Chapter 14

Critical Infrastructure Protection

Learning Outcomes

Careful study of this chapter will help a student do the following:

- Explain how the importance of critical infrastructure protection was realized before 9/11.
- Describe how critical infrastructure protection has been shaped and evolved since PDD-63.
- Explain the role of the Federal government in critical infrastructure protection.
- Assess the importance of various steps in the Risk Management Framework.

"We did find widespread capability to exploit infrastructure vulnerabilities. The capability to do harm—particularly through information networks—is real; it is growing at an alarming rate; and we have little defense against it."

- 1997 President's Commission on Critical Infrastructure Protection

Introduction

In July 1996, President Clinton appointed a Commission on Critical Infrastructure Protection to report on the scope and nature of vulnerabilities and threats to the nation's critical infrastructure. The Commission found concern for cyber attack. As a result, in May 1998, President Clinton issued PDD-63 setting a national goal to protect the nation's critical infrastructure from intentional attack.

9/11 thrust critical infrastructure protection to the forefront of US security concerns. Previously, in July 1996 President Clinton appointed a Commission on Critical Infrastructure Protection to report the scope and nature of vulnerabilities and threats to the nation's critical infrastructure, and recommend a comprehensive national plan for protecting them including any necessary regulatory changes. The Commission was chartered in response to growing concerns stemming from the 1993 attack on the World Trade Center in New York City, 1995 bombing of the Murrah Federal Building in Oklahoma City, and 1996 bombing of the Khobar Towers US military barracks in Dhahran Saudi Arabia. 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) were the same essential technologies used by the general population indicated to the Commission that both threat and vulnerability exist. The Commission Report, released in October 1997, led to Presidential Decision Directive No. 63 (PDD-63) issued in May 1998. PDD-63 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". [1, p. 4]

PDD-63

PDD-63 identified a set of twelve infrastructure "sectors" whose assets 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. A federal Lead Agency (LA) was assigned to each of these "sectors". 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 Sector Security Plan (SSP) which was to be integrated into a National Infrastructure Assurance Plan. [1, p. 4]

Following the attacks of September 11, 2001, critical infrastructure protection became a high priority. On October 16, 2001, President Bush signed Executive Order (EO) 13231 stating that it is US 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." On October 26, 2001, President Bush signed into law the USA PATRIOT Act, defining critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters". In July 2002, the Office of Homeland Security released the first National Strategy for Homeland Security. It identified protecting the nation's critical infrastructures and key assets as one of six critical mission areas. The Strategy also expanded upon the list of sectors considered to comprise critical infrastructure to include public health, the chemical industry and hazardous materials, postal and shipping, the defense industrial base, and agriculture and food. Key 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. Then on December 17, 2003, the Bush Administration released Homeland Security Presidential Directive No. 7 (HSPD-7). HSPD-7 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. For example, the Directive reiterated the Secretary of Homeland Security's role in coordinating the overall national effort to protect critical infrastructure. It also reiterated the role of Sector-Specific Agencies (formerly "Lead Agencies") 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. 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 was still concerned with cybersecurity, its focus on physical threats, especially those that might cause mass casualties, was greater than the pre-September 11 effort. [1, p. 12]

In December 2003, President Bush issued HSPD-7 updating national policy on critical infrastructure protection, following the same pattern established in PDD-63. Because 9/11 had succeeded in subverting critical infrastructure in a physical attack, HSPD-7 gave greater emphasis to physical protection compared to PDD-63's emphasis on cybersecurity.

HSPD-7

HSPD-7 directed development of a National Plan for Critical Infrastructure and Key Resources Protection to outline national goals, objectives, milestones, and key initiatives. Previously, PDD-63 had called for development of a National Infrastructure Assurance Plan. The corresponding focus on cybersecurity resulted in the National Plan for Information Systems Protection released in January 2000. While this plan formed the basis for the 2003 National Strategy to Secure Cyberspace, it did not support the revised focus on physical security stemming from 9/11. After two furtive

Table 14-1: CIP Directives, Strategies, & Plans

HS Law	HS Directives	HS Strategies	CIP Plans
2002 HSA	1998 PDD-63	2002 NSHS	2005 Interim NIPP
	2003 HSPD-7	2007 NSHS	2005 Draft NIPP
	2013 PPD-21	2010 NSS	2006 NIPP
		2015 NSS	2009 NIPP
			2013 NIPP

attempts in 2005, the Department of Homeland Security (DHS) released the National Infrastructure Protection Plan (NIPP) in June 2006. The NIPP identified and integrated specific processes to guide an integrated national risk management effort. It defined and standardized, across all sectors, a Risk Management Framework (RMF) 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. The NIPP also called for implementation plans for these risk reduction activities, with timelines and responsibilities identified, and tied to resources. Each Sector-Specific Agency (SSA) 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 identifying 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. The NIPP was updated in 2009 to adopt an "all-hazards" approach to risk management, and again in 2013 to emphasize the importance of resilience. [1, p. 24]

In February 2013, President Obama issue PPD-21 again updating national policy on critical infrastructure protection. PPD-21 restored emphasis on cybersecurity, and introduced the concept of resilience.

PPD-21

In February 2013, the Obama Administration issued Presidential Policy Directive No. 21 (PPD-21), Critical Infrastructure Security and Resilience, superseding HSPD-7. PPD-21 made no major changes in policy, roles and responsibilities, or programs, but did order an evaluation of the existing public-private partnership model, the identification of baseline data and system requirements for efficient information exchange, and the development of a situational awareness capability (a continuous policy objective since President Clinton's PDD- 63). PPD-21 reflected an increased interest in resilience and all-hazard approach that has evolved in critical infrastructure policy over the years. It also updated sector designations, but made no major changes in Sector-Specific Agency designations. 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. To date, the Obama Administration has kept or slowly evolved the policies, organizational structures, and programs governing physical security of critical infrastructure assets. It has focused much more effort to expand upon the cybersecurity policies and programs associated with critical infrastructure protection. [1, pp. 13-14]

Table 14-2: Infrastructure Sectors and Lead/Sector-Specific Agencies

1998 PDD-63			2003 HSPD-7			2013 PPD-21		
#	Sector	LA	#	Sector	SSA	#	Sector	SSA
1.	Intelligence	CIA	1.	Chemical	DHS	1.	Chemical	DHS
2.	Information & Communications	DOC	2.	Commercial Facilities	DHS	2.	Commercial Facilities	DHS
3.	National Defense	DOD	3.	Communications	DHS	3.	Communications	DHS
4.	Electric, Power, Gas, & Oil	DOE	4.	Critical Manufacturing	DHS	4.	Critical Manufacturing	DHS
5.	Emergency Law Enforcement	DOJ	5.	Dams	DHS	5.	Dams	DHS
6.	Law Enforcement & Internal Security	DOJ	6.	Emergency Services	DHS	6.	Emergency Services	DHS
7.	Foreign Affairs	DOS	7.	Government Facilities	DHS	7.	Information Technology	DHS
8.	Transportation	DOT	8.	Information Technology	DHS	8.	Nuclear Reactors, Materials, & Waste	DHS
9.	Water	EPA	9.	Nuclear Reactors, Materials, & Waste	DHS	9.	Transportation Systems	DHS & DOT
10.	Emergency Fire Service	FEMA	10.	Postal & Shipping	DHS	10.	Government Facilities	DHS & GSA
11.	Emergency Medicine	HHS	11.	Defense Industrial Base	DOD	11.	Defense Industrial Base	DOD
12.	Banking & Finance	TREAS	12.	Energy	DOE	12.	Energy	DOE
			13.	National Monuments & Icons	DOI	13.	Water & Wastewater Systems	EPA
			14.	Transportation Systems	DHS & DOT	14.	Healthcare & Public Health	HHS
			15.	Water	EPA	15.	Financial Services	TREAS
			16.	Healthcare & Public Health	HHS	16.	Food & Agriculture	USDA
			17.	Banking & Finance	TREAS			
			18.	Agriculture & Food	USDA			

Risk Management Framework

The Risk Management Framework has evolved since it was first introduced in the 2005 Interim National Infrastructure Protection Plan. [2, p. 8] Yet it remains, as currently prescribed in the 2013 National Infrastructure Protection Plan, a continuous process for incrementally reducing vulnerability within critical infrastructure. The Risk Management Framework is conducted in voluntary cooperation between the Department of Homeland Security and public and private partners organized into Sector Coordinating Councils representing the sixteen infrastructure sectors listed in Table 2. [3, pp. 10-11] The Risk Management Framework is conducted in five steps comprised of 1) Set Goals and Objectives, 2) Identify Infrastructure, 3) Assess and Analyze Risks, 4) Implement Risk Management Activities, and 5) Measure Effectiveness. [3, p. 15]

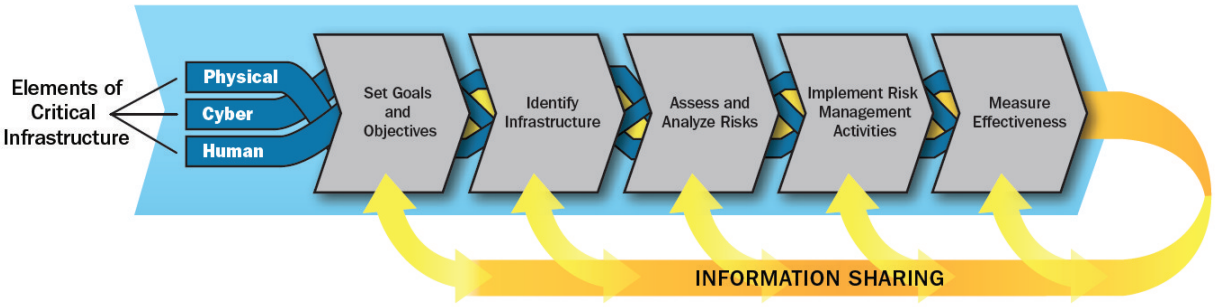

Figure 14-1: 2013 NIPP Risk Management Framework [3, p. 15]

The DHS Risk Management Framework is the implementing procedure of the National Infrastructure Protection Plan.

RMF Step 1: Set Goals and Objectives. The risk reduction priorities for each sector are established in Sector Specific Plans (SSPs). [3, p. 16] The first SSPs were released in May 2007, after the first official National Infrastructure Protection Plan was issued in 2006. Of the 17 plans drafted, 7 were made available to the public. The other 11 plans were designated "For Official Use Only" and withheld from public release. A review by the Government Accountability Office found that while all the plans complied, more or less, with NIPP requirements, some were more developed and comprehensive than others. The Sector Security Plans were revised in 2010 after the NIPP was revised in 2009. HSPD-7 stipulated that the SSPs should be updated annually. However, in 2010, DHS and its sector partners decided that a four-year cycle was sufficient for updating the SSPs. [1, pp. 23-24] As of 2015, the SSPs had yet to be updated and the most recent versions were dated 2010.

RMF Step 2: Identify Infrastructure. Despite the definition in the USA PATRIOT Act, critical infrastructure identification has been fraught with difficulties. While the National Infrastructure Protection Plan was still under development, the Department of Homeland Security undertook Operation Liberty Shield to catalog the nation's critical infrastructure in advance of the U.S. invasion of Iraq. Over the summer of 2003, DHS personnel cataloged 160 assets across various sectors it determined needed additional protection or mitigation against potential attack. Under pressure from Congress, the list was expanded to 1,849 assets and called the Protected Measures Target list (PMTL). At the same time it was conducting Operation Liberty Shield, DHS issued a grant asking states to conduct a critical infrastructure self-assessment. The resulting data call added another 26,359 assets to the PMTL, including zoos, festivals, shopping centers, and other "out-of-place" assets. [4, p. 6] The dubious results were attributed to "minimal guidance" given to the states. Accordingly, in July 2004 DHS issued a second data call to correct the problems from the 2003 data call. The 2004 data call included more precise instructions in the form of separate Guidelines for Identifying National Level Critical Infrastructure and Key Resources. States responded by submitting 47,701 additional assets to the PMTL. Together, the combined data from Operation Liberty Shield and 2003 and 2004 data calls comprised 77,069 assets of what DHS called the National Asset Database (NADB). Still, the DHS Inspector General noted that the list contained too many "out-of-place" assets, making subsequent prioritization difficult. [4, pp. 8-10] Congress intervened with the Implementing Recommendations of the 9/11 Commission Act which mandated the establishment of

a second database containing a prioritized list of assets. [5] DHS complied with Congress by initiating the National Critical Infrastructure Prioritization Program (NCIPP) working with public and private partners to identify and classify critical infrastructure as either Level 1 or Level 2 priority based on the consequences associated with the asset's disruption or destruction. [6, p. 4] In 2006, the NADB was replaced by the Infrastructure Information Collection System (IICS) available from the DHS Infrastructure Protection Gateway. [7] According to the 2013 NIPP, the National Critical Infrastructure Prioritization Program remains the primary program for prioritizing critical infrastructure at the national level. [6, p. 17] The number and identity of assets collected by NCIPP is protected information unavailable to the public.

The Risk Management Framework is a risk-based methodology for prioritizing allocation of scarce national resources to reducing vulnerabilities among critical infrastructure.

RMF Step 3: Assess and Analyze Risks. DHS Protective Security Advisors (PSAs) located in all fifty States and Puerto Rico conduct Security Surveys and Resilience Assessments under the Enhanced Critical Infrastructure Protection (ECIP) and Regional Resiliency Assessment Program (RRAP). [8] According to DHS guidance, PSAs are to conduct Site Assistance Visits (SAVs) with infrastructure owners and operators within their districts giving priority to Level 1 assets. PSAs use an Infrastructure Survey Tool to gather information on 1,500 variables covering six major components and forty-two subcomponents. The results are compiled by Argonne National Laboratory into a "dashboard" indicating the asset's overall protective measure score and compare it with the scores of similar assets that have previously undergone a Security Survey. The interactive dashboard allows owners to consider alternative security upgrades and see how they affect the overall security of the asset as shown in Figure 2. PSA Security Surveys are done in voluntary cooperation with infrastructure owner/operators. [9, pp. 9-10] Out of 2,195 Security Surveys and 655 Vulnerability Assessments conducted during fiscal years 2009 through 2011, GAO identified a total of 135 Security Surveys and 44 Vulnerability Assessments that matched assets on the NCIPP list of high-priority assets. GAO also identified an additional 106 Security Surveys and 23 Vulnerability Assessments that were potential matches with assets on the NCIPP lists of priority assets, but could not be certain that the assets were the same because of inconsistencies in the way the data were recorded in the two different databases. All told, GAO determined that in two years DHS had conducted 241 Security Surveys and 67 Vulnerability Assessments on high-priority assets listed in the NCIPP database. [9, pp. 15-17]

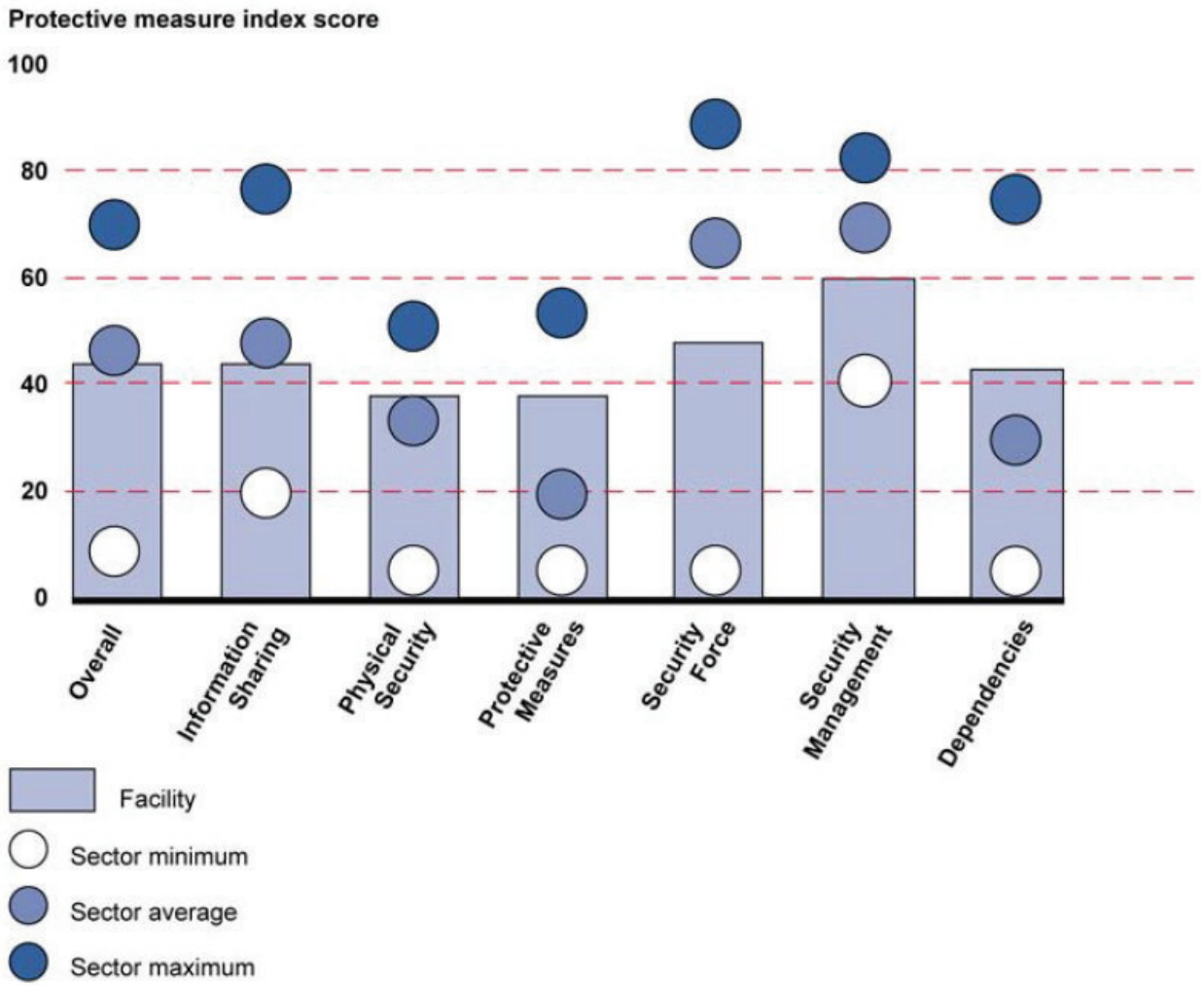

Figure 14-2: PSA Security Survey Example "Dashboard" Results

The Infrastructure Survey Tool is but one method for performing risk analysis on critical infrastructure. Over the years, each sector has developed its own set of risk analysis tools. The 2010 Sector Security Plan for Water identifies three assessment tools: 1) Risk Assessment Methodology-Water (RAM-W), 2) Security and Environmental Management System (SEMS); and 3) Vulnerability Self-Assessment Tool (VSAT). [10, p. 27] Similarly, the 2010 Transportation Systems Sector Specific Plan cites the use of the Aviation Modal Risk Assessment (AMRA) as part of a broader Transportation Systems Sector Security Risk Assessment (TSSRA) program. [11, pp. 135-136] The PSA Site Assistance Visit is listed as the method for conducting risk assessments in the 2010 Sector Specific Plan for Energy. [12, p. 32] Originally, DHS intended for every sector to use the same risk analysis tool in order to facilitate risk comparison across not only

infrastructure assets, but also across infrastructure sectors. In the 2006 National Infrastructure Protection Plan DHS announced it was sponsoring development of a suite of tools based on the Risk Analysis and Management for Critical Asset Protection (RAMCAP). [13, p. 36] RAMCAP was developed at the request of the White House by the American Society of Mechanical Engineers (ASME). [14, p. xiii] The 2006 NIPP deemed RAMCAP to satisfy the "baseline criteria for risk assessment". This "baseline criteria" assessed risk as a function of consequence, vulnerability, and threat, expressed as R=f(C,V,T). [13, pp. 35-36] The 2013 NIPP affirmed this formulation as part of Step 3 in the Risk Management Framework, [3, p. 17] but RAMCAP was no longer the preferred method. It was not mentioned in either the 2009 or 2013 National Infrastructure Protection Plans. It did survive, however, as the American Water Works Association (AWWA) J100-10 standard for Risk and Resilience Management of Water and Wastewater Systems. [14]

The Risk Management Framework has proven problematic at every step. DHS has yet to make the system work as envisioned. Until these problems are solved, the nation's critical infrastructure will remain vulnerable to malicious attack.

RMF Step 4: Implement Risk Management Activities. As a result of risk analysis, owners/operators are expected to take actions to increase resilience and reduce their vulnerability to potential consequences. [3, p. 18] However, infrastructure owner/operators are very sensitive to costs, in many instances regulated, and cannot afford to take all measures on their own. Accordingly, DHS may lend assistance through the FEMA Grants Program Directorate 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, and Buffer Zone Protection Plan. [1, pp. 27-28] Ostensibly, the results from risk analysis are included in a Critical Infrastructure National Annual Report [3, p. 26] submitted each year with the DHS budget to the Executive Office of the President. [15, p. 2]

RMF Step 5: Measure Effectiveness. The 1993 Government Performance and Results Act, as amended, requires all Federal programs to develop "outcome measures" and report them annually to Congress to guide and assess effective investment of taxpayer funds. [16] The Risk Management Framework incorporates this principle in Step 5, before starting all over again with Step 1 in an incremental, continuous improvement process. [3, p. 20]

Conclusion

While supporting aspects of the National Infrastructure Protection Plan including Information Sharing and Analysis Centers (ISACs) and Sector Coordinating Councils have increased awareness and security among participating infrastructure sectors, the core of the plan, the Risk Management Framework, has yet to live up to expectations. Various GAO reports detail fundamental problems with each step of the process including 1) inability to adequately identify infrastructure assets (mobile assets, such as aircraft, are not included in NCIPP criteria), 2) matching PSA Site Assistance Visits with priority assets listed on NCIPP, 3) deploying a standard formulation to uniformly assess risk across all infrastructure sectors, 4) applying risk results to determine Federal grant priorities, and 5) providing an objective risk measure to guide and assess taxpayer investments. While these problems remain, the nation will remain vulnerable to the potential catastrophic effects inherent in critical infrastructure as demonstrated on 9/11.

Challenge Your Understanding

The following questions are designed to challenge your understanding of the material presented in this chapter. Some questions may require additional research outside this book in order to provide a complete answer.

1. What is the scope and authority of a presidential executive order or directive?
2. What was the finding by the Commission on Critical Infrastructure Protection that prompted President Clinton to issue PDD-63?
3. How did HSPD-7 issued by President Bush change the emphasis on critical infrastructure protection from PDD-63?
4. How did PPD-21 issued by President Obama again change the emphasis on critical infrastructure protection from HSPD-7?
5. Why can't owners/operators protect their own infrastructure?
6. What is the purpose of the Risk Management Framework?
7. How does it affect the RMF if you can't correctly identify critical infrastructure?
8. How does it affect the RMF if you can't assess risk uniformly across different infrastructures?
9. As a member of Congress, what would be your priority in allocating funding to protect critical infrastructure?
10. What do you suppose might be a moral hazard of funding infrastructure protection programs?