Order Code RL31556

Report for Congress
Received through the CRS Web

Critical Infrastructures: What Makes an Infrastructure Critical?

August 30, 2002

John Moteff, Claudia Copeland, and John Fischer
Resources, Science, and Industry Division

Critical Infrastructures: What Makes an Infrastructure Critical?

Summary

The Bush Administration's proposal for establishing a Department of Homeland Security includes a function whose responsibilities include the coordination of policies and actions to protect the nation's critical infrastructure. However, the proposal did not specify criteria for how to determine criticality or which infrastructures should be considered critical.

Over the last few years, a number of documents concerned with critical infrastructure protection have offered general definitions for critical infrastructures and have provided short lists of which infrastructures should be included. None of these lists or definitions would be considered definitive. The criteria for determining what might be a critical infrastructure, and which infrastructures thus qualify, have expanded over time. Critical infrastructures were originally considered to be those whose prolonged disruptions could cause significant military and economic dislocation. Critical infrastructures now include national monuments (e.g. Washington Monument), where an attack might cause a large loss of life or adversely affect the nation's morale. They also include the chemical industry. While there may be some debate about why the chemical industry was not on earlier lists that considered only military and economic security, it seems to be included now primarily 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.

A fluid definition of what constitutes a critical infrastructure could complicate policymaking and actions. At the very least, a growing list of infrastructures in need of protection will require the federal government to prioritize its efforts. Essentially the federal government will have to try to minimize the impact on the nation's critical infrastructure of any future terrorist attack, taking into account what those impacts might be and the likelihood of their occurring.

There are number of ways the government can prioritize. First, not all elements of a critical infrastructure are critical. Additional study will be necessary to identify those elements that are the most critical. Other approaches include focusing on vulnerabilities that cut across more than one infrastructure, interdependencies where the attack on one infrastructure can have adverse effects on others, geographic locations where a number of critical infrastructure assets may be located, or focusing on those infrastructure belonging solely to the federal government or on which the federal government depends.

The National Strategy for Homeland Security, released by the Bush Administration in July 2002, states that the federal government will set priorities for critical infrastructure protection based on a consistent methodology and an approach that will allow it to balance the cost and expected benefits. It does not discuss what that methodology or approach might be. Congress may want to focus some of its oversight on how the Administration proposes to set priorities and what criteria it uses to do so.

Contents

List of Tables

Critical Infrastructures: What Makes an Infrastructure Critical?

Introduction

Section II of President Bush's June 2002 proposal for establishing a Department of Homeland Security prescribed the responsibilities of the Department's Undersecretary for Information Analysis and Infrastructure Protection. Those responsibilities included:

- comprehensively assessing the vulnerabilities of the key resources and critical infrastructures in the United States;
- ....identifying protective priorities and supporting protective measures...;
- developing a comprehensive national plan for securing the key resources and critical infrastructures in the United States; and
- taking or seeking to effect necessary measures to protect the key resources and critical infrastructures in the United States....[1]

Nowhere in the Administration's proposed legislation was critical infrastructure defined. However, other documents, including previous legislation, have defined critical infrastructure and provided illustrative lists of infrastructures that fall within those definitions. The following discussion recounts how the definition (and the list of illustrative examples) has broadened over time and what impact this may have on developing and implementing critical infrastructure protection policy.

Background

What Is a Critical Infrastructure?

Before "critical infrastructure" became a term of interest in the terrorism and homeland security debate, the seemingly similar term "infrastructure" was a subject debated by public policymakers. In the 1980s, for example, a much debated issue was whether there was a national crisis in the condition of America's infrastructure–its roads, bridges, dams, wastewater treatment systems, etc. With no standard or agreed definition, the concept of infrastructure in policy terms has been fluid, as it appears to be today. (For more discussion of these earlier definitions of and debate regarding "infrastructure," see the Appendix, *What is Infrastructure?* In this report.)

---

[1]For more information on various aspects of the President's proposal and the Congressional response, see *Homeland Security* on the CRS Home Page [http://www.crs.gov/] .

More recently, as homeland security as been assigned the highest national priority, the term "critical infrastructure" has developed into a major policy concern. Documents dealing with critical infrastructure protection have provided broad definitions of what makes an infrastructure critical.

Executive Order 13010,[2] signed by President Clinton on July 15, 1996, which established the President's Commission on Critical Infrastructure Protection, alluded to what makes an infrastructure critical:

> "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."[3]

According to this Executive Order (EO) these infrastructures included:

- telecommunications;[4]
- 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.

Using the language of this EO, the Commission's final report[5] to the President defined critical infrastructure in the Glossary as:

> "Infrastructures so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security."

The following supporting definitions were provided:

> *Infrastructures*: 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.

---

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

[3]Ibid. p. 37347.

[4]Throughout this report, sectors that are identified as being critical will be bolded the first time they appear.

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

Debilitated: A condition of defense or economic security characterized by ineffectualness.

Defense security: The confidence that Americans' lives and personal safety, both at home and abroad, are protected and the United States' sovereignty, political freedom, and independence, with its values, institutions, and territory intact are maintained.

Economic security: The confidence that the nation's goods and services can successfully compete in global markets while maintaining or boosting real incomes of its citizens.

The Commission's report also defined the infrastructures of each of the sectors mentioned in this EO.

Banking and Finance: Entities such as retail and commercial organizations, investment institutions, exchange boards, trading houses, and reserve systems, and associated operational organizations, government operations, and support activities that are involved in all manner of monetary transactions, including its storage for saving purposes, its investment for income purposes, its exchange for payment purposes, and its disbursement in the form of loans and other financial instruments.

Electric Power Systems: Generation stations, transmission and distribution networks that create and supply electricity to end-users so that end-users achieve and maintain nominal functionality, including the transportation and storage of fuel essential to that system.

Emergency Services: Medical, police, fire, and rescue systems and personnel that are called upon when an individual or community is responding to emergencies. These services are typically provided at the local level. In addition, state and federal response plans define emergency support functions to assist in the response and recovery.

Gas and Oil Production Storage and Transportation: The production and holding facilities for natural gas, crude and refined petroleum, and petroleum-derived fuels, the refining and processing facilities for these fuels and the pipelines, ships, trucks, and rail systems that transport these commodities from their source to systems that are dependent upon gas and oil in one of their useful forms.

Information and Communications: Computing and telecommunications equipment, software, processes, and people that support:

- the processing, storage, and transmission of data and information;
- the processes and people that convert data into information and information into knowledge; and,
- the data and information themselves.

> *Transportation*: Physical distribution systems critical to supporting the national security and economic well-being of this nation, including the national airspace systems, airlines, and aircraft, and airports; roads and highways, trucking and personal vehicles; ports and waterways and the vessels operating thereon; mass transit, both rail and bus; pipelines, including natural gas, petroleum, and other hazardous materials; freight and long haul passenger rail; and delivery services.
>
> *Water Supply System*: Sources of water, reservoirs, and holding facilities, aqueducts and other transport systems, the filtration, cleaning and treatment systems, the pipelines, the cooling systems and other delivery mechanisms that provide for domestic and industrial applications, including systems for dealing with water runoff, waste water, and firefighting.

In response to the Commission's report, President Clinton signed Presidential Decision Directive Number 63 (PDD-63) on May 22, 1998.[6] The Directive defined critical infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and government."[7] According to the Directive, these included, but were not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services.

The Directive also directed certain agencies to identify sector liaisons in those sectors mentioned above, plus:

- intelligent transportation systems;
- continuity of government services;
- public health services (including prevention, surveillance, laboratory services); and,
- personal health services.

---

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

[7]The distinction between physical-security and cyber-security is almost inextricable and not clearly articulated. For example, physical assets in the electric power infrastructure would typically include the generation plant, the turbines and other equipment inside, and distribution lines and towers. However, the computer hardware and communication lines that help control the generation and flow of electricity could be considered physical assets or cyber assets. The data transmitted and stored on the computers and transmitted over the communication lines and the software used to process and control that data are typically considered cyber assets. Physical security typically means protecting the physical assets (including computer equipment) from damage caused by physical forces such as explosion, breakage, wind, fire, etc. Cyber-security could also mean the physical protection of cyber assets. Cyber-security, however, typically includes the protection of both physical and cyber assets from operational failure or from being otherwise compromised by others gaining unauthorized computer access (including remote access) to the operating software or data. Providing physical- and cyber-security of critical infrastructures requires a broad range of effort that can be quite varied (from installing jersey walls to installing firewall software), and different people or policies may be talking about different activities.

It also identified critical infrastructures that are primarily the responsibility of the federal government:

- law enforcement and internal security;
- foreign intelligence;
- foreign affairs; and,
- national defense.

The Directive also set a goal that within five years the nation should be able to protect the national critical infrastructures from intentional attacks that would significantly diminish the abilities of:

- the federal government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and to deliver minimum essential public services; and,
- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services.

"Any disruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States."[8]

The first version of a National Plan for Critical Infrastructure (also called for by PDD-63)[9] 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 national public health and safety."[10] While the Plan concentrated on cyber-security of the federal government's critical infrastructure, the Plan refers to those infrastructures mentioned in the Directive.

Following the September 11, 2001 attacks, President Bush signed new Executive Orders relating to critical infrastructure protection. E.O. 13228,[11] 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 critical infrastructures..[and]...work with federal, state, and local agencies and private entities to:

---

[8]Ibid. p2.

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

[10]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.

[11]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.

> strengthen measures for protecting energy production, transmission, and distribution services and critical facilities; other utilities; telecommunications; **facilities that produce, use, store, or dispose of nuclear material...**;
>
> ...coordinate efforts to protect critical public and privately owned information systems...;
>
> ...to ensure that **special events** determined by appropriate senior officials to have national significance are protected...;
>
> ...to protect transportation systems within the United States, including railways, highways, shipping ports and waterways, and airports and civilian aircraft...;
>
> ...to protect United States **livestock**, **agriculture**, and systems for the provision of water and **food** for human use and consumption...."[12]

In a separate Executive Order 13231,[13] signed October 16, 2001, President Bush established the President's Critical Infrastructure Protection Board. Although the name of the Board might imply a broad mandate, the Board's duties focus primarily on the nation's information infrastructure. However, the EO makes 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."[14]

This EO also reiterates the goal established in PDD-63, although stated within the more limited context of protecting against attacks on the nation's information infrastructure, that "any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible."[15]

Shortly after the Administration issued these Executive Orders, Congress passed the USA PATRIOT Act (P.L. 107-56). Section 1016 of the Act, called the Critical Infrastructures Protection Act of 2001, defined critical infrastructures 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 and safety, or any combination of those matters."[16]

---

[12]Ibid. Section 3 (e) (i), (ii), (iv), (v) and (vi), pp. 5183-5184.

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

[14]Ibid. Section 1 (a), p. 53063.

[15]Ibid. Section 1 (b), p. 53063

[16]H.R. 3162-130 (P.L. 107-56), Section 1016(e). The two bills before Congress establishing a Department of Homeland Security (H.R. 5005 and S. 2452) both use this definition.

Earlier in Section 1016, the legislation mentioned the types of infrastructures Congress intended to include in this definition: information, telecommunications, energy, financial services, water, and transportation.

Although the draft legislation proposed by the President for establishing the Department of Homeland Security did not define critical infrastructure, a companion document[17] went into a little more detail. While not providing a formal definition, the text parenthetically described critical infrastructures as "those assets, systems, and functions vital to our national security, governance, public health and safety, economy, and national morale."[18]

The text also states that the Department would build and maintain a comprehensive assessment of our nation's infrastructure sectors:

- food;
- water;
- agriculture;
- health systems and emergency services;
- energy (electrical, nuclear, gas and oil, dams);
- transportation (air, road, rail, port, waterways);
- information and telecommunications;
- banking and finance;
- energy;
- chemical;
- defense industry;
- postal and shipping; and,
- national monuments and icons.[19]

On July 16, 2002 the Administration released its National Strategy on Homeland Security.[20] Early in the Strategy, critical infrastructure was defined as it was in the above document (i.e. including the mention of national morale).[21] In the separate section focusing on critical infrastructure, the Strategy referred to the definition in the USA PATRIOT Act.[22] The National Strategy mentioned a slightly different list of specific infrastructures, making a distinction between public health systems and emergency systems and dropping national monuments and icons. The latter were picked up in a distinction the Strategy makes between critical infrastructures and key assets. Key assets were defined as individual targets whose "destruction would not endanger vital systems, but could create local disaster or profoundly damage our nation's morale and confidence." Such assets would include historical attractions

---

[17]*The Department of Homeland Security*. June 2002. White House.

[18]Ibid. p15.

[19]Ibid. p15.

[20]Office of the President. Office of Homeland Security. *National Strategy for Homeland Security*. July 2002.

[21]Ibid. p.ix

[22]Ibid. p. 30.

(national, state, and local monuments and icons) and other localized facilities with destructive potential or of high value to a community such as schools, courthouses, and bridges. While these key assets may be more the responsibility of the state and locality to protect, the Strategy offered a federal commitment to help enable those authorities to protect their key assets.

Which Assets of a Critical Infrastructure Need Protection?

After identifying what may be considered a critical infrastructure, a protection strategy must identify which elements of the infrastructure are critical to its function or pose the most significant danger to life and property. Not all assets may be critical, and some may be more so than others. However, the size and complexity of these infrastructures can make identifying which assets of an infrastructure are critical a daunting task.

For example, a recent report by the National Research Council (NRC) characterizes the extent of the U.S. domestic transportation system 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 also contain many other fixed facilities such as terminals, navigation aids, switch yards, locks, maintenance bases and operation control centers.[23]

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

Similarly, the electric power infrastructure includes 92,000 electric generating units (including fossil fueled, nuclear, and hydroelectric units), 300,000 miles of transmission lines, and 150 control centers, regulating the flow of electricity. The nation's water infrastructure includes 75,000 dams and reservoirs, thousands of miles of pipes and aqueducts, 168,000 public drinking water facilities, and 16,000 publically owned waste water treatment facilities. The chemical industry includes thousands of chemical facilities that handle hazardous or toxic substances.[24]

Fortunately, a considerable amount of information that can be used to categorize infrastructure is already available at the federal level. For example, the Federal Highway Administration classifies highways by type and produces copious statistics about them. Some of this information could be quite useful in a discussion about

---

[23]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/

[24]For more information on these infrastructures, see CRS Terrorism Briefing Book, Prevention: Security Enhancements. [http://www.congress.gov/brbk/html/ebter1.shtml]

which parts of the transportation infrastructure are most critical. The National Highway System, which is a category of roads that includes the interstate highway system, constitutes only 4% of the nation's public road milage, but carries over 44% of all travel.[25] A similar situation exists in the aviation system. Of the 546 commercial airports that had airline service in April 2001, fully 70% of all airline passenger boardings occurred at just 31 airports.[26]

What follows are two brief discussions that consider how physical transportation assets and transportation systems might be thought of in the context of whether they are, or are not, critical. The discussion is relevant to the other infrastructures as well.

Surface Transportation: River Crossings

There are 10 bridge spans crossing the Potomac River within the Washington D.C. Beltway. The two Beltway bridges, Woodrow Wilson and American Legion, are both part of the interstate highway system as are the 14th Street Bridge (which has multiple spans) and the Theodore Roosevelt Bridge. Other highway bridges include Memorial Bridge, Key Bridge, and Chain Bridge. Less noticed, but also important components of the area's transportation infrastructure are the rail and Metrorail bridges that parallel the 14th Street Bridge. One additional crossing of the Potomac exists, the Metrorail tunnel between Foggy Bottom and Rosslyn stations.

In the context of homeland security, which of these crossings are critical? At first blush, most observers would probably identify the Woodrow Wilson Bridge as the area's most critical transportation structure. It is the busiest, and carries Interstate 95, the East Coast's busiest highway around Washington. But if the Wilson Bridge were lost to a terrorist attack for some period of time how badly would the local economy and interstate commerce suffer? The answer based on experience with major traffic accidents and other emergencies is that the short term situation would likely be chaotic. Over the longer term, traffic would adjust in some ways. Interstate commerce, for example, would go around the Beltway the other way or through the City. These routes are longer and increased congestion would make these routings costlier and less efficient. All of these additional costs would be added to the cost of travel in the region which affect a host of activities. Nonetheless, the loss of the use of a single bridge or more could likely be handled, albeit with difficulty.

A more difficult question arises if the bridge that is lost is either the Metrorail bridge or the rail bridge. The tunnel crossing does provide a backup of sorts for the Metrorail system, but by all public accounts the rail lines that run through the tunnels are already nearing capacity, at least at certain times of the day. The rail crossing handles most of Amtrak's east coast service, Virginia Rail Express, and a significant amount of freight traffic. The nearest north-south replacement for the 14th St. rail

---

[25]Federal Highway Administration. *Our Nations Highways: 2000.* [http://www.fhwa.dot.gov/ohim]. p.18.

[26]Transportation Research Board. *Aviation Gridlock: Phase II: Airport Capacity and Infrastructure.* Transportation Research E-Circular. [http://trb.org/trb/publications/circulars/ec032/ec032.pdf]. May 2001. p. 5.

crossing is over 40 miles to the west. This is obviously not a suitable replacement for rail passenger service destined for Washington. For freight this might be something less of an issue, but the loss of this rail corridor for any period of time would affect the shipment of a lot of commodities, only some of which could be carried by truck as an alternative. Thus, determination of what is "critical" depends a great deal on ones frame of reference.

Transportation Systems: Air Traffic Control (ATC)[27]

The air traffic control system is a different type of example of the problem of defining critical transportation infrastructure. The ATC system is a large, complex, and highly integrated system that is very reliant on technology. The ATC system has 40,921 operational facilities of all types, staffed by 36,349 employees. Most notable of the facilities from the public perspective are the 21 air route traffic control centers (ARTCC), 496 airport traffic control towers, 75 flight service stations, and 61 automated flight service stations. The ARTCC alone handled almost 7 million aircraft movements during just the months of January and February 2002. For safety reasons a great deal of redundancy is already built into the system.

In structure a highly integrated system like ATC probably has more in common with telecommunications critical infrastructure then with traditional transportation infrastructure. In purpose, however, it is much more of a command and control system for the nation's air system. Aircraft can certainly fly without ATC guidance, and many aircraft flying by visual flight rules (VFR) already do. But the airline system could not function in its present manner without ATC.

The ATC system is strategic and is closely linked with the military ATC system. Considerable cooperation exists between the Department of Defense (DOD) and the ATC. Considerable thought has also been given to how the ATC system would operate in time of war. Many of the plans developed in this process also have application for dealing with terrorism.

The question, however, can be raised about which specific ATC facilities are critical. The system, for example, can, and does, function with the loss of an ATRCC. Coverage, however, is greatly reduced in the affected area and air traffic usually slows dramatically. A long term loss of such a facility would probably engender even further disruption and could lead to major disruptions of commerce in the affected region. The loss of a radar or other flight tracking facility at a major airport, however, at a particular moment could, depending on the circumstances, be either inconsequential or catastrophic.

Observations

The most apparent strength of the U.S. transportation system in the face of a terrorist threat is its redundancy. Although the transportation system is frequently congested in urbanized areas there are usually alternative transportation routes or

---

[27]Information about the ATC in this section is from the Federal Aviation Administration. Administrator's Fact Book. May 2002. available at http://www.ama500.jccbi.gov/factbook/

facilities that come into play. There are a few instances where this is not the case and these are probably the real "critical" pieces of transportation infrastructure. The same is true in the other infrastructures.

Analysis

None of the definitions of what constitutes a critical infrastructure, given over the years, could be considered rigorous. They bound the issue somewhat, but leave plenty of room for interpreting which infrastructures fit the definition. The specific sectors that have been listed, too, are illustrative, i.e. they have been included as examples, but do not form an exhaustive list. Furthermore, as time goes on, the general definition of what constitutes a critical infrastructure has expanded from those vital to the nation's defense and economic security and continuity of government (EO13010), to include those vital to public health and safety (National Plan, Version 1.0), and then again to include those vital to national morale (Department of Homeland Security supporting document). In concert, the list of infrastructures to be protected has expanded from those that are primarily necessary to the function of national defense and the economy (e.g. transportation, energy, banking and finance), to specific assets that could be used to cause massive destruction and/or death (e.g. the production, transport, and storage of nuclear materials, certain biological agents, and hazardous or toxic chemicals), but which may or may not be critical elements in the nation's defense or economy. The list continues to expand to include those assets important to individual communities and national monuments or icons (National Strategy for Homeland Security). Without a more rigorous process for identifying critical infrastructure, the list may keep changing, or growing, or there may exist multiple lists.

Should Congress care if the list of infrastructures remains fluid? One possible issue is that a vague understanding of what constitutes a critical infrastructure could lead to vague and diffuse policies and actions. At the very least, a growing list of infrastructures in need of protection implies a growing commitment on the part of the federal government. The legislation being debated and the National Strategy both commit the federal government to interact with each critical infrastructure, to support and maintain a database on vulnerabilities, to integrate the data base with threat analyses, to monitor incidents on each of the infrastructures, and to release warnings as appropriate. Just this will require time and resources. While the cost of adding additional infrastructures to the list may be marginal, it will not be zero. The federal government may also be asked to assist financially in affecting necessary protective measures, not only for infrastructure owned and operated at the state or local level, but also for privately owned and operated infrastructures.[28] It is not yet clear the amount of resources required or available. There will probably be a need to prioritize effort, to allocate limited resources in a way that can minimize the impact of any

---

[28]Op. cit. National Strategy. p.33-34. The Strategy states that the national infrastructure protection plan called for by the Strategy will describe how to use all policy instruments to raise security levels. These could include federal grants to states and localities and, perhaps, "legislation to create incentives for the private sector to adopt security measures or invest in improved safety technologies."

future terrorist attacks on the nation's infrastructure. The Administration alludes to the need to set priorities throughout the National Strategy.

Essentially, the problem facing the federal government is to minimize, with a limited amount of resources, the expected impact on the nation's critical infrastructure of any future terrorist attack. Impacts could be measured in lives lost, economic dislocations, loss of military capability, loss of national morale (measured perhaps by polling), or some combination. Expected impacts are determined by factoring in the likelihood of various events happening. This is important since policy makers must balance those scenarios with a low probability of occurring, but which, if they did occur, could be catastrophic with scenarios that are less catastrophic, but could happen more easily.

There are a number of ways policy makers may try to prioritize their efforts. As discussed above, some elements within a critical infrastructure are far more critical than others. Some elements, or portions of an infrastructure, may be lightly used or somewhat redundant. If these segments were unavailable, their loss would be an inconvenience, but such a loss would hardly be ruinous. One option, therefore, would be to focus on identifying the truly critical assets and doing things to harden (or toughen) them against attack or to reduce the impact of their loss, either by building in redundancies or through relocation or redesign (to reduce associated hazards) over time.

Another possible way of prioritizing resource allocations is to identify vulnerabilities or solutions that cut across more than one infrastructure. To some extent, information systems are a common vulnerability to many of the other infrastructures. Solutions to information system vulnerabilities could be applied generally, whether it is establishing and implementing best practices or developing more secure software. Another related technology that cuts across more than one infrastructure are remote control systems. Much attention has already been focused on the vulnerabilities of supervisory control and data acquisition systems (SCADAs) used in energy, water, transportation, and chemical infrastructures.[29]

Another way is to identify interdependencies between infrastructures. None of the infrastructures mentioned above are completely isolated from the others. Energy production depends on transportation. Transportation depends on energy. They both depend on information networks. Information networks depend on energy. It is because of these interdependencies that an attack on one segment of an infrastructure could have a debilitating impact on other infrastructures. Identifying and focusing on those assets that connect one infrastructure to another may be a cost-effective way to reduce the overall impact of an attack. The National Infrastructure Simulation and Analysis Center, established in the USA Patriot Act,[30] and slated to be transferred to the Critical Infrastructure Protection function of the new Department of Homeland Security, has this as one of its major tasks.

---

[29] See CRS Report, *Critical Infrastructure, Remote Control Systems, and the Terrorist Threat*, by Dana Shea. CRS Report RL31534.

[30]Op. Cit. USA Patriot ACT. P.L. 107-56. Sec. 1016.

Similarly, there may be geographic locations where a number of critical assets of one or more infrastructures are located that might warrant priority. One of the impacts associated with the attacks on the World Trade Center was that the area housed a number of assets associated with banking and finance, electric power, and telecommunications, some of which had no backup assets located elsewhere. While the impacts associated with the loss of these assets were fairly localized to lower Manhattan, or the services were quickly reconstituted elsewhere, the issue of co-location of critical assets was not lost on people responsible for ensuring services.

Another possible way to prioritize, at least with regard to the expenditure of federal resources, is for the federal government to focus more on those infrastructures that are either entirely owned and operated by the government, or on those private or local infrastructures upon which the federal government depends to carry out its activities, or with which the federal government has a long and close working tradition. This implies letting those infrastructures where the federal government has not been particularly active to take primary responsibility for addressing their own vulnerabilities and impacts.

While the definition of critical infrastructure is broad and the number of infrastructures that are being considered critical has grown, limiting the number of infrastructures under study *a priori* might miss a dangerous vulnerability. At some point, however, priority of effort will be required. According to the National Strategy for Homeland Security, the federal government will apply a consistent methodology to focus its efforts on the highest priorities. The Strategy further states that a forthcoming comprehensive national plan to protect critical infrastructure from terrorist attacks will provide an approach for rationally balancing the costs and benefits of increased security according to the threat. However, the Strategy gives no indication of what these methodologies or approaches will be. Congress may want to focus some of its attention on how the Administration proposes to set priorities and what criteria it uses to do so.

Appendices

What is Infrastructure?

The President's proposal to create a Department of Homeland Security which would, among other responsibilities, assess and develop plans for protecting America's critical infrastructure and key assets is focusing attention on the question of which systems or sectors should be included.

Before "critical infrastructure" became a term of interest in the terrorism and homeland security debate, the seemingly similar term "infrastructure" was a subject debated by public policymakers. With no standard or agreed definition, the concept in policy terms has been fluid, as it appears to be today, including both public and private systems, services, and even amenities. Nearly 20 years ago, infrastructure was debated because of concern that the nation's public works infrastructure was believed to be suffering from severe problems of deterioration, technological obsolescence, and insufficient capacity to serve future growth. Unlike today's focus on security from physical or cyber attacks on systems, the focus of debate at that time was the nature, extent, and severity of poor physical condition, technological adequacy, and capacity of public works systems and about decisions by government at all levels on spending priorities to meet physical and management needs.

Public and private reports at the time analyzed and critiqued the issue, and many sought to define the term "infrastructure." One of these reports, issued by the Council of State Planning Agencies, defined the term as public service and production facilities, which include "a wide array of public facilities and equipment required to provide social services and support private sector economic activity." According to this report, infrastructure commonly included roads, bridges, water and sewer systems, airports, ports, and public buildings, and may also include schools, health facilities, jails, recreation facilities, electric power production, fire safety, solid waste disposal, and telecommunications.[31]

In a 1983 report to Congress about policies regarding the condition of the nation's infrastructure, the Congressional Budget Office (CBO) analyzed seven categories of infrastructure: highways, public transit systems, wastewater treatment works, water resources, air traffic control, airports, and municipal water supply. These seven systems, CBO said, "share 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." CBO noted that "the concept of infrastructure can be applied broadly to include such social facilities as schools, hospitals, and prisons, and it often includes industrial capacity, as well."[32]

---

[31] Vaughan, Roger, and Robert Pollard. REBUILDING AMERICA, VOL. I, PLANNING AND MANAGING PUBLIC WORKS IN THE 1980S. Council of State Planning Agencies. Washington DC, 1984: 1-2.

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

In a 1988 report, CBO utilized a similar but consolidated categorization of infrastructure (highways, aviation, mass transit, wastewater treatment, and water transportation) based on a definition that those facilities:

> provide a foundation or basic framework for the national economy, and in which federal policy plays a significant role...This definition excludes 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.[33]

Congress has on many occasions enacted legislation affecting one or more infrastructure categories, such as surface transportation or water resources, but has rarely done so comprehensively. During the 1980s debate about deteriorating public works systems, Congress did enact a bill that established a National Council on Public Works Improvement with a mandate to analyze and report to Congress and the President on the state of public works infrastructure systems (P.L. 98-501). Title II of that act directed the President to submit certain budgetary information on public civilian and military capital investment programs in the annual budget transmittal. The coverage of this analysis was to be broad. According to the legislation, it 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 projects; hospitals; resource recovery facilities; public buildings; space or communication facilities; railroads; and federally assisted housing."[34]

The Council established by P.L. 98-501 provided yet another definition of infrastructure and included nine categories of systems in its analyses: 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. These categories, the Council said, have strong links to economic development and generally have a tradition of public sector involvement. Facilities have high fixed costs and long economic lives. 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."[35]

Since the 1980s, policymakers' attention has largely moved away from considering the infrastructure issue comprehensively and as it was framed during that earlier period. Legislative proposals generally have addressed meeting the needs of individual sectors and defining the federal government's role, especially concerning

---

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

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

[35]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.

financing. As discussed in this report, the term "critical infrastructure" evolved more recently, and it occurred separately from policies affecting more specific infrastructure issues such as highways and airports. Nonetheless, many of the definitional phrases from the 1980s' debate about infrastructure–that which is "directly critical to activity in the nation's economy" and forms "the underpinnings of the nation's defense"–are echoed in today's discussion of assessing infrastructures and assets that are critical to homeland security.

How the Criteria and Components of Critical Infrastructure Have Expanded Over Time

The table below illustrates how the criteria and components of critical infrastructure have expanded over time. As discussed in the body of this report, for an infrastructure to be judged critical it must be vital to one or more broad national functions. That set of functions has expanded over time, beginning with national defense and economic security, to include public health and safety, and then national morale. This expansion is noted horizontally, from left to right, in the table below. Similarly, the components (or sectors) that have been identified specifically as critical infrastructures has expanded. The expansion of this list is depicted vertically, from top to bottom, in the table below.

The cross-referencing marks, "x", are only meant to be illustrative, and generally coincide with when the specific infrastructure appears on a list. For example, the chemical industry was not on any list of critical infrastructures when the criteria were limited to being vital to national or economic security. It appeared after September 11, 2001, when attention shifted from the more strategic thinking of earlier policy deliberations to the more immediate concern of preventing large single event casualties (more a public health and safety concern). That is not to say that the chemical industry, as a whole, is not an important element in the U.S. economy or that there may not be a unique facility whose loss of operations might have a ripple effect through the economy.

Table 1. What Constitutes Critical Infrastructure Over Time

Infrastructure	Criteria for Being Considered Critical. Vital to			
	national defense	economic security	public health and safety	national morale
telecommunications information networks	x	x		
energy	x	x		
banking/finance		x		
transportation	x	x		
water			x	
emergency services			x	
government			x	
health services			x	
national defense	x			
foreign intelligence	x			
law enforcement			x	
foreign affairs	x			
nuclear facilities, in addition to power plants			x	
special events				x
food/agriculture			x	
manufacturing		x		
chemical			x	
defense industry	x			
postal/shipping			x	
national monuments icons				x

Hard Infrastructure. These make up the physical systems that make it necessary to run a modern, industrialized nation. Examples include roads, highways, bridges, as well as the capital/assets needed to make them operational (transit buses, vehicles, oil rigs/refineries). Critical Infrastructure. These are assets defined by a government as being essential to the functioning of a society and economy, such as facilities for shelter and heating, telecommunication, public health, agriculture, etc. In the United States, there are agencies responsible for these critical infrastructures, such as Homel critical infrastructure. Share this item with your network: By. TechTarget Contributor. Critical infrastructure is the body of systems, networks and assets that are so essential that their continued operation is required to ensure the security of a given nation, its economy, and the publicâ€™s health and/or safety. Although critical infrastructure is similar in all nations due to the basic requirements of life, the infrastructure deemed critical can vary according to a nationâ€™s needs, resources and development level. In the United States, the Department of Homeland Security (DHS) identifies 16 s Critical infrastructure (or critical national infrastructure (CNI) in the UK) is a term used by governments to describe assets that are essential for the functioning of a society and economy â€“ the infrastructure. Most commonly associated with the term are facilities for: Shelter; Heating (e.g. natural gas, fuel oil, district heating); Agriculture, food production and distribution; Water supply (drinking water, waste water/sewage, stemming of surface water (e.g. dikes and sluices)