

# Bridging the public / private security gap

*CSG teleconference examines infrastructure security*

**BY CHAD S. FOSTER**

**M**ore 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 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 sectors in their pursuit of homeland security and safety.

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

## **Private sector concerns**

Many in the private sector are concerned about the amount of public control and regulation. They argue that they have sufficient protective and response plans in place and that public interference places unnecessary resource burdens on their industries.

Their concern extends to 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.

To allay those fears, many states are examining their freedom of information laws and amending or repealing disclosure clauses when they pertain to security-related information. For example, Colorado enacted legislation, 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-scale companies and industries that extend beyond city, county and state boundaries. Large companies are forced to work with public officials in many different jurisdictions, each with their own unique plans and priorities.

“Multistate 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 has formed an Information Analysis and Infrastructure Protection Directorate that, once fully operational, will specifically:

## Critical infrastructure defined

**Critical Infrastructure:** 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 security, national economic security, national public health or safety, or any combination of those matters

— *USA Patriot Act of 2001*

**Key Assets:** Individual targets whose destruction would not endanger vital systems, but would create a local disaster or profoundly damage our nation’s morale or confidence.

— *National Strategy for Homeland Security, July 2002*

- 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; and
- 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 and potentially higher levels of security,” Wong told teleconference participants. To assist the states and the private sector, 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.

### 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. Adding to the overall difficulty, said Mencer, these tasks require the involvement of many stakeholder groups such as the private sector, law enforcement, first responders, government entities, and the military.

In response, Colorado formed seven regional districts based on existing state patrol districts. Each region consisted of representatives from the stakeholder groups. The regions were then given the jobs of identifying critical infrastructures and developing plans to protect them.

“We’ve taken an all-hazards 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.

The primary difference between the all-hazards and the infrastructure approach to planning and preparations, said Mencer, is that “when an attack is directed on an infrastructure, that infrastructure

## 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/costal ports
- Mass Transit – 500 major urban public transit operators
- Banking and Finance – 26,600 FDIC insured institutions
- Chemical Industry – 66,000 chemical plants
- Dams – 80,000 dams
- Commercial Assets – 460 skyscrapers

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

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.

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; and
- help define the five threat levels for each critical infrastructure sector.

These steps are helping Colorado build those 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 effect 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 comprised of the American states of Idaho, Montana, Oregon and Washington and the Canadian provinces of Alaska, Alberta, British Columbia and the Yukon. Its mission is to foster sustainable economic development throughout the entire region.

These infrastructure exercises, called the “Blue Cascades,” included more than 150 participants from 70 public and private sector organizations.

“Even though our states, provinces and countries have these jurisdictional bound-

aries, infrastructures tend to follow economic water sheds or commerce regions,” said Jeff Morris, 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 interconnected 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 local and state partnerships, regional public/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. ★

— Chad S. Foster is a policy analyst in the Public Safety and Justice Group at The Council of State Governments.

## Transcript available

“Bridging the public and private gap” was the first in a series of Homeland Security Teleconferences hosted by CSG. Please visit [www.csg.org](http://www.csg.org) keyword *homeland security* for news on upcoming teleconference sessions and to read or download the transcript and Policy Brief from this session.