush Administration spent the first eight months reviewing its options for coordinating and overseeing critical infrastructure protection. During this time, the Bush Administration continued to support the activities begun by the Clinton Administration.

The Bush Administration review was influenced by three parallel debates. First, the National Security Council (NSC) underwent a major streamlining. All groups within the Council established during previous Administrations were abolished. Their responsibilities and functions were consolidated into 17 Policy Coordination Committees (PCCs). The activities associated with critical infrastructure protection were assumed by the Counter-Terrorism and National Preparedness PCC. At the time, whether, or to what extent, the NSC should remain the focal point for coordinating critical infrastructure protection (i.e. the National Coordinator came from the NSC) was unclear. Richard Clarke, himself, wrote a memorandum to the incoming Bush Administration that the function should be transferred directly to the White House.[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. Some include in the terrorist threat cyber attacks on critical infrastructure. The U.S. Commission on National Security/21st Century (the Hart-Rudman Commission) proposed a new National Homeland Security Agency. The recommendation built upon the current Federal Emergency Management Agency (FEMA) by adding to it the Coast Guard, the Border Patrol, Customs Service, and other agencies. The Commission recommended that the new organization include a directorate responsible for critical infrastructure protection. While both the Clinton and Bush Administration remained cool to this idea, bills were introduced in Congress to establish such an agency. As discussed below, the Bush Administration changed its position in June 2002, and proposed a new department along the lines of that proposed by the Hart/Rudman Commission and Congress.

---

[17] Senior NSC Official Pitches Cyber-Security Czar Concept in Memo to Rice. *Inside the Pentagon*. Jan. 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 Jeffery Seifert.

**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 is the coordination of efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks. This includes strengthening measures for protecting energy production, transmission, and distribution; telecommunications; public and privately owned information systems; transportation systems; and, the provision of food and water for human use. Another function of the Office is to coordinate efforts to ensure rapid restoration of these critical infrastructures after a disruption by a terrorist threat or attack.

The EO also established the **Homeland Security Council**. The Council is made up of the President, Vice-President, Secretaries of Treasury, Defense, Health and Human Services, and Transportation, the Attorney General, the Directors of FEMA, FBI, and CIA and the Assistant to the President for Homeland Security, and the Secretary of Homeland Security. Other White House and departmental officials can be invited to attend Council meetings.[20] The Council advises and assists the President with respect to all aspects of homeland security. The agenda for those meetings shall be set by the Assistant to President for Homeland Security, at the direction of the President. The Assistant is also the official recorder of Council actions and Presidential decisions.

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

The second Executive Order (E.O. 13231) signed October 16, 2001, stated that it is U.S. policy "to protect against the disruption of the operation of information systems for critical infrastructure...and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage

---

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

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

possible."[21] This Order also established the **President's Critical Infrastructure Protection Board**. The Board's responsibility was to "recommend policies and coordinate programs for protecting information systems for critical infrastructure..." The Order also established a number of standing committees of the Board that includes Research and Development (chaired by a designee of the Director of the Office of Science and Technology), Incident Response (chaired by the designees of the Attorney General and the Secretary of Defense), and Physical Security (also chaired by designees of the Attorney General and the Secretary of Defense). The Board was directed to propose a National Plan on issues within its purview on a periodic basis, and, in coordination with the Office of Homeland Security, review and make recommendations on that part of agency budgets that fall within the purview of the Board.

The Board was chaired by a **Special Advisor to the President for Cyberspace Security**.[22] The Special Advisor reported to both the Assistant to the President for National Security and the Assistant to the President for Homeland Security. Besides presiding over Board meetings, the Special Advisor, in consultation with the Board, was to propose policies and programs to appropriate officials to ensure protection of the nation's information infrastructure and to coordinate with the Director of OMB on issues relating to budgets and the security of computer networks.

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

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

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

---

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

[22] President Bush designated Richard Clarke.

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).

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)[23] 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 its establishment of the **Critical Infrastructure Protection Policy Coordinating Committee** which will advise the Homeland Security Council on interagency policy related to physical and cyber infrastructure security.

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

---

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

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

While superseding PDD-63, the Bush Administration policy and approach regarding critical infrastructure protection can be described as an expansion of the policies and approaches laid out in PDD-63. The fundamental policy statements are essentially the same: the protection of infrastructures critical to the people, economy, essential government services, and national security. National morale has been added to that list. Also, the stated goal of the government's efforts is to ensure that any disruption of the services provided by these infrastructures be infrequent, of minimal duration, and manageable. The infrastructures identified as critical were essentially the same (although expanded and with an emphasis placed on targets that would result in large numbers of casualties). Finally, the primary effort is directed at working collaboratively and voluntarily with the private sector owners and operators of critical infrastructure to identify critical assets and provide appropriate protection.

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

The primary difference, at least initially, was the segregation of cyber security from the physical security mission of the Office of Homeland Security. Dissolution of the President's Critical Infrastructure Protection Board and the transfer of its duties to the Department of Homeland Security reintegrated the two, albeit with a greater emphasis on physical security than before. The relationship between physical security and cyber security is discussed in more detail in the Issues section of this report.

## 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 have had, as part of their mission, homeland security-like functions (e.g., Border Patrol, Customs, Transportation Security Administration). The full impact of the act is beyond the scope of this report. The following discussion focuses on those provisions relating to critical infrastructure protection.

In regard to critical infrastructure protection the act transferred the following agencies and offices to the new department: the NIPC (except for the Computer Investigations and Operations Section), CIAO, FedCIRC, the **National Simulation and Analysis Center (NISAC),**[24] other energy security and assurance activities within DOE, and the **National Communication System (NCS).**[25] These agencies and offices were integrated within the **Directorate of Information Analysis and Infrastructure Protection (IA/IP)** (one of four operational Directorates established by the act).[26] 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;

---

[24] 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.

[25] 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.

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

- 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).

**Chertoff Review.** 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 remained, presumably with the same missions as outlined in the Homeland Security Act, but was joined by other existing and new entities. The renamed Directorate includes elements from Office of State and Local Government Coordination and Preparedness, the principal grant-making entity within the Department. 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 long sought by many within the cyber security community) and an Assistant Secretary for Infrastructure Protection.[27]

According to the DHS press release, the mission of the restructured Directorate will be to "facilitate grants and over see 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 may impact infrastructure protection include moving the Homeland Security 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 the Secretary's changes.

---

[27] It is not clear from the DHS press release dated July 13, 2005 what the division of labor will be between the two Assistant Secretaries.

## Policy Implementation

There is an element of continuity in the policies and activities undertaken by the Clinton and Bush Administrations. For example, the Bush Administration maintains the effort to communicate with infrastructure operators through ISACs, although it has also developed parallel mechanisms to communicate with them. The Bush Administration also maintains certain lead agencies as the main liaison with certain sectors. The following discusses the implementation of those still relevant elements of PDD-63 and the Bush Administration's policy as policy and action continue to evolve.

**Lead Agencies and Selection of Sector Liaison Officials and Functional Coordinators.** The *National Strategy for Homeland Security*, released by the Bush Administration in July 2002, maintained the role of lead agencies as outlined in PDD-63, with the then proposed Department of Homeland Security acting as coordinator of their efforts. However, the Strategy did shift liaison responsibilities for some sectors to the new Department. The liaison responsibilities outlined in the National Strategy are noted in **Table 2** below, with the former liaison agency noted in parenthesis. HSPD-7 modified the Strategy assignments slightly, giving the chemical sector to the Department of Homeland Security instead of the Environmental Protection Agency.

**Identifying and Selecting Sector Coordinators.** Different sectors present different challenges to identifying a coordinator. Some sectors are more diverse than others (e.g., transportation includes rail, air, waterways, and highways; information and communications include computers, software, wire and wireless communications) and 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, telecommunications, and energy have more experience than others in working with the federal government and/or working collectively to assure the performance of their systems.

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

**Table 3** below shows those individuals or groups that CRS has been able to determine have agreed to act as Coordinators. Sector coordinators have been identified for most of the major privately operated sectors: banking and finance, energy, information, and communications. In the public sector, EPA early on identified the Association of Metropolitan Water Agency as sector coordinator. In the area of transportation, the Association of American Railroads has been identified as the coordinator for the rail sector. More recently, the American Public Transportation Association was selected to represent commuter transportation systems. The U.S. Fire Administration, a component of FEMA, has an established communication network with the nation's fire associations, the 50 State Fire Marshals, and other law enforcement groups. The Department of Justice, through the NIPC, helped to create the Emergency Law Enforcement Services (ELES) Forum.

The Forum is a group of senior law enforcement executives from state, local, and non-FBI federal agencies.

## Table 2. Current Lead Agency Assignments

| Department/Agency (PDD-63 liaison) | Sector/Function |
|---|---|
| Agriculture | Agriculture |
| | Food |
| Agriculture | Meat/Poultry |
| Health and Human Services | All other |
| Homeland Security (Commerce) | Information and Communications |
| Treasury | Banking and Finance |
| EPA | Water |
| Homeland Security (Transportation) | Transportation |
| Homeland Security (Federal Emergency Management Agency, Justice, Health and Human Services) | Emergency Services |
| Health and Human Services | Public Health |
| | Government |
| Homeland Security | Continuity of Government |
| Individual departments and agencies | Continuity of Operations |
| | Energy |
| Energy | Electric Power |
| Energy | Oil and Gas |
| Nuclear Regulatory Commission (per HSPD-7) | Nuclear (and nuclear materials) |
| Homeland Security-Transportation Security Administration | Pipelines |
| Department of Homeland Security (per HSPD-7) | Chemical Industry and Hazardous Materials |
| Defense | Defense Industrial Base |
| Homeland Security | Postal and Shipping |
| Interior | National Monuments and Icons |

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

## Table 3. Identified Sector Coordinators

| Sector | Identified Sector Coordinators |
|---|---|
| Information and Telecommunications | A consortium of 4 associations: Information Technology Assn. of America; Telecommunications Industry Assn.; U.S. Telephone Assn.; Cellular Telecom. & Internet Assn. |
| Banking and Finance | Donald Donahue - Depository Trust Corp.[28] |
| Water | Assn. of Metropolitan Water Agencies |
| Electricity<br>Oil/Gas | North American Electric Reliability Council<br>National Petroleum Council |
| Railroads<br>Mass Transit<br>Airports | Association of American Railroads<br>American Public Transportation Assn.<br>Airport Council International-North America |
| Emergency Fire Services | U.S. Fire Administration |
| Law Enforcement | Emergency Law Enforcement Services Forum |

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 is a private sector initiative. Five working groups were established (Interdependencies/Vulnerability Assessment, Cross-Sector Information Sharing, Legislation and Policy, Research and Development, and Organization). The federal government is not officially part of the Partnership, but the Department of Homeland Security acts as a liaison and has provided administrative support for meetings. Sector Liaisons from lead agencies are considered ex officio members. The Partnership has helped coordinate its members input to a number of national strategies released to date.

In its FY2006 budget proposal, the IA/IP Directorate mentioned a Program called the Critical Infrastructure Protection Sector Partnership Model. The primary initiative in this program is the formation of **Sector Coordinating Councils** and **Government Coordinating Councils** for each sector. These Councils are described as representing a new model for partnering with owners and operators, in support of efforts to develop the National Infrastructure Protection Plan. How these Councils differ, include, or interact with the above Sector Coordinators and the Partnership was not described in the budget justification document.

---

[28] The financial services sector coordinator is selected by the Secretary of Treasury. Mr. Donahue was selected in May 2004, taking over from Rhonda McLean from Bank America. As sector coordinator, Mr. Donahue also chairs the Financial Services Sector Coordinating Council, a private sector group that works closely with the Treasury Department in securing the banking and financial sector.

**Appointment of the National Infrastructure Assurance Council.** The Clinton Administration released an Executive Order (13130) in July, 1999, formally establishing the council. Just prior to leaving office, President Clinton put forward the names of 18 appointees.[29] The Order was rescinded by the Bush Administration before the Council could meet. In Executive Order 13231,[30] President Bush established a National Infrastructure Advisory Council (with the same acronym, NIAC) whose functions are similar to those of the Clinton Council. On September 18, 2002, President Bush announced his appointment of 24 individuals to serve on Council.[31] The E.O. amending 13231 makes some minor modifications to NIAC. Primarily, the Council now reports to the President through the Secretary of Homeland Security.

**Internal Agency Plans.** There had been some confusion about which agencies were required to submit critical infrastructure plans. PDD-63 directed every agency to develop and implement such a plan. A subsequent Informational Seminar on PDD-63 held on October 13, 1998 identified two tiers of agencies. The first tier included lead agencies and other "primary" agencies like the Central Intelligence Agency and Veteran's Affairs. These agencies were held to the Directive's 180 day deadline. A second tier of agencies were identified by the National Coordinator and required to submit plans by the end of February, 1999. The "secondary" agencies were Agriculture, Education, Housing and Urban Development, Labor, Interior, General Services Administration, National Aeronautics and Space Administration and the Nuclear Regulatory Commission. All of these "primary" and "secondary" agencies met their initial deadlines for submitting their internal plans for protecting their own critical infrastructures from attacks and for responding to intrusions. The Critical Infrastructure Assurance Office assembled an expert team to review the plans. The plans were assessed in 12 areas including schedule/milestone planning, resource requirements, and knowledge of existing authorities and guidance. The assessment team handed back the initial plans with comments. Agencies were given 90 days to respond to these comments. Of the 22 "primary" and "secondary" agencies that submitted plans, 16 modified and resubmitted them in response to first round comments.

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

---

[29] White House Press Release, dated Jan. 18, 2000.

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

[31] See White House Press Release, Sept. 18, 2002.

control of the agency, and prioritize. CIAO offered this analysis to agencies, including some not designated as "primary" or "secondary" agencies, such as the Social Security Administration and the Securities and Exchange Commission. Participation by the agencies has been voluntary. Project Matrix continues.

In the meantime, other agencies (i.e. those not designated as primary and secondary) apparently did not develop critical infrastructure plans. In a much later report by the President's Council on Integrity and Efficiency (dated March 21, 2001), the Council, which was charged with reviewing agencies' implementation of PDD-63, stated that there was a misunderstanding as to the applicability of PDD-63 to all agencies. The Council asserted that all agencies were required to develop a critical infrastructure plan and that many had not, because they felt they were not covered by the Directive. Also, the Council found that of the agency plans that had been submitted, many were incomplete, had not identified their mission-critical assets, and that almost none had completed vulnerability assessments. Two years later, the Government Accountability Office[32] 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.[33]

Interestingly, 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 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 Protection 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 being as specific regarding what that plan should include. HSPD-7 called for a comprehensive National Plan for Critical Infrastructure and Key Resources Protection by the end of 2004.

---

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

[33] 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. Feb. 2003. pp. 4-5.

To date, three National Plans or Strategies have been released. In January 2000, the Clinton Administration released Version 1.0 of a *National Plan for Information Systems Protection*.[34] The Plan focused primarily on cyber-related efforts within the federal government. In September 2002, the Bush Administration, through the President's Critical Infrastructure Protection Board, released a draft of *The National Strategy to Secure Cyberspace*. The latter was released in its final form in February 2003, and could be considered Version 2.0 of the Clinton-released Plan. It addressed all stakeholders in the nation's information infrastructure, from home users to the international community, and included input from the private sector, the academic community, and state and local governments. Also in February 2003, the Office of Homeland Security released the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*.

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. According to media reports, some in the private sector complained they were not adequately consulted.[35] The Department subsequently released for public comment a "draft" National Infrastructure Protection Plan in November 2005.[36]

This latest draft plan is relatively more comprehensive than the previous documents. It identifies and integrates specific processes by which an integrated risk assessment on identified critical infrastructure assets will be performed, with assignments of duties and responsibilities and time lines. It goes a long way toward defining terms and standardizing these processes. However, similar to the other plans and strategies, it still represents the plan for developing a plan. Comments on the plan were due December 5, 2005.

**Information Sharing and Analysis Center (ISAC).** PDD-63 envisaged a single ISAC to be the private sector counterpart to the FBI's National Infrastructure Protection Center (NIPC), collecting and sharing incident and response information among its members and facilitating information exchange between government and the private sector. The idea of a single ISAC evolved into each sector having its own center. Many were conceived originally as concentrating on cyber security issues, and some still function with that emphasis. However, others have incorporated physical security into their missions.

---

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

[35] See "Still Waiting: Plan to Protect Critical Infrastructure Overdue from DHS," Congressional Quarterly. Homeland Security-Transportation & Infrastructure Newsletter, Jan. 28, 2005. This Newsletter is electronic and available by subscription only. It can be found at [http://homeland.cq.com/hs/news.do] in the news archives. The article was last viewed on Feb. 15, 2005.

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

The sectors that have established ISACs to date[37] have followed two primary models. One model involves ISAC members incorporating in some way and contracting out the ISAC development and operations to a security firm. The banking, information, water, oil and gas, railroad, and mass transit sectors have followed this approach.

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

Different federal financial support models have 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 support for its energy and mass transit ISACs). Other ISACs have always been self-supporting.

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. For example, the Department has developed a **Homeland Security Information Network (HSIN)**. HSIN initially served as the primary communication network for communicating and analyzing threat information between government agencies at the federal, state, and local levels. The HSIN is being expanded to include each critical infrastructure sector (dubbed HSIN-CS) as part of the Critical Infrastructure Protection Partnership Model. In addition, soon after September 11, 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.

**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 are:

- 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;

---

[37] A list of ISACs, with links, can be found on the DHS website: [http://www.dhs.gov/dhspublic/display?theme=73&content=1375] . Also, 11 ISACs have formed an ISAC Council. See [http://www.isaccouncil.org/about/]. Both of these sites were last viewed on Feb. 15, 2005.

- 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."

In testimony before the House Appropriations Committee on April 1, 2004, then-Undersecretary for IA/IP, Frank Libutti, stated that the Directorate had assembled a list of 28,000 critical infrastructure assets.[38] This list is now referred to as the **National Asset Database**. Also according to this testimony, from this more general list, DHS has identified 1700 sites and/or facilities which it has judged to be of highest priority and on which DHS has focused its attention. It is DHS's intent to visit each of these high priority 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 Homeland Security 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."

Its not clear how many of the 1700 priority assets have been visited and had their vulnerability assessed to-date. According to the Senate Appropriation Committee's report for its FY2005 DHS appropriation, the vulnerability of 150 priority sites had assessed at the time of the report. The report also stated that the Committee expected another 400 to be assessed in FY2005. In testimony before the Senate Homeland Security and Governmental Affairs Committee on June 15, 2005, acting Undersecretary for Information Analysis and Infrastructure Protection stated that SAVs have been conducted at 38 chemical facilities that pose the highest risks, and that 50 additional high risk chemical facilities would be visited in FY2006.

---

[38] By years end that list had reportedly grown to 80,000. See "Terror Target List Way Behind," USA Today, Dec. 9, 2004. p. 1A.

BZPPs have been prepared for 20 nuclear sites. Additional SAVs and BZPPs at nuclear sites will be conducted in conjunction with the development of a Comprehensive Nuclear Inter-agency Plan.[39] In its FY2006 budget request, IA/IP stated it is planning on performing policy oversight and program management for OSLGCP grants to ensure 1000 BZPPs are implemented at designated priority sites. It is not clear, if these are from DHS's list of 1700 sites, or if these are sites identified by states as being critical.

In regard to the development of a uniform methodology for identifying potential targets of national criticality and for establishing protective priorities, DHS is developing under contract with the American Society of Mechanical Engineers (ASME), a risk assessment methodology called **Risk Analysis and Management for Critical Assets Protection (RAMCAP)**. The goal of the effort is to develop a common methodological framework, with common terminology, common metrics, and a common basis for reporting results that would allow risks to be compared across all assets and all sectors. ASME was awarded its first contract in September 2003. This first phase development focused on the overall risk framework. DHS and ASME are currently in Phase II of the project, to develop refinements that are tailored to specific sectors. Industry sectors will be asked to use RAMCAP, or some comparable methodology approved by DHS, to provide, voluntarily, vulnerability assessments to DHS. While critical infrastructure owners and operators can use this to make their own decisions on increasing protections, DHS plans to use these in an integrated **Strategic Risk Assessment** that compares risks across sectors and identifies assets that are critical to the nation as a whole. DHS will use the Strategic Risk Assessment to make its decisions for identifying nationally critical assets and allocating resources to protect them.

## Issues and Discussion

The following is a brief discussion of some of the issues associated with critical infrastructure protection.

**Allocating Critical Infrastructure Protection Resources Based on Risk.** As a matter of national policy, resources directed toward critical infrastructure protection should be based on risk. What is risk? Risk can be defined as the consequences associated with a specific type of attack against a specific target, discounted by the likelihood that such an attack would occur (threat) and the damage to the asset that the attack might cause (vulnerability).[40] Therefore, a risk assessment may determine that a particularly vulnerable asset may still have a low risk associated with it if the consequences of its loss are not great. Alternatively, the risk associated

---

[39] Briefing by Mark Flynn, Director of the Protective Security Division within the IA/IP Directorate, at the RIC Regulatory Information Conference, Mar. 8, 2005,

[40] 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 Moteff.

with an asset with potentially large consequences may also be low if the asset is not particularly vulnerable to an attack. Alternatively, the risk associated with an asset that would result in a relatively low consequence could be quite high if the likelihood of an attack is very high. Risk (or potential consequences) can be measured in lives lost, dollars' worth of property damage, broader economic impact, etc., or some combination of these.

DHS asserts that it allocates its Urban Area Security Initiative grants based on risk assessments (although it has not fully disclosed its UASI risk assessment methodology). Also, those "priority" assets selected for BZPP support are purportedly based on some assessment of criticality, if not risk. Notwithstanding these protection efforts over the last three years, it appears that DHS is not yet able to base its critical infrastructure protection resource allocations on risk analyzed in a systematic manner across all sectors. It is still building and refining its National Asset Database, from which it identifies "critical" assets. RAMCAP, which would allow it to compare risk assessments across sectors is still in development. The status of RAMCAP raises questions about the status of its Strategic Risk Assessment. Nor has DHS clearly articulated how it determines what is "critical at the national-level."

The State Homeland Security Grant program, however, is not based on risk. This program, established initially by the USA PATRIOT Act, is formula based. When compared on a per capita basis, some states with large populations (such as New York) receive less funding per person than states with fewer people (e.g Wyoming). The President's 9/11 Commission characterized it as a "program for general revenue sharing," and recommended that funds for all state and local assistance programs be based on "risks and vulnerabilities." Congress this year was unable to agree on a more risk-based allocation process. In addition, Congress continues to set levels for port, mass transit, bus, and trucking security grants (now administered through the Urban Areas Security Initiative program), by political give-and-take. In its FY2006 budget request, the Administration proposed combining all of these targeted security grants into the UASI program, with allocation between those sectors based on the UASI risk assessment process. For more discussion of issues related to these programs, see CRS Report RL33050, *Risk Based Funding in Homeland Security Grants Legislation: Issues for the 109th Congress*, by Shawn Reese.

**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 efficiencies, a highly connected, in some cases redundant, network may not be a bad thing. The primary concern is if these mechanisms are being used and if the information needing to be shared is being made available.

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, 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 limiting the sharing of information between national law enforcement agencies and those agencies tasked with gaining intelligence of foreign agents). The legislation establishing the Department of Homeland Security also authorizes efforts to improve the ability of agencies within the federal government to share information 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.[41]

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. Success will depend on the ability of each side to demonstrate it can hold in confidence the information exchanged.

This issue is made more complex by the question of how the information exchanged will be handled within the context of the Freedom of Information Act (FOIA). In particular, the private sector is reluctant to share the kind of information the government wants without its being exempt from public disclosure under the existing FOIA statute. The Homeland Security Act protects information, defined as critical infrastructure information, and voluntarily provided to the Department of Homeland Security, not only from FOIA, but also prohibits it from being used in any civil action against the provider, exempts it from any agency rules regarding ex parte communications, and exempts it from falling under the requirements of the Federal Advisory Committee Act. It only can be shared with other entities in fulfillment of their responsibilities in homeland security, and any unauthorized disclosure by a federal government official can lead to imprisonment. Also, these disclosure rules take precedent over any State rules. Even with these protections in statute, it is

---

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

uncertain how much information on assets, vulnerabilities, incidents, etc. is flowing into DHS.[42]

The FOIA exemptions for CII and the designation of other types of homeland security information as "Sensitive But Unclassified" is not without its critics. The non-government-organizations that actively oppose government secrecy are reluctant to expand the government's ability to to hold more information as classified or sensitive. These critics feel that the protections offered to CII and the use of the "Sensitive But Unclassified" designation is too broad and prevents the public from gaining access to information regarding vulnerabilities and incidents in their own backyard.[43]

**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 Agency 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

---

[42] OMB Watch recently won a FOIA case asking DHS for the number of submissions, rejections, program procedures, etc. associated with the CII program. DHS acknowledged the receipt of 29 submissions of CII documents, 22 of which were approved as CII by DHS. OMB Watch announced its receipt of this information February 22, 2205. Its initial request was almost a year earlier, so it is not known if this is the level of CII use at the time of the initial request, or as of February 2005. See, *DHS Finally Speaks on CII* at [http://www.ombwatch.org/article/articleprint/2683/-1/321]. Site last viewed on Dec. 23, 2005.

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

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.

At the other end of the spectrum are sectors such as information and telecommunication, energy, commercial (i.e. malls and office buildings), and chemical (with the exception of those facilities located within ports) where similar activities (i.e., vulnerability assessments, etc.) are encouraged but not mandated. Congress has been struggling in particular with whether, and to what degree, chemical facilities should be required to carry out such assessments and plans and to provide that information to DHS.[44] Some security experts have also proposed that Congress require greater security measures be taken within the information sector.

[44] See CRS Report RL33043, *Legislative Approaches to Chemical Facility Security*, by Dana A. Shear, and CRS Report RL31530, *Chemical Facility Security*, by Linda-Jo Shierow.

# Appendix

## Federal Funding for Critical Infrastructure Protection

It is not possible to definitively determine how much funding the federal government devotes to critical infrastructure protection. The Homeland Security Act requires the President's Budget to include a budget analysis of homeland security activities across the federal government. For purposes of its analysis, OMB categorizes funding according to the mission areas defined in the *National Strategy for Homeland Security*. These include 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. While there is a separate category for critical infrastructure protection, activities included in some of the other mission areas can also be relevant or necessary for critical infrastructure protection. Table A.1. below shows the funding figures for the critical infrastructure protection mission area taken from the FY2007 budget's analysis.

### Table A.1. Critical Infrastructure Protection Funding by Department

($ in millions)

| Department | FY2005 enacted | FY2005 suppl. | FY2006 enacted | FY2006 suppl. | FY2007 request |
|---|---|---|---|---|---|
| Agriculture | 150.7 | | 93.2 | | 46.0 |
| Defense | 10838.2 | 847.8 | 11096.8 | | 11304.3 |
| Energy | 1456.1 | | 1523.7 | | 1503.6 |
| HHS | 168.2 | | 181.7 | | 188.8 |
| Homeland Security | 2580.9 | | 2678.5 | | 2898.0 |
| Justice | 468.8 | 1.3 | 521.1 | | 568.3 |
| Transportation | 137.0 | | 132.5 | | 154.0 |
| Veterans Affairs | 212.8 | | 273.5 | | 271.2 |
| NASA | 220.5 | | 212.6 | | 203.7 |
| NSF | 315.2 | | 317.2 | | 359.4 |
| Social Security | 150.6 | | 172.0 | | 178.5 |
| Postal Service | 503.0 | | ..... | | ..... |
| Other Agencies | 633.9 | 0.4 | 649.2 | | 675.0 |
| **Grand Total** | 17835.9 | 849.4 | 17851.7 | | 18350.6 |

**Source:** OMB, Budget of the U.S. Government, FY2007 Analytical Perspectives. Chapter 3. Homeland Security Funding Analysis. p. 26.

Much of this funding is spent by agencies to protect their own critical infrastructure. It also includes funds that agencies may spend working with states, local governments, and private owners/operators to reduce their respective

vulnerabilities. DHS activities include both of these as well as activities associated with coordinating the national effort.

Other mission areas include activities that might 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.

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 Congressional appropriations in each of these mission areas within the agencies' appropriations bills. Agencies may not know themselves until their appropriations are allocated.

## The Preparedness Directorate's FY2007 Budget Request for Infrastructure Protection and Information Security and Related Items

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. Below (**Table A.2**) is the budget request and previous year's funding for the Infrastructure Protection and Information Security portion of the Preparedness Directorate's budget.[45] Infrastructure Protection and Information Security (IPIS) is one of seven budget activities within the Preparedness Directorate's budget. In turn, the IPIS budget supports eight program or project activities, as listed in the table. Each of these support a number of subprograms. The Management and Administration activity supports the salaries and administrative expenses of IPIS. While the other subprograms are not discussed further in this Appendix, some of their activities may have been referred to in the text of this report (e.g. activities associated with Critical Infrastructure Information or the National Infrastructure Protection Plan, or the National Asset Database).

[45] The IPIS budget activity supports the same (though slightly restructured) infrastructure protection programs and projects of the "old" Information Analysis and Infrastructure Protection Directorate. The Information Analysis activity of the "old" Directorate are now supported within the Analysis and Operations budget in the departmental Management and Operations account.

## Table A.2 Funding for the Information Analysis and Infrastructure Protection Directorate

($ in millions)

| Infrastructure Protection and Information Security Budget Activity | | | |
|---|---|---|---|
| **Program/Project Activity** | **FY2005 actual** | **FY2006 enacted** | **FY2007 request** |
| Management and administration[a] | | 82,509 | 84,650 |
| Critical infrastructure outreach and partnerships | 98,254 | 111,055 | 101,100 |
| Critical infrastructure identification and evaluation | 43,684 | 67,815 | 71,631 |
| National infrastructure simulation and analysis center | 20,000 | 19,800 | 16,021 |
| Biosurveillance | 1,569 | 13,959 | 8,218 |
| Protective actions | 149,868 | 90,485 | 32,043 |
| Cyber security | 54,205 | 92,415 | 92,205 |
| National security/emergency preparedness telecommunications | 137,523 | 141,206 | 143,272 |
| **Total IPIS (w/o Management and Administration)** | **(505,703)** | **(536,735)** | **(464,490)** |
| **Total IPIS** | | **619,244** | **549,140** |

**Source:** FY2007 Congressional Justification. Preparedness Directorate. Infrastructure Protection and Information Security.

a. The Management and Administration account of the "old" IA/IP Directorate for FY2005 is not comparable to the Management and Administration account of the "new" Preparedness Directorate.
b. Does not include Management and Administration.

Another part of the Preparedness Directorate's budget which includes some critical infrastructure protection activities is the State and Local Programs budget activity. Included in this budget activity are the formula-based State Homeland Security Grant Program and the discretionary Urban Areas Security Initiative Regional Grants, which includes the High-threat, High-density Urban Areas grants, the grant programs directed at specific transportation modes (e.g. ports, rail, trucking, mass transit, etc.), and the grants for Buffer Zone Protection Plans. The State Homeland Security Grants and the High-threat, High-density Urban Areas 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 Administration is once again suggesting that the individual discretionary grants for specific transportation modes, ports and buffer zone protection plans be

aggregated into a single Targeted Infrastructure Protection grant program. Congress rejected that request in its FY2006 appropriation bill. In FY2006, Congress appropriated $1.1 billion for the various Urban Areas Security Initiative grants and $544 million for the formula-based State Homeland Security grants. The Administration is requesting $1.4 billion for the Urban Areas Security Initiative grants (i.e. the High-threat High-density Urban Area grants and the Targeted Infrastructure Protection grants) and $616 million for the formula State Homeland Security grants.

The Transportation Security Administration (TSA) within the Border and Transportation Security Directorate 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). Aviation security consumes a large fraction of the TSA budget. The Administration requested $4.7 billion in FY2007 for all facets of aviation security activities such as passenger and baggage screening; the purchase, installation, and operation of explosive detection equipment; and airport perimeter security. Of this amount, the Administration expects to offset $3.7 billion with fees. TSA requested $37.2 million for its surface transportation security activities, primarily for staffing and for rail inspectors and canines.

The Coast Guard is the lead agency for security of the nation's ports. While the Coast Guard budget does not have specific security-related line items, OMB estimates, in its homeland security analysis, that the FY2007 budget includes more than $2 billion for port security, primarily for Coast Guard activities.