Backgrounder

Published by The Heritage Foundation

No. 1851
May 9, 2005

Who's on First? A Strategy for Protecting Critical Infrastructure

Alane Kochems

Over 85 percent of the critical infrastructure (CI) in the United States is controlled by the private sector.[1] The USA PATRIOT Act defines 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 these matters.[2]

While protecting critical infrastructure has always been a U.S. concern, the urgency has increased in recent years. With so much critical infrastructure under private control, delineating exactly which responsibilities for protecting it should be exercised by private entities and which should be carried out by the federal government has been difficult.

Three critical tasks must be addressed before an effective national critical infrastructure plan that includes the private sector can be implemented:

1. The Department of Homeland Security (DHS) should be reorganized to include an Undersecretary for Protection and Preparedness;
2. Congress and the Administration should remove roadblocks to creating a risk-based system that engages the private sector; and
3. The DHS should create effective means for sharing information among federal and state governments, the private sector, and other entities.

Talking Points

- The federal government—not the private sector—is responsible for preventing terrorist attacks through intelligence gathering, early warning, and domestic counterterrorism.
- The private sector is responsible for taking reasonable precautions to reduce vulnerabilities in its critical infrastructure. This will limit the ability of terrorists to exploit these weaknesses.
- The federal government needs both to define clearly what it believes are reasonable actions for the private sector and to address liability issues.
- Congress and the Administration need to address liability issues related to terrorist acts and work to harmonize U.S. laws with the laws of other countries and international law so that terrorists and other criminals cannot slip through any legal gaps.

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/bg1851.cfm

Produced by the Kathryn and Shelby Cullom Davis Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

The primary objective of a national CI effort must be to share information among federal, state, and local governments and the private sector so that they can better address terrorist threats to critical infrastructure. A secondary objective is to provide standards that promote economic growth and protect civil liberties while making the nation safer.

Threats, Vulnerabilities, and Criticality

Protecting critical infrastructure involves three assessments: threats, vulnerabilities, and criticality. A threat assessment looks at and evaluates threats based on factors such as capability, intention, and lethality of attack. Using threat assessments frees organizations from having to rely solely on worst-case scenarios to guide their planning and resource allocation:

> Worst-case scenarios tend to focus on vulnerabilities, which are virtually unlimited, and would require extraordinary resources to address. Therefore, in the absence of detailed threat data, it is essential that a careful balance exist using all three elements in preparing and protecting against threats.[3]

Vulnerability assessments identify exploitable weaknesses and suggest ways to eliminate or minimize them. Criticality assessments are "designed to systematically identify and evaluate an organization's assets based on the importance of its mission or function, the group of people at risk, or the significance of a structure."[4] These three assessments can then be assembled into a bird's-eye view of the situation. Using these reviews, an organization can create a comprehensive risk management strategy to guide decision-making and resource allocation.

There are two categories of risk: risks with thinkable consequences and those with unthinkable ones. Thinkable risks have few secondary effects and are geographically and temporally bound. For such risks, the goal is to minimize the single points of failure, cascading effects, and uncertainty by focusing on rapid reconstitution and recovery and by building security awareness. Unthinkable risks involve very large loss of life, great damage, and effects spread over time and space, such as a nuclear attack. For unthinkable risks, the entities involved need to focus on countermeasures, recovery, and attribution.

Efforts should be apportioned between thinkable and unthinkable scenarios. Thinkable situations need to be made less terrifying while unthinkable ones are made less likely.

A functional risk management system needs four components.

- *First,* any system needs to be able to analyze several interdependencies. The post–Cold War world is complex, and there are many important variables.
- *Second,* effective information sharing depends on a high degree of trust between data owners and those who want to analyze information.
- *Third,* effective assessments require collecting and inputting as much of the relevant, knowable data as possible. Risk management deals in possibilities and probabilities. The analysis can only be as good as the available information.
- *Finally,* the nation needs to realize that no system is perfect, but that any reasonable attempt to allocate resources should improve the probability of preventing an attack.

Even if information-sharing problems are eliminated, the federal government still needs to determine where to focus its efforts. The federal government should target resources toward the critical infrastructure in which it has a vested inter-

1. U.S. Department of Homeland Security, "Protected Critical Infrastructure Information (PCII) Program: Program Overview," at *www.dhs.gov/dhspublic/display?theme=92&content=3763&print=true* (February 23, 2004).
2. USA PATRIOT Act of 2001, Public Law 107–56.
3. Raymond J. Decker, "Homeland Security: Key Elements of a Risk Management Approach," testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, U.S. House of Representatives, October 12, 2001, p. 3, at *www.gao.gov/new.items/d02150t.pdf* (March 15, 2005).
4. *Ibid.*, p. 1.

est. The current list of critical infrastructure is too expansive, including sectors that are not truly vital to the federal government's functioning. The federal government has a vested interest in only the energy, finance, telecommunications, and transportation sectors.

Once the DHS compiles a limited list of vital critical infrastructure, the responsibility for protecting that infrastructure should be divided according to vulnerabilities and threats. The private sector should work to achieve reasonable reductions in the vulnerabilities (weaknesses) in its infrastructure; the federal government should address outside threats to the infrastructure.

The federal government—not the private sector—is responsible for preventing terrorist acts through intelligence gathering, early warning, and domestic counterterrorism. The private sector is responsible for taking reasonable precautions, much as it is expected to take reasonable safety and environmental precautions. The federal government also has a role in defining what is "reasonable" as a performance-based metric and facilitating information sharing to enable the private sector to perform due diligence (e.g., protection, mitigation, and recovery) in an efficient, fair, and effective manner.

A model public–private regime would (1) define what is reasonable through clear performance measures, (2) create transparency and develop means to measure performance, (3) establish ways for the market to reward good behavior, and (4) ensure that any "fix" does not cripple the economic engine that supports the society and liberties Americans enjoy.

The right national critical infrastructure plan would combine reasonable efforts by the private sector to protect its facilities with government counterterrorism efforts to provide a layered defense.

The National Critical Infrastructure Plan

On paper, the approach to protecting critical infrastructure has been correct. Both the National Strategy for Homeland Security and the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets recommend a risk-based approach with responsibilities shared between the federal government and the private sector:

> Effective and efficient risk assessment, protection planning, and resource allocation go hand in hand.… Because of…resource limitations, federal, state, and local authorities must collaborate more efficiently to assess, plan, and allocate their limited resources.[5]

Congress also acknowledged the importance of critical infrastructure in the Homeland Security Act of 2002 by establishing the Information Analysis and Infrastructure Protection Directorate within the DHS, directing it to:

1. "[C]arry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States";
2. "[I]ntegrate relevant information, analyses, and vulnerability assessments" to "identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities";
3. "[D]evelop a comprehensive national plan for securing key resources and critical infrastructure of the United States"; and
4. "[R]ecommend measures necessary to protect the key resources and critical infrastructure" in cooperation with other federal agencies, state governments, the private sector, and other entities.[6]

In addition, President George W. Bush issued Homeland Security Presidential Directive 7, providing guidance for identifying, prioritizing, and protecting critical infrastructure. According to the directive:

> Federal departments and agencies will identify, prioritize, and coordinate the

5. White House, *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, February 2003, p. 22, at *www.whitehouse.gov/pcipb/physical_strategy.pdf* (February 18, 2005).
6. Homeland Security Act of 2002, Public Law 107–296, §201(d)(2), (3), (5), (6).

> protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Federal departments and agencies will work with State and local governments and the private sector to accomplish this objective.[7]

While the federal government has established a firm policy foundation for protecting critical infrastructure, the structural enablers that actually implement the guidance either are in their infancy or have not yet been created.

Implementing the Plan

To move from plans on paper to a functional system for identifying and protecting critical infrastructure, three actions must occur: (1) The DHS should be reorganized to include an Undersecretary for Protection and Preparedness; (2) Congress and the Administration should remove the roadblocks to creating a risk-based system that engages the private sector; and (3) the DHS should develop effective means for sharing information among federal and state government agencies, the private sector, and other entities.

Reorganizing the DHS. It is improbable that a catastrophic terrorist attack would affect only a single city or that one city would be sufficiently prepared to mount an adequate response. At a minimum, response efforts would require mutual aid from multiple jurisdictions.

Despite this, the DHS lacks an effective regional structure to facilitate coordination with state and local governments and with the private sector.[8] To begin correcting this oversight, critical infrastructure protection, preparedness, and coordination of state, local, and private efforts should be consolidated under an Undersecretary for Protection and Preparedness, including:

1. The infrastructure protection component of the Information Analysis and Infrastructure Protection Directorate;
2. The Office of State and Local Government Coordination and Preparedness;
3. The non-operational transportation infrastructure protection mission of the Transportation Security Administration;
4. The preparedness piece of the Emergency Preparedness and Response Directorate;
5. The private-sector preparedness mission of the Office of Private Sector Liaison; and
6. DHS grant-making authority.

With "these disparate efforts" thus consolidated, the Secretary of Homeland Security would have:

> a stronger platform from which to lead national efforts, determine priorities, identify critical vulnerabilities, work with state/local/private sector entities on securing those vulnerabilities and preparing for attacks, and make grants to help get the job done and to induce cooperation.[9]

In fact, even more consolidation and coordination within the DHS is needed; however, the DHS should exercise care to ensure that any reorganization does not hinder coordination efforts currently underway or create even more confusion in the private sector.

The DHS also needs a high-level policy officer in the form of an Undersecretary for Policy to articulate and coordinate policy guidance throughout the department. This individual should report to the deputy secretary. The undersecretary's responsibilities should be established by law and should include "coordinating DHS policy," "conducting long-range policy planning," "preparing critical strategic documents," "conducting program analy-

7. George W. Bush, "Critical Infrastructure Identification, Prioritization, and Protection," Homeland Security Presidential Directive HSPD–7, December 17, 2003, at *www.whitehouse.gov/news/releases/2003/12/20031217-5.html* (February 18, 2005).
8. For more information, see Edwin Meese III, James Jay Carafano, Ph.D., and Richard Weitz, Ph.D., "Organizing for Victory: Proposals for Building a Regional Homeland Security Structure," Heritage Foundation *Backgrounder* No. 1817, January 21, 2005, at *www.heritage.org/Research/HomelandDefense/bg1817.cfm*.
9. James Jay Carafano, Ph.D., and David Heyman, "DHS 2.0: Rethinking the Department of Homeland Security," Heritage Foundation *Special Report* No. 2, December 13, 2004, p. 14, at *www.heritage.org/Research/HomelandDefense/sr02.cfm*.

sis," and "preparing net assessments."[10] A unified policy office would be the appropriate place to create risk management policies, examine how to balance responses between thinkable risks and unthinkable risks, and sort through information-sharing policy problems.

Engaging the Private Sector. To creating a risk-based system that incorporates private-sector entities, Congress and the Administration should:

- **Strengthen PCII protections.** The DHS set up the Protected Critical Infrastructure Information (PCII) Program to encourage the private sector to share sensitive and proprietary business information about critical infrastructure with the federal government. Members of the private sector can voluntarily submit sensitive information to the DHS with the understanding that the DHS will protect the information from public disclosure, assuming that all the requirements of the Critical Infrastructure Information Act of 2002 have been met. The PCII regulations are very strict, requiring a specific request to consider whether information meets the criteria to be labeled as PCII as well as data to justify such a decision.

  While the program is a good start, it is not yet clear how widely the federal government will disseminate the information. The program is currently set up to distribute PCII within the DHS, but there are plans to disseminate such information as necessary to authorized individuals in federal, state, and local governments and in the private sector. The DHS plans to require agencies, governments, and other entities to meet accreditation requirements (e.g., training staff on proper handling of PCII and obtaining nondisclosure agreements from staff) before receiving PCII. States must also sign memoranda of understanding with the program manager before they receive PCII.

  These measures seem appropriate, but the proof will be in the actual implementation. The guidelines and regulations will need to balance protecting sensitive information with promoting information sharing.

  In addition to fears about public disclosure, the private sector is concerned that the government will use voluntarily submitted information to impose intrusive regulation and that private lawyers could obtain this information through the discovery process and then use it in litigation against the private sector. To encourage private industry to submit information to the PCII program, Congress should clarify to whom and under what conditions the information may be disseminated or used in private litigation.

- **Clarify the Sarbanes–Oxley Act's application to homeland security.** In an attempt to improve corporate governance, the Sarbanes-Oxley Act of 2002[11] mandates that public companies take certain actions. For instance, it requires that chief executive officers certify that they have reviewed the financial practices of their companies and understand risks that may affect the financial reporting process.

  While improved corporate governance sounds good, especially after Enron and other scandals, how the act would apply to homeland security issues is unclear. What would happen under the law if a terrorist attack on a piece of critical infrastructure caused the value of a corporation's stock to plummet? Could a stockholder sue the company for having an inadequate risk management strategy and failing to disclose its vulnerabilities?[12]

  There are at least three ways to address this problem: (1) The Securities and Exchange Commission could clarify how it intends to apply the legislation; (2) Congress could repeal the Sarbanes–Oxley Act; or (3) Congress could carve out a "safe haven" in the law for certain situations (e.g., terrorist attack). SEC guidance would at least alert companies to what the expectations are. Repealing the law, which has other problems, could alleviate burdensome

10. *Ibid.*, pp. 11–12.

11. Sarbanes–Oxley Act of 2002, Public Law 107–204.

reporting requirements while removing worries about its application to homeland security.

- **Minimize liability risks.** If CI owners and operators alert the federal government to vulnerabilities and then terrorists exploit one of these weaknesses, there is concern that such disclosures could be used against owners and operators in lawsuits. Furthermore, owners and operators face liability issues with regard to their piece of infrastructure being turned into a weapon and any resulting death and destruction.

  To counter these concerns, a good first step would be to create safe harbors for certain sectors. Congress should create a list of actions that are deemed to be reasonable precautions. There are parallels in other areas that share similar public policy concerns. Tort reform could also help to reassure the private sector about these liability issues.

  The Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002 is one tort reform measure that is already in existence. However, it has been underutilized by the DHS, and many in industry consider it complex and confusing. The legislation limits liability for tort claims that arise out of, relate to, or result from a terrorist act in which a qualified anti-terrorism technology has been deployed. The act does not limit liability if a terrorist act has not occurred. The SAFETY Act applies to all forms of technology (e.g., products, software, services, and various forms of intellectual property). The Administration and Congress should clarify the SAFETY Act as necessary and push for its use where appropriate.

- **Develop the business case for homeland security.** The DHS frequently argues that it needs access to information from the private sector and that it is putting forth rules to prevent another terrorist attack. While that may be true, the DHS needs to present sound economic and business reasons for the private sector to assist in protecting the nation.

  To bolster this effort, and because current estimates vary significantly, the DHS should commission a rigorous study of the economic consequences of different types of terrorist attacks. Such a study could help to demonstrate the business case for improving security measures. The DHS and the private sector also need to cooperate on rulemaking; otherwise, the DHS is likely to create rules that bear little relation to reality, hindering economic growth and failing to improve the nation's security.

- **Harmonize U.S. laws with the laws of other countries.** U.S. laws need to be harmonized with the laws of other countries and with international law to improve the government's ability to exchange information and prosecute criminals and terrorists. For instance, cyber attacks against U.S. critical infrastructure can originate from anywhere. It is important that other countries have appropriate laws and agreements in place to allow prosecution of cyber crime.

  Other countries' laws also need to mesh with U.S. law so that terrorists and other criminals cannot slip through any legal gaps. In some cases, the Administration will need to conclude agreements with nations that have significantly different laws. For instance, the United States and the European Union negotiated an agreement to share international airline passenger data when privacy laws conflicted. Just as the EU and the United States negotiated ways to share information, the United States should work to reconcile its laws and policies with

12. Some security experts have suggested that the act may implicitly require contingency response plans and that risk assessments could be interpreted to include operational risk that results from insufficient business continuity planning. Al Berman, "Business Continuity in a Sarbanes–Oxley World: How Business Is Leveraging Business Continuity to Comply with the New Regulation," *Disaster Recovery Journal*, Vol. 17, Issue 3 (Summer 2004), at *www.drj.com/articles/sum04/1702-01.html* (April 12, 2005). Since liability is a balance among probability of risk, magnitude of the harm, and the cost of protection, courts will look to see whether companies have observed "due diligence" and acted reasonably. Having a business continuity plan that includes responses to a terrorist attack might be considered a reasonable precaution.

those of other nations and the international community.

- **Promote the effective sharing of information.** Actionable information is central to any counterterrorism effort, and a variety of information-sharing programs already exist. The Homeland Security Operations Center runs two information-sharing networks: the Homeland Security Information Network (HSIN), which is an Internet-based counterterrorism communications tool, and the Homeland Security Information Network—Critical Infrastructure, which provides real-time information to CI owners and operators.[13] Now that the DHS has established these networks, the right people need to use them to exchange information.

  Moreover, these tools need to be integrated with private-sector information-sharing mechanisms because the private sector also shares and analyzes information without government involvement. The DHS has started to address these needs through the HSIN and by encouraging private-sector formation of Sector Coordinating Councils. Whether this effort succeeds will depend in part on whether the federal government and CI owners and operators can divide responsibilities for vital CI according to threats and vulnerabilities. The more the DHS acts as a coordinating agency and focuses on outside threats to important critical infrastructure, the greater the likelihood that the private sector will participate.

  One congressional attempt to promote information sharing is the Intelligence Reform and Terrorism Protection Act of 2004,[14] commonly known as the 9/11 Reform Bill, which requires the President to establish an "information sharing environment" (ISE) to distribute intelligence regarding terrorism to appropriate federal, state, local, and private entities. It requires the President to designate an organizational and management structure to establish and maintain the ISE and report back to Congress within one year on the plans for implementation. It also creates an Information Sharing Council to advise the President and the ISE program manager on developing policies, procedures, guidelines, roles, and standards for establishing and maintaining the ISE.

  Over the long term, the ISE could provide critical capabilities for enhancing the role of state and local agencies in counterterrorism operations. To ensure that they can appropriately access and contribute to the ISE, state and local representatives should be given key positions on the Information Sharing Council so that their needs and potential contributions can be adequately addressed.

Conclusion

The federal government is responsible for preventing terrorist attacks through intelligence gathering, early warning, and domestic counterterrorism. The CI private sector is responsible for taking reasonable precautions to reduce its vulnerabilities, thereby limiting the ability of terrorists to exploit these weaknesses.

The federal government needs both to define clearly what it believes are reasonable actions for the private sector and to address liability issues. Congress and the Administration need to further consolidate and coordinate the DHS, remove impediments to private-sector involvement, and facilitate effective information sharing among public and private entities. Neither the federal government nor private CI owners and operators can fully protect critical infrastructure against terrorist attacks—they must work together to be successful.

—Alane Kochems is a Research Assistant in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation.

13. U.S. Department of Homeland Security, *Fact Sheet: Homeland Security Operations Center (HSOC)*, July 8, 2004, at *www.dhs.gov/dhspublic/display?theme=52&content=3815&print=true* (January 16, 2005).

14. Intelligence Reform and Terrorism Protection Act of 2004, Public Law 108–458.