Congressional Research Service
Informing the legislative debate since 1914

Critical Infrastructures: Background, Policy, and Implementation

John D. Moteff
Specialist in Science and Technology Policy

May 12, 2015

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

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

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

The national security community has been concerned for some time about the vulnerability of critical infrastructure to both physical and cyberattack. 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). Following the destruction and disruptions caused by the September 11 terrorist attacks in 2001, the nation directed increased attention toward physical protection of critical infrastructures. Over the intervening years, policy, programs, and legislation related to physical security of critical infrastructure have stabilized to a large extent. However, current legislative activity has refocused on cybersecurity of critical infrastructure.

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 two primary issues confronting Congress going forward, both in the context of cybersecurity: information sharing and regulation.

Contents

Tables

Appendixes

Contacts

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 hostile acts also depend on some of these activities as well as other more specialized activities like intelligence gathering and command and control of police and military forces. A serious disruption in these activities and capabilities could have a major impact on the country's well-being.[1]

These activities and capabilities are supported by an array of physical assets, functions, information, people, and systems, forming what has been called the nation's critical infrastructures. These infrastructures have grown complex and interconnected, meaning that a disruption in one may lead to disruptions in others.[2]

Any number of factors can cause disruptions: poor design, operator error, physical destruction due to natural causes, (earthquakes, lightning strikes, etc.) or physical destruction due to intentional human actions (theft, arson, terrorist attack, etc.). Over the years, operators of these infrastructures have taken measures to guard against, and to quickly respond to, many of these threats, primarily to improve reliability and safety. However, the terrorist attacks of September 11 in 2001, 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 CRS Issues Before Congress webpage, click on Homeland Security and Terrorism, then Homeland Security, then Critical Infrastructure and Transportation Security.[4]

[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.

[4] See http://www.crs.gov/pages/subissue.aspx?cliid=4585&parentid=28&preview=False.

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. According to Presidential Policy Directive/PPD-21, "it is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats."[5] Critical infrastructure is defined in statute as

> 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.[6]

The federal government works 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 assess those assets' vulnerabilities to the threats facing the nation (natural or manmade, i.e., all hazards), determine the level of risk associated with possible attacks or the impacts of natural events on those assets, and identify and prioritize a set of measures that can be taken to reduce those risks. Primary responsibility for protection, response, and recovery lies with the owners and operators.[7] 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.[8]

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

---

[5] White House, Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience*, February 12, 2013.

[6] See P.L. 107-71, Sec. 1016. Homeland Security Presidential Directive Number 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, released December 17, 2003, went further to describe the level of impact the loss of an asset must have to warrant considering the asset as "critical." This included causing catastrophic health effects or mass casualties comparable to those from the use of weapons of mass destruction; impairing federal agencies' abilities to perform essential missions or ensure the public's health and safety; undermining state and local government capacities to maintain order and deliver minimum essential public services; damaging the private sector's capability to ensure the orderly functioning of the economy; having a negative effect on the economy through cascading disruption of other infrastructures; or undermining the public's morale and confidence in our national economic and political institutions. HSPD-7 has since been superseded by PDD-21.

[7] 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." PPD-21, the most recent policy document, states it less explicitly: "owners and operators are uniquely positioned to manage risks to their individual operations and assets and to determine effective strategies to make them more secure and resilient." See White House, Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience*, February 12, 2013.

[8] *National Strategy for Homeland Security*, 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.[9] 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);[10] 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.[11] 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 cybersecurity. The rapid growth of a computer-literate population (implying a greater pool of potential hackers), the inherent vulnerabilities of common protocols in computer networks, the easy availability of hacker "tools" (available on many websites), and the fact that the basic tools of the hacker (computer, modem, telephone line) are the same essential technologies used by the general population indicated to the Commission that both threat and vulnerability exist.

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

The Commission also proposed a strategy for action:

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

[9] 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.

[10] 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.

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

- 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)[12] 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."[13]

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.

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

[12] 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.

[13] Ibid.

Department/Agency	Sector/Function
Energy	Electric Power, Gas, and Oil
Justice	Law Enforcement and Internal Security[a]
Director of Central Intelligence	Intelligence[a]
State	Foreign Affairs[a]
Defense	National Defense[a]

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

The PDD also assigned duties to the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism.[14] The National Coordinator reported to the President through the Assistant to the President for National Security Affairs.[15] Among his many duties outlined in PDD-63, the National Coordinator chaired the Critical Infrastructure Coordination Group. This Group was the primary interagency working group for developing and implementing policy and for coordinating the federal government's own internal security measures. The Group included high level representatives from the lead agencies (including the Sector Liaisons), the National Economic Council, and all other relevant agencies.

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

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

[14] 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.

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

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

Most of the Directive established policy-making and oversight bodies making use of existing agency authorities and expertise. However, the PDD also addressed operational concerns. These dealt primarily with cybersecurity. The Directive called for a national capability to detect and respond to cyberattacks while they are in progress. Although not specifically identified in the Directive, the Clinton Administration proposed establishing a Federal Intrusion Detection Network (FIDNET) that would, together with the Federal Computer Intrusion Response Capability (FedCIRC), established just prior to PDD-63, meet this goal. The Directive explicitly gave the Federal Bureau of Investigation the authority to expand its computer crime capabilities into a National Infrastructure Protection Center (NIPC). The Directive called for the NIPC to be the focal point for federal threat assessment, vulnerability analysis, early warning capability, law enforcement investigations, and response coordination. All agencies were required to forward to the NIPC information about threats and actual attacks on their infrastructure as well as attacks made on private sector infrastructures of which they become aware. Presumably, FIDNET[16] and FedCIRC would feed into the NIPC. According to the Directive, the NIPC would be linked electronically to the rest of the federal government and use warning and response expertise located throughout the federal government. The Directive also made the NIPC the conduit for information sharing with the private sector through an equivalent Information Sharing and Analysis Center(s) operated by the private sector, which PDD-63 encouraged the private sector to establish. These functions have been transferred to and greatly expanded upon at the Department of Homeland Security. The U.S. Computer Emergency Response Team (U.S. CERT) now handles the computer security incidents occurring on non-national security federal systems and the National Operations Center (NOC) provides all hazard situation awareness.

Quite independent of PDD-63 in its origin, but clearly complimentary in its purpose, the FBI established a program called INFRAGARD to interact with private sector firms. The program facilitates information exchange between FBI field offices and the surrounding business

[16] FIDNET initially generated controversy both inside and outside the government. Privacy concerns, cost and technical feasibility were at issue. By the end of the Clinton Administration, FIDNET as a distributed intrusion detection system feeding into a centralized analysis and warning capability was abandoned. A comparable capability was developed, called the EINSTEIN Program, that addressed the privacy concerns of FIDNET. Under EINSTEIN, participating agencies retain complete control of network data in strict accordance with Federal laws and policies. Agencies gather and subsequently share security data directly with DHS, based on reporting requirements established by the Office of Management and Budget and Department of Homeland Security. In turn, DHS prepares a strategic, cross-agency assessment, which is then shared back with all federal civilian agencies. As part of a broader cybersecurity initiative aimed at better securing federal information systems, the EINSTEIN program has expanded to include all federal agencies and to use improved sensors to monitor network traffic on federal systems. The current phase of the program, EINSTEIN III, would monitor federal network traffic from sensors placed on internet service provider networks servicing federal agencies. These new sensors would also provide the capability to counter intrusion attempts (i.e. intrusion prevention). Notwithstanding the results of privacy impact statements, the involvement of the National Security Agency in developing and implementing the EINSTEIN technology has resurrected privacy concerns.

communities. Its initial focus was network security. After September 11, its focus included both cyber and physical security. INFRAGARD is geographically oriented rather than sector-oriented. Each FBI field office has a Special Agent Coordinator who gathers interested companies of various sizes from all industries to form a chapter. Any company can join INFRAGARD. Local executive boards govern and share information within the membership. Chapters hold regular meetings to discuss issues, threats, and other matters that impact their companies. Chapters may also engage in contingency planning for using alternative systems in the event of a successful large scale attack on the information infrastructure. The program was transferred to the NIPC, before it was absorbed by the Department of Homeland Security. The program is now managed by the FBI's Cyber Division.[17]

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.[18] The Department of Homeland Security is now responsible for creating a data base of critical assets.

Restructuring by the Bush Administration

Pre-September 11

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

The Bush Administration review was influenced by three parallel debates. First, the National Security Council (NSC) underwent a major streamlining. All groups within the Council established during previous Administrations were abolished. Their responsibilities and functions were consolidated into 17 Policy Coordination Committees (PCCs). The activities associated with critical infrastructure protection were assumed by the Counter-Terrorism and National Preparedness PCC. At the time, whether, or to what extent, the NSC should remain the focal point for coordinating critical infrastructure protection (i.e., the National Coordinator came from the NSC) was unclear. Richard Clarke, himself, wrote a memorandum to the incoming Bush Administration advocating that the function be transferred directly to the White House.[19]

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

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

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

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.[20]

Third, there was the continuing debate about how best to defend the country against terrorism, in general. The U.S. Commission on National Security/21st Century (the Hart-Rudman Commission) proposed a new National Homeland Security Agency. The recommendation built upon the current Federal Emergency Management Agency (FEMA) by adding to it the Coast Guard, the Border Patrol, Customs Service, and other agencies. The Commission recommended that the new organization include a directorate responsible for critical infrastructure protection. While both the Clinton and Bush Administration remained cool to this idea, bills were introduced in Congress to establish such an agency. As discussed below, the Bush Administration changed its position in June 2002, and proposed a new department along the lines of that proposed by the Hart/Rudman Commission and Congress.

Post-September 11

Executive Orders

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.[21] Its mission was to "develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats and attacks." Among its functions was the coordination of efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks. This included strengthening measures for protecting energy production, transmission, and distribution; telecommunications; public and privately owned information systems; transportation systems; and the provision of food and water for human use. Another function of the Office was to coordinate efforts to ensure rapid restoration of these critical infrastructures after a disruption by a terrorist threat or attack. Many of the functions of the Office of Homeland Security were transferred to the Department of Homeland Security when the latter was established (see below).[22]

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

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

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

The EO also established the Homeland Security Council. The Council is made up of the President, Vice-President, Secretaries of Treasury, Defense, Health and Human Services, and Transportation, the Attorney General, the Directors of FEMA, FBI, and CIA and the Assistant to the President for Homeland Security. The EO was later amended to add the Secretary of Homeland Security. Other White House and departmental officials could be invited to attend Council meetings.[23] The Council advises and assists the President with respect to all aspects of homeland security. The agenda for those meetings are 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.[24]

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

The second Executive Order (E.O. 13231) signed October 16, 2001, stated that it is U.S. policy "to protect against the disruption of the operation of information systems for critical infrastructure ... and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible."[25] This Order also established the President's Critical Infrastructure Protection Board. The Board, consisting of federal officials, was authorized to "recommend policies and coordinate programs for protecting information systems for critical infrastructure." The Board also was directed to propose a National Plan on issues within its purview on a periodic basis, and in coordination with the Office of Homeland Security, review and make recommendations on that part of agency budgets that fall within the purview of the Board.

The Board was chaired by a Special Advisor to the President for Cyberspace Security.[26] 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, proposed 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 E.O. 13231 also established the National Infrastructure Advisory Council. The Council provides 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.

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

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

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

[26] President Bush designated Richard Clarke.

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

National Strategy for Homeland Security

In July 2002, the Office of Homeland Security released a *National Strategy for Homeland Security*. The Strategy covered all government efforts to protect the nation against terrorist attacks of all kinds. It identified protecting the nation's critical infrastructures and key assets (a new term, different as implied above by the FBI's key asset program) as one of six critical mission areas. The Strategy expanded upon the list of sectors considered to possess critical infrastructure to include public health, the chemical industry and hazardous materials, postal and shipping, the defense industrial base, and agriculture and food. The *Strategy* also added continuity of government and continuity of operations to the list, although it is difficult to see how the latter would be a considered sector. It also combined emergency fire service, emergency law enforcement, and emergency medicine as emergency services, and it dropped those functions that primarily belonged to the federal governments (e.g., defense, intelligence, law enforcement). It also reassigned some of the sectors to different agencies, including making the then proposed Department of Homeland Security lead agency for a number of sectors—postal and shipping services, and the defense industrial base. It also introduced a new class of assets, called key assets, which was defined as potential targets whose destruction may not endanger vital systems, but could create a local disaster or profoundly affect national morale. Such assets were defined later to include national monuments and other historic attractions, dams, nuclear facilities, and large commercial centers, including office buildings and sport stadiums, where large numbers of people congregate to conduct business, personal transactions, or enjoy recreational activities.[27]

The Strategy reiterated many of the same policy-related activities as mentioned above: working with the private sector and other non-federal entities, naming those agencies that should act as liaison with the private sector, assessing vulnerabilities, and developing a national plan to deal with those vulnerabilities. The Strategy also mentioned the need to set priorities, acknowledging that not all assets are equally critical, and that the costs associated with protecting assets must be balanced against the benefits of increased security according to the threat. The Strategy did not create any new organizations, but assumed that a Department of Homeland Security would be established (see below). The Strategy was updated in October 2007.[28] With the exception of a somewhat greater recognition of the role improving resilience can play in reducing the nation's risk, the strategy related to critical infrastructure saw little change.

HSPD-7

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

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

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

overall national effort to protect critical infrastructure. It also reiterated the role of Sector-Specific Agencies (i.e., Lead Agencies)[29] 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 cybersecurity unit, the Directive stated that the Director of the Office of Management remains responsible for overseeing government-wide information security programs and for ensuring the operation of a federal cyber incident response center within the Department of Homeland Security. Also, while the Department of Homeland Security is responsible for transportation security, including airline security, the Department of Transportation remains responsible for control of the national air space system.

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

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

In February 2013, the Obama Administration released Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*, which superseded HSPD-7. For a discussion of PDD-21, see below.

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

Organizationally, there remained an interagency group for coordinating policy across departments and for informing the White House (Homeland Security Council, supported by the Critical Infrastructure Protection Coordinating Committee). Certain agencies were assigned certain sectors with which to work. Sectors were asked to organize themselves to assist in coordination of effort and information sharing. A Council made up of private sector executives, academics, and

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

State and local officials was established to advise the President. Certain operational units (e.g., the Critical Infrastructure Assurance Office (CIAO) and elements of the National Infrastructure Protection Center (at the FBI)) were initially left in place, though later moved to and restructured within the Department of Homeland Security (DHS), where, now, the Undersecretary for National Protection and Programs is responsible for coordinating the implementation of policies and programs (see below). However, DHS takes a much more active role in identifying critical assets, assessing vulnerabilities, and recommending and supporting protective measures than did these earlier operational units. Also, the manpower and resources devoted to these activities have greatly increased.

One major difference between PDD-63 and the Bush Administration's efforts was a shift in focus. PDD-63 focused on cybersecurity. While the post-September 11 effort is still concerned with cybersecurity, its focus on physical threats, especially those that might cause mass casualties, is greater than the pre-September 11 effort. This led to some debate and organizational instability initially. The early executive orders discussed above segregated cybersecurity from the physical security mission with the formation of the Office of Homeland Security and the President's Critical Infrastructure Protection Board. Dissolution of the Board and the subsequent establishment of the Critical Infrastructure Protection Policy Coordinating Committee, responsible for advising the Homeland Security Council on both physical and cybersecurity issues, appears to have reunited these two concerns within a single White House group.[30]

The Obama Administration

Initial Efforts

The Obama Administration has, to date, kept in place much of the policy and organization of the Bush Administration. In February 2009, President Obama ordered a review of the homeland security and counterterrorism structures within the White House (Presidential Security Directive 1).[31] Debate centered on the merging of the Homeland Security Council and the National Security Council. In May, the President directed that the staff of the two councils be merged into the National Security Staff, while retaining the independence of the two councils.[32] President Obama also ordered a review of the federal government's policies and activities on cybersecurity.[33] The results of that review were released on May 29, 2009.[34] One result of the cybersecurity policy

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

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

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

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

[34] White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications* (continued...)

review was to recommend the appointment of a White House official to coordinate cybersecurity policies and activities across the federal government. The recommendation and subsequent appointment reestablished a cybersecurity coordinating function within the White House.[35]

Cybersecurity Legislation and Executive Orders

In May 2012, the Obama administration released proposed legislation aimed to strengthen cybersecurity.[36] Among the provisions was a proposed regulatory framework to enhance the cybersecurity at those infrastructures sites considered by the Secretary of Homeland Security to be critical to the nation. Owners and operators of designated infrastructure assets would be required to develop cybersecurity plans, have those plans evaluated by accredited outside evaluators, and to report to the Securities and Exchange Commission. The 112th Congress considered elements of the Obama Administration's proposal in a number of bills. The Senate debated a comprehensive bill (S. 3414), the House passed four more narrowly designed bills (H.R. 2096, H.R. 3523, H.R. 3834, and H.R. 4257). However, neither the Administration's proposal nor any of the Congressional bills became law.

In the absence of new legislation, the Obama Administration issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, in February 2013. The Executive Order focused primarily on information sharing and the development of a cybersecurity framework for critical infrastructure. In regard to information sharing, the Executive Order instructed the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence to "ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify specific targeted entities," and to rapidly disseminate those reports to the targeted entity. The Executive Order also expanded the Enhanced Cybersecurity Services program to all critical infrastructure sectors. The Enhanced Cybersecurity Services program shares federal classified cybersecurity threat and technical information with infrastructure network service providers which the service providers can use when monitoring the network traffic of their critical infrastructure customers.

The Executive Order defined the cybersecurity framework to be a set of standards, methodologies, procedures, and processes that critical infrastructure owners and operators could use to reduce their cybersecurity risks. The Executive Order instructed the Director of the National Institute of Standards and Technology to lead a voluntary consensus-making effort to develop the framework. The Secretary of Homeland Security was instructed to establish a set of incentives to promote participation in a Voluntary Critical Infrastructure Cybersecurity Program designed to implement the framework. Agencies that have the responsibility of regulating the security of critical infrastructure were instructed to review the sufficiency of their current

(...continued)

Infrastructure, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. For a discussion of the Cyberspace Policy Review in the context of other efforts at that time, see CRS Report R40836, *Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress*, by Catherine A. Theohary and John W. Rollins.

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

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

cybersecurity regulations and consider the adoption or tailored modification of the framework's set of standards. For a more thorough analysis of President Obama's Executive Order 13636, see CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al..

Bills addressing cybersecurity issues were again introduced in the 113th Congress and three passed as the 113th Congress came to an end.[37] P.L. 113-283 amended the Federal Information Security Management Act (FISMA) which governs cybersecurity in the federal government. P.L. 113-282 formally established in statute the National Cybersecurity and Communications Integration Center (NCCIC).[38] P.L. 113-274, among its many provisions related to cybersecurity, amended the National Institute of Standards and Technology Act, to include authorization to carry out the voluntary standards activities mentioned above. These bills, however, left unresolved the more problematic issues associated with greater information sharing between the government and the private sector which many observers argue is still necessary.[39]

In an effort to again address the issue of greater sharing of cybersecurity information, the Obama Administration, in February 2015, put forth another executive order, E.O. 13691, *Promoting Private Sector Cybersecurity Information Sharing*.[40] This E.O. assigns the Secretary of DHS the responsibility of encouraging and supporting the establishment of Information Sharing and Analysis Organizations (ISAOs). ISAOs are defined in the Homeland Security Act and are similar to the ISACs that have evolved out of PDD-63. The E.O. also authorized the establishment of an ISAO Standards Organization that would work with all stakeholders to develop voluntary standards and guidelines for establishing and operating ISAOs. The E.O. also designated the NCCIC, mentioned above, as a critical infrastructure protection program, which allows it to receive and transmit cybersecurity information between the federal government and the ISAOs as protected critical infrastructure information. Bills meant to deal with issues perceived as legal barriers to greater information sharing have been introduced again in the 114th Congress.[41]

PPD-21

In February 2013, the Obama Administration issued PPD-21. PPD-21, *Critical Infrastructure Security and Resilience*, superseded HSPD-7 issued during the George W. Bush Administration (see above). PPD-21 made no major changes in policy, roles and responsibilities, or programs,[42] but did order an evaluation of the existing public-private partnership model, the identification of baseline data and system requirements for efficient information exchange, the development of a situational awareness capability (a continuous policy objective since President Clinton's PDD-63). PPD-21 also called for an update of the National Infrastructure Protection Plan, and a new Research and Development Plan for Critical Infrastructure, to be updated every four years (HSPD-7 also required and led to the development of a research and development plan).

[37] P.L. 113-274, P.L. 113-282, and P.L. 113-283. See CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer.

[38] DHS established the NCCIC in 2009. The NCCIC merged the operations of US-CERT and the communications sector's National Coordination Center (NCC).

[39] Observers view perceived legal liabilities associated with sharing cybersecurity information as inhibiting.

[40] *Federal Register*, Vol. 80, No. 34, February 20, 2015.

[41] See CRS Report R43996, *Cybersecurity and Information Sharing: Comparison of H.R. 1560 and H.R. 1731 as Passed by the House*, by Eric A. Fischer.

[42] PPD-21 did lead to the establishment of a new Office of Cyber and Infrastructure Analysis.

While not yet making any changes in policy, roles and responsibilities, and programs, the text of PPD-21 did reflect the increased interest in resilience and the all-hazard approach that has evolved in critical infrastructure policy over the last few years. It also updated sector designations, but made no major changes in Lead Agency designations (see "Government-Sector Coordination," below). However, PPD-21 did give the energy and communications sectors a higher profile, due to the Administration's assessment of their importance to the operations of the other infrastructures. The directive also required the updated National Infrastructure Protection Plan to include a focus on the reliance of other sectors on energy and communications infrastructure and ways to mitigate the associated risks.

In all, the Obama Administration essentially has kept or slowly expanded the policies, organizational structures, and programs governing physical security of critical infrastructure assets. This included greater integration of resilience and all-hazard into its policy and strategy documents. It has focused much of its efforts on expanding the cybersecurity policies and programs associated with critical infrastructure protection.

Department of Homeland Security

Initial Establishment

In November 2002, Congress passed the Homeland Security Act (P.L. 107-296), establishing a Department of Homeland Security (DHS). The act assigned to the new Department the mission of preventing terrorist attacks, reducing the vulnerability of the nation to such attacks, and responding rapidly should such an attack occur. The act essentially consolidated within one department a number of agencies that had, as part of their missions, homeland security-like functions (e.g., Border Patrol, Customs, Transportation Security Administration). The following discussion focuses on those provisions relating to critical infrastructure protection.

In regard to critical infrastructure protection the act transferred the following agencies and offices to the new department: the NIPC (except for the Computer Investigations and Operations Section), CIAO, FedCIRC, the National Simulation and Analysis Center (NISAC),[43] other energy security and assurance activities within DOE, and the National Communication System (NCS).[44] 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).[45]

[43] 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.

[44] 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.

[45] As the result of reorganizations, the IA/IP Directorate no longer exists. The infrastructure protection activities (continued...)

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

Among the responsibilities assigned the IA/IP Directorate were

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

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

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

Second Stage Review Reorganization

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

(...continued)

originally given to the IA/IP Directorate are now performed by the National Protection and Programs Directorate. See below.

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

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

Other recommendations resulting from the review that impacted infrastructure protection included moving the Homeland Security Operations Center, now called the National Operations Center, out of the old IA/IP Directorate and placing it within a new Office of Operations Coordination; and a new Directorate of Policy, which is described as serving as the primary Department-wide coordinator of policies, regulations, and other initiatives. The conference committee report on the Department's FY2006 appropriations (H.Rept. 109-241) approved these changes.[46]

Post-Katrina Emergency Management Reform Act of 2006

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

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

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

NPPD included the Office of the Undersecretary, the Office of Cybersecurity and Communications (including the new Office of Emergency Communications), the Office of Infrastructure Protection, the Office of Risk Management and Analysis (formerly a division of the Office of Infrastructure Protection), and the Office of Intergovernmental Programs. In addition, the Secretary moved the U.S.-VISIT program into the NPPD.[47]

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

Continued Organizational Evolution

The organizational structure within DHS responsible for critical infrastructure continues to evolve. In 2010, the Federal Protective Service moved into NPPD from Immigration and Custom Enforcement. In 2013, the Office of Risk Management and Analysis was eliminated and its responsibilities moved into the Office of Policy, reporting directly to the Secretary. In 2013, the U.S.-VISIT program evolved into the Office of Biometric Identify Management, but the latter remained in NPPD. In 2014, in response to PPD-21, elements from the Office of Infrastructure Protection were reorganized into the Office of Cyber and Infrastructure Analysis. The following components currently make up the NPPD:

- Federal Protective Service;
- Office of Biometric Identify Management;
- Office of Cyber and Infrastructure Analysis;
- Office of Cybersecurity and Communications; and
- Office of Infrastructure Protection.

Policy Implementation

Government-Sector Coordination

The number and breakdown of sectors and lead, or sector specific agencies, have expanded and changed since the assignments made by PDD-63 (see **Table 1**). As mentioned above, the Bush Administration expanded the number of sectors considered to possess critical infrastructure and made some changes in assignments, and PPD-21 made some additional modifications.

[47] U.S.-VISIT was the Department's effort to verify the identity of people entering and exiting the United States. The effort is now the responsibility of the Office of Biometric Identity Management, still within the NPPD Directorate.

In March 2008, DHS announced that it was designating what would be an 18th critical infrastructure sector, Critical Manufacturing.[48] The sector includes certain sub-groups from the primary metal, machinery, electrical equipment, and transportation equipment manufacturing industries.[49] The designation was made by the Secretary under the authority granted him in HSPD-7, and represented the first exercise of that authority.

PPD-21 also made some adjustments to sector designations: National Monuments and Icons was designated as a subsector of Government Facilities; Postal and Shipping was designated as a subsector of Transportation; Banking and Finance was renamed Financial Services; and Drinking Water and Water Treatment was renamed Water and Waste Water Systems. **Table 2**, below, shows the current list of sectors and their lead agencies.

PDD-63 called for the selection, by each Lead Agency, of a Sector Liaison Official (representing the Lead Agency) and a Sector Coordinator (representing the owners/operators of each sector). While most agencies quickly identified their Sector Liaison Official, it took more time to identify Sector Coordinators. Different sectors present different challenges for coordination. Some sectors are more diverse than others (e.g., transportation includes rail, air, waterways, and highways; information and communications include computers, software, wire and wireless communications) and raised 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.

Table 2. Current Lead Agency Assignments

Department/Agency	Sector/Subsector
Agriculture	Agriculture
	Food
Agriculture	Meat/Poultry
Health and Human Services	All other
Treasury	Financial Services (formerly Banking and Finance)
EPA	Water and Waste Water Systems
	(formerly Drinking Water and Water Treatment Systems)
Health and Human Services	Public Health and Healthcare
Defense	Defense Industrial Base
Energy	Energy[a]
Homeland Security	Transportation Systems[b] (now includes Postal and Shipping)
Homeland Security	Information Technology
Homeland Security	Communications

[48] Department of Homeland Security. Designation of the National Infrastructure Protection Plan Critical Manufacturing Sector. *Federal Register*. Vol 73, No. 84. April 30, 2008. pp. 23476-23478.

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

Department/Agency	Sector/Subsector
Homeland Security	Commercial Nuclear Reactors, Materials, and Waste
Homeland Security	Chemical
Homeland Security	Emergency Services
Homeland Security	Dams
Homeland Security	Commercial Facilities
Homeland Security	Government Facilities (now includes National Monuments and Icons)
Homeland Security	Critical Manufacturing

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

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

In addition to such structural issues were ones related to competition. Inherent in trying to promote coordination is asking competitors to cooperate. In some cases it is asking competing industries to cooperate. This cooperation not only raised issues of trust among firms, but also concerns regarding anti-trust rules.

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

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

While initially working with this organizational structure, the Bush Administration promoted a new Critical Infrastructure Protection Partnership Model. Resembling the Financial Services Sector Coordinating Council approach, this newer Model expanded the sector liaison and sector coordinator model of PDD-63 into Government Coordinating Councils and Sector Coordinating

Councils for each sector. The primary objective was to expand both owner/operator and government representation within all sectors. For example, the Water Sector Coordinating Council expanded to include two owner/operator representatives, along with one non-voting association staff member from each of the following participating organizations: the Association of Metropolitan Water Agencies, the American Water Works Association, the American Water Works Association Research Foundation, the National Association of Clean Water Agencies, the National Association of Water Companies, the National Rural Water Association, the Water Environment Federation, and the Water Environment Research Foundation. The Water Government Coordinating Council is chaired by the Environmental Protection Agency, the Lead Agency, but also includes the Department of Homeland Security, the Food and Drug Administration, the Department of Interior, and the Center for Disease Control. Government Coordinating Councils can also include state, local, and tribal government entities. The Sector Coordinating Councils are to establish their own organizational structures and leadership and act independently from the federal government. Also, under this model, the Partnership for Critical Infrastructure Security has been designated the Private Sector Cross-Sector Council. The Sector Coordinating Councils are to provide input into both the National Infrastructure Protection Plan and the individual Sector Specific Plans (see below). Many of the issues governing the progress made in identifying and working with the sector coordinators model of PDD-63 continue with the sector coordinating councils.[50]

In March 2006, the Department of Homeland Security used its authority under the Homeland Security Act (P.L. 107-296, Section 871) to form advisory committees that are exempt from the Federal Advisory Committee Act (P.L. 92-463) to establish the Critical Infrastructure Partnership Advisory Council (CIPAC).[51] The Federal Advisory Committee Act requires advisory committees generally to meet in open session and make written materials available to the public. The purpose of waiving this act for the CIPAC is to facilitate more open discussion between the sector coordinating councils and the government coordinating councils (if not with the public). DHS acts as the Executive Secretariat. Members include owner/operators that are members of their respective sector coordinating councils or belong to an association that is a member of the coordinating council. Members also include federal, state, local, and tribal government entities that belong to their respective government coordinating councils. While the CIPAC is exempt from the Federal Advisory Committee Act, DHS stated in its public notice that it will make meeting dates and appropriate agendas available. There is a CIPAC webpage on the DHS website.[52]

National Critical Infrastructure Plan

PDD-63 called for a National Infrastructure Assurance Plan that would be informed by sector-level plans and would include an assessment of minimal operating requirements, vulnerabilities, remediation plans, reconstitution plans, warning requirements, etc. The National Strategy for Homeland Security, and the Homeland Security Act each have called for the development of a comprehensive national infrastructure protection plan, as well, although without specifying

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

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

[52] See http://www.dhs.gov/critical-infrastructure-partnership-advisory-council; http://www.dhs.gov/xprevprot/committees/editorial_0843.shtm.

deadlines and what that plan should include. HSPD-7 called for a comprehensive National Plan for Critical Infrastructure and Key Resources Protection by the end of 2004. According to HSPD-7, the National Plan should include (a) a strategy to identify, prioritize, and coordinate the protection of critical infrastructure and key resources, including how the Department will work with other stakeholders; (b) a summary of activities to be undertaken in order to carry out the strategy; (c) a summary of initiatives for sharing critical infrastructure information and threat warnings with other stakeholders; and (d) coordination with other federal emergency management activities.

In January 2000, the Clinton Administration released Version 1.0 of a *National Plan for Information Systems Protection*.[53] In keeping with the original focus of PDD-63, the Plan focused primarily on cyber-related efforts within the federal government. The Bush Administration, through the President's Critical Infrastructure Protection Board, released *The National Strategy to Secure Cyberspace* in February 2003, which could be considered Version 2.0 of the Clinton-released Plan. It addressed all stakeholders in the nation's information infrastructure, from home users to the international community, and included input from the private sector, the academic community, and state and local governments. Also in February 2003, the Office of Homeland Security released *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. This strategy took a broad perspective of the issues and needs associated with organizing the nation's efforts to protect its critical infrastructure; identifying roles and responsibilities, actions that need to be taken, and guiding principles.

The Department of Homeland Security missed the December 2004 deadline for releasing the National Infrastructure Protection Plan called for in HSPD-7. It did publish an Interim National Infrastructure Protection Plan in February 2005. According to media reports, some in the private sector complained they were not adequately consulted.[54] The Department subsequently released for public comment a "draft" National Infrastructure Protection Plan in November 2005.[55] A final version of the National Infrastructure Protection Plan (NIPP) was approved June 30, 2006. The NIPP was revised in early 2009 to reflect the evolution and maturation of the process, including expanded integration of all-hazard and resiliency concepts.[56] The changes did not appear to represent major shifts in policy or programs.

The 2006 NIPP identified and integrated specific processes to guide an integrated national risk management effort. For example, it defined and standardized, across all sectors, the process for identifying and selecting assets for further analysis, identifying threats and conducting threat assessments, assessing vulnerabilities to those threats, analyzing consequences, determining risks, identifying potential risk mitigation activities, and prioritizing those activities based on cost-effectiveness.[57] The 2006 NIPP also called for implementation plans for these risk reduction

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

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

[55] See *Federal Register*, Vol. 70, No. 212, November 3, 2005, pp. 66840-66841.

[56] The 2013 version of the NIPP can be found at http://www.dhs.gov/national-infrastructure-protection-plan.

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

activities, with timelines and responsibilities identified, and tied to resources. Each lead agency was to work with its sector to generate Sector Specific Plans, utilizing the processes outlined in the NIPP. DHS was to use these same processes to integrate the sector specific plans into a national plan that identifies those assets and risk reduction plans that require national level attention because of the risk the incapacitation of those assets pose to the nation as a whole.[58]

According to the 2006 NIPP, Sector Specific Plans (SSPs) were due 180 days after release of the NIPP (i.e., the end of 2006). Apparently, all 17 sectors met that deadline. However, they went through a DHS review process before being released in May 2007. Of the 17 plans submitted, 7 were made available to the public, the rest were designated For Official Use Only.[59] The Government Accountability Office (GAO) reviewed 9 of the SSPs and found that while all complied, more or less, with the NIPP process, some plans were more developed and comprehensive than others.[60] As a result, GAO was unable to assess how far along each sector actually is in identifying assets, setting priorities, and protecting key assets. DHS viewed these SSPs as a first step in the process, and planned to review the sectors' annual progress reports, as required by HSPD-7. Following the 2009 update, some of the SSP's were also updated. In 2010, DHS and its sector partners decided that a four-year cycle was sufficient for updating the NIPP and SSPs.[61]

The NIPP was updated again in 2013, as called for in PPD-21. The 2013 NIPP retains much of what was contained in the two previous NIPPs, with some refinements such as more explicit integration of resiliency and the all-hazard approach. Retained are the basic partnership model and the risk management framework. While discussed to various degrees in the previous NIPPs, the 2013 NIPP highlights seven core tenets and twelve action items to guide the national effort over the next four years. See **Table 3**.

Information Sharing and Analysis Center (ISAC)

PDD-63 envisaged a single ISAC to be the private sector counterpart to the FBI's National Infrastructure Protection Center (NIPC), collecting, analyzing, and sharing incident and response information among its members and facilitating information exchange between government and the private sector. The idea of a single ISAC evolved into each sector having its own center. ISACs differ somewhat from sector coordinating councils in that ISACs were to be 24/7/365 operations, where incidents experienced by owner/operators, as well as threat information from the government, could be reported, analyzed, and shared. Many were conceived originally as concentrating on cybersecurity issues, and some still function with that emphasis. However, others have incorporated physical security into their missions.

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

[59] See http://www.dhs.gov/sector-specific-plans for a short discussion and to access those SSPs that are not designated as For Official Use Only.

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

[61] See Review and Revision of the National Infrastructure Protection Plan. Federal Register. Vol. 78. No. 109. June 6, 2013, p. 34114.

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

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

Different federal financial support models were developed for ISACs, too. In some cases, ISACs received startup funding from their Lead Agency (e.g., drinking water received funding from EPA). In some cases, that support continues, in some cases the support has not continued (e.g., DOE no longer supports the energy ISAC). Other ISACs have always been self-supporting. The individual ISACs have formed a group called the ISAC Council.[62] Their formation and function experience some of the same variation as the coordinating councils, for some of the same reasons.

Table 3. NIPP 2013: Guiding Tenets and Call to Action

Tenets	Call to Action
Risk should be identified and managed in a coordinated and comprehensive way across the critical infrastructure community	Build upon partnership efforts
Understanding and addressing cross-sector (inter)dependencies is essential	Set national focus through jointly developed priorities
Gaining knowledge of risks and interdependences requires information sharing	Determine collective actions through joint planning efforts
The partnership approach recognizes the unique perspectives and comparative advantages of the diverse critical infrastructure community	Empower local and regional partnerships to build capacity
Regional and SLTT partnerships are crucial to improve security and resilience.	Leverage incentives to advance security and resiliency
Infrastructure critical to U.S. transcends national boundaries, requiring cross-border cooperation	Innovate in managing risk
Security and resilience should be considered during the design of assets, systems, and networks	Enable risk-informed decision making through enhanced situational awareness
	Analyze infrastructure (inter)dependencies and cascading effects
	Identify, assess, and respond to unanticipated cascading effects
	Promote recovery following incidents
	Strengthen development and delivery of technical assistance, training, and education

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

Tenets	Call to Action
	Improve security and resilience by research and development
	Focus on outcomes
	Evaluate progress toward achieving goals
	Learn and adapt

Source: CRS; text drawn from NIPP 2013.

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

Shortly after September 11, 2001, the Department established what is now called the Infrastructure Protection Executive Notification Service (ENS), which connects DHS directly with the Chief Executive Officers of major industrial firms. The ENS is used to alert partners to infrastructure incidents, to disseminate warning products, and to conduct teleconferences. The Department is also responsible for operating the Critical Infrastructure Warning Network (CWIN), which provides secure communications between DHS and other federal, state, and local agencies, the private sector, and international agencies. CWIN does not rely on the Public Switch Network or the internet.[64]

As mentioned earlier, the Homeland Security Act defined Information Sharing and Analysis Organizations (ISAOs) as formal or informal entities created or employed by public or private sector organizations for purposes of gathering and analyzing critical infrastructure information and communicating or disclosing that information "to help prevent, detect, mitigate, or recover from the effects of a … compromise … of a critical infrastructure…."[65] While the ISACs that evolved out of PDD-63 are sector-oriented, the ISAOs, as defined by the Homeland Security Act, are not characterized as such. The Obama Administration's E.O. 13691 instructed the Secretary of Homeland Security to support the expansion of these organizations to help facilitate cybersecurity information sharing.

[63] US-CERT continues these function through the National Cybersecurity and Communications Integration Center.

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

[65] See 6 U.S.C. 131 (5).

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

The Homeland Security Act of 2002 assigned to the Information Analysis and Infrastructure Protection Directorate the following activities:

- access, receive, analyze, and integrate information from a variety of sources in order to identify and assess the nature and scope of the terrorist threat;
- carry out comprehensive assessments of the vulnerabilities of key resources and critical infrastructure, of the United States including risk assessments to determine risks posed by particular types of attacks;
- integrate relevant information, analyses, and vulnerability assessments in order to identify priorities for protective and support measures.

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

PDD-21 reiterated these responsibilities which are now carried out by the National Protection and Programs Directorate.

DHS through various mechanisms, including through state homeland security officials and lead agency officials, seeks to identify infrastructure assets that fit the definition of critical infrastructure. The National Critical Infrastructure Prioritization Program and the Critical Foreign Dependencies Initiative, supported with analysis from the National Infrastructure Simulation and Analysis Center and the Office of Infrastructure Analysis, identify those assets (both within the country and abroad) most critical to the nation as a whole, based on the hazards/threats to which the asset is exposed, its vulnerabilities to those hazards/threats, and the potential consequences that might result, including impacts that might cascade to other infrastructure assets. The results of this analysis help populate a classified two-tiered data base of critical infrastructure assets.[66] DHS reaches out to the owner/operators of these assets and offers assistance in conducting more detailed vulnerability/resilience assessments and makes recommendations on how to reduce those risks.

In addition, DHS will conduct regional resiliency assessments. The Regional Resiliency Assessment Program (RRAP) expands the vulnerability assessments to consider clusters of critical infrastructures and key resources within a given geographic region. The results of the

[66] In 2013, a GAO report found that the analyses used to populate the list of high-priority assets generally followed the common approach articulated in the National Infrastructure Protection Plan. However, DHS has departed from this common approach to place assets on the list in certain specific cases. GAO expressed concern that such departures could impact how the list is used (by FEMA for example) and could hinder cross-sector comparisons. GAO also found that the modifications to the approach had not been validated by outside peer review. Finally, there are certain statutory reporting requirements regarding the list that DHS could not demonstrate had been met.

assessments are shared with participants. Participation of owners/operators, state and local governments, in these assessments is voluntary. Adopting the risk-reducing recommendations is also voluntary. However, DHS does make an effort to track those recommendations that have been adopted.[67]

In addition to its selection of high-priority sites and subsequent site visits, vulnerability/resiliency assessments, and risk-reduction recommendations, DHS, through the Federal Emergency Management Agency's (FEMA), also has been supporting infrastructure protection at the state and local level through its State and Local Grant Programs. Specific grant programs include the State Homeland Security Formula-based Grants, the Urban Area Security Initiative (UASI) Grants (both of which primarily support first responder needs, but include certain infrastructure protection expenditures), Port Security Grants, Rail and Transit Security Grants, Intercity Bus Security Grants, and Highway (Trucking) Security Grants. Before receiving funds, grants recipients must identify specific critical infrastructure assets, conduct threat and vulnerabilities assessments, and develop a plan for how they intend to use grant funds to reduce those vulnerabilities through eligible expenditures.

Cybersecurity Framework

As discussed above, President Obama's EO 13636 gave NIST the responsibility for developing a Cybersecurity Framework. The framework is to form the basis for a Voluntary Critical Infrastructure Cybersecurity Program that would encourage critical infrastructure owners and operators to improve the security of their information networks. Also, those agencies that have regulatory authority over certain critical infrastructure owner and operators are to consider using or modifying the Framework in any regulatory action. NIST released Version 1.0 of the Framework February 12, 2014.[68]

Issues and Discussion

Over the last few years, Congressional interest in critical infrastructure protection has focused, principally, on reviewing the progress and effectiveness of DHS's efforts. However, two policy issues remain in debate: how to improve information sharing to the mutual benefit of the federal government and the owner/operators while maintaining privacy protections; and, the need for further regulations. Congress continues to debate these issues primarily in the context of cybersecurity. For a more detailed discussion of these efforts, see CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer.

[67] See Government Accountability Office report, *Critical Infrastructure Protection: DHS Could Strengthen the Management of the Regional Resiliency Assessment Program*. GAO-13-616. July 30, 2013. The report stated that DHS was following up with participants of the program to determine what if any of the assessment's recommendations were adopted. However, the agency was not measuring how the adoption of recommendations were contributing to the goals of the program.

[68] See http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

Information Sharing

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

In the past, information flow between all of these stakeholders had been restrained, or non-existent, for at least three reasons: a natural bureaucratic reluctance to share information, difficulties associated with information and technical compatibility, and legal restraints designed 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 were reexamined and there appears to be a general consensus to change them. Some changes have resulted from the USA PATRIOT Act (including easing the restrictions on sharing of information between national law enforcement agencies and those agencies tasked with gaining intelligence on 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. The legislation also required the President to establish an information sharing environment (ISE) for the sharing of terrorism information among all appropriate federal, state, local, and tribal entities, and the private sector.

As mentioned above, recent executive orders and legislative efforts deal with sharing cybersecurity information and how to improve and incentivize sharing cybersecurity information between the federal government and the owner/operators in the private sector, while protecting the privacy of average citizens and providing some liability protection for the companies providing the information. It should be noted that the exchange of cybersecurity information may tend to introduce issues of privacy more so than the exchange of information related to physical security. This is because the exchange of cybersecurity information meant to assist in analyzing attack modes, software vulnerabilities, etc. may involve the content of electronic messages in which malware is embedded and which are held by, or transit through, third parties. For an analysis of legislative activity in the 114th Congress related to sharing cybersecurity information see CRS Report R43996, *Cybersecurity and Information Sharing: Comparison of H.R. 1560 and H.R. 1731 as Passed by the House*, by Eric A. Fischer, and CRS Report R43941, *Cybersecurity and Information Sharing: Legal Challenges and Solutions*, by Andrew Nolan.

While the federal government is trying to increase the amount of information shared among appropriate stakeholders, it is also trying to maintain a tight control (short of classification) on who gets to see what information. A variety of designations have been given to information the federal government wishes to control (critical infrastructure information [see below], homeland

security information, terrorism information, sensitive security information). A catch-all term for these and other designations of controlled information is "sensitive but unclassified."

Since much of what is considered to be critical infrastructure is owned and operated by the private sector, critical infrastructure protection relies to a large extent on the ability of the private sector and the federal government to share information. However, it is unclear how open the private sector and the government have been in sharing information. The private sector primarily wants information from the government on specific threats whereas the government may want to protect that information 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 from industry on vulnerabilities and incidents whereas companies may want to protect that information to prevent adverse publicity or to keep company practices confidential. The private sector, too, is concerned about whether providing this information might lead to future regulatory action or other liabilities. Successful information sharing will depend on the ability of each side to demonstrate it can hold in confidence the information exchanged.

Sharing information between government and the private sector is made more complex by the question of how the information will be handled within the context of the Freedom of Information Act (FOIA). In particular, the private sector is reluctant to share the kind of information the government wants without it being exempt from public disclosure under the existing FOIA statute. The Homeland Security Act (P.L. 107-296, Sec. 214) exempts information defined as critical infrastructure information from FOIA (as well as providing other protections). Similar FOIA exemptions are offered in other legislation. For example, the Public Health Security and Bioterrorism Preparedness Act (P.L. 107-188, Sec. 401, see below) exempts certain security-related information from FOIA. Even with these protections in statute, it is uncertain how much information on assets, vulnerabilities, incidents, etc. is being shared with DHS, or how useful it is.[69]

The FOIA exemptions for critical infrastructure information (CII) and other types of sensitive but unclassified information is not without its critics. The non-government-organizations that actively oppose government secrecy are reluctant to expand the government's ability to hold more information as classified or sensitive. These critics, and others, feel that the protections offered to CII and other types of sensitive but unclassified information is too broad and believe that controls are stifling public debate and oversight, as well as impeding technological advances that could benefit both security and the economy.[70]

[69] In February 2005, DHS acknowledged the receipt of 29 submissions of CII documents, 22 of which were approved as CII by DHS. See *DHS Finally Speaks on CII* at http://www.foreffectivegov.org/node/2286t. In previously cited testimony (before the Senate Ad Hoc Subcommittee on State, Local, and Private Sector Preparedness and Integration, July 12, 2007), the Assistant Secretary for Infrastructure Protection stated that since the final rule governing implementation of the CII program was released, DHS had received about 5,400 submissions.

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

Regulation

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

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

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

As mentioned above, the security community, the Obama administration, industry, and Congress have debated the need to regulate more comprehensively the cybersecurity of critical infrastructure assets. However, it has proven difficult to pass additional regulations. Some in the security community suggest that strategic national needs are market externalities that require regulation to encourage more owner/operators (in particular, those who may not be at the forefront in cybersecurity capabilities or practices) to take the type of action that the security community considers necessary. Industry groups are concerned about the costs and benefits and the potential for duplicative reporting requirements associated with additional regulations.

Appendix. Funding for Critical Infrastructure

Federal Funding for Critical Infrastructure Protection

It is difficult to determine how much funding the federal government devotes to the protection of critical infrastructure. The Homeland Security Act requires the President's Budget to include a budget analysis of homeland security activities across the federal government. This analysis appears in Chapter 3 of the Analytical Perspectives volume of the President's Budget.[71] However, beginning with the FY2010 budget request, the Administration changed the way homeland security activities are accounted for, making the estimate of how much is spent on critical infrastructure less clear.

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

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

For FY2010, OMB reformulated the categories for tracking homeland security activity, rearranging them into three new categories: prevent and disrupt terrorist attacks; protect the American people, our critical infrastructure, and key resources; and respond to and recover from incidents. As a result, it is not possible to compare the FY2010 figures with those from prior budgets. The category "protect the American people, our critical infrastructure, and key resources" now includes more activities than were counted in the "critical infrastructure and key resources protection" category in FY2009 and before. These additional activities include ones that were previously counted in the "defending against catastrophic events" category. The latter represents a significant addition in funding, and includes activities meant to protect the general population from weapons of mass destruction and not necessarily focused on infrastructure protection. Since this report does not cover many of the activities associated with defending against or responding to catastrophic events, the OMB accounting is no longer representative of the activities covered in this report.

[71] An explanation of the budget can be found in the Budget's Analytical Perspective, Special Topics, Chapter 22, pp 314-348. See https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/ap_22_homeland_security.pdf.

FY2016 DHS Budget Request and Prior Year Appropriations for Infrastructure Protection and Information Security Program and Other Relevant DHS Budget Activities

Just as it is difficult to account for all the federal activities associated with critical infrastructure protection in the federal government, it is also difficult to track the critical infrastructure protection activities within the Department of Homeland Security. Funding for activities related to critical infrastructure protection is found in numerous places within the Department, including the National Protection and Programs Directorate, the Transportation Security Administration, the Coast Guard, Secret Service, the Science and Technology Directorate, FEMA, and U.S. Customs and Border Protection. However, much of the funding for the organizations and activities discussed in the body of this report can be found in the Infrastructure Protection and Information Security (IPIS) Program. See **Table A-1**, below.[72]

IPIS

The Infrastructure Protection and Information Security Program (IPIS) supports the activities of the Office of Infrastructure Protection (OIP), the Office of Cybersecurity and Communications (OCS&C), and the Office of Cyber and Infrastructure Analysis (OCIA). OIP coordinates the national effort to reduce the risks associated with the loss or damage to the nation's critical infrastructure due to terrorist attack or natural events. This effort is a cooperative one between the federal government; state, local, and tribal governments; and the private sector, to identify critical elements of the nation's infrastructure, their vulnerabilities, the potential consequences of their loss or damage, and ways to mitigate those losses. The OCS&C performs a similar function, but specifically focuses on the nation's information and communications networks, including the communications systems and programs that ensure the President can communicate with selected federal agencies, state, local, and tribal governments, and certain private sector entities during times of national emergencies. OCIA provides analytic support to OIP and OCS&C. Funding is aligned with this organizational structure and provided in a set of program/project activities (PPAs) as noted in the table below.

The Administration requested $1,312 million for the IPIS program for FY2016, a net increase of $123 million above the amount enacted for FY2015. For further discussion of the IPIS budgets, see CRS Report R43796, *Department of Homeland Security: FY2015 Appropriations*, coordinated by William L. Painter.

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

Table A-1. Funding for the Infrastructure Protection and Information Security Program

(budget authority in millions of dollars)

Program/ Project Activity	FY2014 Actual	FY2015 Enacted (P.L. 114-4)	FY2016 President's Request
Infrastructure Protection	$263	$271	$295
Identification, Analysis, and Planning	*63*	*64*	*76*
Sector Management and Governance	*63*	*65*	*71*
Regional Field Operations	*57*	*57*	*53*
Infrastructure Security Compliance	*81*	*85*	*95*
Cybersecurity	790	753	818
Cybersecurity Coordination	*4*	*4*	*4*
US-CERT Operations	*101*	*99*	*99*
Federal Network Security	*199*	*171*	*131*
Network Security Deployment	*381*	*377*	*480*
Global Cybersecurity Management	*26*	*26*	*20*
Critical Infrastructure Cyber Protection and Awareness	*73*	*71*	*77*
Business Operations	*5*	*6*	*7*
Communications	131	164	198
Office of Emergency Communications	*37*	*37*	*33*
Priority Telecommunications Services	*53*	*53*	*64*
Next Generation Networks	*21*	*53*	*80*
Programs to Study and Enhance Telecommunications	*10*	*10*	*10*
Critical Infrastructure Protection	*9*	*10*	*11*
Total, Infrastructure Protection and Information Security	**1,185**	**1,189**	**1,312**

Source: Department of Homeland Security. National Protection and Programs Directorate. Infrastructure Protection and Information Security. Fiscal Year 2016 congressional Justification. FY2015 enacted data taken from Explanatory Statement Submitted by Mr. Rogers of Kentucky, Chairman of the House Committee on Appropriations, Regarding H.R. 240. Congressional Record. Vol. 161. No. 6. January 13, 2015. H.R. 284.

Notes: Columns may not add due to rounding.

Other Infrastructure Related Programs

In addition to the IPIS program within the National Protection and Programs Directorate, other areas in DHS support infrastructure protection. For example, the Federal Emergency Management Agency (FEMA) manages a number of grant programs, some of which allow for protecting or mitigating the risks to critical infrastructure assets. These grants include the State Homeland Security Grant Program, the Urban Area Security Initiative, Public Transportation Security Assistance and Railroad Security Assistance (which includes the Intercity Passenger

Rail-AMTRAK Program and the Intercity Bus Security Grant Program), and the Port Security Grant Program. The State Homeland Security grants and the Urban Areas Security Initiative grants primarily support first responder capabilities, but funding can also be spent on critical infrastructure protection expenses (such as the purchase of cameras, sensors, etc.). The port, transit, and intercity bus and rail security grants focus primarily on protecting infrastructure assets and passengers. For the last three fiscal years, the Administration has been requesting that these grants be aggregated into a single National Preparedness Grant Program. Congress has chosen not to agree and continues to appropriate funding for them individually. **Table A-2** shows the amount of funding appropriated for these programs in FY2015. The Administration requested $1,043 million for its proposed National Preparedness Grant Program for FY2016.

Table A-2. FY2015 Funding for Selected FEMA Grants

Grant Program	FY2015 Allocation (millions)
State Homeland Security Program	$467
Urban Area Security Initiative	600
Public Transportation Security Assistance and Railroad Security Assistance	100
Intercity Passenger Rail-AMTRAK Program	*(10)*
Intercity Bus Security Grant Program	*(3)*
Port Security Grant Program	100
Total	**1,267**

Source: Department of Homeland Security. National Protection and Programs Directorate. Infrastructure Protection and Information Security. Fiscal Year 2016 congressional Justification. FY2015 enacted data taken from Explanatory Statement Submitted by Mr. Rogers of Kentucky, Chairman of the House Committee on Appropriations, Regarding H.R. 240. Congressional Record. Vol. 161. No. 6. January 13, 2015. H.R. 286.

The Transportation Security Administration (TSA) oversees 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, including support for: passenger and baggage screening; the purchase, installation, and operation of explosive detection equipment; and airport perimeter security; air marshals; crew vetting; etc. Congress appropriated $5,639 million for TSA aviation security activities in FY2015. TSA also receives funds for surface transportation security and security-related support activities. For FY2015 Congress provided $917 million. For FY2016 the Administration requested $7,092 million in direct appropriations (not counting offsetting receipts and capital fund accounts), which included $931 million for transportation security support. For more information on issues associated with transportation security, see CRS Report RL33512, *Transportation Security: Issues for the 114th Congress*, by Bart Elias, David Randall Peterman, and John Frittelli. The Coast Guard, too, receives funding for its role in protecting U.S. ports. However, funding for these functions cannot be found in a single line item.

The Science and Technology Directorate budget supports research and development in a number of areas relevant to critical infrastructure protection. This includes research and development in cybersecurity, risk analysis, explosive detection, blast protection, modeling and simulation, safe

cargo containers, and more. The Directorate also works with the Office of Infrastructure Protection to develop and maintain a National Critical Infrastructure Protection R&D Plan. It is difficult to determine how much funding is devoted overall to critical infrastructure protection-related research, given the budget structure of the programs. For additional information regarding DHS's Science and Technology program, including legislation calling for a critical infrastructure research and development plan, see CRS Report R43064, *The DHS S&T Directorate: Selected Issues for Congress*, by Dana A. Shea.

Author Contact Information

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