

TOP PRIORITIES FOR PROTECTING THE NATION'S INFRASTRUCTURE

A Report of the Working Group on Infrastructure Protection and Internal Security¹

Michael Scardaville, Working Group Rapporteur

The aftermath of the September 11, 2001, attacks on the Pentagon and the World Trade Center illustrates the high vulnerability of America's infrastructure to terrorist attacks and the massive consequences of not protecting it. While the terrorists were able to utilize deficiencies in America's overall approach to intelligence sharing and aviation security, similar vulnerabilities exist in every infrastructure vital to the security, economy, and survival of the nation, such as computer networks, energy supplies, transportation, and the global positioning satellite system.

Today, most Americans recognize that responsibility for protecting critical infrastructure from terrorism does not rest with any one level of government. Structural, cultural, institutional, and statutory changes are needed to secure the nation's infrastructure so that terrorists have less incentive to attack them and the nation can respond quickly if they do. Primarily, the success of efforts to defend and protect

-
1. The members of the Working Group on Infrastructure Protection and Internal Security are The Honorable Carol Hallett, President and CEO of the Air Transport Association; The Honorable Frank Keating, Governor of Oklahoma; Jules McNeff, Director, U.S. GPS Industry Council, with SAIC; Col. Joseph Muckerman, USA (Ret.), former Director of Emergency Management, Office of the Secretary of Defense; Captain Bruce Stubbs, USCG (Ret.), Technical Director, Theater Air Defense, Systems Engineering Group, Anteon Corporation; Thomas L. Varney, Director of Technology Assurance and Security, McDonald's Corporation; and The Honorable Pete Wilson, former Governor of California. The following individuals contributed to this report in an advisory capacity: Dr. Billy Cook, MTS Technologies, Inc.; Richard J. Doubrava, Managing Director, Security, Air Transport Association; Rob Houseman, Counsel, Bracewell and Patterson; John M. Meenan, Senior Vice President, Industry Policy, Air Transport Association; Edward A. Merlis, Senior Vice President, Legislative and International Affairs, Air Transport Association; Robert W. Poole, Jr., Director of Transportation Studies, Reason Public Policy Institute; John Powers, Executive Director, President's Commission on Critical Infrastructure Protection; Kenneth P. Quinn, Partner, Pillsbury Winthrop LLP; Scott Rayder, Director of Government Relations, Consortium for Ocean Research; Maureen Sirhal, reporter, *Technology Daily*; and Gary Tyler, Director, Matcom Corporation.

infrastructure will rest on the ability of Federal, State, and Local governments to cooperate with each other and the private sector.

In this regard, the Working Group on Infrastructure Protection and Internal Security reviewed various commission reports and government studies² and developed a list of top new priorities for protecting America's critical infrastructure in the near term. The following priorities (1) represent new approaches to protecting the nation's infrastructure and (2), if implemented, will enhance Federal, State, and Local efforts.

- **Priority #1: Reorganize by presidential directive all Federal agencies involved in protecting infrastructure.** The President should issue a new directive to reorganize the federal government to enhance its effectiveness in protecting the American homeland. The new National Security Presidential Directive (NSPD) should correct the failure of President Bill Clinton's directive, PDD-63, to create a system of oversight and establish a clear chain of command for protecting infrastructure. PDD-63 merely assigned responsibilities for addressing the security of 12 nationally important infrastructure sectors to various Federal agencies.
- **Priority #2: Designate the Global Positioning System (GPS) frequencies and network as critical national infrastructure.** The GPS satellite network is now an enabling system for other vital infrastructure, such as telecommunications, yet it has not been designated as a vital asset. It should be added to the current list of vital national infrastructure, and responsibility for ensuring its security should reside with the U.S. Department of Defense.
- **Priority #3: Facilitate communication on infrastructure issues between the new Office of Homeland Security (OHS) and State and Local officials.** State and Local governments play a vital role in protecting infrastructure within their jurisdictions, but they cannot do so without effective communication with the Federal government.
- **Priority #4: Enhance the private sector's role in infrastructure protection.** Market forces provide a strong incentive for the private sector to protect infrastructure that it owns and operates; government should ensure both that it does not inhibit an industry's efforts to do so and that business has the tools it needs for that protection.
- **Priority #5: Institute new rules to monitor more closely who or what is entering America's airports and seaports.** Since September 11, new efforts to increase security at these vital transportation nodes have focused largely on

2. For a summary of recommendations from prior commissions and studies that remain unimplemented, see the table at the end of this chapter. The status of post-September 11 legislative efforts may be found in the Appendix.

manpower concerns, such as federalizing baggage handlers. However, a comprehensive program for airport and seaport security requires that tighter controls must be implemented to monitor who and what passes through them.

- **Priority #6: Secure all Federal networks and information systems.** The U.S. General Accounting Office has reported that information systems vital to Federal operations are not being sufficiently protected. Without tighter security, Federal networks cannot guarantee continuity of operations. Federal agencies' technology purchasing guidelines must be revised to place a premium on security. The Administration should also explore how to make Internet-based networks more secure, in addition to solutions that would rely on a federal government intranet separate from the Internet (GOVNET).
- **Priority #7: Accelerate government compliance with the Nuclear Waste Policy Act.** Despite legislation requiring it to do so, the U.S. Department of Energy has not uniformly secured the nation's nuclear waste, which could be used by terrorists to build radiologic weapons.

PRIORITY #1: REORGANIZE BY PRESIDENTIAL DIRECTIVE ALL FEDERAL AGENCIES INVOLVED IN PROTECTING INFRASTRUCTURE.

Planning for infrastructure protection should cover all facilities and utilities that are vital to the nation's security and economic well-being. President George W. Bush, as Chief Executive of the Federal government, should reorganize the agencies involved in infrastructure protection to enhance coordination and implementation of Federal

Table 1

**Lead Agencies Assigned to Vital Infrastructure
by President Clinton in PDD-63**

Department / Lead Agency	Infrastructure Sector/Function
Commerce	Information and Communications
Defense	Defense
Director of Central Intelligence	Intelligence
Energy	Electric Power, Gas, and Oil
Environmental Protection Agency	Water
Federal Emergency Management Agency	Emergency Fire Service
Health and Human Services	Emergency Medicine
Justice	Emergency Law Enforcement
Justice	Law Enforcement and International Security
State	Foreign Affairs
Transportation	Transportation
Treasury	Banking and Finance

efforts to protect that infrastructure from terrorist attack and to establish oversight and accountability.

PDD-63. Many of the problems the Federal government currently faces in protecting critical infrastructure stem from a May 1998 Presidential Decision Directive issued by President Clinton titled “Critical Infrastructure Protection” (PDD-63). This presidential directive attempted to address the problem of information warfare and cyberterrorism. It tasked specific agencies with responsibility for a particular infrastructure. (See Table 1.)

PDD-63 was based on recommendations from the President’s Commission on Critical Infrastructure Protection in 1997. However, it has three major flaws that inhibit the development of an effective infrastructure protection policy:

1. Lack of accountability and oversight. PDD-63 tasked specific agencies with responsibility for infrastructure protection. But it did not establish an oversight mechanism to ensure that these departments or agencies would give sufficient attention to this mission. It did not, for example, mandate sufficient reporting requirements or timetables.
2. No clear chain of command. PDD-63 did not establish a clear chain of command for decision-making within the Federal government. Though it designated the lead agencies for each infrastructure it considered essential to the nation’s operations and made a National Coordinator responsible for synchronizing Federal efforts, it failed to explain how the relationship between the National Coordinator and the lead agencies would work.
3. Misdirected responsibilities. PDD-63 also gave responsibility for some functions to the wrong agency, such as placing the National Information Protection Center (NIPC) under the Federal Bureau of Investigation (FBI) and gave it the often conflicting missions of information sharing and law enforcement. In addition, it ignored the advantages that the Coast Guard could offer maritime security.³

Time for a New Presidential Directive. President Bush recently took a good first step to correct these deficiencies. On October 9, 2001, he appointed former National Coordinator for Security, Infrastructure Protection and Counter-Terrorism Richard A. Clarke as Special Adviser to the President for Cyber Space Security. The following week, the President issued Executive Order 13231 on “Critical Infrastructure Protection in the Information Age”⁴ to create the President’s Critical Infrastructure Protection Board, with the Special Adviser to the President for Cyber Space Security as its chairman. It also created the National Infrastructure Advisory

3. See also chapter on Military Operations.

4. See *Federal Register*, Vol. 66, No. 202, October 18, 2001, pp. 53063–53071.

Council, which includes private-sector and State and Local representatives and reports to the Critical Infrastructure Protection Board.

The purpose of the new board is to “recommend policies and coordinate programs for protecting information systems.” In this capacity, it is responsible for coordinating actions of Sector Liaison Officials in most of the Federal lead agencies. While this will improve oversight of cyber security efforts, clear and regular reporting requirements are still needed. The Board also is directed to make recommendations to the Office of Management and Budget (OMB) on Federal agency budgets dealing with cyber security in coordination with the Office of Homeland Security. This directive will improve both oversight and the budgetary chain of command for cyber security efforts.

While the President’s recent actions are a good first step, further actions need to be taken to address a broader spectrum of infrastructure that is vital to national operations beyond information systems. To correct PDD–63’s remaining deficiencies, President Bush should issue a National Security Presidential Directive (NSPD) that involves the following key steps:

Key Step #1. The President should require the Office of Homeland Security to provide annual assessments of Federal efforts on protecting vital infrastructure. Though PDD–63 designated lead agencies to be held responsible for protecting vital infrastructure, it failed to implement effective oversight. As a first step in remedying this deficiency, President Bush established the OHS to “develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks.”

Further steps are needed. For example, the NSPD should mandate that Sector Liaison Officials report as soon as possible, and thereafter annually, to the Director of OHS, the Assistant to the President for Homeland Security, on the status of security for infrastructure under their jurisdiction. These reports should include an assessment of infrastructure vulnerability (further discussed in the chapter on Intelligence and Law Enforcement), initiatives to promote security (including cross-agency efforts), progress on implementing current protection programs, private-sector cooperation, research and development on infrastructure security, and a list of priority actions for the next budget year. Such information would enable the Federal government to develop a more realistic national plan on infrastructure protection and facilitate White House oversight of infrastructure protection efforts.

The OHS Director should compile the Sector Liaisons’ reports into one assessment of Federal infrastructure protection programs to give to the President and Congress. Portions of the report dealing with cyber security should also be delivered to the President’s Critical Infrastructure Protection Board. Such oversight will ensure

that Federal agencies are focusing on this mission and are not compromising infrastructure protection to pursue other bureaucratic interests.

Key Step #2. The President's NSPD should establish a chain of command for Federal planning in core homeland defense areas. The President should task the Director of OHS with developing a plan for federal infrastructure protection efforts that establishes a clear chain of command.

Working with the States and Private Sector. The Director of OHS should consult with the heads of Federal agencies with infrastructure protection missions and Sector Liaison Officials to ascertain the critical weaknesses in infrastructure. Sector Liaison Officials, sector coordinators or Information Sharing and Analysis Centers (ISACs) when available, and the National Infrastructure Advisory Council (NIAC) should monitor and communicate private sector concerns.

The OHS should appoint a staff member or person from an appropriate lead agency to work with the states to develop their individual inventories of infrastructure at risk.⁵ The Federal government and State and Local agencies all have a stake in compiling an accurate inventory of vulnerable assets. It would be extremely difficult to coordinate Federal, State, and Local planning without one common vulnerability assessment to use as a model. By determining which areas need to be improved immediately and which could be addressed at a later date, such an inventory could assist governments in developing more effective infrastructure protection programs.

Federal agencies should continue to manage relations with private-sector industry through the Sector Liaison Officials. The OHS should hold these officials accountable by establishing clear reporting requirements.

Working with Congress. The OHS has been criticized as weak because it lacks the authority to formally approve budget requests and agency legislative proposals, as well as government-wide policy on homeland security. Granting the OHS such authority would require a statutory change, but the President can increase the OHS's voice in this process informally through presidential directions.

President Bush should create a Cabinet Council for homeland defense policy modeled after those used by President Ronald Reagan for various issues. All federal homeland defense policy should be discussed in this forum. The Cabinet Council should be chaired by the President. When the President is not in attendance, the Vice President should preside as chairman. The Assistant to the President for Homeland Security should function as executive officer, carrying out communica-

5. See discussion on national threat assessment in chapter on Intelligence and Law Enforcement.

tions and acting as the key contact point between the Cabinet Council members and the White House.

At the first meeting of this Cabinet Council, President Bush should make clear that the Director of OHS speaks for him in his absence.⁶ While not as formal and direct as statutory authority, this forum would increase the OHS Director's role in policymaking in accord with his mandate to coordinate Federal policy. By having a greater say in agency homeland security policy, the Director would indirectly influence budget requests and legislative proposals associated with those policies.

Key Step #3. The President should move the position of National Coordinator for Security, Infrastructure Protection and Counter-Terrorism into the OHS.

PDD-63 created the position of National Coordinator for Security, Infrastructure Protection and Counter-Terrorism in the National Security Council (NSC), under the National Security Adviser. The National Coordinator, a now-vacant position, is tasked with coordinating Federal efforts for infrastructure protection, a role similar to that of the new Assistant to the President for Homeland Security. The Office of Homeland Security is responsible for coordinating national policy on homeland security, of which infrastructure protection is one part. In order to avoid creating redundant structures in both the OHS and the NSC, the National Coordinator position should be moved to OHS and report to the OHS Director, the Assistant to the President for Homeland Security. The staff office created to support the National Coordinator, the Critical Infrastructure Assurance Office (CIAO), should also be moved to the OHS from the Department of Commerce. This office was created as a policy coordinating body, not a policy implementation office, and thus belongs in the new OHS.

Key Step #4. The President should move the National Information Protection Center (NIPC) out of the FBI. PDD-63 authorized the FBI to expand its warning and information-sharing efforts by creating the NIPC as a "national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity."

This dual-track mission undermines cooperation with the private sector on information sharing. Though the NIPC's information-sharing mechanisms work rather well, many in the private sector remain cautious in sharing such information as network intrusions with the Center because of its concurrent law enforcement role. Businesses have no way of knowing whether the information they share about network security could be used to build a criminal case against them. Further, the

6. For a more in-depth discussion of the Cabinet Council, see Alvin S. Felzenberg, *The Keys to a Successful Presidency* (Washington, D.C.: The Heritage Foundation, 2000), Chapter 4.

FBI's operational guidelines encumber the work of the NIPC—for example, by restricting access to foreign intelligence.

Protection of computer infrastructure would be facilitated more through cooperation with the private sector than through investigations. Moving the NIPC out of the FBI would increase the industry's willingness to cooperate. The NIPC should, for the time being, be placed in the Department of Commerce. PDD-63 designated the Commerce Department as lead agency for information technology and the communication industry, and moving the NIPC to Commerce will complement this mission. Further, the Commerce Department has significant experience working with the hi-tech industry and implementing policy, both through the National Telecommunications and Information Agency (NTIA), which administers the department's responsibilities under PDD-63, and the Technology Administration.

If Congress passes legislation creating a permanent Federal agency for homeland security, as suggested by the Hart-Rudman Commission and proposed by Representative William (Mac) Thornberry (R-TX) and Senator Joseph Lieberman (D-CT), consideration should be given to moving the NIPC to this agency to highlight the vital nature of secure information systems.

The relocated Center also should forge a consultative and information-sharing relationship with the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University in Pittsburgh. This federally funded program operates as a private-sector clearinghouse for network security and provides services similar to those of the NIPC. Once the NIPC is removed from the law enforcement purview, it will be easier to forge a cooperative relationship with CERT and other private-sector counterparts.

Key Step #5. The President should assign the Coast Guard as lead agency for maritime homeland security. PDD-63 designated the Department of Transportation (DOT) as the lead agency for all transportation infrastructure. Within the DOT, the Coast Guard should have responsibility for protecting coastal transportation. The Coast Guard is well equipped to develop and execute a national strategy for maritime security in cooperation with the OHS. It maintains unique defense, law enforcement, intelligence, and port management authorities and capabilities.

The Commandant of the Coast Guard should work with State and Local port authorities, as well as the Immigration and Naturalization Service and the U.S. Customs Service, to develop Port Security Task Forces in every U.S. port.⁷ Each task force should be responsible for developing each port's own security plan and conducting threat and vulnerability assessments. Members of these groups should

7. For more on the role of INS and Customs, see chapter on Intelligence and Law Enforcement.

include representatives from Federal, State, and Local agencies as well as representatives of private-sector participants in that port.

Key Step #6. The President should create a Center for Interagency Maritime Intelligence and Communications. The Intelligence Community, law enforcement agencies (LEAs), and the private sector regularly obtain information vital to port security. However, no uniform mechanism exists for coordinating this information and delivering it to the owners and operators of U.S. ports. A system should be implemented through a new Center for Interagency Maritime Intelligence and Communications (CIMIC) to ensure that intelligence is delivered to the owners/operators in a way that allows them to respond with appropriate security measures. The Center should be located in the Coast Guard Intelligence Coordination Center (CGICC) in Suitland, Maryland, which manages the collection and distribution of intelligence from all Federal sources for the Coast Guard and represents it in inter-agency intelligence functions.

CGICC's information-sharing and cooperative culture makes it the appropriate place to build the new interagency center. CIMIC should be staffed with representatives of the intelligence and law enforcement communities that are active in maritime security. Current databases should be networked so that decision-makers and operational commanders can respond quickly to an emerging threat.⁸

PRIORITY #2: DESIGNATE THE GPS FREQUENCIES AND NETWORK AS CRITICAL NATIONAL INFRASTRUCTURE.

PDD-63 did not include the Global Positioning System (GPS) in the list of critical infrastructure. GPS is a space-based positioning, navigation, and timing system developed by the Department of Defense for both defense and civilian applications. Like computer networks, GPS is now integrated into the operations of other forms of telecommunications and electronic infrastructure, and public and private-sector operations critical to national security and economic stability increasingly rely on it. The telecommunications industry relies on GPS for time and frequency synchronization. The national electric grid relies on GPS to ensure line stability and find disruptions. The financial sector employs GPS timing to synchronize its encrypted computer networks. The transportation industry relies increasingly on GPS for navigational purposes.

GPS is vulnerable because it uses a very low-power signal that can be corrupted or interrupted, causing loss of information. Access to the GPS network can be disrupted in a number of ways. Russia is actively marketing handheld GPS jamming

8. For additional discussion, see chapter on Intelligence and Law Enforcement and chapter on Military Operations.

equipment that can block receiving equipment for up to 120 miles.⁹ The proliferation of ballistic missile technology presents a similar threat to the GPS satellite system. State sponsors of terrorism such as Iraq, Iran, and North Korea already possess the missile technology to mount an attack on the system, and could do so with either conventional or nuclear weapons. Because GPS networks, as well as the commercial satellite assets on which GPS relies, are critical to homeland security, the President should take the following steps:

Key Step #1. The President should include the GPS as infrastructure critical to homeland security in the NSPD and create a national program office to manage it. The program office should be modeled loosely after the early Atomic Energy Commission and consist of a council of members appointed by the President and a small staff of senior government personnel who coordinate GPS policy between Federal agencies, Congress, State and Local agencies, and the private sector.

Key Step #2. The President should assign the Department of Defense as the lead agency for GPS. The Department of Defense developed GPS, and the system serves vital national security purposes. The civil and economic value it provides are products of the Pentagon's decision to make the system publicly available. As a result, the Defense Department should be made responsible for coordinating GPS security with private-sector stakeholders and other federal agencies.

Key Step #3. The President should issue new directives to amend existing ones on critical infrastructure to include GPS. A number of existing directives on infrastructure protection, including Executive Order 13231, "Critical Infrastructure in the Information Age," issued by President Bush on October 18, 2001, do not include GPS in the list of programs they cover. In order for infrastructure protection to apply also to GPS, the President should issue new directives amending the earlier orders' lists of critical infrastructure to include GPS.

Key Step #4. The Department of Defense should deploy a more secure GPS network. The President should direct the Department of Defense—with support from the Office of Science and Technology Policy, the National Security Council, and the Office of Management and Budget—to accelerate modification of GPS satellites currently in production to include more robust signals. It should begin launching these satellites at an increased rate to augment the fragile constellation currently in operation and to establish a larger constellation over time (some 30 to 36 satellites).

9. The availability of this jamming equipment was highlighted in the Report of the Commission to Assess United States National Security Space Management and Organization (Rumsfeld Commission), released on January 11, 2001.

Additional satellites with stronger, better designed signals would increase availability and ensure operations by providing a more robust signal structure that is considerably less vulnerable to jamming. Consideration should be given to flying a mixed constellation of commodity service and specialized satellites to improve system affordability, operability, and robustness. Immediate planning is necessary to begin acquiring additional satellites to sustain a larger constellation. In the interim, the Office of Science and Technology Policy and Coordination, with the National Security Council, should place greater emphasis on developing means to protect satellite assets, particularly the GPS network.

PRIORITY #3: FACILITATE COMMUNICATION ON INFRASTRUCTURE ISSUES BETWEEN OHS AND STATE AND LOCAL OFFICIALS.

Recent events illustrate that, faced with a potential threat to infrastructure, accurate communication between State and Federal officials is critical. In November 2001, for example, the FBI warned California Governor Gray Davis that it had “uncorroborated information” that a number of the state’s bridges could come under attack. Governor Davis then issued a warning to Californians that there was “credible evidence” specific bridges might be attacked. The public announcement made an attack on specific infrastructure seem imminent. Clear communication between Federal, State, and Local officials about threats to critical infrastructure is vital.

Greater intelligence sharing also is hampered by public meeting laws in many localities. Such laws require State or Local governing bodies to make the proceedings of their meetings public. This transparency means that such venues are not conducive to discussions of classified information about risks to infrastructure; vital intelligence sources could be put at risk.

While the Office of Homeland Security is responsible for coordinating with State and Local agencies on detection, preparedness, prevention, and protection missions, action will be required at all levels of government to enhance cooperation. In addition to the national alert and warning system discussed in the chapter on Intelligence and Law Enforcement, the following actions should be taken:

Key Step #1. States should review their public meeting and disclosure laws to guarantee that classified information will not be compromised in such forums. While Federal agencies will need to share more information with State and Local agencies on suspected terrorists, potential attacks, and vulnerabilities, State and Local legislatures must make sure this information does not fall into the wrong hands. Maximum transparency should be encouraged, but current laws allow the public to attend meetings at which classified information would be exchanged, or require govern-

ment to make the proceedings of those meetings public. Where such potential exists, Local and State laws should be amended to protect secret information regarding infrastructure.

Key Step #2. The Office of Homeland Security should conduct government-wide response exercises for infrastructure attack scenarios. The response exercises should include all levels of government, from Washington to local town offices. Such exercises would allow the OHS to determine other areas where communications may be deficient, testing the nation's ability to respond to an attack. Such exercises have proven valuable for national security planning in the past and could offer similar value for homeland security. The 1978 "Nifty Nugget" exercise identified numerous communications and other gaps in American mobilization planning, resulting in a restructuring of Department of Defense transportation commands. This restructuring proved successful in 1991 when the U.S. Transportation Command (USTRANSCOM) mobilized for Operation Desert Storm. OHS should learn from DOD's experience in conducting such large-scale exercises and make plans to simulate a simultaneous attack on different infrastructures.

PRIORITY #4: ENHANCE THE PRIVATE SECTOR'S ROLE IN INFRASTRUCTURE PROTECTION.

Most of America's critical infrastructure is owned or operated by the private sector. The White House strives to include the private sector in its policymaking decisions through the National Infrastructure Advisory Council (NIAC). OHS also has hired a number of workers from industry, on a temporary basis, to help develop new policies. The private sector is a vital and reliable partner, because bottom lines and consumer and shareholder confidence are strong incentives to take steps to protect their infrastructure. Yet legal concerns and a lack of detailed information can limit the extent to which the private sector can be involved in the Federal government's efforts.

In addition to moving the National Information Protection Center out of the FBI, the Federal government should take the following actions:

Key Step #1. Congress should remove legislative roadblocks to closer communications with industry.

Freedom of Information Act (FOIA) exemptions. The Administration should work with Congress to include FOIA exemptions in authorization legislation for Federal agencies that deal with information on infrastructure from the private sector. Many private firms are reluctant to provide extensive information on vulnerability or intrusion because they fear that this information could become

public. Release of such information could adversely affect public or shareholder confidence. Similarly, competitors could use FOIA requests to gain information on company practices or systems. These fears are a major roadblock to a dialogue with the private sector. Enabling legislation for each lead agency should include FOIA exemptions for businesses that cooperate in efforts to assess threats to infrastructure.

Narrow antitrust exemptions. Congress should provide narrow antitrust exemptions for companies that share information on infrastructure protection. When corporations work together, concerns inevitably arise that they are trying to subvert the market. Antitrust laws, which try to prevent such practices as price fixing and market division, also inhibit companies from sharing information on the vulnerability of their infrastructure or the means to protect it. Cooperation on protecting critical infrastructure should be exempt from antitrust laws to protect companies that share information from unjust lawsuits. Similarly, independent private-sector mechanisms for sharing information, known as Information Sharing and Analysis Centers (ISACs), should be exempt from antitrust laws in this area.

It should be noted that the 105th Congress adopted similar legislation in the Information Readiness Disclosure Act (P.L. 105–271), signed into law on October 19, 1998, to exempt from antitrust laws any information-sharing on Y2K preparedness. In adopting the Act, Congress recognized the need to provide antitrust exemptions in areas in which public safety and national civil and government operations are concerned. This precedent should be applied to homeland security applications.

Addressing liability concerns. Legislative action should be taken to reduce liability for operators who adopt best-practices security. Such legislation should resemble the protective structure provided to consumers in the Electronic Funds Transfer Act (15 U.S.C. Sec. 1693). Congress should hear testimony on this from operators, insurance companies, and Sector Liaison Officials to establish a framework for infrastructure protection. Reducing the liability of service providers that adopt strict security measures in the event of a terrorist attack would add another incentive for businesses to adopt new standards of security and to share intrusion information.

Key Step #2. Lead Federal agencies should develop new security standards for industry.

Although security standards in the aviation industry received the most attention after September 11, a similar lack of standards exists in most infrastructure sectors. The President should direct the lead agency heads and Sector Liaison Officials for each vital infrastructure to work with the private sector to develop security standards and to determine how best to enforce them. Federal agencies should support voluntary standards that industry will be willing to adopt with federal oversight. Sector Liaison Officials should report annually to Congress and the President through the Assistant to the President for Homeland Security on the status of voluntary implementation of these standards.

Each lead agency also should publish a biannual “Honor Roll” of the top 100 operators that implement the new security standards to highlight their efforts. This program would create a competitive atmosphere in industry to adopt the most comprehensive security systems; potential customers, investors, and insurers would likely utilize such a list when deciding whether to do business with a prospective provider. A flexible free market, as opposed to a rigid bureaucracy, would serve to regulate the industry. However, if a standard vital to national homeland security proves unpopular, direct regulation with penalties for failing to comply may be necessary.

Key Step #3. Lead Federal agencies should create risk assessment programs for the private sector. Federal agencies also should assist each infrastructure sector in developing its own risk, vulnerability, and survivability assessment programs. Though the government can advise owners and operators of infrastructure of a suspected threat, it cannot assess the risk, vulnerability, or survivability of each asset. Lead agencies should develop a best-practices model for the private sector that enables them to conduct more accurate risk, vulnerability, and survivability assessments. This model would allow industry to address security necessities by meeting a set of performance standards instead of firm government specifications. In developing these models, the head of each lead agency should use the Defense Department’s internal assessment program as a guide.

Key Step #4. Congress should remove tax penalties that make it more difficult for the private sector to invest in security. Congress should revise the tax code to allow infrastructure owners to deduct the full cost of security-related spending in the year such expenses are incurred. At present, industry is only allowed to depreciate its spending for security-related purchases, often over an extended period. As a result, this creates a tax on investment spending, increasing the effective cost. Since private industry must keep the bottom line in mind, increased costs create a hurdle to private-sector spending on security. Allowing infrastructure industries to write off security spending all at once will reduce these costs, thereby improving the bottom line for companies investing in security.

PRIORITY #5: INSTITUTE NEW RULES TO MONITOR MORE CLOSELY WHO OR WHAT IS ENTERING AMERICA’S AIRPORTS AND SEAPORTS.

According to the Department of Transportation, 211,000 ships entered U.S. waters in 2000. Air traffic between the United States and the rest of the world in any one month can exceed 11 million passengers and over 700,000 tons of freight. Yet beyond the consular visa application process, there are few government programs to

monitor foreign passenger traffic for potential terrorists. And only 3 percent of shipping containers that enter the United States are inspected after they enter a port. Clearly, a more robust means for monitoring such traffic without interfering with international commerce or travel is key to protecting the nation's infrastructure.

To further protect the nation's airports and seaports:

Key Step #1. The FAA should issue new regulations and develop a system to assure that airlines are preventing terrorists from boarding an aircraft. An interagency office, under the Department of Transportation with oversight from OHS, should be responsible for developing a system to cross-check airline reservations with government-wide databases of known and suspected terrorists.¹⁰ This should be done in real time using advanced virtual technology that can collate data from a number of databases into one source.

After this technology is in place, the FAA should require airlines to use this system, which would alert ticket counter or gate employees that a suspected terrorist may be planning to board a flight. The new technology would then inform law enforcement officials and airport security, and action could be taken before the suspect boards the aircraft and the flight is cleared for takeoff. In practice, this program should function similarly to that of the Advanced Passenger Information System (APIS), which is administered by Customs, the Immigration and Naturalization Service (INS), and the Animal Plant Health Inspection Service (APHIS). Under the APIS program, which all airlines are now required to use, passenger manifests for all flights originating outside the United States must be provided before the flights arrive, to be checked for any illicit activity or suspected terrorists.

The new system of cross-checking airline reservations with government-wide databases would accomplish a similar function for all aircraft regardless of point of departure, and in real time. In order to protect Americans' freedoms, the system should not collect information on passengers' travel habits and should share only limited information (such as a warning to put a hold on a ticket) with airlines.

Key Step #2. The Administration should create an interagency center to analyze data on people and products entering the United States by sea. This interagency center, which should be managed by the new Center for Interagency Maritime Intelligence and Communications (CIMIC),¹¹ would cross-check passenger, crew, and cargo manifests of all vessels entering American territorial waters with all Federal watch lists of suspected and known terrorists before a ship is allowed to enter port.¹²

10. For a discussion on how federal agencies can better share database information, see chapter on Intelligence and Law Enforcement.

11. As discussed in Priority #1.

12. See chapter on Military Operations.

Like the system discussed above, the new center would have to use virtual office technology to check manifests against the numerous federal databases. However, it would not have to operate under the strict time and operational constraints that the airline system faces. Suspected terrorists attempting to enter the United States on an airline or to ship weapons by air would have to be intercepted before departure for two reasons: the relatively short amount of time it takes for a modern airliner to reach its destination and the limited number of options available in intercepting a passenger during the flight. Traveling by ship takes significantly longer and increases interception options.

Ships wishing to enter American ports are already required to give advance notice of this intention. Before September 11, ships were required to give 24 hours notice. Since September 11, the Coast Guard has increased that requirement to 96 hours. When a ship gives the Coast Guard notice of its wish to enter an American port, it should be required to provide the CIMIC a complete manifest of passengers and cargo. This would give the Center ample time to review these documents and deploy Coast Guard or Navy assets to intercept and investigate any ship suspected of transporting terrorists or their weapons.

Key Step #3. The U.S. Customs Service should experiment with a point-of-origin inspections program for maritime trade. Numerous measures should be developed to protect Americans from terrorism, but the most effective means remains preventing terrorists and their weapons from even entering the United States. Inspecting vessels before they leave their points of origin would make it more difficult for potentially deadly weapons and people to enter U.S. territorial waters.

To this end, the Administration should direct the U.S. Customs Service to create a pilot point-of-origin inspection program in order to determine whether such inspections can be done in a cost-efficient manner. The pilot program should include three countries to start. Initially, the Administration should negotiate with one significant trade partner each in Europe, Asia, and the Third World to implement the pilot program. This geographic diversity will allow the Administration to determine the potential success of a general program across different political systems, cultures, and levels of economic development. The pilot program also should experiment with different ways of cooperating with the government of origin, and with outsourcing functions to private industry to keep costs down.

If the pilot program proves successful and cost-efficient, the Administration should include point-of-origin inspection agreements in international trade agreements. Provisions should be included to prevent the use of a point-of-origin inspection program as a non-tariff barrier to trade. Nations that want to trade freely with the United States should also want to trade securely. The U.S. Ambassador to the United Nations should propose a treaty on point-of-origin inspections while

assuring potential trade partners that bilateral programs would not be held hostage to any multilateral efforts in this area.

Key Step #4. Congress should authorize a nationwide Sea Marshals Program. Sea Marshals should be organized into two-, four-, and six-person teams based on lessons learned from the pilot program in California. The teams must be capable of boarding deep-draft vessels to inspect their cargo and passenger manifests. Team members may include representatives of the military, Federal law enforcement, and the private sector, and must meet federally established and certifiable standards. The program should include Special Maritime Security Strike Teams within the Coast Guard—rapid response teams that are specially trained and equipped to take control of a facility or vessel that is a potential threat to security.

Key Step #5. The Transportation Security Agency should require airport administrators and port authorities to employ systems that prevent unauthorized people from gaining access to secure areas. Both airports and seaports should, at a minimum, be required to screen employees seeking access to secure areas before permitting them to enter. The Secretary of Transportation should direct the Transportation Security Agency (TSA) to issue new regulations to ensure that only those who need access are able to enter the secure areas of airports. Similarly, local port authorities, in cooperation with the Coast Guard and Federal, State, and Local law enforcement agencies, should adopt new programs to improve security for port employees and users. Advanced biometrical technologies, smart cards, and background checks for employees may also be employed to ensure greater safety.¹³

PRIORITY #6: SECURE ALL FEDERAL NETWORKS AND INFORMATION SYSTEMS.

All federal agencies rely on computers and information networks for day-to-day operations. The U.S. General Accounting Office, in a recent report titled *Computer Security: Improvements Needed to Reduce the Risk to Critical Federal Operations and Assets*,¹⁴ found that “federal systems were not being adequately protected from computer based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations.” Poor purchasing decisions caused some of these problems.

13. For further discussion of the use of biometric technologies for homeland security, see chapter on Civil Defense and chapter on Intelligence and Law Enforcement.

14. GAO-02-231T, November 9, 2001.

Key Step #1. All Federal agencies should focus network purchasing decisions more on security than on cost. The Office of Management and Budget, in Circular A-76, “Performance of Commercial Activities,” directs Federal agencies to make many purchasing decisions on a lowest bid basis. OMB Circular A-76, which was last revised in October 1998 to conform with the Federal Activities Reform Act of 1998 (P.L. 105-270), calls for basing agency decisions on contracting out commercial activities solely on cost estimates. This may be the best way to make procurement decisions for food services and other non-security-related services, but outsourcing vital Federal information systems should not be conducted on a lowest price basis.

Priority must be placed on ensuring the security of Federal information systems. OMB Circular A-76 should be amended to make security the key consideration—at least as important as keeping costs in line—when outsourcing information technology services. In addition, the revised reporting requirements should include an analysis of how procurement decisions on information technology systems will affect network security.

Key Step #2. The executive branch should explore alternatives to the proposed government-only Internet system (GOVNET) before making procurement decisions.

The Special Adviser to the President for Cyber Space Security has proposed creating a government-only intranet that would rely on routers and servers separate from those of the regular Internet. The General Services Administration (GSA) has begun consulting with the computer industry for recommendations on implementation.

The idea behind this proposal is to increase security of unclassified government networks by “running them on fiber [optic cable] that doesn’t touch the Internet routers,” according to the Special Adviser in a recent interview with the *National Journal’s Technology Daily*.¹⁵ It would operate similarly to the independent network already operated by the Defense Department for classified information.

Many experts, however, including former Director of Central Intelligence James Woolsey and former National Security Adviser Sandy Berger, argue that GOVNET would improve security only marginally at best. GOVNET would not be secure from operator error, hacking, or even e-mail viruses such as the “I Love You Bug” that hit Pentagon computers in 2001. Moreover, purchasing or leasing an entirely separate network could be very expensive. Security must be placed at a premium, of course, but GSA must ensure that the security provided justifies the expenditures. The President should direct GSA to consult with industry about achieving the same or greater level of security through the use of intranets that rely on the Internet. GSA and OMB should evaluate both the GOVNET and standard Internet options in consultation with OHS, the Office of Science and Technology Policy (OSTP),

15. Bara Vaida, “Transcript: Clarke Talks Cyber Security,” *Technology Daily*, November 27, 2001.

and the Special Adviser to the President for Cyber Space Security to determine which one would provide better security for the dollar.

PRIORITY #7: ACCELERATE GOVERNMENT COMPLIANCE WITH THE NUCLEAR WASTE POLICY ACT.

The Nuclear Waste Policy Act of 1982 (P.L. 100–207) requires the Department of Energy (DOE) to build a secure underground repository for high-level nuclear waste. Currently, spent nuclear fuel is stored in numerous facilities around the country with varying levels of security. The Act mandated that DOE begin transferring waste to the new facility at Yucca Mountain, Nevada, in 1998. DOE, on its Web site, now estimates that it cannot begin transferring any nuclear waste to this site until 2010. If that is the case, DOE is already running 12 years behind schedule.

Spent nuclear fuel, if acquired by enemies of the United States, could be used to build a “dirty bomb” that could be exploded to spread radiation across a designated area. The destruction of infrastructure caused by such a bomb would be much less than the human toll, but it would still be immense. Providing greater security for this waste material must be a priority, and DOE must be held to its statutory obligations.

Key Step #1. Congress should hold hearings to determine how DOE can bring the Yucca Mountain facility on-line more quickly and improve security. Once operational, the Yucca Mountain, Nevada, facility should provide the appropriate level of security for nuclear waste. A top priority should be given to accelerating implementation of DOE’s legal responsibility. In the meantime, Congress should explore how the private sector and government can work together to ensure that nuclear material is secure.

CONCLUSION

Critical infrastructure protection is vital for the nation’s economic, physical, and social well-being. Some actions need to occur immediately to increase near-term security and create a more open atmosphere for cooperation and coordination among government agencies and with the private sector. President Bush should issue a presidential directive on infrastructure protection to reflect the realities of the post-September 11 world.

Federal agencies must work together and with their counterparts at the State and Local levels to create security standards for infrastructure protection. To improve security, Federal action must be taken in key infrastructure areas, including the Global Positioning System, airport and seaport security, Federal network security,

Table 2

A Key Unimplemented Commission Recommendation for Infrastructure Protection

Recommendation	Name of Commission	Status
The Coast Guard and U.S. Department of Transportation, in cooperation with State and Local agencies and the private sector, should develop and institute “Model Port Standards” for ports’ physical security.	Seaports Commission, <i>Report of the Interagency Commission on Crime and Security in U.S. Seaports</i> (Fall 2000)	Currently, no Federal program available to oversee the implementation of standards or to advise owners and operators on how to implement them.

and nuclear waste security. Roadblocks that currently hinder information sharing with the private sector must also be eliminated. Over the long term, an effective infrastructure protection policy will require restructuring the government agencies involved and how they interact and operate as well as addressing security shortcomings in specific industries.