October 2003

DRINKING WATER

Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-29, a report to the Committee on Environment and Public Works, U.S. Senate

Why GAO Did This Study

After the events of September 11, 2001, Congress appropriated over $100 million to help drinking water systems assess their vulnerabilities to terrorist threats and develop response plans. As the Environmental Protection Agency has suggested, however, significant additional funds may be needed to support the implementation of security upgrades. Therefore, GAO sought experts' views on (1) the key security-related vulnerabilities of drinking water systems; (2) the criteria for determining how federal funds should be allocated among drinking water systems to improve their security, and the methods for distributing those funds; and (3) specific activities the federal government should support to improve drinking water security.

GAO conducted a systematic Web-based survey of 43 nationally recognized experts to seek consensus on these key drinking water security issues.

What GAO Recommends

GAO recommends that as EPA refines its efforts to help drinking water utilities reduce their vulnerability to terrorist attacks, the agency consider the information in this report to help determine: how best to allocate security-related federal funds among drinking water utilities; which methods should be used to distribute the funds; and what specific security-enhancing activities should be supported.

www.gao.gov/cgi-bin/getrpt?GAO-04-29.

To view the full product, including the scope and methodology, click on the link above. For more information, contact John Stephenson at (202) 512-3841 or Stephensonj@gao.gov.

What GAO Found

GAO's expert panel cited distribution systems as among the most vulnerable physical components of a drinking water utility, a conclusion also reached by key research organizations. Also cited were the computer systems that manage critical utility functions, treatment chemicals stored on site, and source water supplies. Experts further identified two overarching vulnerabilities: (1) a lack of information individual utilities need to identify their most serious threats; and (2) a lack of redundancy in vital system components, which increases the likelihood that an attack could render an entire utility inoperable.

According to over 90 percent of the experts, utilities serving high-density areas deserve at least a high priority for federal funding. Also warranting priority are utilities serving critical assets, such as military bases, national icons, and key academic institutions. Direct federal grants were clearly the most preferred funding mechanism, with over half the experts indicating that such grants would be very effective in distributing funds to recipients. Substantially fewer experts recommended using the Drinking Water State Revolving Fund for security upgrades.

When experts were asked to identify specific security-enhancing activities most deserving of federal support, their responses generally fell into three categories:

- *physical and technological upgrades* to improve security and research to develop technologies to prevent, detect, or respond to an attack (experts most strongly supported developing near real-time monitoring technologies to quickly detect contaminants in treated drinking water on its way to consumers);
- *education and training* to support, among other things, simulation exercises to provide responders with experience in carrying out emergency response plans; specialized training of utility security staff; and multidisciplinary consulting teams to assess utilities' security preparedness and recommend improvements; and
- *strengthening key relationships* between water utilities and other agencies that may have key roles in an emergency response, such as public health agencies, law enforcement agencies, and neighboring drinking water systems; this category also includes developing protocols to encourage consistent approaches to detecting and diagnosing threats.