2005

Technical Assistance Briefs: Issue Paper on Critical Infrastructure Protection

NARUC

The National Association of Regulatory Utility Commissioners

Prepared by
The Institute of Public Utilities

April 2005

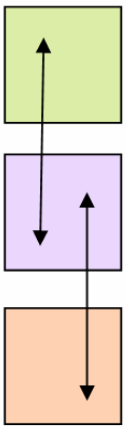
Funded by the U.S. Department of Energy's Office of Electricity and Energy Assurance

TECHNICAL ASSISTANCE BRIEF ON CRITICAL INFRASTRUCTURE PROTECTION

ISSUE PAPER ON CRITICAL INFRASTRUCTURE PROTECTION

NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS
AD HOC COMMITTEE ON CRITICAL INFRASTRUCTURE

APRIL 2005



NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS
1101 Vermont, N.W., Suite 200
Washington, DC 20005, USA
Phone: (202) 898-2200
Fax: (202) 898-2213
admin@naruc.org

NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS
AD HOC COMMITTEE ON CRITICAL INFRASTRUCTURE

Letter from the Chair
Commissioner Connie O. Hughes, New Jersey Board of Public Utilities
March 2005

As Chair of the NARUC Ad Hoc Committee on Critical Infrastructure, I am proud to present to public utility regulators, policymakers, utility industry leaders, and consumers, this landmark series of technical briefs on a complex set of issues pertaining to our nation's critical utility infrastructures. These documents identify key strategies for our consideration as we meet ongoing challenges within each of the electricity, natural gas, water, and telecommunications sectors.

I trust that the documents will enhance the understanding and appreciation of critical infrastructure protection, particularly with respect to the role of state public utility commissions, as well as assist in the development of appropriate policies and strategies in this vital area.

The Committee appreciates and is grateful for the assistance in preparing these reports by Dr. Janice A. Beecher, Institute of Public Utilities at Michigan State University and Dr. James B. Atkins, Regulatory Heuristics. I also acknowledge the support and funding provided by the U.S. Department of Energy's Office of Electricity and Energy Assurance under the leadership of Mr. Alex de Alvarez and assistance of Ms. Alice Lippert. I also thank the National Association of Regulatory Commissioners, the NARUC Staff Subcommittee on Critical Infrastructure, and our other state partners including the National Association of State Energy Officials, the National Conference of State Legislatures and the National Governors Association.

Commissioner Connie O. Hughes
Chair, Ad Hoc Committee on Critical Infrastructure

This Technical Brief (Paper No. 1) is part of a series of reports prepared under the direction of the NARUC Ad Hoc Committee on Critical Infrastructure. Funding for this project was provided to NARUC by the U.S. Department of Energy in cooperation with the National Association of State Energy Officials.

The purpose of these complementary and reinforcing papers is to provide public utility commissioners and other participants in the regulatory policy community with introductory overviews, suggested protocols, and additional resources on critical infrastructure protection issues.

Paper 1. *Issue Paper on Critical Infrastructure Protection.* The federal and state roles in critical infrastructure protection are introduced and explored, with a special focus on the role of the state agencies and public utility commissions.

Paper 2. *Utility and Network Interdependencies: What State Regulators Need to Know.* As explored here, almost all utilities operate networks, and these sector networks are highly interdependent, which in turn relates to consideration of vulnerability and planning which takes on an added dimension of complexity needs, as well as regulatory considerations.

Paper 3. *A Primer on Energy Assurance for Public Utility Commissions.* The primer provides an introduction to energy assurance planning, which broadens traditional energy emergency response and planning to include critical infrastructure protection and energy and fuel shortage mitigation.

Paper 4. *State Government Organizational Issues, Roles, and Policy.* This discussion paper explores state governmental roles with respect to critical infrastructure protection, with a focus on the state public utility commissions and regulatory policy considerations.

Paper 5. *Regional Coordination and Intergovernmental Communication in the Energy Sector.* This paper highlights the importance of regional coordination and communication, focusing in particular on the protocols developed for the Energy Emergency Assurance Coordinators (EEAC) system that has identified state level energy experts for petroleum, gas and electricity.

Paper 6. *Critical Infrastructure Information Sharing Rules: Model Protocols for States.* The paper discusses both federal and state actions to date regarding the sharing of critical infrastructure information and provides a framework for future cooperation and efforts to harmonize information sharing among state commissions, the FERC and the Department of Homeland Security.

Paper 7. *NARUC Inventory on State Energy Assurance Planning.* The paper reports in detail the findings of a 2004 assessment of state commissions regarding energy assurance planning and related policy issues.

Paper 8. *NARUC Inventory on Gas Curtailment Planning.* The paper reports in detail the findings of a 2004 assessment of state commissions regarding gas curtailment planning and related policy issues.

WHAT IS CRITICAL INFRASTRUCTURE PROTECTION (CIP)?

Critical Infrastructure Protection (CIP) is the shared responsibility of the private sector, local and state governments, and the federal government to protect the nation's critical infrastructure. The Homeland Security Act, and the subsequent Presidential strategies on CIP, defined *what* must be done to protect the nation's infrastructure. Many experts believe that America remains largely unprepared to prevent and respond to a catastrophic terrorist attack—even three years after 9/11/01. Many fear that a future attack could result in even greater casualties and more widespread disruption to American lives and the economy. "Critical" infrastructures are those that, if disrupted, would significantly impact public health and safety, the economy, and/or national security. Any prolonged interruption of the supply of basic energy - whether it is electricity, natural gas, or petroleum products - would do considerable harm to the U.S. economy and the American people.

No single government agency, industry group, or company can secure the energy infrastructure. Collaboration at all levels is essential for securing an interdependent infrastructure that is owned, operated, hosted, and regulated by many entities, all of which have limited resources and expertise for infrastructure protection. Voluntary partnerships help leverage resources, facilitate the useful exchange of security-related information, and maximize the effectiveness of infrastructure protection efforts. The U.S. Department of Energy (DOE) is working to coordinate CIP efforts in the energy sector and with private, federal, state, and local partners.

CIP includes proactive activities for protecting physical and cyber systems so vital to the operations of the United States that their incapacity or destruction will seriously weaken national security, economic stability, or public safety. CIP methods and resources deter or prevent attacks against critical infrastructures by people (e.g., terrorists, other criminals, hackers, etc.), by nature (e.g., hurricanes, tornadoes, earthquakes, floods, etc.), and by hazardous materials accidents involving nuclear, biological, or chemical substances. The U.S. is in the process of identifying and prioritizing the most critical assets in each sector of the economy and developing sustainable programs to protect these assets.

WHAT IS THE FEDERAL ROLE IN CIP?

Federal efforts to protect critical infrastructure began well before 9/11/01. Concerns driven by domestic terrorism following the Oklahoma City bombing led to a number of initiatives focusing on weapons of mass destruction (WMD) and task forces were set up to address the threat of terrorist actions. Concerns about Y2K led to a considerable effort to upgrade computer systems and

networks and was a further driving effort that focused on the critical cyber infrastructure. In 1997, President Clinton commissioned a report titled, *Critical Foundations - Protecting America's Infrastructures,* and issued Presidential Decision Directive 63 (PDD 63).

PDD 63 set a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003, and significantly increased security to government systems by the year 2000. To accomplish this goal, PDD 63 established the National Infrastructure Protection Center (NIPC) within the Federal Bureau of Investigation (FBI), which fused representatives from FBI, Department of Defense (DOD), Secret Service, Department of Energy (DOE), Department of Transportation (DOT), and the intelligence community to provide a mechanism for assuring cooperation and information sharing between private industry and federal agencies.[1]

Following the 9/11/01 terrorist attack, the President created the Department of Homeland Security (DHS). The new cabinet-level department incorporated a number of existing federal agencies that had already been working on critical infrastructure protection, e.g., Federal Emergency Management Agency, the Coast Guard and other agencies of DOT, DOE's original Office of Energy Assurance, FBI's National Infrastructure Protection Center (NIPC), the Department of Commerce's Office of Critical Infrastructure Protection and others.

In July 2002, DHS released the *National Strategy for Homeland Security* to mobilize the nation to secure it from terrorist acts. The strategy aligns homeland security functions into six critical mission areas: intelligence and warning, border and transportation security, domestic counter terrorism, protecting critical infrastructure, defending against catastrophic terrorism, and emergency preparedness and response. The first three mission areas focus primarily on preventing terrorist attacks, the next two on reducing the nation's vulnerabilities, and the final one on minimizing the damage and speed recovery from attacks. It is in protecting critical infrastructure that the public utility commissions have an important role.[2]

The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* released in February 2003*,* called upon DOE to establish R&D strategies for the energy industry in concert with DHS and industry. In addition, *The National Strategy to Secure Cyberspace* also called upon DOE to develop best practices and new technology to increase security of DCS/SCADA systems in concert with DHS and industry. In order to fulfill these mandates, DOE, in partnership with the private sector and federal, state and local governments, must develop a comprehensive R&D program that improves the robustness, security, and reliability of the energy infrastructure.

[1] The White House. "Critical Infrastructure Protection," Presidential Directive 63 (May 22, 1998).
[2] The White House. *The National Strategy for Homeland Security: Office of Homeland Security* (July 2002).

In December 2003, the President signed Homeland Security Presidential Directive 7 (HSPD-7), which established the roles and responsibilities of federal organizations involved in CIP. HSPD-7 designates DOE as the federal agency with primary responsibility for facilitating the protection of critical infrastructures and key assets in the energy sector, including the production, refining, storage and distribution of oil and gas, and electric power except for commercial nuclear power facilities. HSPD-8, also signed in December 2003, establishes how federal agencies will prepare for responding to disasters and incidents, and requires that DOE provide federal preparedness assistance to state and local governments and support efforts to ensure that first responders are prepared to respond to major events.

HSPD-7 calls for the creation of a National Infrastructure Protection Plan across all critical sectors of the economy. This plan is a mechanism for establishing a dynamic, integrated national CIP program that reduces the vulnerability of key resources to terrorist attacks. The DOE developed the energy sector input to this plan, which was reviewed by key private and public stakeholders before being delivered to DHS in September 2004. In 2005, the federal government will be asked to refine its plans and begin implementing key features of the plans.

In addition to various activities mandated by DHS and the White House, the federal government has been working with the private sector to share information on threats and warnings. One such effort was the creation of Information Sharing and Analysis Centers (ISACs) for each major sector of the economy. DOE works with both the Energy ISAC, which represents the oil and gas sectors, and the Electricity Sector ISAC (ES-ISAC) to define the roles of DHS, DOE and issues related to energy infrastructure protection.

In January 2005, DOE and DHS formed the Government Coordinating Council (the Council). The Council provides coordination of energy strategies and activities, policy, and communication across government relevant to the protection of the critical infrastructure, and between government and the energy sector to support the nation's homeland security mission. The Council includes participation by DHS, DOE, FERC, DOT, and DOI. The Council acts as the counterpart and partner to the private industry-led Coordinating Councils to plan, implement and execute sector-wide security programs for the nation's energy critical infrastructure.

The DOE also "hosts" the Energy Emergency Assurance Coordinator (EEAC) network composed of state energy offices, public utility organizations, and some state governors' offices. The objectives of the EEAC group are to establish a cooperative communications environment to address energy emergencies or energy supply disruptions; to protect critical energy infrastructure; and to increase federal-state communication.

In February 2005, the Department of Homeland Security issued the Interim National Infrastructure Protection Plan (February 2005).[3] The interim plan emphasizes a risk management framework, prioritization of critical infrastructure protection activities, and an integrated and comprehensive approach to addressing physical, cyber, and human threats.

WHAT IS THE STATE ROLE IN CIP?

States are crucial stakeholders in providing a secure and reliable energy infrastructure for the nation. State agencies are responsible for emergency planning and response, developing energy security and reliability policies and practices, and facilitating energy sector protection activities in conjunction with federal, private sector, and local groups. State governments are the organizations that citizens turn to in times of crisis, and they play a significant role in preventing energy supply crises and mitigating the impacts of those emergencies that do arise. State organizations that play a role in energy sector security and assurance include the following:

State energy offices, represented by the National Association of State Energy Officials (NASEO), typically serve many energy-related functions at the state level, including coordinating responses to energy emergencies, developing state energy emergency plans, and developing practices to improve energy security and reliability at the state-level.

State utility commissions, represented by the National Association of Regulatory Utility Commissioners (NARUC), are government agencies engaged in the regulation of utilities (energy, water, and telecommunications) at the state-level. In this role, these organizations are involved in cost recovery issues (including energy security costs), energy supply curtailment plans, and CIP activities.

Governors' offices and state legislators, represented by the National Governors Association (NGA) and the National Conference of State Legislatures (NCSL), respectively, develop policies that affect energy security and assurance and play a major role in responding to energy emergencies. These state-level decision makers coordinate with federal and industry groups on energy security and emergency issues, and possess emergency authorities which they can exercise to mitigate the impacts of energy crises.

State Homeland Security Directors and their offices coordinate and conduct homeland security activities at the state level, including programs involving infrastructure protection and vulnerability analysis.

State and local emergency management agencies and first responders prepare for and respond to all emergencies, including those with implications for the energy

[3] U.S. Department of Homeland Security. Interim National Infrastructure Protection Plan (February 2005).

infrastructure. These organizations are on the front line of emergency response at the state and local level.

Every state government has designated a primary contact for homeland security matters. These contacts vary significantly by state, ranging from the state director for homeland security to the head of emergency management agencies, state police officials, attorney generals, Lt. Governors and others. This lack of consistency complicates inter-state dialogue and collaboration, which is required since infrastructure critical to one state may not reside in that state or country.

Each state is approaching CIP according to its own unique circumstances. A few examples are provided below to highlight the differences in approach and key agencies involved.

In **Michigan**, the Governor created the Michigan Homeland Protection Board, whose membership consists of directors of the Departments of Military and Veteran Affairs, Civil Rights, Agriculture, Community Health, Environmental Quality, Information Technology and Transportation. The Director of the Michigan State Police is the state's director of Homeland Security. To advise the Board, a Homeland Security Advisory Council was created and under the Council are four Committees: Indications and Warnings, Critical Infrastructure Protection, Response and Health. The Critical Infrastructure Protection Committee is chaired by Michigan Public Service Commission staff.

In **Maine** the Adjutant General is overseeing development of a State Homeland Security Strategic Plan. Maine Public Utilities Commission (PUC) staff serve on or participate with teams identified to develop key plan objectives in support of homeland security efforts. PUC staff have been added to the Maine Emergency Response Team to advise the Governor and Maine Emergency Management Agency on utility-related issues. The Maine PUC has signed an agreement with the FBI NIPC as a secure NIPC InfraGard program member, so that the PUC can assist with dissemination and collection of infrastructure threats, particularly with the State's smaller and more rural utilities. The PUC assists the Adjutant General, State Police, National Guard, and emergency managers in contacting utilities whose infrastructure may be threatened. A small number of PUC staff members are being cleared for access to classified information to facilitate the PUC's role in warning and assessment support.

In **New Jersey**, the Board of Public Utilities, after the 9/11/01 attack, collaborated with the Governor's Office, the New Jersey Domestic Security Preparedness Task Force and the New Jersey State Police Office of Emergency Management with respect to infrastructure security and service recovery. The New Jersey Board of Public Utilities served as the coordinator and facilitator of information from the utilities to the respective groups. A report was filed by four industry specific (energy, telecommunications, cable and water) workgroups that included a self-assessment of infrastructure security provisions and practices and policies. These self-assessments consisted of: 1) a review of existing corporate

response plans; 2) preliminary security best practices for standardization across industries. (These protocols addressed issues such as background checks for employees and contractors, perimeter security, etc); and 3) the review of service recovery protocols to determine adequacy in the event of an attack on the critical utility infrastructure. This report was provided to the Governor in December 2001. Concurrently, the Board ordered that each utility should implement the measures called for in the relevant protocols and refine these security measures as necessary, in conjunction with the New Jersey Domestic Security Preparedness Task Force. Efforts continue in refining state strategies and plans, presently a small number of the Board staff are being cleared for access to classified information to facilitate the Board's role in coordination and support.

In **New York**, the Department of Public Service (DPS) created a Utility Security Team to meet with all the major electric, natural gas and telecommunications utilities to assess security provisions planned following the terrorist attacks. After this review, the team recommended that an independent third party cyber and physical security assessment be conducted on the major telephone (including subsidiaries) and energy utilities. Three of the utilities declined to commit to this plan and were required to hire third-party consultants to conduct security evaluations. As a final check, the DPS is in the process of hiring its own security expert to assess the work done by the third-party firms.

WHAT IS THE PUC ROLE IN CIP?

Traditionally the role of public utility commissions has been to assure a safe, adequate, and reliable supply of regulated services at a reasonable cost. Increasingly, since 9/11, state PUCs have become involved in issues related to the security of the nation's electric, natural gas, telecommunications, and water infrastructures. This is a somewhat natural fit as most if not all public utility commissions have historically been concerned with emergency plans and response for energy issues. Many, if not all, have approved emergency electrical procedures and natural gas curtailment plans. They have dealt with issues affecting emergency 911 calling plans and emergency matters dealing with water utilities. Major power outages caused by storms, tornadoes, or hurricanes have required commission attention under authority to insure reliable service and for recovery of utility costs associated with these events.

State commissions have always been concerned about long-term mitigation strategies (see Exhibit 1), including electric generation reserve margins, long-term capacity plans, fuel diversity, distributed generation, renewable energy, demand management, energy efficiency, natural gas supply contract portfolios, natural gas safety programs, etc. Electric utility tree trimming programs are an example of mitigation efforts designed to reduce outages from fallen tree limbs.

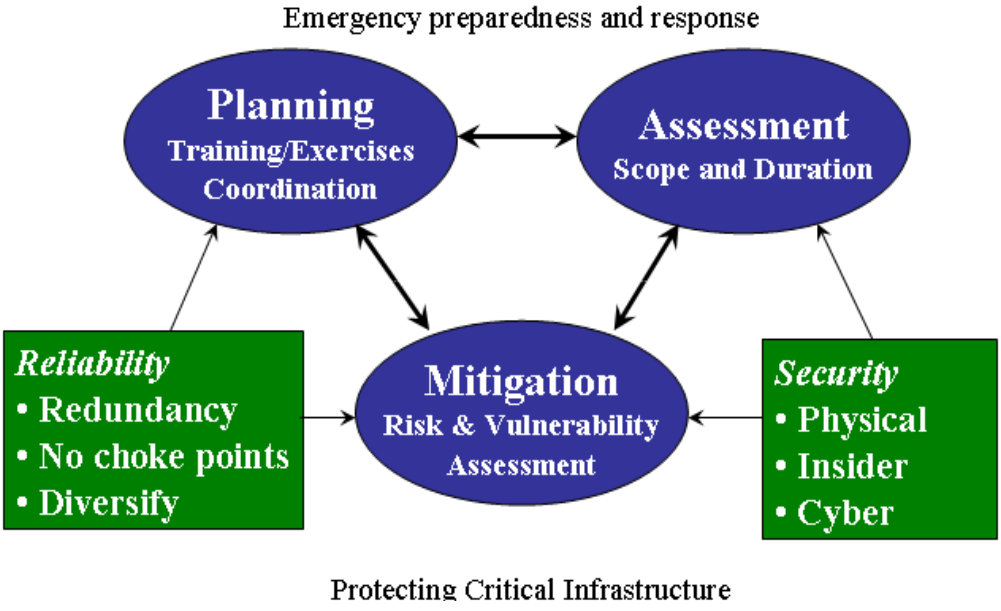


Exhibit 1. Emergency Preparedness and Response.

Source: National Association of State Energy Officials, "Using the Energy Assurance Guidelines," The State Energy Assurance Planning Workshop, Camp Dawson, West Virginia, June 30, 2004.

The security perspective and concerns about terrorism are relatively new to the list of regulatory concerns. Potential threats include physical security, employee security and computer systems security. With the ever-increasing reliance on the Internet and automated control systems, there is a need to be sure these systems are hardened to attacks.

The NARUC Ad Hoc Committee on Critical Infrastructure recognizes that public utility commissions should develop strategies and approaches to assure that their regulated industries take appropriate, cost-effective measures to improve CIP. Many are doing so. This includes identification of policies that may work to inadvertently discourage appropriate risk reduction efforts. Additionally, such an effort should be made in coordination with other state agencies that may have homeland security as their primary charge. The overwhelming majority of the nation's critical infrastructure is owned and operated by the private sector, and there are opportunities for the forging of private-public partnerships on homeland security issues that can strengthen national security.

HOW CAN STATE PUCS PROVIDE FOR CIP?

The following are among some of the areas that commissions should consider and that are subject to further inquiry by the NARUC Ad Hoc Committee on Critical Infrastructure.

Surveys by the National Regulatory Research Institute (NRRI) provided insights on a number of these issues:[4]

- Cost recovery and prudence of investment. A large majority of commissions (83%) do not have guidelines for determining the prudence of security investments: only 15 % have such guidelines and 2 percent are developing them.

- Information disclosure. Most PUC respondents (82 percent) indicated that they offer exception from provision of their Freedom of Information Act for sensitive utility security information.

- Communication/Threats and Warning. Rapid sharing of information and clear communication channels are essential.

- Update Emergency Plans. All commission respondents indicated that they coordinate with other state entities regarding emergency planning and response, with the majority indicating frequent coordination efforts.

- Interdependencies. PUC staff need to understand interdependencies in order to assure a well-developed effort to protect these vital assets.

- Regional Coordination. What may be a critical facility for one state may be located in another state. Because of this there is a clear need for states to engage in regional coordination and response.

The NARUC Committee and Staff Subcommittee will continue to work to address each of these issues to determine recommended courses of action for PUC consideration.

[4] National Regulatory Research Institute, *Survey on Critical Infrastructure Security,* NRRI 04-01 (2004). *Survey conducted in July 2003 (48 states and jurisdictions responded)

APPENDIX: NARUC RESOLUTION ON CRITICAL INFRASTRUCTURE (2003)

WHEREAS, The National Association of Regulatory Utility Commissioners (NARUC) finds that further ensuring the security and reliability of the Nation's critical infrastructures is of the highest public interest due to the risk of terrorism, as well as other natural and technological hazards; *and*

WHEREAS, NARUC has formed the Ad Hoc Committee on Critical Infrastructure to identify appropriate role(s) of regulatory commissions with respect to the security of the Nation's electric, natural gas, petroleum, water and telecommunications infrastructure; *and*

WHEREAS, The Ad Hoc Committee on Critical Infrastructure is responsible for ensuring State Commissions and has the information and tools needed to work with the industries to keep critical infrastructure secure; *and*

WHEREAS, NARUC's Ad Hoc Committee on Critical Infrastructure is committed to continue to work with State Commissions to provide appropriate tools to further address this important issue; *and*

WHEREAS, NARUC has strongly encouraged coordinated security efforts by federal, State and local authorities; *now therefore be it*

RESOLVED, That the National Association of Regulatory Utility Commissioners (NARUC), convened in its November 2003 Convention in Atlanta, Georgia, recommends that State Commissions address the matter of how critical infrastructure or systems are being protected, how this protection is being financed and sensitive information is protected from disclosure; *and be it further*

RESOLVED, That NARUC recommends that State Commissions initiate a dialogue with stakeholders not later than the end of the first quarter of 2004 to address these issues. State Commissions may reference forthcoming cost recovery resource materials to be issued by the Critical Infrastructure Committee. This dialogue could take any number of forms ranging from an order issued by the commission at its own motion to open a docket and commence a hearing to less formal approaches such as informational meetings. Other State agencies that have a role in critical infrastructure protection should be included in this dialogue as appropriate; *and be it further*

RESOLVED, That NARUC urges the U.S. Department of Energy, the U.S. Department of Homeland Security, the Federal Energy Regulatory Commission, the Federal Communications Commission, Environmental Protection Agency and other key federal agencies to support State actions by providing assistance and guidance in protection of critical infrastructure.

Sponsored by the Ad Hoc Committee on Critical Infrastructure. Recommended by the NARUC Board of Directors November 18, 2003. Adopted by NARUC November 19, 2003

FOR FURTHER READING

National Regulatory Research Institute, Critical Infrastructure Clearinghouse.

National Council of State Legislatures. *A Call for State Action to Protect and Strengthen Our Democracy* (Interim Report, July 2002).

U.S. Department of Homeland Security. *Interim National Infrastructure Protection Plan* (February 2005).

U.S. General Accounting Office. *Critical Infrastructure Protection: Significant Challenges Need to be Addressed* (July 24, 2002).

The White House. "Critical Infrastructure Identification, Prioritization, and Protection," Homeland Security Presidential Directive SPD-7 (December 17, 2003).

The White House. "Critical Infrastructure Protection," Presidential Directive 63 (May 22, 1998).

The White House. *The National Strategy for Homeland Security: Office of Homeland Security* (July 2002).

The White House. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (February 2003).

The White House. *The National Strategy to Secure Cyberspace* (July 2003).