Order Code RL32531

CRS Report for Congress
Received through the CRS Web

Critical Infrastructure Protections: The 9/11 Commission Report and Congressional Response

Updated October 20, 2004

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

Critical Infrastructure Protections: The 9/11 Commission Report and Congressional Response

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.

Two bills have been introduced as legislative vehicles for enacting some or many of the Commission recommendations — S. 2845 and H.R. 10. Both of these bills have passed their respective chambers. Like the Commission's recommendations, those portions of the bills relating to critical infrastructure primarily strengthen or reinforce existing policy and organizational structures, with one exception. The House bill proposed elevating the head of the National Computer Security Division from a Division Chief to an Assistant Secretary position.

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.*

This report will be updated as appropriate.

Contents

Critical Infrastructure Protections: The 9/11 Commission Report and Congressional Response

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 efforts have 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 identifies those recommendations and the Congressional response to them, and briefly discusses the possible impacts 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

---

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

Commission's report, "Strategies for Aviation and Transportation Security"). In this section, the Commission mentioned the Aviation and Transportation Security 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 (as called for by the Aviation and Transportation Security Act), 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]

The Commission was more specific in regard to aviation security, recommending 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.

---

[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.

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.

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 Infrastructure Security 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 is 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]

Congressional Action

In response to the 9/11 Commission's report, Members introduced a number of bills addressing some or all of the Commission's recommendations. Most of these bills take on the issue of reorganizing and reforming the intelligence community. A few address directly or indirectly those Commission recommendations discussed above which relate to critical infrastructure protection.[13] Two bills were chosen as the legislative vehicles: S. 2845 and H.R. 10. Some of the provisions of the other bills have found their way into these two bills as amendments.

---

[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].

[13] These include H.R. 5024 (Pelosi), H.R. 5040 (Shays), H.R. 5082 (Young), H.R. 5121 (Young), H.R. 5132 (Menendez), S. 2774 (McCain/Lieberman), and S. 2884 (Shelby).

S. 2845 passed the Senate October 6, 2004. As introduced the bill primarily addressed intelligence reform. However, on the floor, amendments to the bill expanded coverage to many of the other recommendations of the 9/11 Commission. The provisions most relevant to this report include the requirement, as recommended by the Commission, that the Secretary of Homeland Security develop, implement, and revise as necessary a National Strategy for Transportation Security. The Strategy is to identify transportation assets that, in the interest of national security, must be protected. Those assets span all transportation modes. The Strategy must also develop risk-based priorities for addressing security needs, the assignment of roles and missions across federal, state, local, and private entities, the prioritization of security-related research and development, and budgets to meet the objectives of the Strategy. Also, as recommended by the Commission, the bill set a deadline for this Strategy. The Secretary must provide the Strategy to Congress no later than April 1, 2005, and no less frequently every even numbered year after that.

In addition, the bill reiterates DHS's responsibility under the Homeland Security Act and HSDP-7 to develop a plan that identifies, prioritizes, and coordinates the protection of all critical infrastructures. In slightly different language than that used by the Commission,[14] the bill requires the Secretary of Homeland Security to identify those elements of the nation's critical infrastructure that need protection, develop plans to protect them, and exercise mechanism to enhance preparedness. The Secretary must report to Congress 180 days after enactment, and annually thereafter, the progress being made in assessing the vulnerability and risk associated with the nation's critical infrastructures, the adequacy of the government's plans to protect them, and the readiness of the government to respond.

The bill also provides for the more specific protections aimed at aviation, including expanded use of explosive detection, perimeter security, securing cockpits, and reporting on the efforts to protect aircraft from man-portable air defense systems (i.e. shoulder-fired missiles).

The bill also seeks to streamline federal assistance to states and localities. It establishes an Interagency Committee to coordinate and eliminate duplication in grant programs. It also establishes a Homeland Security Information Clearinghouse to interact with grant recipients. The bill language essentially puts in statute the guidance associated with the current grant program applications listed above. States must submit homeland security plans that include, among other requirements, strategies for mitigating the risks associated with attacks on critical infrastructure and identify protective measures that need to be taken by private owners of critical infrastructure. In addition, the allocation of Urban Area Security Initiative Grant Program funds are to go to localities with a high degree of threat, risk, and vulnerability to their critical infrastructure. The Senate bill modifies, but does not eliminate, the formulae used to distribute the State Homeland Security Grant funds, which the Commission implied should be eliminated.

---

[14] The Commission emphasized the need to reevaluate on a regular basis the terrorist threat and then to assess the adequacy of government plans to protect against and respond to that threat.

H.R. 10 goes beyond the recommendations made by the 9/11 Commission, while remaining silent on others. The bill as introduced includes many of the same specific aviation-related security measures as those added to S. 2485, including expanded explosive detection, perimeter security, and a report on the protecting aircraft from man-portable air defense systems. It does not include provisions relating to the development of a National Strategy for Transportation Security, nor the reiteration of the DHS's responsibilities across all critical infrastructures and associated reporting requirements. It does set a deadline of December 31, 2004 for the National Maritime Transportation Security Plan and the Facility and Vessel Assessments called for in the Maritime Transportation Security Act of 2002 (P.L. 107-295).

In another critical infrastructure-related provision, H.R. 10 also includes the Emergency Securities Response Act of 2004 (Title V, Subtitle G, Chapter 2). This provisions expands the authority of the Securities Exchange Commission and the Secretary of the Treasury to intervene in security markets under their jurisdictions to protect those markets in times of emergencies.

H.R. 10 includes a provision that amends the Homeland Security Act of 2002 by elevating the Division Chief of the National Cybersecurity Division to a position of Assistant Secretary under the Under-Secretary for Information Analysis and Infrastructure Protection. This addresses somewhat the concern of some in the cybersecurity community that the current position was too low in the bureaucracy given their perception of the importance of cybersecurity to national security.

H.R. 10 also includes Title XVIII, Funding for First Responders, which is devoted to modifying the current federal assistance programs. The grants covered by this title include the State Homeland Security Grants, the Urban Area Security Initiative Grants, and the Law Enforcement Terrorism Prevention Grants, and the Citizens Corps Grants. This title requires that the Secretary of Homeland Security develop standard essential capabilities that States and localities should have in place to be adequately prepared for a terrorist attack. These capabilities are to be determined, in part, based upon the most current risk assessment available for the Information Analysis and Infrastructure Protection Directorate, and the types of threat, vulnerability, and consequences with respect to the nation's population and critical infrastructure. Grants are to be awarded to assist states and localities achieve the essential capabilities for first responders.

As currently is the case, states must submit a state homeland security plan which includes a priority list of what the state or locality needs to achieve the essential capabilities noted above. These needs should be prioritized based on threat, vulnerability, and consequences. Allocation of grants is to be prioritized based upon the degree to which the funds would, by virtue of enhancing or preserving essential capabilities, lessen the threat to, vulnerability of, and consequences for persons and critical infrastructure, as determined by a First Responder Grants Board. H.R. 10 establishes the Board, which is made up of top officials of the Department, including the Undersecretary for Information Analysis and Infrastructure Protection.

While the funds for these grants are still focused on first responders, they also still can be spent on protecting critical infrastructure (including the addition of

barriers, fences, and other devices). Also, while the allocation of these grants are to be made primarily based on threat, vulnerability, and consequences (i.e. risk), the bill still guarantees states and other qualifying entities a minimum level of funding. The title does eliminate the grant formula developed by the USA PATRIOT Act. The House bill arguably goes further than the Senate bill in basing the allocation of federal assistance grants on threat, vulnerability, and risk.

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

Similarly, the bills progressing through Congress which deal with 9/11 Commission recommendations primarily reinforce or strengthen current policies and organizational structures regarding critical infrastructure protection, with one exception. H.R. 10 does introduce a substantial organizational change by elevating the Division Chief of the National Cybersecurity Division to that of Assistant Secretary, reporting directly to the Under-Secretary for Information Analysis and Infrastructure Protection.

Progress in identifying critical assets, assessing their vulnerabilities and associated risks, and developing prioritizing cost-effective protective measures to date has been mixed, depending on the sector. Nor is it 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. In the final Homeland Security Appropriations bill (H.R. 4567, P.L 108-334), Congress appropriated $150 million each to port security grants and rail and transit grants, $10 million to intercity bus security grants, and $5 million to trucking grants.

With much of the attention focusing on the Commission's recommendations and Congress's efforts to reorganize the intelligence community, it remains to be seen what effect this activity will have on critical infrastructure protection efforts.