Order Code RL32631

CRS Report for Congress
Received through the CRS Web

# Critical Infrastructure and Key Assets: Definition and Identification

**October 1, 2004**

John Moteff and Paul Parfomak
Resources, Science, and Industry Division

# Critical Infrastructure and Key Assets: Definition and Identification

## Summary

The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (NSPP) details a major part of the Bush administration's overall homeland security strategy. Implementing this Strategy requires clear definition of "critical infrastructures" and "key assets." Although the Strategy provides such definitions, the meaning of "critical infrastructure" in the public policy context has been evolving for decades and is still open to debate.

Twenty years ago, "infrastructure" was defined primarily with respect to the adequacy of the nation's public works. In the mid-1990's, however, the growing threat of international terrorism led policy makers to reconsider the definition of "infrastructure" in the context of homeland security. Successive federal government reports, laws and executive orders have refined, and generally expanded, the number of infrastructure sectors and the types of assets considered to be "critical" for purposes of homeland security. The USA PATRIOT Act of 2001(P.L. 107-56) contains the federal government's most recent definition of "critical infrastructure." The NSPP contains the most recent detailed list of critical infrastructures and assets of national importance. The list may continue to evolve, however, as economic changes or geopolitical developments influence homeland security policy.

There is some debate among policy makers about the implications of an ambiguous or changing list of critical infrastructures. Ambiguity about what constitutes a critical infrastructure (or key resource) could lead to inefficient use of limited homeland security resources. For example, private sector representatives state that they need clear and stable definitions of asset criticality so they will know exactly what assets to protect, and how well to protect them. Otherwise, they risk protecting too many facilities, protecting the wrong facilities, or both. On the other hand, arbitrarily limiting the number of critical infrastructures *a priori* due to resource constraints might miss a dangerous vulnerability. Clear "criticality" criteria will also be important if federal agencies intend to implement and enforce any potential future security regulations related to critical infrastructure.

This report will not be updated.

## Contents



## List of Tables

# Critical Infrastructure and Key Assets: Definition and Identification

## Introduction

The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* details a major part of the Bush administration's overall homeland security strategy.[1] Implementing this strategy requires government agencies and private sector partners to identify and prioritize assets most essential to the United States' economic and social well-being. A key implementation requirement, therefore, is clear definition of what the administration considers to be critical infrastructures and key assets. While the Strategy provides the administration's definitions, along with its rationale for including specific infrastructures on the critical list, the meaning of "critical infrastructure" in the public policy context has been evolving for decades and is still open to debate.

This report reviews the concept and definition of "critical infrastructure" as it has appeared in federal reports, legislation and regulation since the early 1980s. The report highlights the changes and expansion of that definition as the focus of public policy debates shifted from infrastructure adequacy to infrastructure protection. Finally the report summarizes current policy issues associated with critical infrastructure identification by federal agencies and the private sector. The report is intentionally limited to definitional issues and categorization of infrastructure. For a more general discussion of national policy regarding critical infrastructure protection, including its evolution, implementation, and continuing issues, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation.*

## Background

### What is "Infrastructure"?

The *American Heritage Dictionary,* defines the term "infrastructure" as

> The basic facilities, services, and installations needed for the functioning of a community or society, such as transportation and communications systems, water and power lines, and public institutions including schools, post offices, and prisons.[2]

---

[1] Office of the President. *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.* February, 2003.

[2] *The American Heritage Dictionary of the English Language,* Fourth Edition. Houghton (continued...)

This definition, however, and others like it, are broad and subject to interpretation. As a practical matter, what is considered to be infrastructure depends heavily upon the context in which the term is used.

In U.S. public policy, the definition of "infrastructure" has been evolutionary and often ambiguous. Twenty years ago, "infrastructure" was defined primarily in debates about the adequacy of the nation's public works—which were viewed by many as deteriorating, obsolete, and of insufficient capacity. A typical report of the time, issued by the Council of State Planning Agencies, defined "infrastructure" as "a wide array of public facilities and equipment required to provide social services and support private sector economic activity." According to the report, infrastructure included roads, bridges, water and sewer systems, airports, ports, and public buildings, and might also include schools, health facilities, jails, recreation facilities, electric power production, fire safety, waste disposal, and communications services.[3]

In a 1983 report, the Congressional Budget Office (CBO) defined "infrastructure" as facilities with "the common characteristics of capital intensiveness and high public investment at all levels of government. They are, moreover, directly critical to activity in the nation's economy." The CBO included highways, public transit systems, wastewater treatment works, water resources, air traffic control, airports, and municipal water supply in this category. The CBO also noted that the concept of infrastructure could be "applied broadly to include such social facilities as schools, hospitals, and prisons, and it often includes industrial capacity, as well."[4] In a subsequent report, however, CBO narrowed this definition of "infrastructure" to exclude

> some facilities often thought of as infrastructure–such as public housing, government buildings, private rail service, and schools–and some environmental facilities (such as hazardous or toxic waste sites) where the initial onus of responsibility is on private individuals.[5]

Congress, itself, has often enacted legislation defining or affecting one or more infrastructure sectors, but has rarely done so comprehensively. In 1984, Congress did enact a bill that established the National Council on Public Works Improvement with a mandate to report on the state of public works infrastructure systems (P.L. 98-501). Analysis required by that act was to include "any physical asset that is capable of being used to produce services or other benefits for a number of years" and was to include but not be limited to "roadways or bridges; airports or airway facilities; mass transportation systems; wastewater treatment or related facilities; water resources

---

[2] (...continued)
Mifflin Company. Boston, MA. 2000. (Definition 2).

[3] Vaughan, R. and Pollard, R. *Rebuilding America, Vol. I, Planning and Managing Public Works in the 1980s*. Council of State Planning Agencies. Washington, DC. 1984. pp 1-2.

[4] U.S. Congressional Budget Office. *Public Works Infrastructure: Policy Considerations for the 1980s*. April 1983. p 1.

[5] U.S. Congressional Budget Office. *New Directions for the Nation's Public Works*. September 1988. pp xi-xii.

projects; hospitals; resource recovery facilities; public buildings; space or communication facilities; railroads; and federally assisted housing."[6]

The Council established by P.L. 98-501 provided yet another definition of "infrastructure." The Council's report characterized "infrastructure" as facilities with high fixed costs, long economic lives, strong links to economic development, and a tradition of public sector involvement. Taken as a whole, according to the Council, the services that they provide "form the underpinnings of the nation's defense, a strong economy, and our health and safety." Under this definition of "infrastructure," the Council included highways, streets, roads, and bridges; airports and airways; public transit; intermodal transportation (the interface between modes); water supply; wastewater treatment; water resources; solid waste; and hazardous waste services. [7]

The Council's report was one of the last significant federal initiatives during the 1980s to consider the definition of "infrastructure." By the early 1990s, policy makers' attention had largely moved away from infrastructure issues broadly. Instead, legislative proposals tended to address the needs of individual infrastructure sectors.

## "Critical" Infrastructure and "Key Resources"

The growing threat of international terrorism in the mid-1990s renewed federal government interest in infrastructure issues. Unlike the previous period, which was focused on infrastructure adequacy, federal agencies in the 1990s were increasingly concerned about infrastructure protection. This concern, in turn, led policy makers to reconsider the definition of "infrastructure" in a security context.

On July 15, 1996, President Clinton signed Executive Order 13010 establishing the President's Commission on Critical Infrastructure Protection (PCCIP).[8] This Executive Order (E.O.) defined "infrastructure" as

> The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole.

This definition of "infrastructure" is consistent with the broad definitions from the 1980's. E.O. 13010 went further, however, by prioritizing particular infrastructure sectors, and specific assets within those sectors, on the basis of national importance.

---

[6] P.L. 98-501, sec. 203.

[7] National Council on Public Works Improvement. *Fragile Foundations: A Report on America's Public Works, Final Report to the President and Congress*. Washington D.C. February 1988: 33.

[8] Executive Order 13010—*Critical Infrastructure Protection*. Federal Register, July 17, 1996. Vol. 61, No. 138. pp 37347-37350. Reference is on page 37347.

E.O.13010 stated that "certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[9] The Commission's final report to the President echoed the E.O.'s definition of vital infrastructure.[10]

The general concept of "vital" or "critical" infrastructure in E.O. 13010 was not entirely new, having appeared in some form in many of the policy debates in the 1980s. The Order did break new ground, however, in listing what it considered to be critical infrastructures. According to E.O. 13010, these critical infrastructures were:

- telecommunications;
- electrical power systems;
- gas and oil storage and transportation;
- banking and finance;
- transportation;
- water supply systems;
- emergency services (including medical, police, fire, and rescue); and,
- continuity of government.

The list of critical infrastructure sectors in E.O. 13010 was much broader than that reported by the National Council on Public Works Improvement. In addition to transportation, water systems, and public services—sectors with "a tradition of public sector involvement"—E.O. 13010 included infrastructures predominantly owned by private companies: telecommunications, energy, and financial services.

**Presidential Decision Directive 63.** In response to the President's Commission on Critical Infrastructure Protection final report, President Clinton signed Presidential Decision Directive 63 (PDD-63) on May 22, 1998.[11] The Directive's goal was to establish a national capability within five years to protect "critical" infrastructure from intentional disruption. According to PDD-63, "critical" infrastructures were "those physical and cyber-based systems essential to the minimum operations of the economy and government." This definition expanded little on that in E.O. 13010, but was noteworthy for its specific mention of "cyber" infrastructure.[12]

---

[9] Executive Order 13010. p 37347.

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

[11] *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive No. 63*, White Paper, May 22, 1998.

[12] The distinction between physical security and cyber-security is almost inextricable and not clearly articulated. For example, physical assets in electric power include the generation plant, transformers, and power lines. The computer hardware and communication links that control the generation and flow of electricity could be considered physical or cyber assets. Data transmitted and stored on the computers and transmitted over the communication lines and the software used to process that data are considered cyber assets. Physical security

(continued...)

To help achieve its goal, PDD-63 directed certain federal agencies to lead the government's security efforts and identify private sector liaisons in specific critical infrastructure sectors. These lead agencies and associated critical infrastructures are summarized in **Table 1.**

**Table 1: Critical Infrastructures and Lead Agencies Under PDD-63**

| **Lead Agency** | **Critical Infrastructure** |
|---|---|
| Dept. of Commerce | Information and communications |
| Dept. of the Treasury | Banking and finance |
| Environmental Protection Agency | Water supply |
| Dept. of Transportation | Aviation<br>Highways (including trucking)<br>Mass transit<br>Pipelines<br>Rail<br>Waterborne commerce |
| Dept. of Justice/FBI | Emergency law enforcement services |
| Federal Emergency Management. Agency | Emergency fire service<br>Continuity of government services |
| Dept. of Health and Human Services | Public health services, including prevention, surveillance, laboratory services, and personal health services |
| Dept. of Energy | Electric power<br>Oil and gas production and storage |

Source: PDD-63

PDD-63 also identified certain "special functions" related to critical infrastructure protection to be chiefly performed by federal agencies: national defense, foreign affairs, intelligence, law enforcement.

The first version of a National Plan for Critical Infrastructure (also called for by PDD-63)[13] defined "critical infrastructures" as "those systems and assets—both physical and cyber—so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, and/or

---

[12] (...continued)
typically means protecting assets (including computers) from damage caused by physical forces such as explosion, impact, and fire. Cyber-security typically means protecting both physical and cyber assets from operational failure or manipulation due to unauthorized access to operating software or data. Securing critical infrastructures may require a broad combination of both physical and cyber measures (from installing fences to installing firewall software).

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

national public health and safety."[14] While the Plan concentrated on cyber-security of the federal government's critical infrastructure, the Plan refers to those infrastructures mentioned in the Directive.

**Executive Order 13228.** Following the terror attacks of September 11, 2001, President Bush signed new Executive Orders relating to critical infrastructure protection. Executive Order 13228,[15] signed October 8, 2001, established the Office of Homeland Security and the Homeland Security Council. Among the duties assigned the Office was to coordinate efforts to protect:

- energy production, transmission, and distribution services and critical facilities
- other utilities
- telecommunications
- facilities that produce, use, store, or dispose of nuclear material
- public and privately owned information systems
- special events of national significance
- transportation, including railways, highways, shipping ports and waterways
- airports and civilian aircraft
- livestock, agriculture, and systems for the provision of water and food for human use and consumption.[16]

The list in E.O. 13228 is noteworthy for its specific inclusion of nuclear sites, special events, and agriculture, which were not among the sectors identified in PDD-63.

In a separate Executive Order 13231,[17] signed October 16, 2001, President Bush established the President's Critical Infrastructure Protection Board. Although the name of the Board implied a broad mandate, its duties focused primarily on information infrastructure. However, the E.O. made reference to the importance of information systems to other critical infrastructures such as "telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services."[18]

**The USA PATRIOT and Homeland Security Acts.** In response to the terror attacks of September 11, 2001, Congress passed the USA PATRIOT Act of 2001(P.L. 107-56). The PATRIOT Act was intended to "deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes." In its findings, P.L. 107-56 states that

---

[14] Ibid. Executive Summary. p 1. Section 1016 of the USA PATRIOT Act (P.L.107-56), passed October 16, 2001, used essentially the same definition.

[15] Executive Order *13228—Establishing the Office of Homeland Security and the Homeland Security Council*. Federal Register, Vol. 66, No. 196, October 8, 2001. pp51812- 51817.

[16] E.O. 13228. Section 3 (e) (i), (ii), (iv), (v) and (vi), pp. 51813-51814.

[17] Executive Order *13231—Critical Infrastructure Protection in the Information Age*. Federal Register, Vol. 86, No. 202. October 18, 2001. pp. 53063-53071.

[18] E.O. 13231. Section 1 (a), p. 53063.

> Private business, government, and the national security apparatus increasingly depend on an interdependent network of critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors (Sec. 1016(b)(2)).

The act goes on to define "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 (Sec. 1016(e)).

This definition was adopted, by reference, in the Homeland Security Act of 2002 (P.L. 107-296 , Sec. 2(4)) establishing the Department of Homeland Security (DHS).

The Homeland Security Act also formally introduces the concept of "key resources," defined as "publicly or privately controlled resources essential to the minimal operations of the economy and government" (Sec. 2(9)). Without articulating exactly what they are, the act views key resources as distinct from critical infrastructure, albeit worthy of the same protection (Sec. 2(15)(A)).

**National Strategy for Homeland Security.** The President's *National Strategy for Homeland Security* (NSHS), issued in July 2002, restates the definition of critical infrastructure provided in the PATRIOT Act. The Strategy expands on this definition, however, summarizing its rationale for classifying specific infrastructure sectors as critical.

> Our critical infrastructures are particularly important because of the functions or services they provide to our country. Our critical infrastructures are also particularly important because they are complex systems: the effects of a terrorist attack can spread far beyond the direct target, and reverberate long after the immediate damage.
>
> America's critical infrastructure encompasses a large number of sectors. Our agriculture, food, and water sectors, along with the public health and emergency services sectors, provide the essential goods and services Americans need to survive. Our institutions of government guarantee our national security and freedom, and administer key public functions. Our defense industrial base provides essential capabilities to help safeguard our population from external threats. Our information and telecommunications sector enables economic productivity and growth, and is particularly important because it connects and helps control many other infrastructure sectors. Our energy, transportation, banking and finance, chemical industry, and postal and shipping sectors help sustain our economy and touch the lives of Americans everyday.[19]

---

[19] U.S. Office of Homeland Security. *The National Strategy for Homeland Security*. July 16, 2002. p 30.

The National Strategy listed the following critical infrastructure sectors:

- Agriculture
- Food
- Water
- Public Health
- Emergency Services
- Government
- Defense Industrial Base
- Information and Telecommunications
- Energy
- Transportation
- Banking and Finance
- Chemical Industry
- Postal and Shipping[20]

This list of critical infrastructures encompasses those of E.O. 13228, but adds chemicals, and postal and shipping services due to their economic importance. While there may be some debate, in particular, about why the chemical industry was not on earlier lists that considered military and economic security, it seems to have been added also because individual chemical plants could be sources of materials that could be used for a weapon of mass destruction, or whose operations could be disrupted in a way that would significantly threaten the safety of surrounding communities. While not identifying it as such in this list, the National Strategy also discusses "cyber infrastructure" as closely connected to, but distinct from, physical infrastructure. The Strategy states that DHS "will place an especially high priority on protecting our cyber infrastructure."[21]

In addition to identifying critical infrastructure, the Strategy also introduces the concept of "key assets" as a subset of nationally important key resources. The Strategy defines "key assets" as

> individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage our Nation's morale or confidence. Key assets include symbols or historical attractions, such as prominent national, state, or local monuments and icons. In some cases, these include quasi-public symbols that are identified strongly with the United States as a Nation.... Key assets also include individual or localized facilities that deserve special protection because of their destructive potential or their value to the local community.[22]

The Strategy also mentions "high profile events ... strongly coupled to our national symbols or national morale" as worthy of special federal protection.

---

[20] U.S. Office of Homeland Security. July 16, 2002. p 30.

[21] U.S. Office of Homeland Security. July 16, 2002. p 31.

[22] U.S. Office of Homeland Security. July 16, 2002. p 31.

**National Strategy for Physical Infrastructure Protection.** The Bush Administration's *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (NSPP), released in February, 2003, reaffirms the critical infrastructure sectors identified in the *National Strategy for Homeland Security*. The 2003 Strategy also defines three categories of what it considers to be "key assets."

> One category of key assets comprises the diverse array of national monuments, symbols, and icons that represent our Nation's heritage, traditions and values, and political power. They include a wide variety of sites and structures, such as prominent historical attractions, monuments, cultural icons, and centers of government and commerce.... Another category of key assets includes facilities and structures that represent our national economic power and technological advancement. Many of them house significant amounts of hazardous materials, fuels, and chemical catalysts that enable important production and processing functions.... A third category of key assets includes such structures as prominent commercial centers, office buildings, and sports stadiums, where large numbers of people regularly congregate to conduct business or personal transactions, shop, or enjoy a recreational pastime.[23]

The Strategy specifically identifies nuclear power plants and dams as key assets.

**Homeland Security Presidential Directive 7.** On December 17, 2003, President Bush issued Homeland Security Presidential Directive 7 (HSPD-7) clarifying executive agency responsibilities for identifying, prioritizing and protecting critical infrastructure. The Directive requires that DHS and other federal agencies collaborate with "appropriate private sector entities" in sharing information and protecting critical infrastructure (Par. 25). HSPD-7 supercedes PDD-63 (Par. 37).

HSPD-7 adopts, by reference, the definitions of "critical infrastructure" and "key resources" in the Homeland Security Act (Sec.6). It also adopts the critical infrastructure and key asset categories in the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. HSPD-7 does revise the list of lead federal agencies and associated critical infrastructures included in PDD-63 to reflect the role of the Department of Homeland Security as an independent cabinet department, as shown in **Table 2**.

Although HSPD-7 specifies a list of infrastructures, it leaves open the possibility that the list could be expanded. According to the Directive, DHS "shall ... evaluate the need for and coordinate the coverage of additional critical infrastructure and key resources categories over time, as appropriate" (Sec. 15). Nonetheless, the list of critical infrastructures in **Table 2** appears to be the most recent and still in force.

---

[23] Office of the President. *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.* February, 2003. p 71.

**Table 2: Critical Infrastructures and Lead Agencies Under HSPD-7**

| Lead Agency | Critical Infrastructure |
|---|---|
| Dept. of Homeland Security | Information technology<br>Telecommunications<br>Chemicals<br>Transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems<br>Emergency services<br>Postal and shipping services |
| Dept. of Agriculture | Agriculture, food (meat, poultry, egg products) |
| Dept. of Health and Human Services | Public health, healthcare, and food (other than meat, poultry, egg products) |
| EPA | Drinking water and waste water treatment systems |
| Dept. of Energy | Energy, including the production refining, storage, and distribution of oil and gas, and electric power (except for commercial nuclear power facilities[24]) |
| Dept. of the Treasury | Banking and finance |
| Dept. of the Interior | National monuments and icons |
| Dept. of Defense | Defense industrial base |

Source: HSPD-7

## Differentiating Critical and Non-Critical "Assets"

Identifying and prioritizing which assets of an infrastructure are most essential to its function, or pose the most significant danger to life and property if threatened or damaged, is necessary for developing an effective protection strategy. But the scope and complexity of critical infrastructure sectors can make it a daunting task to identify which specific *assets* are critical. For example, a recent report by the National Research Council (NRC) characterizes the extent of the U.S. domestic transportation system, one of the critical infrastructures, as follows:

> The U.S. highway system consists of 4 million interconnected miles of paved roadways, including 45,000 miles of interstate freeway and 600,000 bridges. The freight rail networks extend for more than 300,000 miles and commuter and urban rail system's cover some 10,000 miles. Even the more contained civil aviation system has some 500 commercial-service airports and another 14,000 smaller general aviation airports scattered across the country. These networks

[24] The security of nuclear power plants and nuclear materials, including nuclear materials used in medical, industrial, and academic work, and the transportation of those materials is primarily the responsibility of the Nuclear Regulatory Commission. HSPD-7 requires the Department of Homeland Security, the Department of Energy and the Commission to work to together to ensure the security of these key assets and materials.

> also contain many other fixed facilities such as terminals, navigation aids, switch yards, locks, maintenance bases and operation control centers.[25]

Left out of this description of the transportation system is a large maritime network of inland waterways, ports, and vessels.

As the definitions of "critical infrastructure" and "key resources" have evolved in U.S. homeland security policy, responsible agencies have been seeking greater refinement and prioritization within these categories. In 1999, for example, the Critical Infrastructure Assurance Office (CIAO), which was established to support President Clinton's National Infrastructure Protection Plan, determined that many federal agencies responsible for critical infrastructure protection lacked a clear understanding of what constituted a "critical asset" within an infrastructure. As a result, the CIAO instituted a new program by which an agency could identify and assess its critical assets, identify the dependencies of those assets on other systems, including those beyond the direct control of the agency, and prioritize. The Homeland Security Act implies some type of critical asset differentiation as well by requiring DHS to "identify priorities for protective and support measures" within the nation's critical infrastructure sectors (Sec. 201(d)(3)).

President Bush's *National Strategy for Homeland Security* explicitly adopts critical asset differentiation. The Strategy states:

> The assets, functions, and systems within each critical infrastructure sector are not equally important. The transportation sector is vital, but not every bridge is critical to the Nation as a whole.[26]

The Strategy formally introduces the concept of "critical assets" as a way for the federal government to "focus its efforts on the highest priorities" in critical infrastructure protection.[27]

The Bush Administration's *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* reaffirms the requirement to prioritize critical assets. The Strategy calls for what amounts to a prioritized master list.

> To frame the initial focus of our national protection effort, we must acknowledge that the assets, systems, and functions that comprise our infrastructure sectors are not uniformly "critical" in nature, particularly in a national or major regional context... We must develop a comprehensive, prioritized assessment of facilities, systems, and functions of national-level criticality and monitor their preparedness across infrastructure sectors.[28]

---

[25] National Research Council. Transportation Research Board. TRB Special Report 270. *Deterrence, Protection, and Preparation--The New Transportation Security Imperative.* July 2, 2002. Available in preprint form at [http://www.trb.org/]

[26] U.S. Office of Homeland Security. July 16, 2002. p 31.

[27] U.S. Office of Homeland Security. July 16, 2002. p 31.

[28] Office of the President. February, 2003. p 2.

While the Strategy calls for objective assessment of critical assets it acknowledges that the "criticality"of individual assets is potentially fluid. The Strategy states that, "as we act to secure our most critical infrastructures and assets, we must remain cognizant that criticality varies as a function of time, risk, and market changes."[29]

The requirements of HSPD-7 continue the policy of critical asset prioritization and protection in the Strategy. It is interesting to note, however, that HSPD-7 requires DHS to do so "with an emphasis on critical infrastructure and key resources that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction." This emphasis on health and safety appears to imply yet another basis for prioritizing infrastructure protection.

## Challenges Identifying Critical Assets

Private companies and federal agencies have shared responsibility for identifying critical assets since PDD-63 was issued in 1998. That Directive required each lead federal agency to work with "private sector entities" in their respective infrastructures to "contribute to a sectoral National Infrastructure Assurance Plan by ... assessing the vulnerabilities of the sector to cyber or physical attacks," among other tasks (Sec. IV). According to PDD-63 "these assessments shall ... include the determination of the minimum essential infrastructure in each sector" (Sec. VIII.1). The responsibility of the private sector to work with federal agencies in developing and maintaining lists of "minimum essential infrastructure," or critical assets, continues to be an essential part of the government's infrastructure protection strategy.

Individual critical infrastructure sectors have implemented independent and often varying approaches for identifying their own critical assets. For example, the June 2001 security guidance issued by the National Petroleum Council (NPC) for oil and natural gas infrastructure stated the following:

> The first step in the risk management process is to identify and put a value on each of the key assets of the organization. These key assets can be people, facilities, services, processes, programs, etc. Next, the "impact of loss" for each of these assets is estimated. This is a measure of the loss to the company if the asset is damaged or destroyed. A simple rating system based on user-defined criteria can be used to measure the value of the asset (e.g., very low, low, moderate, high, extremely high) and the impact of its loss. In a more complex risk management system, the value of an asset and impact of loss can be calculated in monetary units. These values may be based on such parameters as the original cost to create the asset, the cost to obtain a temporary replacement for the asset, the permanent replacement cost for the asset, costs associated with the loss of revenue, an assigned cost for the loss of human life or degradation of environmental resources, costs to public/stakeholder relations, legal and liability costs, and the costs of increased regulatory oversight.[30]

---

[29] Office of the President. February, 2003. p 3.

[30] National Petroleum Council. *Securing Oil and Natural Gas Infrastructures in the New* (continued...)

While it acknowledged the need to identify critical assets, the NPC's guidance left it up to individual companies to determine the specific basis for "criticality" in their security assessments. It is important to note that the NPC initially defined a "key asset" with respect to a potential "loss to the company" rather than broader economic or social welfare impacts as called for in federal critical infrastructure strategies. This emphasis illustrates the practical challenge of relying on private companies to identify critical assets in the context of national infrastructure security.

In an effort to establish and implement a more consistent standard for what constitutes a critical asset, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* requires DHS to "develop a uniform methodology for identifying facilities, systems, and functions with national-level criticality ... [and] build a comprehensive database to catalog these critical facilities, systems, and functions."[31] Under Section 201 of the Homeland Security Act (P.L. 107-296), responsibility for this critical asset catalog lies with the DHS's Information Analysis and Infrastructure Protection Directorate (IAIP).

Developing a uniform methodology for identifying critical assets, and compiling a critical asset list for the United States as whole, has been difficult for IAIP. In April 2004, IAIP reported that it had compiled a list of 1,700 critical assets, but confusion among private sector and state government partners about what constituted a critical asset cast doubt on the validity and completeness of that list.[32] For example, among electric utilities, there was some question as to why certain assets were considered critical by IAIP, since some of those assets were not in use and others did not support significant electric loads.[33] Similar inconsistencies emerged when IAIP's list was compared to critical asset lists developed by state agencies. As the Assistant Secretary for Infrastructure Protection in DHS testified before Congress "what we have done to identify critical assets in the United States and what the states and local municipalities and cities have done often do not reconcile."[34] According to press accounts, subsequent classified briefings with Members of Congress to review lists of critical assets in their states have continued to raise concerns about IAIP's critical asset identification.[35]

---

[30] (...continued)
*Economy*. Washington, DC. June 2001. p 41.

[31] Office of the President. February, 2003. p 23.

[32] These 1,700 assets, considered to be "nationally" critical by IAIP, were derived from a database of 33,000 assets considered regionally or locally critical, as compiled from submissions by state agencies and other infrastructure security partners.

[33] Personal communication with industry official, September 29, 2003.

[34] Liscouski, Robert, Asst. Sec., Infrastructure Protection, Dept. of Homeland Security, Testimony before the House Select Committee on Homeland Security; Infrastructure and Border Security Subcommittee. April 21, 2004.

[35] Starks, T., and Andersen, M.E. "Congress, Industry Both in Dismay Over Homeland Security's Performance on Critical Infrastructure." *CQ Homeland Security*. July 29, 2004.

## Critical Infrastructure in the 9/11 Commission Report

The National Commission on Terrorist Attacks Upon the United States (known as the 9/11 Commission) made its final report public on July 22, 2004. Among other things, the Commission was chartered to report on the United States' preparedness for, and response to, the terror attacks of September 11, 2001. Many of the recommendations made in the 9/11 Commission's report deal indirectly with critical infrastructure protection, especially as the goals of critical infrastructure protection have evolved to include countering the type of attack that occurred on September 11. However, the Commission's report does not specifically address the definition or identification of critical infrastructure, although the report does call for using a systematic risk management approach to set priorities and allocate resources for critical infrastructure protection. Although the Commission discussed in more detail issues related to transportation security, none of its recommendations advocate a change in the direction of, or the organizational structures that have evolved to implement, existing infrastructure protection policies. Nevertheless, the Commission's recommendations could speed up implementation in some areas, given the attention and renewed urgency expressed by the Commission.[36]

# Policy Issues

The U.S. government's definition of "critical infrastructure" has evolved over the years, and at any given time has left considerable room for interpretation. Furthermore, since the 1980's, the number of sectors included under that definition has generally expanded from the most basic public works to a much broader set of economic, defense, government, social and institutional facilities, as illustrated in **Table 3.** The list may continue to evolve and grow as economic changes or geopolitical developments influence homeland security policy.

Should Congress care if the overall list of critical infrastructures remains fluid? One concern is that an unclear or unstable understanding of what constitutes a critical infrastructure (or key resource) could lead to inefficient security policies. At the very least, a growing list of infrastructures in need of protection implies growing attention from the federal government and, implicitly, a need for more resources devoted to protect them. Under the Homeland Security Act and other legislation, the federal government is required to interact with each critical infrastructure, to support and maintain a database of vulnerabilities, to integrate the database with threat analyses, to monitor incidents on each of the infrastructures, and to issue warnings as appropriate. These activities call for time and resources. The federal government also may choose to assist financially in effecting necessary protective measures, not only for infrastructure owned and operated at the state or local level, but also for privately owned and operated infrastructures. Allocating limited public resources across an excessively broad range of infrastructures may be an inefficient use of resources. However, arbitrarily limiting the number of critical infrastructures *a priori* due to resource constraints might miss dangerous vulnerabilities.

---

[36] For additional discussion, see CRS Report RL3253, *Critical Infrastructure Protections: The 9/11 Commission Report*, by John Moteff..

## Table 3. Critical Infrastructure and Key Assets Over Time

| Infrastructure | U.S. Government Reports and Executive Orders | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **CBO (1983)** | **NCPWI (1988)** | **E.O. 13010 (1996)** | **PDD-63 (1998)** | **E.O. 13228 (2001)** | **NSHS (2002)** | **NSPP (2003)** | **HSPD-7 (2003)** |
| Transportation | X | X | X | X | X | X | X | X |
| Water supply /waste water treatment | X | X | X | X | X | X | X | X |
| Education | X | | | | | | | |
| Public health | X | | | X | | X | X | X |
| Prisons | X | | | | | | | |
| Industrial capacity | X | | | | | | | |
| Waste services | | X | | | | | | |
| Telecommunications | | | X | X | X | X | X | X |
| Energy | | | X | X | X | X | X | X |
| Banking and finance | | | X | X | | X | X | X |
| Emergency services | | | X | X | | X | X | X |
| Government continuity | | | X | X | | X | X | |
| Information systems | | | | X | X | X | X | X |
| Nuclear facilities | | | | | X | | | |
| Special events | | | | | X | | | |
| Agriculture/food supply | | | | | X | X | X | X |
| Defense industrial base | | | | | | X | X | X |
| Chemical industry | | | | | | X | X | X |
| Postal / shipping services | | | | | | X | X | X |
| Monuments and icons | | | | | | | X | X |
| Key industry / tech. sites | | | | | | | X | |
| Large gathering sites | | | | | | | X | |

Source: CRS compilation. See earlier footnotes. Note that the cross-referencing marks, "X", in Table 3 are meant to be illustrative, and generally correspond to the specific mention of infrastructure sectors in the cited reports.

Unclear or shifting criteria for identifying individual critical assets and key assets may also lead to protection inefficiencies, especially where private companies are responsible for security spending. These criteria may become particularly important if federal agencies intend to implement and enforce any potential future security regulations related to critical infrastructure. Various private sector representatives state that they need clear and stable definitions of asset criticality so they will know exactly what assets to protect, and how well to protect them. Otherwise, they risk protecting too many facilities, protecting the wrong facilities, or both. Either outcome would increase ultimate costs passed through to consumers without commensurate security benefits, and could potentially divert scarce private resources from better uses, such as public safety or environmental protection.

As oversight of the federal role in infrastructure security continues, questions may be raised concerning the ongoing efforts of DHS to define and priortize critical and key assets. In addition to this specific issue, however, Congress may wish to assess how critical infrastructure identification fits in the nation's overall strategy to protect critical infrastructure. For example, if asset criticality is not clearly defined, increasing resources for infrastructure security inspections by DHS officials could be of limited value. Likewise, diverting infrastructure resources away from safety to enhance security might further reduce terror risk, but not overall public risk, if safety programs become less effective as a result. U.S. infrastructure security necessarily involves many groups: federal agencies, industry associations, large and small asset operators, and critical and non-critical asset owners. Reviewing how these groups work together to achieve common security goals is an oversight challenge for Congress.