



# Homeland Security

December 2003 A publication of The Council of State Governments

BRIEF

## Right to know vs. need to know

### States are re-examining their public-records laws in the wake of Sept. 11

The governor's emergency escape route went from his office on the second floor of the state Capitol, through a conference room and employee offices, and down a hidden shaft once used for a dumbwaiter. Then he could use any of the first floor doors or exit through the basement.

The plan, designed to protect Arkansas' chief executive in an emergency, had one main flaw: Once it was published in the *Arkansas Democrat Gazette* in December 1998, complete with a map of the route, it had to be changed.

Similarly, when the *Idaho Statesman* requested the security codes for the Boise City Hall in 2001, the city had to release them as a matter of public record. It then immediately had to reprogram all the doors.

These incidents illustrate the tension between the need to make government records accessible to the public, and the need to preserve certain information for security or other purposes.

The question of what government records should or should not be open to the public has taken on a whole new meaning since Sept. 11. After the attacks, the threat of terrorism and the abundance of infrastructure information possessed by the hijackers and found in caves in Afghanistan sent a strong message to the nation: Be concerned about public information for security's sake.

Nationwide, federal, state and city officials, members of the press, and the private sector are engaged in a dialogue about how to deal with public records in this new environment. In November, a national teleconference hosted by The Council of State Governments examined the issues around state public-records laws and homeland security information, including arguments for and against disclosure, legislative changes and best practices.

Most states have some form of freedom of information, sunshine, or public-records laws that allow public access to government information. Many state laws with similar intent were adopted soon after passage of the federal Freedom of Information Act of 1966. Essentially, this act required all fed-

eral agencies to make records available when they receive requests and to publish certain items in the Federal Register.

However, federal agencies may deny requests on the grounds that the information sought is exempt from mandatory disclosure. Permissible exemptions include national defense or foreign policy material classified as secret; agency personnel rules and records; trade secrets; law enforcement investigations records; and inter- or intra-agency memoranda or letters.

Like the federal act, state and local laws shifted the burden of proof from the requesting individual or organization to the government body. In other words, government agencies must show why they need to deny a request for information. Previously, the burden was on the requestor to prove why they needed the information.

State public-records laws vary widely in terms of openness as well as the number, type, and scope of exemptions. In fact, some states have as many as 600 exemptions, such as law enforcement investigation records; information that would reveal the identity of an undercover agent; financial assets of an offender; records that would disclose an individual's Social Security number; trade secrets or financial information; physician-patient privilege records; and bids to enter a contract.

#### Close or disclose?

After September 11, many states began top-down reviews of all state laws surrounding terrorism. "We looked at quarantine laws, weapons of mass destruction, wire taps, price gouging, and public records laws," said William von Tegen, deputy attorney general from Idaho.

As a result of these reviews, many states have proposed changes to limit access to records such as critical infrastructure blueprints, emergency operations plans, evacuation plans, and vulnerability assessments. According to the Freedom of Information Center, 28 states have changed their laws to address the issue of open records.

Colorado, for example, adopted HB 1315 in 2002 to exempt terrorism preparedness plans submitted to the new Of-



Office of Preparedness, Security and Fire Safety from public disclosure. Massachusetts passed S 2122 in 2002 to exempt documents that relate to internal layout and structural elements, security measures, emergency preparedness, threat or vulnerability assessments, or any other records relating to the security or safety of persons or buildings.

Proponents of these changes argue that terrorists could use certain records, such as vulnerability assessments and hazardous material routes, to plan future attacks. They also argue that such measures are necessary for public officials to gain access to publicly and privately owned infrastructure information. Without such exemptions, private companies are often reluctant to share information with the government, because they are afraid that terrorists (or competitors) could gain access to valuable data. The private sector owns approximately 85 percent of the nation's critical infrastructure. Typically, any industry information in the hands of a public official is subject to that state's freedom of information laws and exemptions.

Legislative changes have not been without strong opposition, and many state legislatures have blocked proposals that suggest sweeping changes to public-records laws. Opponents argue that the provisions are too broad and provide companies an avenue to hide potentially damaging information, security-related or not, from the public. And they provide agencies and companies with ammunition to prosecute people who release such damaging information, even though it may benefit the public.

Further complicating the issue, many cities and counties have their own open-record laws, which often conflict with each other. This is especially troublesome for large infrastructures such as water and energy systems that span multiple local jurisdictions and, in many cases, state jurisdictions.

"New York City's water system is served by reservoirs in counties outside of the city, so we are forced to look at New York's sunshine laws as well as multiple local laws spanning that sector," said Rich Anderson, senior advisor for the Urban Water Council of the U.S. Conference of Mayors.

Businesses and state and local officials have also expressed concerns that sensitive material they provide to the federal government may be disclosed to the public. To ease such concerns, the U.S. Department of Homeland Security has proposed a new rule to govern security-sensitive information.



A draft of the rule, released for public comment last spring and summer, would exempt government agencies or businesses that submit critical infrastructure information to the department from the federal Freedom of Information Act and from any state laws if the information is shared with the states. Further, the rule would grant agencies and businesses immunity from civil liability for violations of laws related to securities; civil rights; environmental, labor and consumer protections; and health and safety should such violations be revealed in the information they provide to the department. The final rule was expected in December or January, but it had not been announced at the time this article was written.

Combined with a wide array of state and local policies, these federal changes will add to the already complex system of public-records policy and governance.

Finally, there is no solid precedence of court action and judicial interpretation around the public-records issue as it relates to homeland security. Without solid guidance from the courts, policy-making becomes much more difficult.

### **Striking a balance: Idaho and Michigan's experiences**

Idaho and Michigan both recently updated their states' freedom of information laws to exempt homeland security information.

Idaho's changes began from general concerns about evacuation procedures, escape routes, agriculture-related facilities, transportation of hazardous materials (including nuclear waste), and the blueprints of buildings that housed those materials.

Gov. Dirk Kempthorne signed the resulting proposal, HB 560, into law on March 4, 2002. The bill exempts from disclosure "the records of buildings, facilities, infrastructures and systems held by or in the custody of any public agency

only when the disclosure of such information would jeopardize the safety of persons or the public safety.” Exempted records may include emergency evacuation, escape or other emergency response plans, vulnerability assessments, operation and security manuals, plans, blueprints and security codes.

Likewise, Michigan changed its Freedom of Information Act to add a new exemption for security information. Robert Ianni, bureau chief in the Department of the Attorney General, said officials were concerned about “the considerable amount of information that could be of use to potential terrorists ... things like maps of water resources and information about the location of emergency management centers, energy plants, pipelines, and chemical plants.”

Then-Gov. John Engler signed the final reform, HB 5349, into law on March 29, 2002. The law exempts the following: “Building, public works, and public water designs to the extent that those designs relate to the ongoing security measures of a public body, capabilities and plans for responding to a violation of the Michigan antiterrorism act ... emergency response plans, risk planning documents, threat assessments, and domestic preparedness strategies.”

Idaho and Michigan’s experiences reveal several lessons from which other states can benefit.

First, each state brought together and involved many different stakeholders throughout the legislative process. Idaho’s legislation was the result of negotiations by state lawmakers, the attorney general’s office, media groups and the American Civil Liberties Union. “We ended up working very closely with the Idaho Press club and other newspaper associations,” said von Tegen.

Likewise, “The Michigan Press Association and other interested groups played an active role in the discussions,” said Tom Quasarano, assistant attorney in Michigan’s Department of the Attorney General. Input from many different stakeholders early in the legislative process helped facilitate the nearly unanimous passage of both bills.

Second, the new exemptions are narrow in scope, identifying specific information such as records, plans and codes. Narrow exemptions decrease the chance that a public body could hide or attempt to hide non-security information from the public in the name of security. They also prevent businesses from attempting to conceal potentially damaging information through a public entity, which a broad security-related exemption would more likely allow.

Finally, each of the new exemptions includes a balance test to ensure that the public safety and interest are ultimately served. Idaho’s law exempts records, “only when the disclosure of such information would jeopardize the safety of persons or the public safety.”

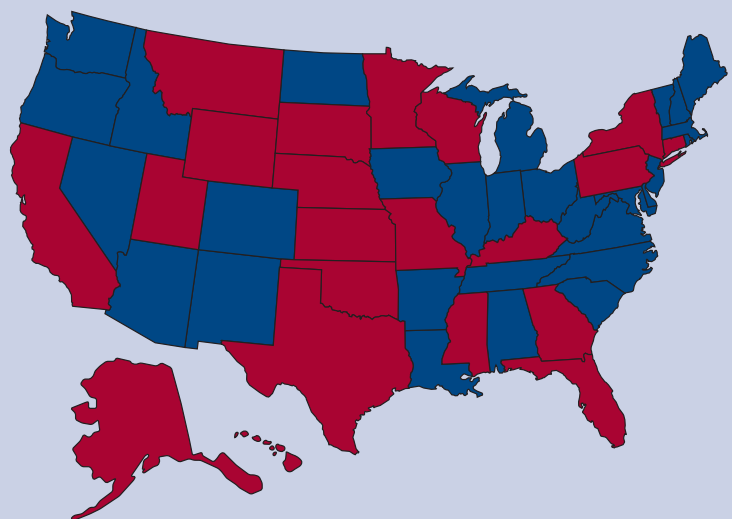
Michigan’s balancing language is slightly more detailed, providing that records may be exempted “unless disclosure would not impair a public body’s ability to protect the security or safety of persons or property or unless the public interest in disclosure outweighs the public interest in non-disclosure in the particular instance.” When a state office receives a request for information protected through the new exemption, it must weigh the benefits of denial against the benefits of disclosure in order to ensure that the public interest is best served.

The combination of appropriate stakeholder involvement, narrow exemptions, and a balancing test or requirement has helped Idaho and Michigan improve their homeland security and public-records laws. “What also makes sense is for state legislators to consult with local governments over their particular needs in terms of vulnerability issues and non-disclosure,” said Anderson.

Possibly more than any other policy area, homeland security requires the careful scrutiny of records, mainly those that could assist terrorists in planning and executing future attacks. But the public could also be harmed by the lack of open policies that reveal environmental risks, health and safety issues, and other community concerns. This conflict, combined with the wide array of state, local and federal policies, makes the public-records issue extremely sensitive and complicated.

Despite these complexities, states can learn from the experiences and practices of others to find a balance between security requirements and the need for open government.

### State public-record changes since Sept. 11, 2001



Blue: Have added homeland security exemptions

Red: Have not added homeland security exemptions



Many thanks to the  
**Chlorine Chemistry Council®**  
for supporting this important teleconference.

CSG also thanks the session speakers and the National Emergency Management Association for their assistance.

Speakers:

- Charles N. Davis, associate professor, School of Journalism, University of Missouri
- William A. von Tagen, deputy attorney general, Idaho
- Robert Ianni, bureau chief, Consumer Protection Bureau, Department of Attorney General, Michigan
- Tom Quasarano, assistant attorney, Department of Attorney General, Michigan
- Rich Anderson, senior advisor, Urban Water Council, U.S. Conference of Mayors

## Homeland Security Briefing Series

—National Teleconference—

For additional information on **Information War: Right to Know vs. Need to Know**, visit [www.csg.org](http://www.csg.org) (keyword: homeland security). A transcript of the teleconference and copy of this *Homeland Security Brief* publication can be found at the site. Also available are materials from the previous homeland security teleconference sessions:

### Bridging the public and private gap – March 2003

This teleconference examined the challenges facing public and private sector officials in addressing infrastructure security.

### Color-coding security – July 2003

This briefing addressed the issues and practices surrounding state homeland security advisory systems.

### Coming in January 2004:

#### State Official's Guide to Critical Infrastructure Protection

This guide addresses the unique characteristics of critical infrastructures and the challenges associated with protecting them.



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**  
*Chief 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](http://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