



Homeland Security

April 2003 A publication of The Council of State Governments



BRIEF

Infrastructure security in the states

Bridging the public and private gap

More than 85 percent of the nation's critical infrastructures are privately owned and operated. But the responsibility for safeguarding the electric, gas, oil and telecommunications networks that crisscross the United States lies primarily with local, state and federal governments.

To ensure the steady flow of energy, the Internet and other vital services it is essential that state and local governments unite with the private sector. There are many legal, organizational and cultural barriers, however, that prevent effective communications and teamwork between the public and private sector in their pursuit of homeland security and safety.

These barriers and potential solutions were highlighted March 20, 2003 during a national teleconference hosted by The Council of State Governments.

Private sector concerns

The USA Patriot Act of 2001 defines critical infrastructures as those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on physical security, national economic security, national public health and safety, or any combination of those matters.

Is a bridge connecting two states across a river a critical infrastructure in both states? Likewise, does it require uniform protective measures? Is a nuclear power plant a critical infrastructure for neighboring states? Surely, neighboring states need to be prepared for potential disasters at those infrastructures. Likewise, critical infrastructures for a city may not be critical for a state. Many private industries are caught amid this confusion and struggle to determine what exactly is critical and, therefore, what protective measures must be implemented.

Further complicating matters, some critical infrastructures are owned and operated by the private or public sectors while

others are owned and operated by quasi-public/private entities. Many critical infrastructures are owned, operated and highly regulated by the federal government, making it difficult for state and local officials to develop plans for additional protective measures and incident response.

The nation's larger dam structures, producers of hydroelectric power, are examples of complex infrastructures. Like other energy industries, hydroelectric power is owned and governed by a mix of private, federal, and public nonprofit organizations. The Army Corps of Engineers and the Bureau of Reclamation, an agency within the U.S. Department of Interior, are the top two producers of hydroelectric power. The National Park Service is traditionally responsible for security at larger dams and national park sites.

Besides an increased use of National Park Service employees for security, the federal government is providing the Bureau of Reclamation and other hydropower suppliers with the authority to provide law enforcement at the facilities by contracting with federal, state, local and tribal law enforcement organizations. Likewise, other critical infrastructures consist of complex ownership and operational arrangements.

A major concern of the private sector is public control and regulation. Many in the private sector argue that sufficient protective and response plans remain in place and that public interference places unnecessary resource burdens on their specific industry.

Another concern is the amount of information sharing between public and private entities. Industries are wary of providing public officials vulnerability assessments and detailed security plans for fear of disclosure to the public. Many states, however, have freedom of information laws that require disclosure of information to the public. Industries argue that competitors could use this information to gain an advantage and that disclosure of vulnerabilities to the public would present opportunities for potential terrorist acts.

Many states are examining their freedom of information laws and, in many cases, amending or repealing disclosure clauses when they pertain to security-related information. For example, Colorado enacted HB 1315 in 2002 that created the Office of Preparedness, Security and Fire Safety and included language that protects from public disclosure plans and information collected by the office.

The private sector is also concerned with cross-jurisdictional problems for large companies and industries that extend beyond city, county, and state boundaries. These companies are forced to work with public officials in many different jurisdictions, each with their own unique plans and priorities.

“Multi-state companies are inundated with numerous, but well meaning, local, state and federal requests aimed at security and disaster preparedness,” said David Heller, vice president of risk management for Qwest Communication. According to Heller, one solution is for public and private officials to work together to develop a uniform set of industry specific cyber and physical security and disaster preparedness practices.

Federal reorganization

Adding to the challenges at the state-level, the federal government is undertaking one of the largest reorganizations in history with the establishment of the Department of Homeland Security. This new department consolidates many outside infrastructure protection agencies such as the Critical Infrastructure Assurance Office (Department of Commerce), Federal Computer Incident Response Center (General Services Administration), National Communications System (Department of Defense), National Infrastructure Protection Center (Federal Bureau of Investigation), and the Energy Security and Assurance Program (Department of Energy).

Why is public and private cooperation critical?

- **Agriculture and Food:** 1,912,000 farms; 87,000 food-processing plants
- **Water:** 1,800 federal reservoirs; 1,600 municipal waste water facilities
- **Telecommunications:** 2 billion miles of cable
- **Electricity:** 2,800 power plants
- **Oil and Natural Gas:** 300,000 producing sites
- **Railroads:** 120,000 miles of major railroads
- **Pipelines:** 2 million miles of pipelines
- **Maritime:** 300 inland/coastal ports
- **Mass Transit:** 500 major urban public transit operators
- **Banking and Finance:** 26,600 FDIC insured institutions
- **Dams:** 80,000 dams
- **Commercial Assets:** 460 skyscrapers

Source: National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, Feb. 2003

Once formed and fully operational, the Information Analysis and Infrastructure Protection Directorate of DHS will specifically:

- Identify critical infrastructures and key assets.
- Conduct strategic threat assessments.
- Assess vulnerabilities.
- Conduct risk assessments by mapping threats against vulnerabilities.
- Detect threats in real-time and disseminate timely warnings.
- Share security-related information.
- Recommend and prioritize protective actions and support measures.
- Assist in response and recovery operations.

According to Nancy Wong, director of the office of planning and partnership at DHS, the new directorate will focus on private sector security investments. “Industry increased security following the Sept. 11, 2001 terrorist attacks and the question is whether or not they can sustain these levels of security,” said Wong. To assist the states and private sectors, the directorate will invest resources to explore non-regulatory means of promoting security as well as planning for situations that require public sector intervention or external security assistance.

Two national strategies are available to help state and local officials as well as the private sector identify their roles in infrastructure protection: The National Strategy for Homeland Security (July 2002) and the Physical Protection of Critical Infrastructures and Key Assets (Feb. 2003). Both can be accessed at <<http://www.whitehouse.gov/homeland>>.

Intrastate solutions

According to C. Suzanne Mencer, Executive Director for the Colorado Department of Public Safety, two of the biggest challenges facing the states are identifying and verifying critical infrastructures, and developing or modifying plans to secure those infrastructures. These tasks cannot be completed in a vacuum and require the involvement of many stakeholder groups such as the private sector, law enforcement, first responders, government entities, and the military, adding to overall difficulty.

In response, Colorado formed seven regional districts based on existing state patrol districts. Each region consisted of representatives from the entities listed above. Next, the regions were tasked with both identifying critical infrastructures and developing plans to protect those infrastructures.

“We’ve taken an all hazard approach to planning in the past such as those related to snowstorms or tornadoes . . . but we’ve never really looked at our plans as they relate to the infrastructures,” said Mencer. She adds that the main difference between the all-hazards and the infrastructure approach to planning and preparations is that “when an attack is directed on an infrastructure, that infrastructure becomes a crime scene . . . and you have to maintain the integrity of that crime scene.” Therefore, plans must take into account the heightened role of law enforcement in securing the scenes and conducting investigations.

Case study: New Jersey Business Force

The New Jersey Business Force, a first-of-its-kind partnership between the state of New Jersey and leading companies in the state, is an innovative solution to America's continuing vulnerability to attacks on the homeland. The project is being built by Business Executives for National Security (BENS), a nationwide, non-partisan organization, that serves as a channel through which senior business executives help enhance the nation's security.

As of March 2003, charter members included: The Amelior Foundation, Atlantic Health System, Automatic Data Processing, Inc., The CIT Group, Inc., DRS Technologies, KPMG LLP, Pfizer Inc., Prudential Financial, Saint Barnabas Health Care System, Stevens Institute of Technology, United Retail Group, Inc., and Verizon Communications.

The New Jersey Business Force will focus on high priority areas where the unique expertise of the private sector can complement ongoing state efforts and provide genuine contributions in preparing for and responding to catastrophic events or terrorists attacks. For example:

- An Internet-based Business Response Network will inventory the capabilities needed in an emergency—transportation, warehouses, communications, medical supplies, construction equipment—and identify companies willing to provide these services on short notice.
- A Business Volunteer training program will prepare companies and employee volunteers in discrete tasks that the state requires but lacks resources to execute in an emergency or rehearse in advance.
- A Rapid Medical Distribution Plan will draw on resources of participating transportation, trucking, shipping and freight companies to ensure that vital medical supplies reach hospitals during an outbreak of an infectious disease.

BENS plans to promote the New Jersey Business Force as a model for other states, providing businesses and their employees with a way to help protect their community and serve their country.

For more information on the New Jersey Business Force, please visit <http://www.njbusinessforce.org>.

Colorado has also formed an Infrastructure Committee at the state level with representatives from each of the primary infrastructures. The purpose of this committee is to:

- Serve as an advisory group to the state's regions and to the Governor.
- Affirm the infrastructure list as identified by the regions.
- Help define the five threat levels for each critical infrastructure sector.

These steps are helping Colorado build the critical public and private relationships necessary to keep citizens safe and secure.

Regional partnerships

Many infrastructures extend well beyond state boundaries and even cross national frontiers. For example, 80 percent of the natural gas consumed on the West Coast of the United States comes out of Western Canada.

Destruction of one infrastructure in a region could have a cascading affect on other infrastructures in that same region. To identify and address these interdependencies at the regional level, the Pacific Northwest Economic Region has conducted a series of infrastructure exercises. PNWER is a public-private partnership consisting of the American states of Alaska, Idaho, Montana, Oregon, and Washington and the Canadian provinces of Alberta, British Columbia, and the Yukon Territory. Its mission is to foster sustainable economic development throughout the entire region.

These exercises, called "Blue Cascades," included more than 150 participants from 70 public and private sector organizations. "Even though our states, provinces and countries have jurisdictional boundaries, infrastructures tend to follow economic water sheds or commerce regions," said Jeff Morris, a state representative from Washington and a past president of PNWER. He adds, "We started the partnership with the goal of creating a disaster resilient region, to strengthen regional security, and to look for cost effective means to litigate identified vulnerabilities in the region."

PNWER's exercises focused on three areas: high-voltage transmission grids, natural gas and oil pipelines, and the telecommunications industry. Each participant reacted to different disaster scenarios. In doing so collectively, public and private sector representatives quickly identified inter-connected weaknesses and vulnerabilities.

Learning from "Blue Cascades," other regional partnerships are taking shape including the San Diego Regional Infrastructure Security Initiative and the Great Lakes Partnership.

Like state and local partnerships, regional public and private partnerships and exercises are one way to identify many infrastructure vulnerabilities. Further, they serve to help the states overcome many of the legal, organizational, and cultural barriers that prevent effective communication and teamwork in pursuit of homeland security and the safety of all citizens.



Many thanks to the
Chlorine Chemistry Council®
 and
CSG's 21st Century Fund
 for supporting this important teleconference.

CSG's 21st Century Fund contributors include:

- American Express Company ■ BellSouth Corporation ■ BP America
- DuPont ■ Eastman Kodak Company ■ GlaxoSmithKline
- Intuit ■ Loeffler Jonas & Tuggey LLP ■ Metabolife International, Inc.
- Pfizer Inc. ■ Pharmacia Corporation
- Philip Morris Management Corporation ■ PhRMA
- The Procter & Gamble Company ■ R.J. Reynolds Tobacco Company
- SBC Communications, Inc. ■ 3M ■ United Parcel Service
- USAA ■ Wyeth

Homeland Security Briefing Series

—National Teleconference—

Color-Coding Security: State Homeland Security Advisory Systems July 2003

CSG will host a national teleconference briefing on the issues surrounding state homeland security advisory systems. Many states, like the federal government, have implemented color-coded advisory systems to communicate threat conditions to state and local officials, businesses and citizens. However, these systems vary from state to state and there is little understanding between public and private officials regarding the systems as a whole. This session will examine these systems with a focus on the issues hindering progress and understanding, with possible solutions and best practices.

For more information,
 visit: <http://www.csg.org>, keyword: homeland security.



The *Homeland Security Brief* reports on homeland security issues facing state governments. This publication is produced as a result of the Homeland Security Briefing Series, CSG's national teleconference series for state officials to hear and question national and state experts on important homeland security issues.

Daniel M. Sprague
CSG Executive Director

Albert C. Harberson
Director of National Policy

John J. Mountjoy
Associate Director of Policy

Chad S. Foster
Policy Analyst

Chad J. Kinsella
Policy Analyst



P.O. Box 11910 ■ Lexington, KY 40578-1910
 ph (859) 244-8000 ■ fax (859) 244-8001 ■ www.csg.org



Homeland Security Brief
 The Council of State Governments
 P.O. Box 11910
 Lexington, KY 40578-1910

Nonprofit Organization
 U.S. Postage
PAID
 Lexington, KY 40578
 Permit No. 355