Order Code RL32531

CRS Report for Congress
Received through the CRS Web

Critical Infrastructure Protections: The 9/11 Commission Report

August 16, 2004

John Moteff
Specialist in Science and Technology Policy
Resources, Science, and Industry Division

Critical Infrastructure Protections: The 9/11 Commission Report

Summary

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, relatively few recommendations in the Commission's report address critical infrastructure protection specifically. These call for using a systematic risk management approach for setting priorities and allocating resources for critical infrastructure protection. The Commission discussed in more detail issues related to transportation security. However, none of these 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.

For a more detailed 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*. For a brief discussion on the question of what is a critical infrastructure and the need to set priorities, see CRS Report RL31556, *Critical Infrastructures: What Makes an Infrastructure Critical?*

This report will not be updated.

Contents

Introduction 1
Recommendations Related to Critical Infrastructure Protection 1
Potential Impact of Commission Recommendations on Critical Infrastructure Protection Activities 3
Concluding Remarks 6

Critical Infrastructure Protections: The 9/11 Commission Report

Introduction

Federal efforts to protect the nation's critical infrastructure pre-date the September 11, 2001 attacks on the World Trade Center and the Pentagon. Since the attacks, critical infrastructure protection has evolved to include countering that type of an attack. Because the purpose of the Commission's report was to answer, "How did the terrorist attack of September 11, 2001 happen?" and "How can such a tragedy be avoided in the future?," most, if not all, of the recommendations made in the 9/11 Commission's report deal indirectly with critical infrastructure protection. However, there are relatively few recommendations that specifically address critical infrastructure protection. This report will identify those recommendations and briefly discuss the possible impacts those recommendations might have on the nation's efforts to protect its critical infrastructure.

Recommendations Related to Critical Infrastructure Protection

Much of what the Commission recommended for critical infrastructure protection can be found in Chapter 12, Section 12.4 of the Commission's report (Protect Against and Prepare For Terrorist Attack, starting on page 383).

The majority of this section is devoted to the importance of disrupting terrorists' ability to travel unchallenged around globe and into the United States. It discussed the integration of travel intelligence gathering and analysis with border protection and law enforcement operations. It discussed screening techniques and technologies to be integrated at all points in the process, from visa application to walking through detectors at entry points, to checking identification upon entrance to certain sensitive facilities. This section also discussed at some length the need to incorporate biometric screening technologies into the processes. These issues, however, are beyond the scope of this report. For more discussion of these issues, see the Homeland Security: Border and Transportation Security page on CRS's Congressional Legislative Issues webpage.[1]

Section 12.4 of the Commission's report also focused on issues related to securing the nation's transportation sector from attack (see page 390 of the Commission's report, "Strategies for Aviation and Transportation Security"). In this section, the Commission mentioned the Aviation and Transportation Security

---

[1] See, [http://www.crs.gov/products/browse/is-homelandsecurity.shtml]

Act (P.L. 107-71) which established the Transportation Security Administration (TSA, which is now part of the Department of Homeland Security). Among other tasks, the act assigned the TSA the responsibility of developing strategic plans to provide security for critical parts of the U.S. transportation system. The Commission expressed concern that 90% of the annual federal investment made in transportation security goes toward commercial aviation security without a systematic risk assessment to determine if this is the most cost-effective allocation of resources. The Commission noted that "major" vulnerabilities still exist in cargo and general aviation, and that the security improvements in commercial air traffic may shift the threat to ports, railroads, and mass transit systems. The Commission noted that the TSA has yet to develop an integrated plan for the transportation sector, nor specific plans for the various transportation modes.

The Commission reiterated the need for the federal government to:

- identify those transportation assets that need to be protected;
- set risk-based priorities for defending them;
- select the most practical and cost-effective ways to do so;
- develop a plan and a budget;
- and, then fund implementation.

The Commission went on to recommend that Congress set a specific date for the completion of the plan and hold the TSA and the Department of Homeland Security accountable for achieving it.[2]

In regard to aviation security, the Commission recommended the timely implementation of improved "no-fly" and "automatic selectee" lists (including the recommendation that air carriers be required to supply information to help develop these lists) and that a greater priority be given to detecting explosives on passengers and on studying human factors affecting the effectiveness of screeners' performances.

Also in Section 12.4, the Commission again discussed the need for a systematic assessment of risks, vulnerabilities, threat, and need when allocating federal resources to help states and localities protect against and respond to terrorist attacks (see page 395 of the Commission's report, "Setting Priorities for National Preparedness"). The Commission suggested that these federal funds should act as a supplement to state and local funding in those instances where additional protection is merited based on the systematic assessment, and not as part of a general revenue sharing mechanism. The Commission suggested that these assessments should consider such factors as population, population density, vulnerability, and the presence of critical infrastructure within each state.

Furthermore, the Commission recommended that a panel of experts be convened to develop a set of benchmarks by which to evaluate a community's needs and by which to distribute federal funds through the state to those localities.

---

[2] The Commission continues to make this point in subsequent Congressional hearings. See, "Deadlines Urged for Terror Fixes", Washington Post, August 17, 2004, p A13.

Finally, the Commission made a recommendation at the end of Chapter 13, Section 13.4 (see page 428 in the Commission's report), which specifically addressed all critical infrastructure. The Commission, in discussing the different roles assumed by the Department of Defense and the Department of Homeland Security in homeland security, noted that DHS is responsible for identifying, within the sectors that possess critical infrastructure, those elements (or assets) that need to be protected. The Commission recommended that DHS, and its oversight committees, should regularly assess the types of threats the country faces to determine a) the adequacy and status of the government's plans to protect critical infrastructure and b) the readiness of the government to respond to those threats.

Potential Impact of Commission Recommendations on Critical Infrastructure Protection Activities

The Commission recommendations specifically directed at critical infrastructure protection, while lending the weight of the Commission to certain elements of existing federal policy, do not advocate any change in the direction of, or the organizational structures that have evolved to implement, that policy. The recommendations, however, could speed up implementation is some areas, given the attention and renewed urgency expressed by the Commission.

Federal policy on critical infrastructure protection is laid out in law, presidential directives, and national strategies.[3] As noted by the Commission, the Homeland Security Act of 2001 (P.L.107-296, enacted in November 25, 2002) assigned to the Department of Homeland Security the task of coordinating the national effort in critical infrastructure protection. Specifically, it gave DHS the responsibility to:

- "... identify and assess the nature and scope of terrorist threats to the homeland;"
- "... understand such threats in light of actual and potential vulnerabilities of the homeland;"
- "... carry out comprehensive assessments of the vulnerabilities of the key resource and critical infrastructure of the United States, including the performance of risk assessments to determine the risk posed by particular types of terrorist attacks within the United States ...."
- "... integrate relevant information, analyses, and vulnerability assessments...in order to identify priorities for protective and support measures...."
- "... develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States ...."
- "... recommend measures necessary to protect the key resources and critical infrastructure of the United States ...."

[3] For a more thorough review of national policy and its evolution and implementation, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation.*

The *National Strategy for Homeland Security*,[4] anticipating the establishment of the Department of Homeland Security, stated:

- "... the Department would build and maintain a complete, current, and accurate assessment of vulnerabilities and preparedness of critical targets across critical infrastructure sectors .... [This assessment will] guide the rational long-term investment of effort and resources.[5]"
- "... we must carefully weigh the benefit of each homeland security endeavor and only allocate resources where the benefit of reducing risk is worth the amount of additional cost.[6]"

The *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* [7] stated:

- "DHS, in collaboration with other key stakeholders, will develop a uniform methodology for identifying facilities, systems, and function with national-level criticality to help establish federal, state, and local government, and the private-sector protection priorities. Using this methodology, DHS will build a comprehensive database to catalog these critical facility, systems, and functions.[8]"

Homeland Security Presidential Decision Directive Number 7 (HSPD-7, released by the current Bush Administration in December 2003) reiterated these tasks, including directing Sector Specific Agencies (i.e. those agencies acting as lead agency liaison with certain critical infrastructure possessing sectors) to: "conduct or facilitate vulnerability assessments"; and, "encourage risk management strategies to protect against and mitigate the effects of attacks." These responsibilities actually pre-date the September 11 attack, as authorized by the Clinton Administration's Presidential Decision Directive Number 63 (released in May 1998). HSPD-7 also reiterated that the Secretary of Homeland Security is to produce a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection and set a date of December 17, 2004 by which that report should be developed.

Implicit in these directives to integrate threat and vulnerabilities, and to use risk assessment and risk management techniques to set priorities and allocate resources is the need to do so on a continuous basis as new information becomes available. Also, the Administration has budgeted for activities aimed at validating protection plans and to anticipate new potential threats by using "red teams" and other performance measures.

---

[4] Office of Homeland Security, National Strategy for Homeland Security. July 2002.

[5] Ibid. p.33.

[6] Ibid. p. 64.

[7] Office of Homeland Security, The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. February 2003.

[8] Ibid. p 23.

For more discussion of what is happening in specific infrastructures, see both the Homeland Security: Critical Infrastructures Protection page and the Homeland Security: Border and Transportation Security page of CRS's Congressional Legislative Issues webpage.[9]

In regard to the allocation of funds to state and localities, DHS administers a number of infrastructure-related security grants. One of these grants, the State Homeland Security Grant Program, established soon after the September 11 attacks by the U.S.A. PATRIOT Act (P.L. 107-56, enacted on October 26, 2001), and primarily aimed at first-responders, is the general revenue sharing grant alluded to in the Commission's report. Every state, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories, receive a minimum fixed percentage of the program's appropriated resources.

In addition to the State Homeland Security Grant Program are the Urban Areas Security Initiative Grant Program, to which have been added Port Security Grants, and Transit System Security Grants.[10] According to these grants' application guidelines, the Urban Areas, Ports, and Transit System security grants are allocated to selected cities and port areas based on a formula developed by DHS which considers current threat estimates, critical assets within the urban area, and population density. One reason for consolidating these grants was to allow states and localities more flexibility to direct grant resources to those critical assets that warrant additional protection, as determined by a risk assessment.

According to grant application guidelines, grantees must provide a risk assessment for review. The risk assessment must include threat and vulnerability assessments. For each potential target, the vulnerability assessment is to consider factors such as target visibility, its criticality to the jurisdiction, its impact outside the jurisdiction, the potential access of a threat element to the target, the target's population capacity, and the potential for mass casualties. In turn, the risk assessment is supposed to inform a capabilities and a needs assessment to justify expenditures.

---

[9] [http://www.crs.gov/products/browse/is-homelandsecurity.shtml]

[10] The Urban Area Security Initiative Grant Program was first established in the Consolidated Appropriations Resolution, 2003 (P.L. 108-7), in part to address the issue raised by the Commission. Port Security grants were first established in the U.S.A. PATRIOT Act (P.L. 107-56), and continued in the Maritime Transportation Security Act (P.L. 107-295). The Emergency Wartime Supplemental Appropriations Act of 2003 (P.L. 108-76), allowed the Secretary of Homeland Security to provide funding for the protection of critical infrastructure. Under that authority the Secretary provided funds to 14 ports and 25 transit authorities. The Port Security Grants, initially started by the USA PATRIOT Act have been transferred to the Office of State and Local Government Coordination and Preparedness and administered as part of the Urban Areas grant program. The transit grants have continued as Transit System Security Grants, also administered as part of the Urban Areas grant program. These grant programs have been combined to promote comprehensive regional planning and coordination. However, Congress continues to specify appropriations to both transit system grants and port security grants, and other areas like security for intercity bus systems.

For a more thorough discussion of the Commission's recommendations regarding the distribution of funds to states and localities, see CRS Report RL3247, *First Responder Grant Formulas: The 9/11 Commission Recommendation and Other Options for Congressional Action*.

The four primary recommendations related to security of transportation infrastructure — basing resource allocation on risk assessment across all transportation modes, timely implementation of improved "no-fly" and "automatic selectee" lists, use of biometric technology in travel documents and other forms of identification, and giving priority to improving the ability to screen passengers (not just baggage or cargo) for explosives — are all in various stages of implementation already.

According to hearing testimony by a TSA official[11] at a hearing of the Subcommittee on Infrastructure and Border Security of the House Select Committee on Homeland Security (May 12, 2004), TSA will develop over the next several months a sector specific plan covering all transportation modes. This plan will include prioritizing assets that need protection, assessing their vulnerabilities, identifying protective measures, assessing the performance of those protective measures, and prioritizing research and development. Models have been developed for assessing the criticality of a particular transportation asset and for assessing its vulnerability. According to the testimony, these assessment are in progress and, in some cases, build upon earlier assessments performed shortly after September 11 (especially in the rail, transit, and ports sectors). Also mentioned in the testimony are pilot efforts under way to test equipment used to detect trace amounts of explosives on individual passengers. For more discussion of the issues related to transportation security and the how the recommendations of the 911 Commission may impact those issues, see CRS reports listed on the Homeland Security/Border and Transportation Security page of CRS's Congressional Legislative Issue website.[12]

Concluding Remarks

The above discussion indicates that, for some time, federal policy has called for the integration of threat information with vulnerability assessments, and to use risk assessment and risk management to inform the planning for and allocation of resources to protect critical infrastructure. The DHS is supposed to use this approach in coordinating the overall national effort. Sector Specific Agencies are supposed to use it when working with their individual sectors. States and localities are supposed to use it when applying for the Urban Areas, Ports, and Transit System security grants. Also, TSA already has some efforts underway in those more specific areas discussed in the Commission's report regarding improved transportation security. In this regard, the 9/11 Commission's report less breaks new ground than points

---

[11] Stephen McHale, Deputy Administrator, Transportation Security Administration, Testimony before the Subcommittee on Infrastructure and Border Security, House Select Committee on Homeland Security, May 12, 2004. This "deadline" has been repeated by the Undersecretary for Border and Transportation Security, Asa Hutchinson. See, Washington Post article cited above.

[12] [http://www.crs.gov/products/browse/is-homelandsecurity.shtml].

attention to continuing shortcomings in efforts to follow through on prior policy goals and objectives.

Progress to date has been mixed depending on the sector and it is not clear how coordinated this effort has been across sectors. Nor is the allocation of resources transparent enough to know to what extent the allocations actually have been based on risk assessments. Also, Congress continues to appropriate grant funds to specific areas, not necessarily with the benefit of an overall risk mitigation strategy. By giving attention to these issues, the Commission's report may provide some political momentum to speed up implementation in some of these areas. However, with much of the attention focusing on the Commission's recommendations to reorganize the intelligence community, the effect the Commission's report will have on critical infrastructure protection activities remains to be seen. Arguably, the Commission's final recommendation, to regularly assess plans against threats, is to underscore the need to monitor progress and to prevent surprises.