United States General Accounting Office

GAO

Report to the Committee on Environment and Public Works, U.S. Senate

October 2003

# DRINKING WATER

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


GAO-04-29

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.

# Contents

## Abbreviations

| | |
|---|---|
| AMSA | Association of Metropolitan Sewerage Agencies |
| AMWA | Association of Metropolitan Water Agencies |
| AWWA | American Water Works Association |
| BASIC | Bay Area Security Information Collaborative |
| CDC | Centers for Disease Control and Prevention |
| DWSRF | Drinking Water State Revolving Fund |
| EPA | Environmental Protection Agency |
| ETV | Environmental Technology Verification |
| FBI | Federal Bureau of Investigation |
| ICMA | International City/County Management Association |
| ISAC | Information Sharing and Analysis Center |
| MADIRT | Mutual Aid Disaster and Intervention and Response Teams |
| NRWA | National Rural Water Association |
| NRDC | Natural Resources Defense Council |
| PDD | Presidential Decision Directive |
| SCADA | Supervisory Control and Data Acquisition |
| VA | vulnerability assessment |
| VSAT | Vulnerability Self Assessment Tool |
| WEF | Water Environment Federation |

GAO
Accountability * Integrity * Reliability

**United States General Accounting Office**
**Washington, D.C. 20548**

October 31, 2003

The Honorable James Inhofe
Chairman
The Honorable James Jeffords
Ranking Minority Member
Committee on Environment and Public Works
United States Senate

As requested, this report discusses the views of nationally recognized experts on key issues concerning drinking water security, including serious vulnerabilities of drinking water systems, criteria for allocating federal funds among systems, and activities that most warrant federal support to mitigate the risk of terrorism.

As agreed in discussions with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the date of this letter. We will then send copies to other appropriate congressional committees, and to the Administrator of the Environmental Protection Agency. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staffs have any questions concerning this report, please call me at (202) 512-3841 or my Assistant Director, Steve Elstein, at (202) 512-6515. Major contributors to this report are listed in appendix II.

John B. Stephenson
Director, Natural Resources
and Environment

# Executive Summary

## Purpose

Drinking water utilities across the country have long been recognized as potentially vulnerable to terrorist attacks of various types, including physical disruption, bioterrorism, chemical contamination, and cyber attack. Damage or destruction by terrorists could disrupt not only the availability of safe drinking water, but also the delivery of vital services that depend on these water supplies, such as fire suppression. Such concerns were greatly amplified by the September 11, 2001, attacks on the World Trade Center and the Pentagon and then by the discovery of training manuals in Afghanistan detailing how terrorist trainees could support attacks on drinking water systems.

Congress has since committed significant federal funding to assist drinking water utilities, with over $100 million appropriated through fiscal year 2004 to help systems assess their vulnerabilities to terrorist threats and develop response plans. As significant as these funds are, it is likely that drinking water utilities will ask the federal government to provide larger sums to go beyond the *planning* for upgrading drinking water security to the actual *implementation* of security upgrades. Consequently, as agreed with the Chairman and Ranking Minority Member of the Senate Committee on Environment and Public Works, this report identifies (1) the key security-related vulnerabilities affecting the nation's drinking water systems; (2) the criteria that should be used to determine how federal funds are allocated among recipients to improve their security, and the methods that should be used to distribute these funds; and (3) specific activities the federal government should support to improve drinking water security.

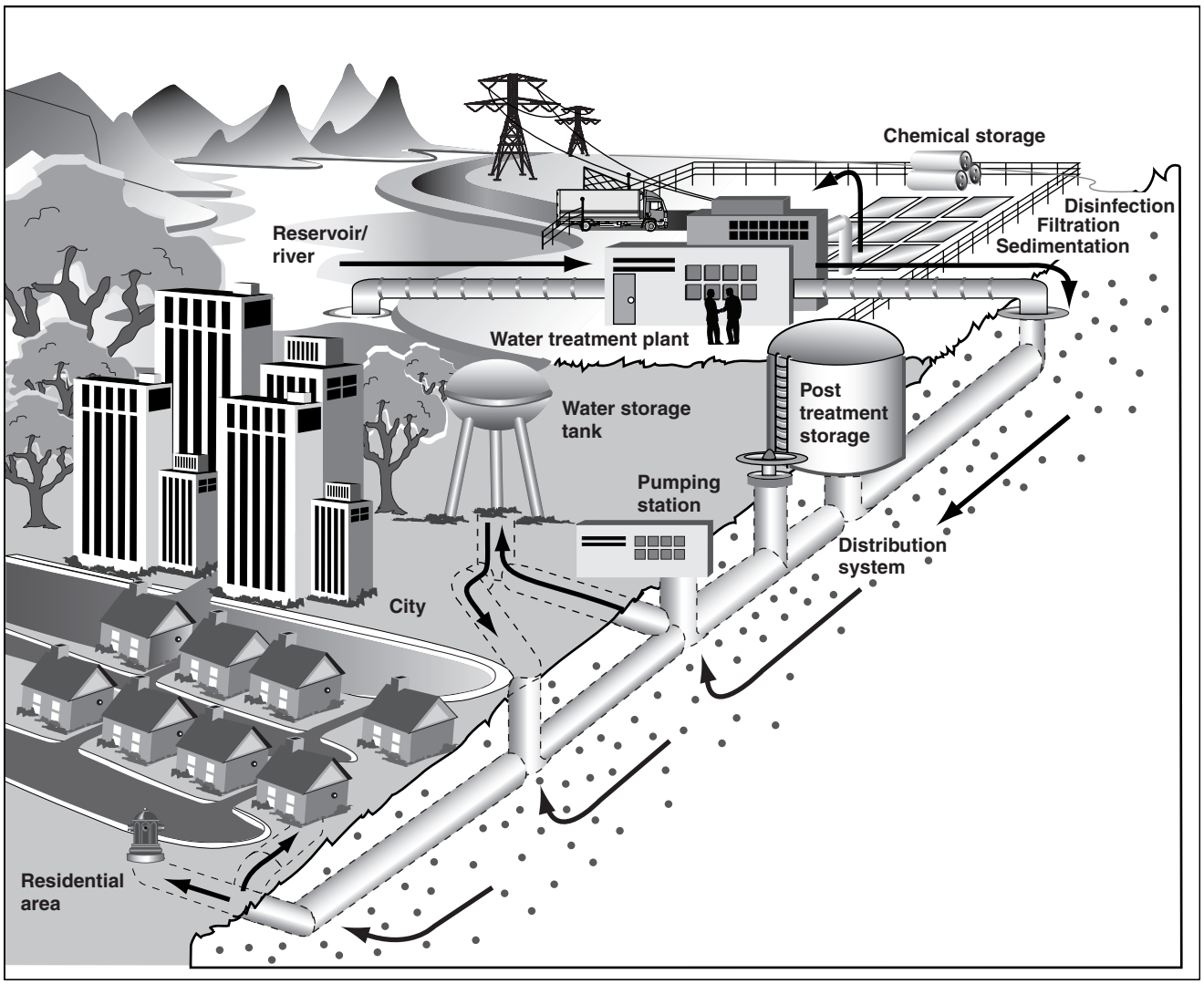
To address these issues, GAO conducted a Web-based Delphi survey process involving 43 nationally recognized experts. The Delphi method is a systematic process for obtaining individuals' views on a question or problem of interest and seeking consensus, if possible. In selecting members for the expert panel, GAO sought individuals who were widely recognized as possessing expertise on one or more key aspects of drinking water security. GAO also sought to achieve balance in representation from key federal agencies, key state or local agencies, key industry and nonprofit organizations, and water utilities of varying sizes. A detailed description of GAO's methodology is presented in chapter 1.

## Background

Drinking water systems vary by size and other factors, but as illustrated in figure 1, they most typically include a supply source, treatment facility, and distribution system. A water system's supply source may be a reservoir,

aquifer, or well, or a combination of these sources. Some systems may also include a dam to help maintain a stable water level, and aqueducts and transmission pipelines to deliver the water to a distant treatment plant. The treatment process generally uses filtration, sedimentation, and other processes to remove impurities and harmful agents, and disinfection processes such as chlorination to eliminate biological contaminants. Chemicals used in these processes, most notably chlorine, are often stored on site at the treatment plant. Distribution systems comprise water towers, piping grids, pumps, and other components to deliver treated water from treatment systems to consumers. Particularly among larger utilities, distribution systems may contain thousands of miles of pipes and numerous access points.

**Figure 1: Key Components of a Typical Drinking Water System**




Source: GAO.

Until the 1990s, emergency planning at drinking water utilities generally focused on responding to natural disasters and, in some cases, domestic threats such as vandalism. In the 1990s, however, both government and industry officials broadened the process to account for terrorist threats. Among the most significant actions taken was the issuance in 1998 of Presidential Decision Directive 63 to protect the nation's critical

infrastructure against criminal and terrorist attacks. The directive designated the Environmental Protection Agency (EPA) as the lead federal agency to address the water infrastructure and to work with both public and private organizations to develop emergency preparedness strategies. EPA, in turn, appointed the Association of Metropolitan Water Agencies to coordinate the water industry's role in emergency preparedness. During this time, this public-private partnership focused primarily on cyber security threats for the several hundred community water systems that each served over 100,000 persons. The partnership was broadened in 2001 to include both the drinking water and wastewater sectors, and focused on systems serving more than 3,300 people.

Efforts to better protect drinking water infrastructure were accelerated dramatically after the September 11 attacks. EPA and the drinking water industry launched efforts to share information on terrorist threats and response strategies. They also undertook initiatives to develop guidance and training programs to assist utilities in identifying their systems' vulnerabilities. As a major step in this regard, EPA supported the development, by American Water Works Association Research Foundation and Sandia National Laboratories, of a vulnerability assessment methodology for larger drinking water utilities. The push for vulnerability assessments was then augmented by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act). Among other things, the act required each community water system serving more than 3,300 individuals to conduct a detailed vulnerability assessment by specified dates in 2003 or 2004, depending on their size.

## Results in Brief

GAO's expert panel identified several key physical assets as the most seriously vulnerable to terrorist attacks. In general, their observations were similar to those of major public and private organizations that have assessed the vulnerability of these systems to terrorist attacks, including the National Academy of Sciences, Sandia National Laboratories, and key industry associations. In particular, when asked to identify what they believed to be among the top vulnerabilities of drinking water utilities, nearly 75 percent of the experts (32 of 43) identified the distribution system (one or more components). More experts identified the distribution system as the top vulnerability (12 of 43) among the components of the drinking water system. The other physical assets most frequently cited were source water supplies, critical information systems, and chemicals stored on site that are used in the treatment process. Importantly, the experts also identified overarching vulnerability issues that may involve multiple system

components, or even an entire drinking water system. Chief among these issues were (1) a lack of redundancy in vital systems, which increases the likelihood that an attack could render a system inoperable; and (2) the difficulty many systems face due to a lack of information on the most serious threats to which they are exposed.

Key criteria experts cited for determining how federal funds to improve drinking water security should be allocated included (1) the extent to which information on utilities' vulnerabilities should be considered in making allocation decisions; and (2) characteristics of the utilities themselves, such as size and proximity to population centers.

- About 90 percent of the panelists strongly agreed or somewhat agreed that allocation decisions should be based on vulnerability assessment information. Several factors, however, complicate the government's ability to use utilities' vulnerability assessments for this purpose.

- Panelists favored funding priority for utilities serving high-density populations, with over 90 percent indicating that they deserve at least a high priority and over 50 percent indicating they deserve highest priority. Utilities serving critical assets (such as military bases and other sensitive government facilities, national icons, and key cultural or academic institutions) were also recommended as high-priority recipients, while relatively few experts recommended priority for utilities serving rural or isolated populations.

When asked to identify the most effective mechanisms of distributing federal drinking water security funds to recipients, over half the experts indicated that direct federal grants would be very effective in doing so. Many also favored including a requirement for matching funds as a grant condition. Fewer experts recommended using the Drinking Water State Revolving Fund (DWSRF) for this purpose, particularly to support upgrades that need to be implemented quickly.

When asked to identify and set priorities for security-enhancing activities most deserving of federal support, the experts most frequently identified activities that generally fell into three broad categories:

- *Physical and technological improvements* includes both physical alterations to improve the security of drinking water systems and the

development of technologies to prevent, detect, or respond to an attack. The need to develop near real-time monitoring technologies, which would be particularly useful in quickly detecting contaminants in water that has already left the treatment plant for the consumer, had by far the strongest support.

- *Education and training* would be used for both utility and nonutility personnel responsible for preventing, responding to, and recovering from an attack. These activities include, among other things, support for simulation exercises to provide responders with experience in carrying out utilities' emergency response plans; specialized training of utility personnel responsible for security; general training of utility personnel to augment security awareness among all staff; and multidisciplinary consulting teams to independently analyze utilities' security preparedness and recommend security-related improvements.

- *Strengthening relationships* is seen as critical between water utilities and other agencies (public health agencies, enforcement agencies, and neighboring utilities, among others) that may have key roles in an emergency response. This category also includes developing common protocols to engender a consistent approach among utilities in detecting and diagnosing threats, and the testing of local emergency response systems to ensure that participating agencies coordinate their actions effectively.

# Principal Findings

## Key Vulnerabilities

Nearly 75 percent of the experts on GAO's panel (32 of 43) named the distribution system (one or more components) as among the top vulnerabilities of drinking water systems. In fact, 12 of the 32 experts identified the distribution system as the single most important vulnerability, a considerably greater number than any other element of the drinking water system. Their explanations most often related to the accessibility of distribution systems at numerous points. One expert, for example, cited the difficulty of preventing the introduction of a contaminant into a distribution system from inside a public building. Another expert noted that since the water in a distribution system has already been treated and is in the final stages of being transferred to consumers, the distribution of a chemical, biological, or radiological agent

in such a manner could be difficult to detect until it is too late to reverse any harm done.[1]

Several other components, though not considered as critical as the distribution system, were still the subject of concern. Nearly half the experts (20 of 43) identified source water as among drinking water systems' top vulnerabilities. One expert noted, for example, that "because of the vast areas covered by watersheds and reservoirs, it is difficult to maintain security and prevent intentional or accidental releases of materials that could have an adverse impact on water quality." Yet some experts cited factors that mitigate the risks associated with source water, including (1) that source water typically involves a large volume of water, which in many cases could dilute the potency of contaminants; (2) the length of time (days or even weeks) that it typically takes for source water to reach consumers; and (3) that source water will go through a treatment process in which many contaminants are removed. In addition, EPA pointed out that as source water goes through the treatment process, many contaminants are removed.

Also cited as a vulnerability were the sophisticated computer systems that drinking water utilities have come to rely upon to manage key functions. These Supervisory Control and Data Acquisition (SCADA) systems allow operators to monitor and control processes throughout their drinking water systems. Although SCADA systems have improved water utilities' efficiency and reduced costs, almost half of the experts on GAO's panel (19 of 43) identified them as among these utilities' top vulnerabilities. Finally, 13 of the 43 experts identified treatment chemicals, particularly chlorine used for disinfection, as among utilities' top vulnerabilities. Experts cited the inherent danger of storing large cylinders of a chemical on site, noting that their destruction could release toxic gases in densely populated areas. Some noted, however, that this risk has been alleviated by utilities that have chosen to use the more stable liquid form of chlorine instead of the more vulnerable compressed gas canisters that have traditionally been used.

Experts also identified overarching issues that compromise the integrity of multiple physical assets, or even the entire drinking water system. Among these is the lack of redundancy among vital systems. Many drinking water

[1]An EPA official noted, however, that distribution systems generally carry disinfectant residuals that can counteract the potentially harmful effects of contaminants.

systems are "linear"—that is, they have single transmission lines leading into the treatment facility, single pumping stations along the system, and often employ a single computer operating system. They also depend on the electric grid, transportation systems, and single sources of raw materials (e.g., treatment chemicals). Many experts expressed concern that problems at any of these "single points of failure" could render a system inoperable unless redundant systems are in place. Experts also cited the lack of sufficient information to understand the most significant threats confronting individual utilities. According to the American Water Works Association, assessments of the most credible threats facing a utility should be based on knowledge of the "threat profile" in its specific area, including information about past events that could shed light on future risks. Experts noted, however, that such information has been difficult for utilities to obtain. One expert suggested that the intelligence community needs to develop better threat information and share it with the water sector.

## Allocation and Distribution of Federal Funds

Many drinking water utilities have been financing at least some of their security upgrades by passing along the costs to their customers through rate increases. Given the cost of these upgrades, however, drinking water industry representatives have also sought federal assistance. GAO asked its expert panel to comment on the factors that should be considered in allocating federal funds. Specifically, GAO asked the experts to comment on the following:

- *Appropriate use of vulnerability assessment information.* About 90 percent of the experts (39 of 43) strongly agreed or somewhat agreed that funds should be allocated on the basis of vulnerability assessment information, with some citing the vulnerability assessments (VA) required by the Bioterrorism Act as the best available source of this information. Several experts, however, pointed to a number of complicating factors. Perhaps the most significant constraint is the Bioterrorism Act's provision precluding the disclosure of any information that is "derived" from vulnerability assessments submitted to EPA. It is important to protect sensitive information about each utility's vulnerabilities from individuals who may then use the information to harm the utility. The law specifies that only individuals designated by the EPA Administrator may have access to the assessments and related information. Yet even those individuals would face constraints in using the information. They would have difficulty, for example, in citing vulnerability assessments to support decisions on

allocating security-related funds among utilities, as well as decisions concerning research priorities and guidance documents. Others cited an inherent dilemma affecting *any* effort to set priorities for funding decisions based on the greatest risk—whatever does not receive attention becomes the best target.

- *Criteria to help determine which utilities should receive funding priority.* According to 93 percent of the experts (40 of 43), utilities serving high-density population areas should receive a high or highest priority in funding (55 percent deemed this criterion as the highest priority). Most shared the view of one expert, who noted that directing limited resources to protect the greatest number of people is a common factor when prioritizing funding. Experts also assigned high priority to utilities serving critical assets, such as national icons representing the American image, military bases, and key government, academic, and cultural institutions. At the other end of the spectrum, only about 5 percent of the experts (2 of 43) stated that utilities serving rural or isolated populations should receive a high or highest priority for federal funding. Generally, these panelists commented that such facilities are least able to afford security enhancements and are therefore in greatest need of federal support. Importantly, the relatively small percentage of experts advocating priority for smaller systems may not fully reflect the concern among many of the experts for the safety of these utilities. For example, several who supported higher priority for utilities serving high-density populations cautioned that while problems at a large utility will put more people at risk, utilities serving small population areas may be more vulnerable because of weaker treatment capabilities, fewer highly trained operators, and more limited resources.

As for effective mechanisms for distributing federal funds, the expert panelists viewed direct federal grants as most effective, with 86 percent of the experts (37 of 43) indicating that this mechanism would be somewhat or very effective in allocating federal funds. One expert cited EPA's recent distribution of direct security-related grant funds to larger systems to perform their VAs as a successful initiative. Also, 74 percent cited a matching requirement for such grants as somewhat or very effective. One expert pointed out that such a requirement would effectively leverage limited federal dollars, thereby providing greater incentive to participate. The Drinking Water State Revolving Fund received somewhat less support, with a number of the experts cautioning that as a funding mechanism, it is suited more for longer-term improvements than for those requiring more immediate attention.

## Security-Enhancing Activities That Most Warrant Federal Support

When experts were asked to identify and set priorities for the security-enhancing activities most deserving of federal support, their responses generally fell into three broad categories:

- *Enhancing Physical Security and Supporting Technological Improvements*. These activities fell into nine subcategories. Of these, the development of "near real-time monitoring technologies," capable of providing near real-time data for a wide array of potentially harmful water constituents, received far more support for federal funding than any other subcategory—over 93 percent of the experts (40 of 43) rated this subcategory as deserving at least a high priority for federal funding. More significantly, almost 70 percent (30 of 43) rated it highest priority. These technologies were cited as critical in efforts to quickly detect contamination events, minimize their impact, and restore systems after an event has passed. The experts also voiced strong support for (1) increasing laboratories' capacity to deal with spikes in demand caused by chemical, biological, or radiological contamination of water supplies, and (2) "hardening" the physical assets of drinking water facilities through improvements such as adding or repairing fences, locks, lighting systems, and cameras and other surveillance equipment. Some experts, however, cited the limitations inherent in attempts to comprehensively harden a drinking water facility's assets. They noted in particular that, unlike nuclear power or chemical plants, a drinking water system's assets are spread over large geographic areas, particularly the source water and distribution systems.

- *Improving Education and Training*. Over 90 percent of the experts (39 of 43) indicated that improved technical training for security-related personnel warrants at least a high priority for federal funding, with over 55 percent (24 of 43) indicating that it deserved highest priority. To a lesser extent, experts supported general training for other utility personnel to increase their awareness of security issues. The panelists also underscored the importance of conducting regional simulation exercises to test emergency response plans, with more than 88 percent (38 of 43) rating this as a high or highest priority for federal funding. Such exercises are intended to provide utility and other personnel with the training and experience needed both to perform their individual roles in an emergency, and to coordinate these roles with other responders. Finally, about half the experts assigned at least a high priority to supporting multidisciplinary consulting teams ("Red Teams"), comprising individuals with a wide array of backgrounds, to provide independent analyses of utilities' vulnerabilities.

- *Strengthening Relationships between Utilities and Other Key Organizations*. Experts cited the need to improve cooperation and coordination between drinking water utilities and certain other organizations as key to improving utilities' security. Among the organizations most often identified as critical to this effort are public health and law enforcement agencies, which have data that can help utilities better understand their vulnerabilities and respond to emergencies. In addition, the experts reported it is valuable for utilities to develop mutual aid arrangements with neighboring utilities. Such arrangements sometimes include, for example, the sharing of back-up power systems or other critical equipment. One expert described an arrangement in the San Francisco Bay Area—the Bay Area Security Information Collaborative (BASIC). The collaborative's eight utilities meet regularly to address security-related topics. Finally, over 90 percent of the experts (39 of 43) rated the development of common protocols among drinking water utilities to monitor drinking water threats as warranting a high or highest priority for federal funding. Drinking water utilities vary widely in how they perceive threats and detect contamination, in large part because few common protocols exist that would help promote a more consistent approach toward these critical functions. Some experts noted in particular the need for protocols to guide the identification, sampling, and analysis of contaminants.

## Making Key Security Decisions in the Face of Great Uncertainty

EPA has identified improved drinking water security as an important national goal, and has stated in its Strategic Plan on Homeland Security that as funds are appropriated, federal resources will be available to help achieve this goal. Yet key judgments about who should receive priority for federal resources, and how those funds should be spent, will have to be made in the face of great uncertainty about the likely target of an attack, the nature of an attack (whether physical, cyber, chemical, biological, or radiological), and its timing. The experts on GAO's panel have had to consider these uncertainties in deriving their own judgments about these issues. Their judgments, while not unanimous on all matters, suggested a high degree of consensus on a number of key issues.

GAO recognizes that sensitive funding decisions ultimately must take into account political, equity, and other considerations. It also believes such decisions should consider the judgments of the nation's most experienced individuals on these matters, such as those included on its panel. It is in this context that GAO offers the results presented in this report as information

for Congress and the Administration to consider as they seek the best way to use limited financial resources to reduce the threat to the nation's drinking water supply.

## Recommendation for Executive Action

GAO recommends that, as EPA refines its efforts to help drinking water utilities reduce their vulnerability to terrorist attacks, the EPA Administrator 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.

## Agency Comments

We provided EPA with a draft of this report for review and comment. EPA did not submit a formal letter but did provide comments from officials in its Office of Water and its Office of Homeland Security. The comments from the Office of Water said that the report's results were "useful and well thought out." EPA's Office of Homeland Security said that the report "demonstrates a well conceived and executed project," and that "a number of the issues raised in the document will be useful to the agency as it moves forward in the drinking water security program." Both offices also offered specific technical comments and suggestions, which have been incorporated.

# Introduction

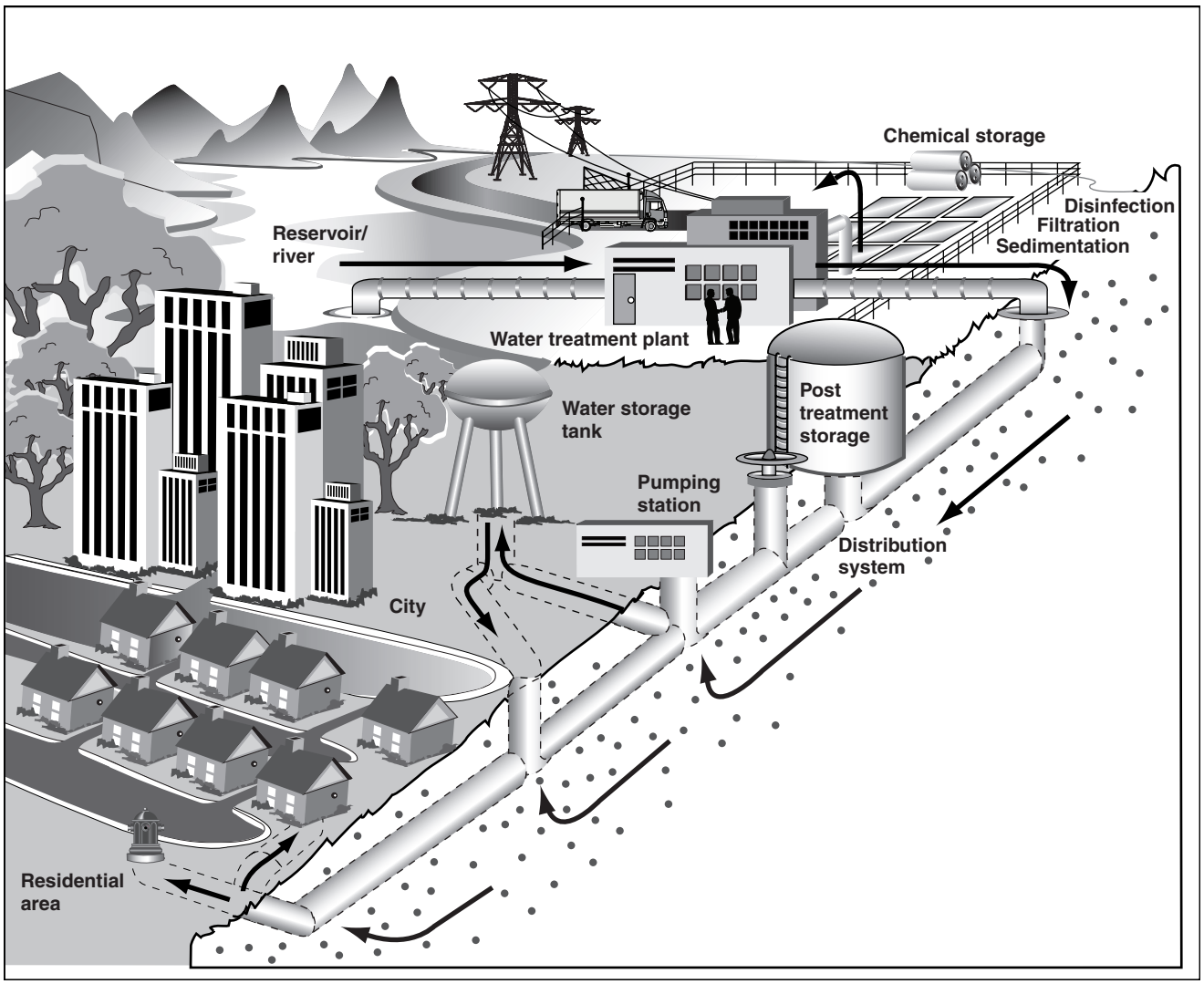
Drinking water utilities across the country have long been recognized as being potentially vulnerable to terrorism of various types, including physical disruption, bioterrorism, chemical contamination, and cyber attacks. Damage or destruction by such a terrorist attack could disrupt not only the availability of safe drinking water to consumers, but also the delivery of vital services that depend on these water supplies, such as fire suppression.

These concerns were greatly amplified by the September 11, 2001, attacks on the World Trade Center and the Pentagon. They were further amplified in ensuing months when training manuals were discovered in Afghanistan detailing how terrorist trainees could support attacks on drinking water systems.

## Key Components of a Typical Drinking Water System

Drinking water systems vary by size and other factors but, as illustrated in figure 2, most typically include a supply source, treatment facility, and distribution system.

**Figure 2: Key Components of a Typical Drinking Water System**




Source: GAO.

As the figure shows, a water system's supply source may include a reservoir, aquifer, or well, or a combination of these sources. The supply source may also include a dam as well as aqueducts and transmission pipelines to deliver the water to a distant treatment plant. Many water systems rely on groundwater as their primary water source, but most

systems, particularly larger systems, rely on surface water such as lakes, rivers, and streams.

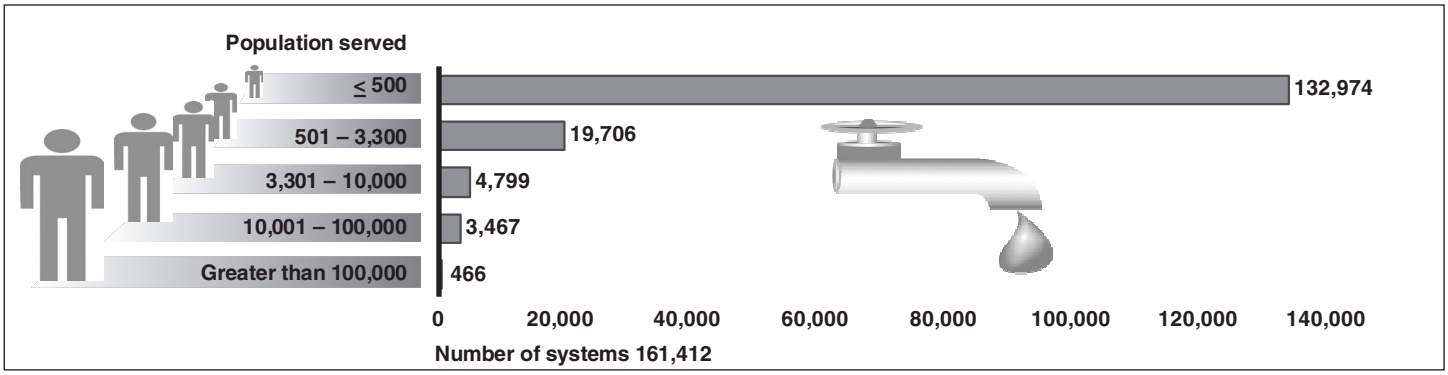
Water treatment generally uses filtration, flocculation, sedimentation, and other processes to remove impurities and harmful agents, and disinfection processes (such as chlorination) to eliminate biological contaminants. Chemicals used in these processes, most notably chlorine, are often stored on site.

The distribution system comprises several components, such as water towers, piping grids, and pumps that deliver treated water from treatment systems to consumers. A key feature of most distribution systems is their size: Particularly among larger utilities, distribution systems may have many thousands of miles of pipes.

## The Nation's Drinking Water Systems and the Populations They Serve

Nationwide, there are more than 160,000 public water systems that individually serve from as few as 25 people to 1 million people or more. As figure 3 illustrates, nearly 133,000 of these water systems serve 500 or fewer people. Only 466 systems serve more than 100,000 people each, but these systems, located primarily in urban areas, account for nearly half of the total population served.

**Figure 3: Number of Drinking Water Systems That Serve Various Populations**




Source: GAO.

## Government and Industry Have Recently Sought to Improve Security

Most drinking water systems long ago developed and maintained emergency preparedness plans that specified how to notify the public in cases of emergency, and how to coordinate an emergency response with law enforcement and other emergency response officials. These plans, however, paid little attention to the kinds of threats posed by international terrorist organizations. Rather, they were generally oriented toward responding to natural disasters and, in some cases, domestic threats such as vandalism.

Both government and industry officials took a number of steps to broaden emergency planning in the 1990s. In 1996, the President issued Executive Order 13010, which listed water supply as one of eight national infrastructures vital to the security of the United States. In 1997, the President's Commission on Critical Infrastructure Protection, also established by executive order, issued a report on the vulnerabilities of the eight categories of infrastructure and strategies for protecting them. The report identified three attributes crucial to water supply users: Water must be available on demand, it must be delivered at sufficient pressure, and it must be safe for use.[1] It warned that susceptibility to contamination and the loss of flow or pressure can be caused by extensive water main breaks, the destruction of pumps, or the disruption of power supplies, and cited these as major vulnerabilities to the nation's water supply systems.

In response to the report's findings, the President issued Presidential Decision Directive (PDD) 63 on critical infrastructure protection in 1998. This directive established a public-private partnership to put in place prevention, response, and recovery measures that would augment the security of the nation's critical infrastructure components against criminal or terrorist attacks. The directive designated the Environmental Protection Agency (EPA) as the lead federal agency to work with both public and private organizations to protect the nation's water infrastructure through the development of emergency preparedness strategies. The agency, in turn, appointed the Association of Metropolitan Water Agencies, a nonprofit organization representing the nation's largest utilities, to coordinate the water industry's role in emergency preparedness.

[1]The President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, October 1997.

Initially, this public-private partnership focused on the several hundred community water systems that each served more than 100,000 persons; the partnership was broadened in 2001 to include systems serving more than 3,300 people. Moreover, as was the case with other infrastructure sectors, PDD-63 focused primarily on threats to cyber security. Specifically, the directive established a goal to develop, within five years, a Water Information Sharing and Analysis Center (Water ISAC). The intent of the Water ISAC is, among other things, to facilitate the dissemination of alerts to drinking water and wastewater utilities about threats to their systems, to analyze incident information, and to serve as a secure source of sensitive information.

## Efforts to Further Improve Security after the September 11 Attacks

Efforts to improve protection of drinking water infrastructure were broadened and accelerated after the September 11 attacks. In particular, the partnership accelerated efforts to develop the Water ISAC, which became operational in December 2002. EPA and the drinking water industry also launched efforts to develop guidance, tools, and training programs to assist utilities in identifying their systems' vulnerabilities. As a major step in this regard, EPA supported the American Water Works Association Research Foundation and the Sandia National Laboratories to develop a vulnerability assessment (VA) methodology and training primarily for the largest water systems. EPA awarded approximately $51 million in fiscal year 2002 for water security grants to help these water systems complete vulnerability assessments.

These efforts to better understand drinking water systems' vulnerabilities were given a significant boost when the President signed the Public Health Security and Bioterrorism Preparedness and Response Act in June 2002.[2] Among other things, title IV of the Bioterrorism Act amended the Safe Drinking Water Act to require each community water system serving more than 3,300 individuals to conduct "an assessment of the vulnerability of its system to a terrorist attack or other intentional acts intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water." As illustrated in table 1, the act phased in this requirement according to system size, requiring vulnerability assessments for all systems serving populations greater than 3,300 to be completed by June 30, 2004.

[2]Pub. L. No. 107-188, 116 Stat. 594 (2002) ("Bioterrorism Act").

**Table 1: Vulnerability Assessment Completion Deadlines**

| System size (based on population served) | Vulnerability assessment completion deadline |
|---|---|
| 100,000 or more | March 31, 2003 |
| 50,000 to 99,999 | December 31, 2003 |
| 3,301 to 49,999 | June 30, 2004 |

Source: Bioterrorism Act, S 401(a)(2).

EPA guidance calls for these assessments to include: a characterization of the water system; the identification of possible consequences of malevolent acts; the critical assets subject to malevolent acts; an assessment of the threat of malevolent acts; an evaluation of countermeasures; and a plan for risk reduction. The Bioterrorism Act also requires each community water system serving more than 3,300 individuals to prepare or revise an emergency response plan incorporating the results of the VA no later than 6 months after completing the assessment. In addition, it directed EPA to provide guidance to smaller systems on how to conduct vulnerability assessments, prepare emergency response plans, and address threats.

## Potentially Larger Federal Financial Commitment Sought in Future Years

While significant federal funds have been committed to assist utilities in developing vulnerability assessments and emergency response plans, the likelihood exists that Congress and the Administration will be asked to provide much larger sums to go beyond *planning* for upgrading drinking water security to the actual *implementation* of security upgrades. By most accounts, it will cost billions of dollars to upgrade security for drinking water utilities. The American Water Works Association, for example, estimates that it will cost $1.6 billion for initial security upgrades at all drinking water utilities.

## Objectives, Scope, and Methodology

As requested in a June 9, 2003, letter to the Comptroller General from the Chairman and Ranking Minority Member of the Senate Committee on Environment and Public Works, this report identifies experts' views on the following questions:

- What are the key security-related vulnerabilities affecting the nation's drinking water systems?

- What are the criteria that should be used to determine how federal funds are allocated among recipients to improve drinking water security, and how should the funds be distributed?

- What specific activities should the federal government support to improve drinking water security?

To obtain information on these three questions, we conducted a three-phase Web-based survey of 43 experts on drinking water security. We identified these experts from a list of more than 50 widely recognized experts in one or more key aspects of drinking water security. In compiling this initial list, we also sought to achieve balance in terms of area of expertise (i.e., state and local emergency response, engineering, epidemiology, public policy, security and defense, drinking water treatment, risk assessment and modeling, law enforcement, water infrastructure, resource economics, bioterrorism, public health, and emergency and crisis management).

In addition, we attempted to achieve participation by experts from (1) key federal organizations (e.g., Argonne National Laboratory, Centers for Disease Control and Prevention, Department of Defense, Department of the Interior's Bureau of Reclamation, Environmental Protection Agency, and Federal Bureau of Investigation; (2) key state and local agencies, including health departments and environmental protection departments; and (3) key industry and nonprofit organizations such as the American Water Works Association (AWWA), RAND Corporation, Natural Resources Defense Council (NRDC), and National Rural Water Association (NRWA); and (4) water utilities serving populations of varying sizes. Of the 50 experts we contacted, 43 agreed to participate and complete all three phases of our survey. A list of the 43 participants in this study is included in appendix I.

To obtain information from the expert panel, we employed a modified version of the Delphi method. The Delphi method is a systematic process for obtaining individuals' views and seeking consensus among them, if possible, on a question or problem of interest. Since first developed by the RAND Corporation in the 1950s, the Delphi method has generally been implemented using face-to-face group discussions. For this study, however, we administered the method through the Internet. We used this approach, in part, to eliminate the potential bias associated with group discussions. These biasing effects include the dominance of individuals and group pressure for conformity. Moreover, by creating a virtual panel, we were

able to include many more experts than possible with a live panel, which allowed us to obtain a broad range of opinions.

For each phase in the Delphi method, we posted a questionnaire on GAO's survey Web site addressing the issues of our study. Panel members were notified of the availability of the questionnaire with an e-mail message. The e-mail message contained a unique user name and password that allowed each respondent to log on and fill out a questionnaire but did not allow respondents access to the questionnaires of others.

In the first questionnaire, we asked several broad questions, such as, "What strategies or methods should the federal government consider for allocating funds to water utilities (or other relevant entities) so as to ensure that allocation achieves the greatest mitigation of risk per dollar?" We pretested these questions with officials from the water utility industry, a nonprofit research group, and academe. Participants were invited to provide detailed narrative explanations for their responses.

In the case of two key questions, we sought to identify both additional detail and the degree to which consensus could be achieved among the experts on our panel. We used experts' responses to phase 1 questions to develop more detailed questions for phase 2 about specific actions or strategies regarding two overall issues: how federal funds could best be allocated among potential recipients to achieve the most security improvements per dollar, and which specific activities are most deserving of federal support. This second questionnaire included closed-ended questions that allowed panelists to rate the relative priority or effectiveness of these activities. It also provided experts with the opportunity to comment on their ratings.

During the third phase of the Delphi process, we provided the aggregated results from the ratings made in the second questionnaire. We also provided panel members with the individual ratings they had made in response to each question. We then invited panel members to use this information as a basis for changing their answers if they desired.

In addition to the information obtained from our expert panel, we obtained documentation from representatives of professional organizations, such as the National Academy of Sciences, RAND Corporation, American Water Works Association Research Foundation, and Association of Metropolitan Water Agencies. We also held several interviews with officials at EPA on the agency's drinking water security programs. During our interviews, we

asked officials to provide information on program operations, policies, guidance, and funding levels. We also received training on the Vulnerability Self Assessment Tool supported by the Association of Metropolitan Sewerage Agencies, and attended specialized conferences addressing drinking water security by the Water Environment Federation and other organizations.

We conducted our work from July 2002 through August 2003 in accordance with generally accepted government auditing standards.

# Experts Identified Key Vulnerabilities That Could Compromise Drinking Water Systems' Security

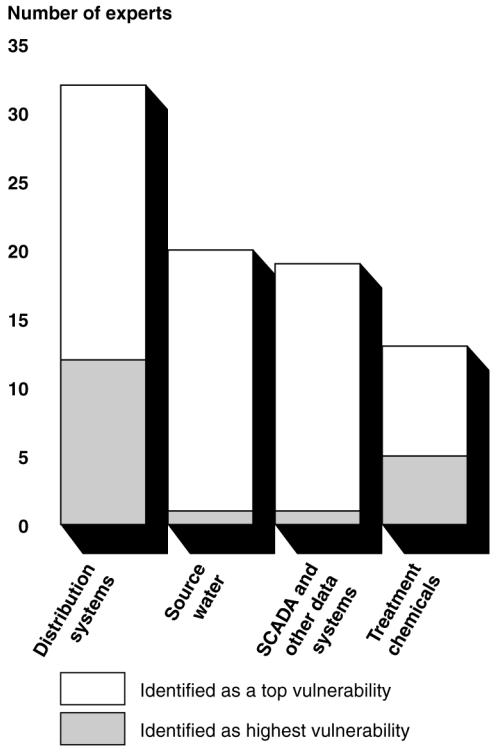
Our panel of experts identified several key physical assets of drinking water systems as the most vulnerable to intentional attack. In general, their observations were similar to those of public and private organizations that have assessed the vulnerability of these systems to terrorist attacks, including the National Academy of Sciences, Sandia National Laboratories, and key industry associations. In particular, nearly 75 percent of the experts (32 of 43) identified the distribution system or its components as among the top vulnerabilities of drinking water systems.

In addition to identifying systems' physical assets, experts also identified overarching issues compromising how well these assets are protected. Chief among these issues are (1) a lack of redundancy in vital systems, which increases the likelihood that an attack could render a system inoperable; and (2) the difficulty many systems face in understanding the nature of the threats to which they are exposed.

## Vulnerability of Physical Assets

As illustrated in figure 4, when asked to identify what they believed to be the top vulnerabilities of drinking water utilities, the four physical assets most frequently identified by the panel were: (1) the distribution system, (2) source water supplies, (3) Supervisory Control and Data Acquisition (SCADA) and other information systems, and (4) chemicals stored on site that are used to treat source water.

**Figure 4: Key Vulnerabilities Identified As Compromising Drinking Water Systems' Security**




Source: GAO analysis of expert panel's responses to GAO survey.

## Experts Identified Distribution Systems as Most Vulnerable

The distribution system delivers drinking water primarily through a network of underground pipes to homes, businesses, and other customers. While the distribution systems of small drinking water utilities may be relatively simple, larger systems serving major metropolitan areas can be extremely complex. One such system, for example, measures water use through 670,000 metered service connections, and distributes treated water through nearly 7,100 miles of water mains that range from 2 inches to 10 feet in diameter. In addition to these pipelines and connections, other key distribution system components typically include numerous pumping stations, treated water storage tanks, and fire hydrants.

Nearly 75 percent, or 32 of 43 of the experts on our panel, named one or more components of the distribution system as among the top vulnerabilities of drinking water systems. In fact, 12 of the 32 experts

identified distribution systems as the most critical vulnerability, a considerably greater number than any other system component. The explanations they offered most often related to the accessibility of distribution systems at numerous points. One expert, for example, cited the difficulty in preventing the introduction of a contaminant into the distribution system from inside a building "regardless of how much time, money, or effort we spend protecting public facilities." Experts also noted that since the water in the distribution system has already been treated and is in the final stages of being transferred to the consumer, the distribution of a chemical, biological, or radiological agent in such a manner would be virtually undetectable until it has affected consumers. An EPA official added, however, that distribution systems generally carry disinfectant residuals that can counteract the potentially harmful effects of contaminants. This official further stated that routine monitoring performed in drinking water systems might provide some advance warning. While research on the fate and transport of contaminants within water treatment plants and distribution systems is under way, according to one expert, limited technologies are readily available that can detect a wide range of contaminants once treated water is released through the distribution system for public use.

## Source Water

Nearly half the experts (20 of 43) identified source water as among drinking water systems' top vulnerabilities. Drinking water may come from surface water, groundwater, or both. The water cycle begins with rainwater and snowmelt that collect in lakes and rivers and that, in many cases, interact with groundwater. Large urban water supply systems tend to rely on surface water sources (rivers, lakes, and reservoirs), while smaller systems tend to rely more heavily on groundwater.

One expert raised concerns about the inherent challenge in protecting source waters, noting, "Because of the vast areas covered by watersheds and reservoirs, it is difficult to maintain security and prevent intentional or accidental releases of materials that could have an adverse impact on water quality." Other experts raised additional concerns about the vulnerability of water intake transmission lines, which regulate the transfer of water supplies to the systems' treatment plants.

Panel experts and others, however, have stated that concerns over source water contamination are mitigated somewhat by a number of factors. First, a large volume of water generally exists at the source, which in many cases can dilute the potency of agents introduced at this stage of the drinking

water production process. Second, unlike treated water in the distribution system, it generally takes many days before source water reaches the consumer, making it more likely that a contamination problem at this early stage of the drinking water production process can be detected or treated before consumers are affected. One utility official noted, for example, that his water system's surface water supplies travel hundreds of miles before reaching the treatment plant. Water that was contaminated at the source would take between 10 days and 6 months to reach the treatment plant, depending on the source, providing ample opportunity for detection and adjustments to protect public health.

## SCADA Systems

To improve their efficiency and reduce operating costs, drinking water utilities (particularly larger utilities) have come to rely increasingly on sophisticated computer systems to manage their facilities' key functions. These Supervisory Control and Data Acquisition (SCADA) systems allow utility operators to monitor and control processes throughout their systems, even at remote facilities. SCADA systems communicate with other control facilities and provide the necessary data to ensure that the right chemicals are mixed in the right amounts for treatment processes, and that water pressure and flow are at proper levels. SCADA systems may also monitor activity along water transmission pipelines, detecting breaks or pressure loss.

While SCADA systems help utilities manage their operations, they can create an additional opportunity for sabotage. Almost half of the experts on our panel (19 of 43) identified SCADA and other information systems as being among the top vulnerabilities of drinking water systems (although only one expert ranked it as the top vulnerability). Experts' concerns include cyber attacks on SCADA systems from a remote location, which could, for example, release harmful amounts of water treatment chemicals (such as chlorine) into treated water.

## Treatment Chemicals

The types and amounts of treatment chemicals applied by a drinking water facility to its influent varies, depending on the type of source water (for example, surface water or groundwater) as well as its quality. Because surface water systems are exposed to direct wet-weather runoff and to atmospheric forces, they generally require more treatment under federal and state regulations than do groundwater systems.[1]

Water suppliers use a variety of treatment processes to remove contaminants from drinking water. The most commonly used treatment processes for surface water include filtration to remove particles such as clays, silts, and microorganisms; flocculation and sedimentation to consolidate small particles into larger particles that can be more easily removed from the water; and disinfection to eliminate bacteria and other microbiological contaminants.

Treatment chemicals are used in some of these processes. The disinfection process is particularly noteworthy in this regard; chlorine, chloramines, or chlorine dioxide not only are used at the treatment plant, but also are frequently present in some form in the pipes that distribute water to homes and businesses.

Thirteen of the 43 experts identified treatment chemicals as among the top vulnerabilities of drinking water systems, second only to the distribution system. Experts commented that it was inherently dangerous to use and store large cylinders of gaseous chlorine, noting that the destruction of these storage containers could release toxic chlorine gas in densely populated areas. Some of these experts noted, however, that this risk is being alleviated as utilities increasingly use the more stable liquid form of chlorine instead of the more vulnerable large compressed-gas chlorine canisters that have traditionally been used. In addition to the risks of chemical sabotage at the treatment facility, one expert cited the risk of using tainted treatment chemicals at the facility. According to another expert, "If these treatment chemicals have been purposely contaminated . . . prior to delivery, every precautionary measure taken by the water system has been bypassed."

[1]A discussion of the influence of these factors on treatment is available in the preamble in both the Surface Water Treatment Rule and the Stage I Disinfectants/Disinfection Byproducts Rule.

## Overarching Issues Affecting Drinking Water Systems' Security

In addition to the vulnerabilities associated with specific water system components, experts identified several overarching issues that compromise the integrity of physical assets and the drinking water system in its entirety. Chief among these issues are (1) the lack of redundancy among vital systems, and (2) the difficulty many operators face due to a lack of information on the most serious threats to which their systems might be exposed.

### Lack of Redundancy among Vital Systems

Drinking water systems are generally "linear" in nature in that they have single transmission lines leading into the treatment facility, single pumping stations along the system, and a single computer operating system. Furthermore, drinking water systems may rely on outside sources of power and communications, and depend on the transportation sector for the delivery of supplies, often from a limited number of suppliers. If any of these external sources were impaired or destroyed, the entire system could be compromised. Under these circumstances, any "single point of failure" could render a system inoperable unless there are redundant systems in place.

Several experts reflected concerns relating to a single point of failure as a vulnerability. For example, according to one expert, the destruction of a single physical component of the system, such as a single water transmission line into the treatment facility, could render the entire system inoperable. Moreover, she noted, a system that depends on pumps can be completely put out of service if its electrical supply were interrupted. Echoing this point, another expert commented, "Experience with Y2K planning efforts revealed one of the critical interdependencies nearly all water utilities have is with the electrical power supply system. Disruption of power supply could have significant impacts on source, treatment and distribution systems."[2]

According to one expert, efforts are needed to add redundancy to drinking water systems and to mitigate systems' near-total reliance on power suppliers, communications systems, and the transportation sector. However, such efforts to duplicate major system components would be expensive and could conflict with the systems' goals of controlling rate

[2]These comments, made prior to the electric supply disruption of August 2003, were vividly illustrated when that power outage severely disrupted the water supplies of several cities.

increases. To address the problem, some experts advocated the creation of utility consortia, such as the Bay Area Security Information Collaborative (BASIC) and the Mutual Aid Disaster Intervention Response Teams (MADIRT), through which regional utilities share resources in the event of a disaster.

## Insufficient Information to Understand the Most Significant Threats

A number of experts commented that it is impossible to accurately identify a utility's most significant vulnerabilities unless the utility has reliable intelligence regarding its most significant threats. Threats include the type of adversary (a casual vandal, an anonymous hacker, a disgruntled employee, or a dedicated terrorist) as well as the mode of attack (physical, psychological, chemical, biological, or radiological). According to the American Water Works Association, a utility's assessment of its most credible threats should be based on knowledge of the threat profile in its specific area, including such information as past events, that could shed light on future risks. These assessments often require information from outside sources, such as local law enforcement officials.

Many experts on our panel noted, however, that such information has not been easy for utilities to obtain. The following examples illustrate some of the difficulties utilities have regarding threats:

- According to one expert, "The utility community has very little specific and useful information on the threat posed to this industry. This represents a real vulnerability since it makes it harder to judge where resources might do the most good." Furthermore, "an ongoing working relationship with groups (mostly federal) that do this type of analysis could prove extremely valuable in determining how to allocate the limited resources available."

- Utilities may be preoccupied with unsubstantiated threats, according to another expert. She noted, "There are many very vulnerable areas, but the terrorists may not be technically able to target them, or they may not be interested."

- Another expert stated that utilities need to better understand "how the threats may . . . exploit utility operations and infrastructure," through such things as simulation exercises.

- One expert suggested that the intelligence community provide better threat information and share it with the water sector through the Water ISAC.

Since the consequences associated with various potential threats are markedly different, EPA guidance suggests that the threats be analyzed in the system's vulnerability assessments.[3] Some vulnerability assessment methodologies refer to the threats selected for consideration as a Design Basis Threat. Because there is no single Design Basis Threat[4] for all water systems in the United States, water systems often have a difficult time identifying their unique threat profile. As a result, EPA developed a Baseline Threat Information document for systems serving populations greater than 3,300 to help assess the most likely threats to their systems.

[3]Environmental Protection Agency, *Vulnerability Assessment Fact Sheet*, EPA 816-F-02-025, November 2002, available on the Web at http://www.epa.gov/ogwdw000/security/va_fact_sheet_12-19.pdf.

[4]Design Basis Threat: The threat serves as the basis for the design of countermeasures as well as the benchmark against which vulnerabilities are assessed.

# Experts' Views on the Allocation and Distribution of Federal Funds

Many drinking water utilities have been financing at least some of their security upgrades by passing along the costs to their customers through rate increases. Given the cost of these upgrades, however, the utility industry is also asking that the taxpayer shoulder some of the burden through the congressional appropriations process. Should Congress and the Administration agree to this request, they will need to address key issues concerning who should receive the funds and how they should be distributed. With this in mind, we asked our panel of experts to focus on several key questions: (1) To what extent should utilities' vulnerability and risk assessment information be considered in making allocation decisions? (2) What types of utilities should receive funding priority? and (3) What are the most effective mechanisms for directing these funds to recipients? Overall, we found a high degree of consensus on the following:

- Vulnerability assessment may be a useful tool in determining which utilities receive priority for federal funds to improve security. Several factors, however, complicate the government's ability to use a primary source of this information—the vulnerability assessments (VA) required of utilities under the Bioterrorism Act. Among the factors, the act prohibits disclosure of information derived from these assessments submitted to EPA.

- Almost all of the experts gave utilities serving high-density populations a high or highest funding priority. Utilities serving critical assets (such as military bases and other sensitive government facilities, national icons, and key cultural or academic institutions) were also recommended as high-priority recipients, while relatively few experts recommended a high or highest priority for utilities serving rural or isolated populations.

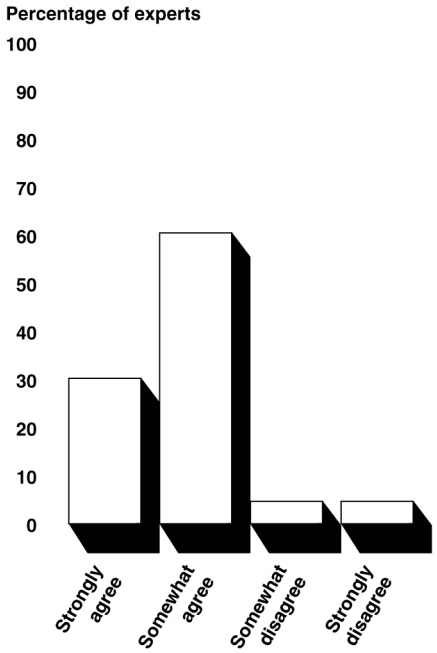
- Direct federal grants are the most favored funding mechanism, with many experts indicating that such grants should include a requirement for matching funds from the recipient. Relatively fewer experts recommended the use of the Drinking Water State Revolving Fund, particularly for upgrades to be implemented in the near term.

## Strong Agreement That Allocation Decisions Should Consider a Utility's Vulnerability Assessment

As noted in chapter 1, the Bioterrorism Act requires that vulnerability assessments be prepared by all community water systems serving more than 3,300 individuals. EPA guidance on preparing these assessments states that the assessments should (1) characterize the water system, including its mission and objectives; (2) identify and rank the possible consequences of malevolent acts; (3) determine the critical assets subject to malevolent acts; (4) assess the threat of malevolent acts; (5) evaluate existing countermeasures; and (6) analyze risk and develop a plan for reducing risk and addressing critical priorities first.

In considering whether it is appropriate to use vulnerability and risk assessment information when making federal funding decisions, about 90 percent of the experts on our panel (39 of 43) strongly agreed or somewhat agreed that funds should be allocated on the basis of VA information. Some experts cited the vulnerability assessments required by the Bioterrorism Act as the best available information about the current condition of our security infrastructure for drinking water (see fig. 5).

**Figure 5: Experts' Views on Whether Federal Funds Should Be Allocated Based on Vulnerability Assessment Information**




Source: GAO analysis of expert panel's responses to GAO survey.

It may not be a straightforward matter, however, to use this information in making such decisions. Several experts pointed to a number of complicating factors. One pointed out that "vulnerability assessment (VA) tools were not set up for the purpose of identifying and prioritizing capital improvement needs for EPA or other federal agencies." He added, "Using the VAs would require a high degree of interpretation and judgment on someone's part . . ., using a tool that was not designed to clearly delineate capital construction needs." Another expert noted similarly that "since there is no written guidance for threat analysis, there will have to be some method to rank relative threats among different areas." In addition, one expert pointed out an inherent dilemma affecting *any* effort to prioritize

funding decisions based on the greatest risk—whatever does not receive attention becomes the best target.[1]

In addition, a provision of the Bioterrorism Act precludes disclosing all information "derived" from the vulnerability assessments submitted to EPA. The provision's intent was to protect sensitive information about utilities' vulnerabilities from falling into the hands of individuals who seek to harm the utility. The act therefore specifies that only individuals designated by the EPA Administrator may have access to the copies of the VA and information contained in or derived from it. It further specifies that the information must remain protected at all times.

Thus, while some EPA officials may have access to the information, the requirement limits how the agency may use that information. EPA would have difficulty, for example, in citing vulnerability assessment findings to support decisions or recommendations on allocating security-related funds among utilities, as well as decisions concerning research priorities or guidance documents.

To compensate somewhat for these limitations, the American Water Works Association Research Foundation has initiated a project in which consultants and trainers, who have conducted multiple assessments, are seeking to identify lessons learned from the vulnerability assessments done to date. According to EPA's draft Water Security Research and Technical Support Implementation Plan, this project is designed to obtain a more accurate picture of the major vulnerabilities that are generally facing the nation's drinking water systems and to share that understanding with interested parties.[2] EPA and the Research Foundation plan to use the results of this project to identify high priority needs and concerns that could likely be best addressed by EPA, the research community, or both. This project is scheduled for completion in mid-2004.

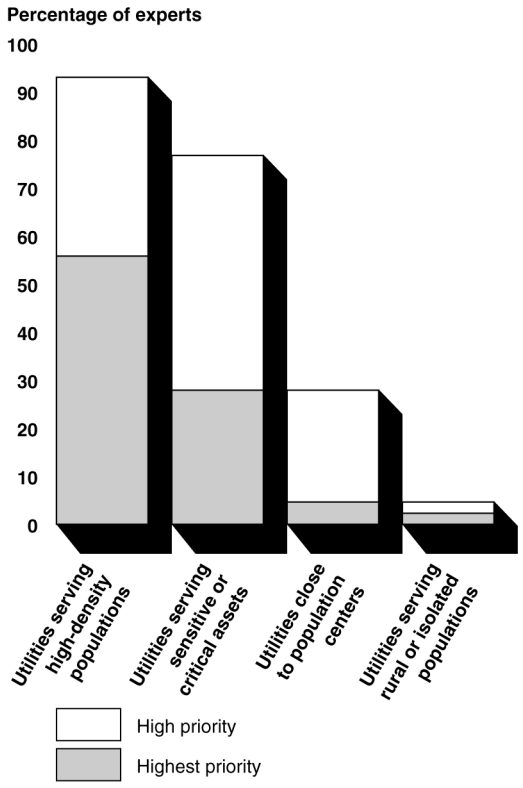
[1]Citing this reason, one expert suggested the addition of a "dual use" criterion in which the funds spent would also fix some existing utility deficiency, such as noncompliance with a drinking water standard.

[2]Environmental Protection Agency, Office of Water, Office of Research and Development, *Water Security Research and Technical Support Implementation Plan*, *Preliminary Working Draft*, July 2003.

## Key Criteria to Help Determine Which Utilities Should Receive Funding Priority

The experts identified several characteristics of utilities that should be used to set funding priorities. The most frequently identified were utilities (1) serving high-density populations; (2) serving sensitive or critical assets, such as military bases, academic institutions or icons of American culture; (3) in proximity to population centers (whether they serve these population centers or serve outlying areas); and (4) serving rural or isolated populations, such as small systems with less sophisticated water systems (see fig. 6).

**Figure 6: Experts' Views on Which Types of Water Utilities Should Receive Priority for Federal Funds**




Source: GAO analysis of expert panel's responses to GAO survey.

*Utilities Serving High-Density Populations*. Approximately 93 percent of the experts (40 of 43) gave high or highest priority to funding utilities serving high-density populations. As one expert commented, directing

limited resources to protect the greatest number of people is a common strategy when setting priorities. Most experts shared this view, including one who noted the "population served would probably lead to economies of scale—you can protect the most people by spending monies at the large systems." This expert and others, however, though supportive of funding priority for utilities serving high-density populations, cautioned that while targeting high-density populations may be the most equitable to the entire country, it might not allocate enough to small systems.

*Utilities Serving Sensitive or Critical Assets*. Seventy-seven percent of the experts (33 of 43) indicated that utilities serving sensitive or critical assets should receive a high or highest priority for federal funding. Experts identified such utilities as those servicing national icons that represent the American image, those serving military bases, or those serving sensitive government, academic and cultural institutions. In addition, according to one expert, utilities in areas typically receiving extensive media coverage, or that serve venues where large groups gather, may be of interest to terrorists.

*Utilities in Proximity to Population Centers*. Twenty-eight percent of the experts (12 of 43) cited the proximity of a given utility to a major population center as at least a high funding priority. While most utilities close to population centers would be expected to serve the population center in which they are located (hence, this third criterion would overlap with the first criterion above—utilities serving high-density populations), some experts pointed out that this is not always the case. Exceptions cited include suburban utilities that may serve communities or their major metropolitan areas. Several particularly noted that the risks associated with an airborne release of chlorine gas elevated their funding priority for this criterion.

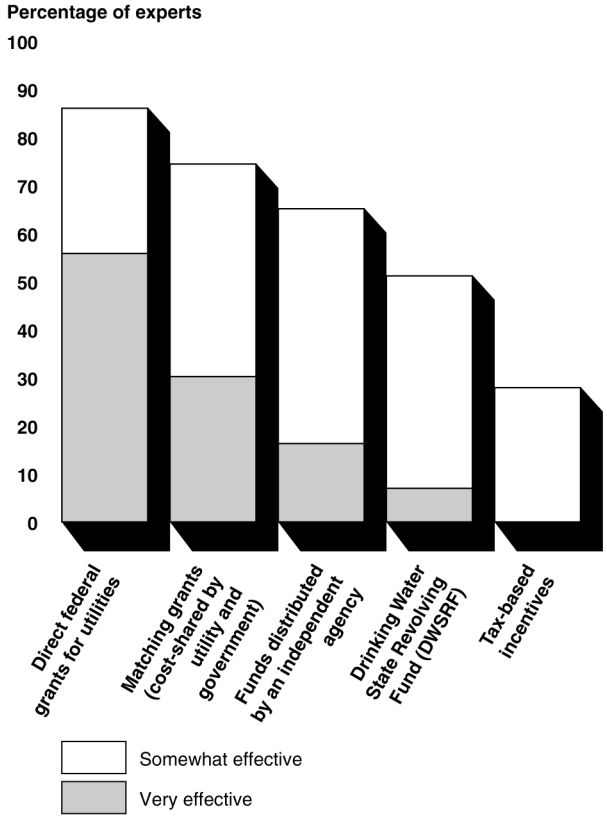
*Utilities Serving Rural or Isolated Populations*. About 5 percent of the experts (2 of 43) identified utilities serving rural or isolated populations as at least a high priority for federal funding. Generally, these panelists commented that such facilities are least able to afford security enhancements, and therefore most need federal support. One expert, for example, stated that in light of their financial constraints, "smaller utilities do the cheapest thing possible, which means you do a quick checklist and then forget about it." He added that because these smaller systems do not have enough staff to do a comprehensive assessment, they need funding to either hire additional staff or to contract for outside expertise.

Importantly, the relatively small percentage of experts supporting funding for rural utilities may not fully reflect the concern many panel experts have for the safety of these utilities. For example, several who supported higher priority for utilities serving high-density populations cautioned that, while problems at a large utility will put more people at risk, utilities serving small population areas may be more vulnerable because of weaker treatment capabilities, fewer highly trained operators, and more limited resources. Another expert added that most waterborne disease outbreaks have occurred in the systems of smaller utilities.

## Funding Mechanisms Recommended for Distributing Federal Funds

We also asked the expert panel to comment on how federal funds should be distributed to recipients. Nearly 90 percent said that direct federal grants to utilities would be a somewhat or very effective means of distributing funds to support security improvements. The experts also showed strong support for grants in which some type of match is required of recipients. Figure 7 shows their views on these and other funding mechanisms.

**Figure 7: Recommended Approaches for Distributing Federal Funds**




Source: GAO analysis of expert panel's responses to GAO survey.

## Direct Federal Grants

Eighty-six percent of the experts (37 of 43) indicated that direct federal grants to the utility would be somewhat or very effective in allocating federal funds. Federal grants typically provide funding for fixed or known periods for specific projects and often have associated terms and conditions. One expert cited EPA's recent efforts to quickly distribute security-related grant funds to systems serving over 100,000 people (mentioned earlier in this chapter), noting, "By far the most successful funding program I have seen to date was the large water system Vulnerability Assessment Grant program directed through the EPA."[3]

Many experts commented that direct grants could be particularly useful in quickly addressing lower-cost and more obvious fixes, such as adding gates and security cameras. Two others said that with some of these shorter-term items addressed, it may then be appropriate to deal with more complex issues that require longer-term fixes, such as new buildings and security-oriented building design. Another expert added that the use of direct EPA grants could help ensure proper use of the funds, noting, "Direct EPA grants to water systems should be made available and should carry a requirement to use Sandia-like methodologies and concepts," and that "the use of [these tools] will lead water systems to develop cost-effective risk reduction through effective physical systems, better policies, procedures and training and through creative consequence mitigation."

## Matching Grants

Many favoring direct grants were among those who said that a matching requirement for such a grant would be desirable for distributing future federal funds. Specifically, 74 percent of the experts (32 of 43) said that federal grants with a matching requirement would be somewhat or very effective in distributing federal funds. One expert pointed out that such a requirement would effectively leverage limited federal dollars. Another agreed, noting that such a cost-sharing approach would offer "a big incentive" in getting utilities to devote their own funds to enhance their security. The expert cautioned, however, that the required match would

[3]As noted earlier in this report, these grants supported VAs, remediation planning, and emergency plan development through August 2002. EPA issued grant awards to over 400 publicly owned and privately owned community water systems that regularly serve populations over 100,000. This program was noncompetitive, and all eligible utilities that submitted completed grant applications received awards. The value of each grant did not exceed $115,000. An EPA official pointed out that higher dollar grant programs might have additional administrative requirements.

have to be low enough to make the grant attractive, suggesting a maximum of 50 percent.

Another suggested a strategy to get the most out of a matching grant program. One, for example, said that participating utilities should be provided with some initial matching funds to get started, and that additional funds would then be contingent upon how effective or creative they were in using the first round of funding.

## Funds Distributed by an Independent Agency

Sixty-five percent of the experts (28 of 43) indicated that it would be somewhat or very effective to have federal funds distributed through an independent agency. Experts generally characterized an independent agency as, among other things, being independent of regulatory decision making, and not bound by traditional points of view.

Several experts elaborated on the desirability of such an independent entity to allocate security-related funds. One expert, for example, favored moving the responsibility for allocating funds to a disinterested third party—one with no infrastructure to support or hidden agenda but instead with strong decision analysis and consensus building expertise. Another expert suggested that federal funding be "leveraged with industry funding through an organization like [the American Water Works Association Research Foundation.]" The expert further stated that the use of an organization like the Research Foundation is important because it has a demonstrably effective two-way communication with the end users, namely the U.S. water utility industries; the Research Foundation can adequately represent the needs of industry to the research community as well as inform the industry of important national-level research findings that will influence their day-to-day operations. He indicated that communication between the water utilities and such an independent agency would be superior to communication between the utilities and EPA, noting, "Although [EPA] is legitimately engaged in research, [it] is also perceived as an agency with regulatory authority and is thus viewed somewhat circumspectly by industry as a whole."

## Drinking Water State Revolving Fund

About 51 percent of the experts (22 of 43) indicated that the Drinking Water State Revolving Fund (DWSRF) would be somewhat or very effective in distributing federal funds. The DWSRF program provides federal grant funds to states, which in turn allow the states to help public water systems in their efforts to protect public health and ensure their compliance with the Safe Drinking Water Act. States may use DWSRF funds to provide loans to public water systems, and may reserve a portion of their grants to finance other projects that protect sources of drinking water and enhance the technical, financial, and managerial capacity of public water systems. In particular, under EPA's November 2001 guidance, states may use DWSRF assistance to help systems complete both vulnerability assessments, and contingency and emergency response plans.[4] Many types of security-related infrastructure improvements to ensure security are also eligible for DWSRF funding, as specified in the EPA guidance.

According to one expert who favored existing grant and loan programs like the DWSRF for enhancing security, continuing to support the training and assistance efforts of lead state agencies "is the most beneficial activity the federal government could play to encourage water utilities across the country to address security related issues in a comprehensive and cost-effective manner." Another shared this view, explaining that states are well-positioned to help manage the process, and that they "must approve system upgrades anyway." This expert also suggested that by using the state-administered DWSRF, "states could track this information and report it on a regular basis to EPA and Congress," thereby documenting what has been accomplished and what still needs to be done.

One expert cautioned, however, that the DWSRF would be effective only if a process were established that separated funding for security-related needs from other infrastructure needs. Reflecting the concern expressed by many others about the timeliness of distributing funds through the DWSRF, this individual commented that the current DWSRF process is too bureaucratic and requires too many hurdles for it to be an expeditious means for providing funds.

[4]Environmental Protection Agency, Office of Water, *Use of the Drinking Water State Revolving Fund (DWSRF) to Implement Security Measures at Public Water Systems*, EPA 816-F-02-040, November 2001, available on the Web from http://www.epa.gov/ogwdw000/dwsrf/security-fs.pdf.

## Tax-Based Incentives

About 28 percent of the experts (12 of 43) reported that tax-based incentives would be somewhat effective in encouraging water utilities—specifically privately owned utilities—to invest in security improvements. The inducements offered in these programs may include tax credits, property tax exemptions or abatements, and sales and use tax exemptions.

According to one expert, tax incentives could increase the efficiency of dollars spent on water security, generating new ideas and approaches. Furthermore, by offering additional funds for creative and cost-effective solutions, these ideas could become best practices and shared with others. Finally, he commented, "If allocations were phased and secondary funds were based upon how well the first funds were spent, there would be incentive to spend the first funds wisely." Another expert suggested that the provision of financial or other tax incentives to utilities should be contingent upon evidence that they have improved their security as defined by a standard set of measurements.

# Activities Experts Identified As Most Deserving of Federal Support

When experts were asked to identify and rate the specific security-enhancing activities most deserving of federal support, the activities experts most frequently identified fell into three broad categories:

- *Physical and technological improvements*. These improvements include altering drinking water systems to improve physical security, and conducting research and development on technologies to prevent, detect, or respond to an attack. Experts most strongly supported near real-time monitoring technologies, which they considered particularly useful in quickly detecting contaminants in water that has left the treatment plant for consumers.

- *Education and training*. This category includes, among other things, supporting simulation exercises to provide responders with experience in carrying out utilities' emergency response plans; specialized training of utility personnel charged with security and general training to improve the security awareness of their staffs; and multidisciplinary teams that can provide independent analysis of utilities' security preparedness and recommend security-related improvements.

- *Strengthening working relationships between utilities and other public agencies*. This category includes strengthening relationships between water utilities and other entities that may have key roles in an emergency response (such as public health agencies, enforcement agencies, and neighboring utilities). It also includes developing common protocols to engender a consistent approach among utilities in detecting and properly diagnosing threats, and testing local emergency response systems to ensure that participating agencies coordinate their actions effectively.

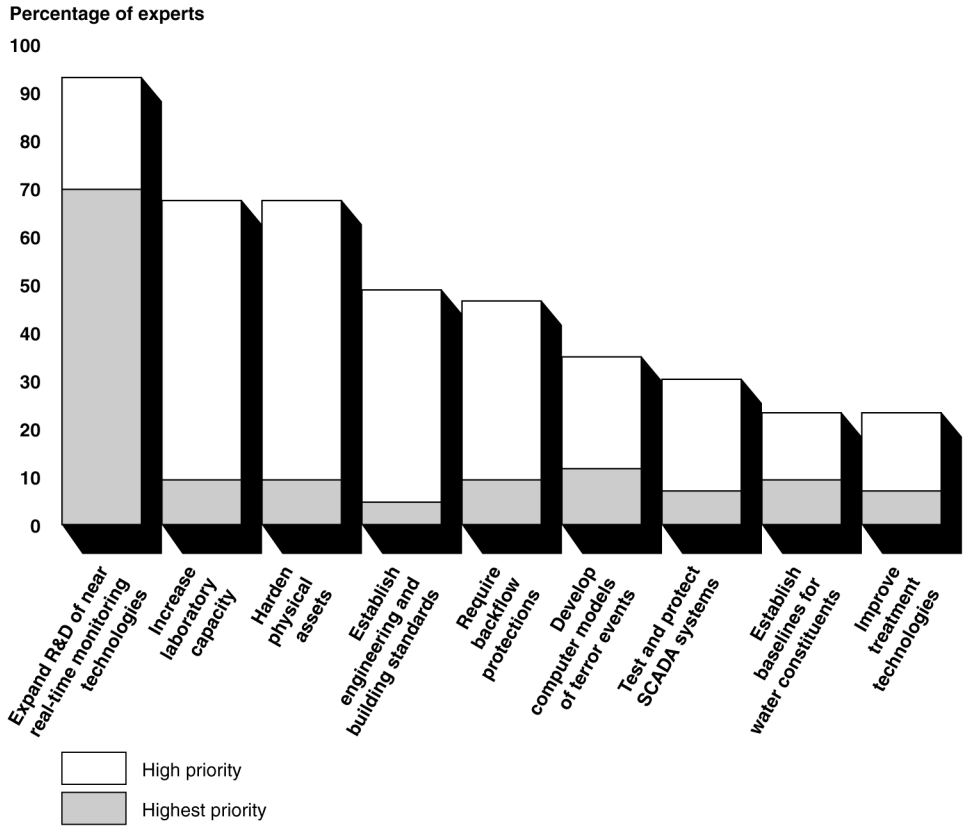
We found that EPA has a number of initiatives that address many of these activities, some of which are required by the Bioterrorism Act. In most cases, however, the activities are in the planning stages, are limited in scope, or are dependent on the availability of future appropriations.

## Activities to Enhance Physical Security and Support Technological Improvements

Our panel of experts most frequently recommended nine types of activities to improve physical security and support technological improvements, as figure 8 shows. Of the nine types, the development and implementation of near real-time monitoring technologies was rated by far the most important activity warranting federal support, with many experts stating that this

critical activity would probably not be implemented by many utilities without some degree of federal support.

**Figure 8: Activities Identified by Expert Panel to Enhance Physical Security and Support Technological Improvements**




Source: GAO analysis of expert panel's responses to GAO survey.

## Developing Near Real-Time Monitoring Technologies Viewed As Highest Priority

Approximately 93 percent of the panel experts (40 of 43) rated the expansion of research and development of near real-time monitoring technologies as having at least a high priority. These technologies were cited as critical to helping drinking water systems detect and respond quickly to threats or actual contamination events, to minimize the impact of any contamination by facilitating a quick response, and to help in restoring systems after an event. Significantly, almost 70 percent of the experts (30 of 43) rated this activity as warranting the highest priority for

federal funding—far surpassing the rating of any other category. Most of these experts indicated that smaller utilities would be unable to use these technologies without federal support.

A wide variety of monitoring technologies can be used in drinking water systems and, depending on their specific functions, may be deployed at locations upstream from, within, or downstream from drinking water treatment plants. Conventional monitors typically measure things such as pH (acidity and alkalinity), turbidity, conductivity, temperature, organic compounds and other contaminants. Biomonitors employ living organisms, such as fish or algae, to provide information on other water constituents that may impair human health or the environment.

Emerging monitoring technologies are capable of providing near real-time results for a wider array of potentially harmful water constituents. According to some experts, near real-time monitors may be strategically placed at points within the distribution system, where they may be able to quickly detect potentially dangerous backflows that may enter the system. They may also be used to augment a system's conventional monitoring system. As some experts suggested, for example, pressure sensor systems and biodetector networks could benefit the utility in its security preparedness as well as its regular operations by describing breaches or leaks in water mains, or by observing microbial contamination in a nonterrorist event. Some monitors based on emerging technologies capable of providing near real-time results may also be placed at the "point of service," where they can alert the consumer or utility about the potential for contaminated water entering a home or business.

These views are substantiated by a 2002 report by the National Academies of Science, which also highlighted the need for improved monitoring technologies as one of the four highest-priority areas for drinking water research and development. The report noted that such technologies differ significantly from those currently used for conventional water quality monitoring, stating further that sensors are needed for "better, cheaper, and faster sensing of chemical or biological contaminants."[1]

[1]The National Research Council of the National Academies, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington, D.C.: The National Academies Press, 2002).

The need for near real-time monitoring technologies was also recognized in the Bioterrorism Act, which directed EPA to review analytical methodologies and detection techniques that can quickly and accurately provide information on contaminants.[2] As an initial step in meeting this requirement, the agency is reviewing such early warning systems, including those designed to monitor levels of chemical, biological, and radiological contaminants or indicators of contaminants.

EPA is also planning to launch a number of projects through its Office of Water and Office of Research and Development. For example, one project, planned for November 2003 through May 2004, would entail a detailed examination of commercially available real-time monitors. According to EPA, the information derived from this project would be placed in a compendium for manufacturers and vendors of monitoring technology, allowing them to better focus technology development efforts.[3] Another project aims to evaluate how well many currently used water monitoring technologies would deal with the introduction of various contaminants.[4] Among other efforts, EPA also hopes to begin a project in November 2003 to test and evaluate the applicability of other industries' monitoring technologies to the security-related monitoring needs of drinking water systems. EPA's preliminary cost estimates for monitoring-related projects are about $5 million, and their initiation or completion will depend on the availability of fiscal year 2004 and 2005 funds.

[2]Bioterrorism Act, S 402.

[3]In addition, since August 2002, EPA has augmented its Environmental Technology Verification (ETV) Program to include water security issues. The ETV Program can be used to test, evaluate, and eventually bring promising technologies (e.g., detection and "point of use" treatment technologies) to the marketplace. EPA has spent approximately $2 million of fiscal year 2002 supplemental funds on the ETV Program and its related projects, and estimates the total costs for the ETV projects at $8.1 million. Once technologies are verified, EPA believes the technology can be tested in pilot-scale studies and potentially used at drinking water systems.

[4]This work is planned to review both large and small treatment system monitoring capabilities, distribution systems, and remote telemetry monitoring research, and will be conducted in controlled conditions at the Office of Research and Development's Water Awareness Technology Evaluation Research and Security Center, located at EPA's Test & Evaluation Facility. The work is projected to end around December 2005.

## Increasing Laboratories' Capacity to Deal with Terrorist Attacks

Over two-thirds of the experts (29 of 43) rated increasing laboratory capacity as a high or highest priority for federal funding. Many experts on our panel commented that laboratories are being challenged just to keep up with their normal responsibilities to collect, test, and analyze large volumes of water samples for water utilities and other clients. Consequently, they expressed reservations about the ability of laboratories to handle these responsibilities in the event of "surge" events caused by the chemical, biological, or radiological contamination of water supplies.

As one expert explained, few laboratories can test for a full range of contaminants, and these limitations would be amplified if the laboratories had to respond to a terror-related emergency. Another expert believed that in the event of an emergency, many utilities would be confused about which labs to use for testing samples of suspect water, and that a network of labs needs to be established so that quick results of tests could be obtained. The National Academies of Science report raised similar concerns, adding that legal concerns over the accuracy of laboratories' tests may make them reluctant to participate in testing under such severe conditions. The report concludes that a "dearth of laboratory capacity poses a serious limitation to our ability to respond to a contamination attack on the water system."[5]

One panelist suggested that state health departments need additional federal funds to better develop the regional capacity to sample water, and to improve analytical techniques used to detect contaminants. He further noted that state laboratories can and would serve as a component of an emergency response team, and that it would be effective for state laboratory programs to integrate these new or increased responsibilities with their existing responsibilities under grants from the Centers for Disease Control and Prevention.[6]

[5]The National Research Council of the National Academies, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington, D.C.: The National Academies Press, 2002).

[6]The Centers for Disease Control and Prevention (CDC) currently supports programs directed to states in order to improve laboratory capacity and to ensure public health preparedness, such as the Emerging Infections Program, the infectious disease Epidemiology and Laboratory Capacity Program, and the National Electronic Disease Surveillance System. For fiscal year 2003, CDC made approximately $870 million available to applicants.

EPA is actively supporting research in order to improve laboratory capacity nationwide, and has identified a series of ongoing and future projects toward that end. One project, which was due for completion in September 2003, would result in a water-specific compendium of laboratories that may be able to assist water utilities if contamination occurs. A related project would assess existing laboratory capacity to analyze drinking water samples in emergency situations. Another project, initiated in June 2003, is intended to analyze resource limitations at laboratories, such as personnel, equipment, training, and methods, and to provide recommendations to address these limitations.

According to EPA water officials, the agency may spend approximately $2.4 million starting in fiscal year 2003 to carry out these and other projects to assess and address the capacity of the nation's laboratories to deal with emergency situations. However, the experts' views on this matter suggest that given the magnitude of this long-standing problem—even under normal circumstances—it will be difficult enough to accurately characterize the challenge of laboratory analysis during a drinking water emergency, much less address the problem effectively.

## "Hardening" Assets and Completing Other Physical Improvements

Over two-thirds of the experts (29 of 43) rated activities that would improve (or "harden") the basic physical security of drinking water systems as warranting either a high or highest priority for federal funding. These activities include, among others, adding or repairing fences, locks, lighting systems, and cameras and other surveillance equipment. The National Academies of Science report reached similar conclusions about the need to harden certain facilities. It describes how many parts of the drinking water infrastructure remain highly accessible, and notes that access controls need to be improved. The report further noted that improved technologies are needed to protect against explosives delivered by motor vehicle or rail.[7]

However, the experts' support for hardening activities came with some notable caveats. For example, one expert said that many utility operators are reluctant to invest in physical upgrades because of fiscal shortfalls and other competing Safe Drinking Water Act requirements, despite the potential for such upgrades to be relatively cheap (many costing less than

[7]The National Research Council of the National Academies, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington, D.C.: The National Academies Press, 2002).

$5,000 per system). According to this expert, if "an effective and adequate grant program could be developed and managed," small amounts of funding could address the problems of many small drinking water systems.

Some experts also cited the limitations inherent in efforts to comprehensively harden the physical drinking water facility. For example, unlike nuclear power or chemical plants, drinking water system assets are not concentrated in a geographically secure area that can be hardened against all types of contamination or attack. Rather, they are spread over large geographic areas, particularly the source water and distribution systems. Thus, these panelists noted, while some degree of physical security enhancement at drinking water facilities is appropriate, efforts to construct physical barriers to comprehensively thwart attacks would be of limited effectiveness. Several said that efforts might be better directed at intruder detection, or adding security guards or electronic equipment.

The American Water Works Association Research Foundation is designing a project that will collect information on vulnerabilities, threats, potential security improvements, and innovative solutions to certain physical vulnerabilities. This project began in June 2003 and is scheduled for completion in July 2004. EPA also noted that utilities may be eligible to use a portion of the Drinking Water State Revolving Fund for this purpose.[8]

## Establishing Engineering Building Standards

Approximately 49 percent of the experts (21 of 43) rated the establishment of engineering and building standards for drinking water systems, which integrate security concepts into building design, as having either a high or highest priority for federal funding. Some noted that improved standards could yield multiple benefits by improving upon the design and functionality of a drinking water system while augmenting security to guard against attack.

Others wrote that new drinking water systems, which are being constructed and designed regularly, provide opportunities for incorporating security measures. One expert noted specifically that new design measures "may include increased physical security, elimination of

[8]Environmental Protection Agency, Office of Water, *Use of the Drinking Water State Revolving Fund (DWSRF) to Implement Security Measures at Public Water Systems*, EPA 816-F-02-040, November 2001, available on the Web at http://www.epa.gov/ogwdw000/dwsrf/security-fs.pdf.

'single points of failure,' the inclusion of redundancy into the overall design," or the creation of multiple pathways from source to tap. Another noted that the development and implementation of new or upgraded systems with better layouts can reduce unauthorized access, improve detection, and assist in isolating problems at the water facility.

According to another expert, standardization is needed across local jurisdictions so that neighboring providers may assist one another in a crisis. This view was echoed in the National Academies of Science report, which concluded that the lack of standardization impedes the introduction of new processes and technology."[9]

According to the EPA Action Plan, the agency is also considering the development of information on building standards that could enhance security of drinking water facilities, while improving operations and better protecting water quality. The plan noted that such standards would be modeled after those developed by the Department of Defense, which found that "dual use" aspects of improved design features are desirable because many security enhancements are not cost effective without some form of multiple benefit.[10] Specifically, the proposed EPA plan includes working with standards-setting organizations to develop voluntary design standards and recommendations for new construction, reconstruction, and retrofitting of drinking water facilities with a focus on integrating security with ongoing operations.

## Requiring Backflow Protections in Water Distribution Systems

Inappropriate use of piping systems, whether intended or not, could result in a backflow of contaminated water into distribution systems, where it could then find its way to other consumers. Backflow protection devices are one way to potentially mitigate this threat when installed either at access points to buildings or homes, or at cross connections in the distribution system.

[9]The National Research Council of the National Academies, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington, D.C.: The National Academies Press, 2002).

[10]Department of Defense, *Unified Facilities Criteria (UFC): Department of Defense Minimum Antiterrorism Standards for Buildings*, UFC 4-010-01, July 2002, available on the Web at http://www.acq.osd.mil/ie/irm/irm_library/UFC%204_010_01%20-%2031JUL2002.pdf.

Approximately 47 percent of the experts in our study (20 of 43) said research and implementation of such backflow protection warranted a high or highest priority for federal funding. These backflow protection devices could be coupled closely with monitoring and metering technologies that can sense contaminant concentrations in drinking water systems. Another noted further that automated meter reading is already being used, but the ability to get real-time readings is essential in order to rapidly notify technicians or officials if a backflow is detected. This could help reduce or eliminate threats to the distribution system.[11]

## Testing and Further Protecting SCADA and Cyber Systems

Section 402 of the Bioterrorism Act requires a review of "methods and means by which information systems, including process controls and Supervisory Control and Data Acquisition (SCADA) and cyber systems at community water systems, could be disrupted by terrorists or other groups." Slightly more than one-third (15 of 43) of the experts on our panel rated federal funding to test and further protect SCADA systems as warranting a high or highest priority. Information provided at the 2003 American Water Works Association (AWWA) Water Security Congress highlighted the limited security features inherent in many SCADA systems, citing few security protocols, lack of firewalls, and SCADA data being routed outside of a facility. Other SCADA systems are placed in networks that are accessible through the Internet and, therefore, are exposed to additional vulnerabilities. One expert added that because the majority of the SCADA software is created outside the United States, the expert favored establishing and enforcing security standards for the software, as well as testing the software before installation at water utilities. This expert believed that federal activities should include working with vendors of SCADA systems and related software in order to ensure that security concerns are appropriately incorporated into the design of these systems.

According to EPA, to meet its responsibilities under the Bioterrorism Act, the agency is planning to pursue research in a number of areas to reduce

[11]The Bioterrorism Act recognized the importance of dealing with this potentially serious source of contamination. Specifically, section 402 of the Bioterrorism Act calls for a review of "methods and means by which pipes, constructed conveyances, collection, pretreatment, treatment, storage and distribution systems that are utilized in connection with public water systems could be altered or affected so as to be subject to cross-contamination of drinking water supplies." In addition, section 402 requires the review of "procedures and equipment necessary to prevent the flow of contaminated drinking water to individuals served by public water systems."

the risks of attacks on drinking water SCADA systems and to better understand their potential consequences, starting with an identification of the possible threats posed to such systems. Starting in fiscal year 2004, EPA also intends to (1) develop models that can simulate the consequences of physical and cyber attacks, emphasizing the distribution system and eventually cascading or interrelated consequences; (2) assess the consequences of a loss of pressurized water on other critical infrastructure sectors such as power, transportation, chemical supplies, and communications; (3) compile technical information and informational tools that can help in analyzing the consequences of potential physical and cyber threats; and (4) establish minimum security standards for the protection of SCADA systems.

## Developing Computer Models of Terrorist Events in Water Systems

Computer modeling can be an important tool in understanding how to prevent or mitigate contamination episodes. Specifically, modeling can be used to simulate contamination events, which in turn can enhance the development of emergency response plans, help select critical locations in distribution systems for positioning and placing monitoring devices, and guide the actions of first responders.

About 30 percent of the experts (13 of 43) rated the development of computer models of terrorist events as deserving a high or highest priority for federal funding. A number of experts noted the relevance of this work for understanding the characteristics of distribution systems. One expert, for example, advocated a "model-based distribution system flow simulator that can be easily tailored to a specific water system such that 'what-if' contamination scenarios can be posed to the system through simulation in order to explore weaknesses in the system." The expert further stated that such a modeling system would also have to take into account the fate and transport of the candidate contaminants throughout the system, and that the approach "would be a fusion of information from both threat assessment and system modeling research efforts."

According to EPA officials, the agency is evaluating distribution system and source water hydraulic models, such as EPANET, PipelineNet, and Riverspill, that can be used to follow water movements and tracer chemicals through distribution systems. EPA notes that several large utilities are currently using such models, but that medium and small utilities face challenges in applying them to their systems. EPA was also planning to initiate a project in September 2003 that will attempt to improve these models by incorporating health-related data, data

concerning consumer complaints, Geographic Information System data, and information from SCADA systems. Overall, EPA's preliminary cost estimates are $2.8 million for modeling projects to develop more effective protection of distribution systems.

## Establishing Baseline Values for Water Constituents

About 23 percent of the experts (10 of 43) rated the importance of establishing baseline values (e.g., concentrations of certain chemicals typically found in a drinking water system) for drinking water system constituents as a high or highest priority warranting federal support. One expert noted that developing and understanding the basic characteristics and typical monitoring results of a distribution system are essential to understand if and when a drinking water system is subject to contamination. According to other experts, because distribution systems may be the most vulnerable portion of a system, and the most complex in terms of understanding appropriate response actions, baseline data available from pre-emergency studies could be helpful.

In addition to providing utility operators with information on normal operating conditions within their systems, understanding baseline levels of water constituents is often needed to develop certain monitoring technologies. For example, monitoring devices that measure the light given off during certain organic reactions can be indicative of possible water contaminants, but only if baseline luminescence levels are known and can be incorporated into measurements and calibrations.

In March 2004, EPA plans to launch a project to survey available information on background levels of certain contaminants of concern that are known or suspected to occur in source or treated drinking water. The initiation of this project depends on the progress of another planned project to develop an improved understanding of the biological, physical, chemical, and toxicological properties of contaminants.

## Improving Treatment Technologies

About 23 percent of the experts (10 of 43) rated the improvement of technologies that can better treat the kind of chemical or biological agents likely to be used in attacking a drinking water system as warranting a high or highest priority for federal funding. While water treatment technologies have advanced, as indicated in EPA's research and implementation action plans, treatment capabilities still need to be evaluated and improved for a wide array of microbial and other contaminants. One expert noted that research on membranes (filters that can remove small particulates or

microorganisms) and other advanced treatment techniques is producing promising results, and that further progress in this area may be important in making "water an unattractive target."[12] Specifically, treatment technologies needing further development include ultraviolet systems and improved reverse osmosis techniques. Finally, other experts believed that there should be more research and development of point-of-use treatment devices (possibly installed at the meter), and that a distributed treatment process—one that involves the treatment of water at multiple locations within a drinking water system or uses a variety of methods—would provide additional security against contamination.

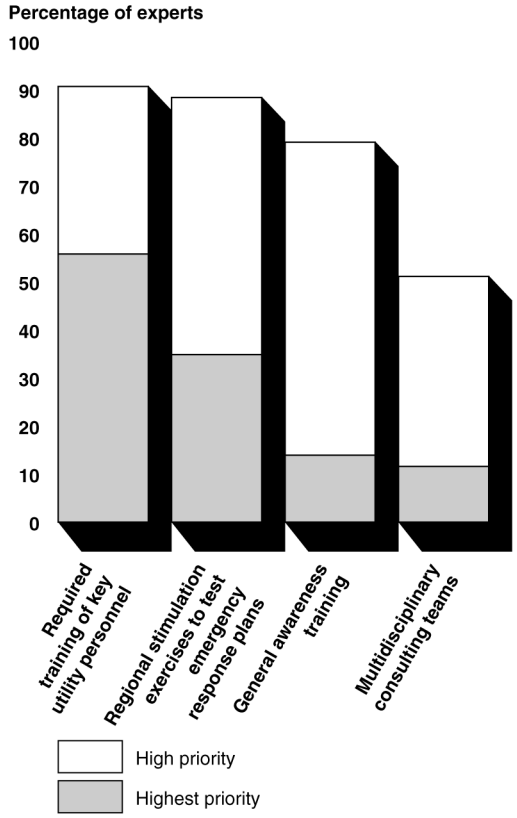
According to EPA officials, the agency hopes to initiate a series of projects to address drinking water treatment issues. Among these are efforts to (1) identify alternative treatment options by reviewing literature on contaminants most likely to be used in attacking drinking water systems; (2) prepare systematic methods to evaluate treatment technologies for likely contaminants; (3) perform bench-scale studies (those performed in a laboratory under controlled conditions) to determine the effectiveness of typical disinfection and contaminant removal technologies; (4) identify alternative treatment options at the point of use or point of entry; and (5) develop guidance for discharging contaminated water that had been used to clean contaminated substances or equipment.

## Activities to Improve Education and Training

Experts strongly supported improved training and education to help ensure that utility personnel can detect and respond to malevolent acts affecting their facilities. As shown in figure 9, the education and training activities most frequently recommended for federal support generally fell into four categories: (1) specialized training of utility personnel with security-related responsibilities, (2) support for regional simulation exercises to test emergency response plans, (3) general security awareness training for utility personnel not specifically charged with security-related responsibilities, and (4) use of multidisciplinary consulting teams ("Red Teams") to independently evaluate drinking water utilities and their security concerns.

[12]For general information on membrane treatment options or examples, refer to EPA's proposed draft *Membrane Filtration Guidance Manual*, EPA 815-D-03-008, Office of Water, June 2003.

**Figure 9: Activities Identified by Experts to Improve Education and Training**




Source: GAO analysis of expert panel's responses to GAO survey.

## Required Training of Key Utility Personnel

Many experts underscored the importance of training drinking water personnel with security-related responsibilities in techniques to prevent, detect, and, if necessary, respond to an attack on their system. This training would include, for example, training for laboratory technicians who test for potential contaminants; for utility operators who perform day-to-day duties or who are uniquely positioned to monitor and respond to potential contaminants at a treatment facility; and for mechanical, civil, and environmental engineers who design, repair, and maintain drinking water systems.

Overall, over 90 percent of the experts (39 of 43) indicated that required training for security-related personnel warrants at least a high priority for

federal funding, with approximately 56 percent (24 of 43) indicating that it deserved highest priority. One expert said that there should be mandatory federal training for employees at drinking water systems serving 10,000 people or more.

To date, EPA has launched at least three programs that emphasize technical training, one directed to states and another to utility employees and officials. Through one program, beginning in fiscal year 2002, EPA has made grants available to states and territories that, in part, are intended to support security-related training and education.[13] Also, EPA has developed two train-the-trainer programs. One of these, begun in fiscal year 2003 to provide assistance to drinking water systems serving fewer than 50,000 people, awarded $1.5 million in grants to five nonprofit training and technical assistance organizations.[14] Another program makes available "no cost" security training for drinking water systems that serve populations of 50,000 to 100,000.[15] This program, which also provides assistance to develop vulnerability assessments and emergency response plans, includes provisions for follow-up technical assistance and training.

## Regional Simulation Exercises to Test Emergency Response Plans

Regional simulation exercises to test emergency response plans are intended to provide utility and other personnel with the training and experience needed both to perform their individual roles in an emergency and to coordinate these roles with other responders within and outside the utility. A successful emergency response plan can help these staff members more quickly identify and respond to an emergency and more quickly restore services and public confidence.

[13]The additional monies are for coordination within the state or territory on homeland security issues, developing or enhancing vulnerability assessments and emergency response plans, and setting up a communications strategy for states and utilities.

[14]The grants (up to $300,000 per entity) were intended to build staff expertise in drinking water security, after which these individuals would train state, tribal and local agencies at no cost on security and technical issues. Grant recipients included the Maryland Center for Environmental Training, the National Environmental Services Center, the National Rural Water Association, the Rural Community Assistance Program, and the Water Environment Federation.

[15]This is a program implemented by the International City/County Management Association (ICMA), an organization representing local government leaders, and the Water Environment Federation (WEF), a not-for-profit technical and educational organization.

The experts on our panel underscored the importance of conducting such exercises, with more than 88 percent (38 of 43) rating these exercises as warranting a high or highest priority for federal funding. Exercises not only give individuals invaluable practice, but also allow officials to better determine what kind of coordinated response is best for a given adverse event. Other experts described the need to identify responsible agencies that will make difficult decisions during an emergency, such as whether to restrict use of the drinking water supplies. And if water supplies were disrupted, subsequent issues would also need to be anticipated, such as how to fight fires, mobilize resources (such as the distribution of bottled water), and communicate among the emergency responders and to the public.

EPA's Water Protection Task Force has developed a program to support training exercises across the United States at systems serving over 100,000 people. In 2003, the agency intends to conduct workshops at approximately 30 to 45 locations across the United States to provide guidance on emergency response plans and on the Bioterrorism Act's requirements; to present an overview on protocols for responding to contamination events; and to provide information on environmental laboratory capabilities.[16]

## General Awareness Training on Security Issues

In addition to supporting the specialized training recommended for responders "on the front lines" of an emergency, experts strongly endorsed a more general level of training for all utility personnel. The need to emphasize culture change at utilities, as well as among law enforcement staff, was summarized by an AWWA official who commented at a recent security conference about how multimillion-dollar investments in security technology can be undermined by an employee using a brick to prop open a usually locked door.

About 79 percent of the experts (34 of 43) rated such "general awareness" training as warranting at least a high priority for federal funding. One expert noted that such training is needed because the water sector has traditionally been slow to respond to new challenges (such as new

[16]In addition to these workshops, EPA published a guidance document for utilities to provide for uniform response, recovery and remediation processes. (See *Guidance for Water Utility Response, Recovery & Remediation Actions for Man-Made and/or Technological Emergencies*, EPA 810-R-02-001, April 2002).

regulations), and that such training could therefore be particularly important in raising the consciousness of staff to security-related issues.

During fiscal year 2002, EPA completed general security training, in collaboration with the American Water Works Association and the Water Environment Federation, to educate water utility managers and operators about the "entire spectrum of security issues," including vulnerability assessments, development of emergency response plans, and risk communication. The organizations convened workshops, conducted webcasts, and offered online courses. More recently, EPA's Office of Research and Development has developed a draft Water Security Research and Technical Support Implementation Plan for key research-related projects, some of which involve developing training modules and related guidance documents that will address monitoring, threat evaluation, and analytical protocols. This training would address the specialized needs of field and laboratory personnel. However, according to EPA officials, some of these efforts would also support the general awareness training needs of the larger universe of utility personnel.

## Multidisciplinary Consulting Teams to Analyze Utilities' Risks and Vulnerabilities

Multidisciplinary consulting teams, often called "Red Teams," consist of experts in a wide variety of security- and drinking water-related disciplines. Red Teams could be used to provide independent analyses of utilities' vulnerabilities, and to assess their emergency response preparedness, as well as to educate law enforcement and public health agencies. Approximately half of the experts (22 of the 43) rated support for certified Red Teams as warranting either a high or highest priority for federal funding.

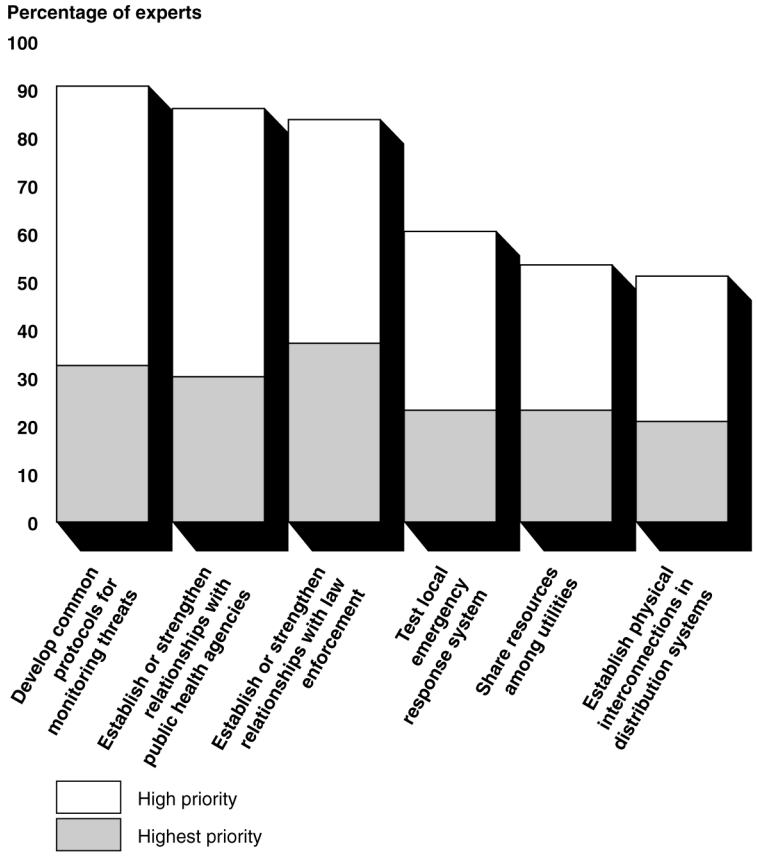
According to one expert, an effective Red Team would consist of "at least six people with widely varying areas of expertise (physical, water quality, SCADA, policies and procedures, emergency response, etc.), and are able to work together and sort through various concerns and priorities to develop a unified understanding of the security issues at a given utility." He noted further that the team would visit utilities, and recommend changes or upgrades to security standards, procedures, and facilities, based on their best professional judgment. Another expert noted that Red Teams could make client utilities aware of threat assessment information, and may be able to review vulnerability assessments independently.

## Activities to Strengthen Relationships between Agencies and Utilities

Experts also cited enhanced cooperation and coordination among government organizations and utilities as a key component in drinking water utilities' efforts to improve their security. Our analysis of experts' responses identified six types of activities in this category as most deserving of federal support.[17] These activities, in figure 10, include (1) developing common protocols for monitoring drinking water threats, (2) improving relationships between drinking water utilities and public health agencies, (3) improving relationships between utilities and law enforcement agencies, (4) testing local emergency response systems, (5) sharing resources among utilities, and (6) establishing physical interconnections between drinking water facilities and distribution systems.

[17]More than 50 percent of the experts rated these activities as deserving a high or highest priority for federal funding relative to the other activities. Experts also identified three other activities scoring under 50 percent, including the formation of better relationships between water associations and federal agencies (about 26 percent), developing public education programs (about 19 percent), and forming a tracking system to monitor security funding (about 12 percent).

**Figure 10: Activities Identified by Experts to Strengthen Relationships between Agencies and Utilities**




Source: GAO analysis of expert panel's responses to GAO survey.

## Developing Common Protocols to Monitor Drinking Water Threats

According to EPA, drinking water utilities vary widely in how they perceive threats and detect contamination. These differences often occur because utilities have few common protocols to help promote a more consistent approach in performing activities such as assessing or monitoring threats.

The experts in our study also identified this lack of consistency, with over 90 percent (39 of 43) rating the development of common protocols to monitor drinking water threats as warranting a high or highest priority for federal funding. Some experts described the need for a nationally consistent and uniform analytical response to contamination threats,

noting in particular the need to have protocols in place for identifying, sampling, and analyzing contaminants. Some also cautioned that older methodologies need to be reexamined in the context of terrorism, and that new protocols need to be reviewed as they are developed. For example, any standard process developed for detecting potentially harmful microorganisms in drinking water needs first to be validated, and then implemented appropriately for different sizes and types of utilities.

EPA officials cited a number of projects under way to develop or improve protocols that address a variety of activities highlighted in other sections of this chapter. They noted that guidance documents in development will include a "toolbox" with information on how to respond to threats and attacks. EPA also intends to develop guidance to assist law enforcement officers and utility officials in assessing the credibility of threats, and guidance on sampling and performing recovery and remediation work at the sites of potential or real contamination.

## Improving Relationships between Utilities and Public Health Agencies

Drinking water utilities and public health agencies would appear to be natural allies in a common health-related enterprise—delivering safe, sanitary water supplies to the vast majority of the nation's population. Their relationship is seemingly reinforced further in many states where the state's drinking water office is located within its health department.

Nonetheless, about 86 percent of the experts in our study (37 of 43) recommended a high or highest funding priority for activities devoted to improving working relationships between drinking water utilities and health agencies. Such activities may include

- characterizing and studying potential biological, chemical, and radiological contaminants and getting this information to all levels of public health departments and officials;
- clarifying and testing the effectiveness of disinfectants or other approaches to neutralize such contaminants; and
- standardizing effective public notification processes in the event of potential or real contamination of drinking water systems.

For example, one expert described an array of potentially valuable information that should be developed and made available to utilities—information typically held by public health agencies. Examples cited

include (1) epidemiological data on diseases or other health incidents in communities, and (2) data on infections in subgroups of the population (such as nursing homes) and on hospital laboratory diagnoses, absenteeism from schools, and pharmacy sales of certain medications such as antidiarrheal medications. Because state health agencies often regulate public water utilities and therefore are highly knowledgeable about them, these agencies should serve an enhanced role in the security of water systems by, for example, disseminating timely information to utilities and the public about possible contamination.

EPA has devoted funds to address drinking water security issues as they relate to public health concerns. For example, the agency's Office of Water is developing contaminant lists that officials say will better guide future research and identify information needs. Other planned work includes determining the infectious or toxic doses of potential contaminants, and providing information (including restricted information) to utility operators, public officials, and other security stakeholders.

## Strengthening Relationships between Drinking Water Utilities and Law Enforcement Agencies

More than 80 percent of the experts (36 of 43) rated establishing or strengthening relationships between drinking water utilities and law enforcement as having either a high or highest priority for federal funding. Several experts noted that a close working relationship between these organizations could help to prevent incidents, through increased police patrols and the sharing of intelligence information. One expert noted also that improving these relationships might result in a more rapid and comprehensive response to adverse or malevolent acts. Another expert, however, pointed to an underlying problem that often characterizes this relationship: "There are very few people that currently have a good understanding of utility operations as well as security issues and approaches. The lack of understanding of utility operations by law enforcement and even regulatory agencies is detrimental, as is the lack of law enforcement and security understanding at utilities. Development of people that understand both types of knowledge would be highly valuable in addressing water security." He said that the development of such people is currently being done by chance.

To date, EPA has largely facilitated security-related training programs intended for utility officials, although it has recently initiated programs involving outreach to law enforcement organizations. One program involves developing outreach materials such as a "top 10" list of tips on water security for law enforcement officials, a "citizens brochure," and law

enforcement training workbooks. EPA has also contacted the National Chiefs of Police and the National Sheriffs' Association to improve awareness about drinking water security.

## Testing Local Emergency Response Systems

It has long been accepted that in light of the critical function they serve in local communities, drinking water utilities should have effective emergency response plans to deal with emergencies. This imperative was further reinforced by the Bioterrorism Act's recent requirement for such plans. However, the execution of these plans requires staff to perform functions beyond their day-to-day responsibilities, as well as coordinate with personnel from different organizations that may have little to do with each other except in emergency situations.

Further, an emergency response plan can only be considered reliable if it is tested periodically. About 60 percent of the experts (26 of 43) in our study indicated that testing of local emergency response systems warrants a high or highest priority for federal funding. One expert stated that funds should be made available to ensure that plans are updated, perhaps annually. Another noted, "Everyone has been concentrating on assessment and addressing vulnerabilities [to drinking water systems]. What is even more important to public safety are the correct response actions to any emergency situation."

In September 2003, EPA conducted a study to evaluate the performance of a group of laboratories in a simulated emergency situation involving a chemical contamination threat to drinking water. This study also assessed the effectiveness of draft guidance provided by EPA to laboratories for developing their own response protocols. EPA plans to deliver a series of workshops in early 2004 that will involve tabletop exercises and drills for various emergency responders, such as public health and law enforcement officials, laboratory staff, and selected utility employees.

## Sharing Resources among Utilities

Experts cited mutual aid arrangements among neighboring drinking water utilities as activities that may result in a more efficient use of resources during a terrorist action. Over half of the experts (23 of 43) said that a high or highest priority should be assigned to federal funding of activities that facilitate the sharing among utilities of such resources as common back-up power systems and other critical equipment. One expert described a collaborative in the San Francisco Bay Area, the Bay Area Security Information Collaborative (BASIC), in which eight utilities meet regularly

to address a wide range of security-related topics. Topics have included the development of a database of chemical and biological contaminants and response protocols, regional exercises to prepare for an event, regional training, information sharing on preparing vulnerability assessments, and public information messages. Such mutual aid arrangements might be designed in coordination with state water agencies and their related water security programs.

Another expert cited standardized Mutual Aid Disaster and Intervention Response Teams (MADIRT) established by the North Carolina League of Municipalities, the North Carolina Urban Water Consortium, and North Carolina's Disaster Preparedness Committee. This cooperative approach is intended to allow municipalities a means to share personnel, equipment, materials, and emergency assistance with other communities. MADIRT allows communities to identify their capabilities in advance of an event, increase standardization to save time and reduce costs, and simplify communications. One key effort of this cooperative has been to draft specifications for water pipe repair, although other repair actions (e.g., for generators or SCADA systems) are being considered. The cooperative also establishes mutual aid coordinators—volunteers across the state who are trained in the types of aid that utilities may need during emergencies. At present, municipalities that sign a statewide mutual aid agreement, and in turn use the teams, would be able to fully qualify for reimbursement from the Federal Emergency Management Agency, the state, or both.

## Establishing Physical Interconnections between Drinking Water Facilities and Distribution Systems

Physical interconnections—the linkages and junctions between pipes both within and between utilities—can be useful in mitigating intentional contamination. Once contamination has occurred and has been identified, interconnections might allow a utility operator or emergency response official to continue to provide service from another source, and aid in isolating contaminated water from reaching the population at large. They can also allow fresh, clean water to be pumped in from another part of the system or from an entirely different system.

Approximately 51 percent of the experts (22 of 43) indicated the establishment of such interconnections deserves either a high or highest priority for federal funding. The overarching idea is to have a higher degree of redundancy in a drinking water system, with distributed sources of water (e.g., water from both wells and surface water); a wider and more redundant distribution of treated water (e.g., more than one pipeline of treated water at a critical location); and increased controls over the flow of

such water. According to one expert, system interconnections have been used for some time, but that more recently, efforts have focused increasingly on developing them to handle emergency situations. Another expert commented on the need for remote-controlled valves, and on the need to be able to connect or bypass pipelines to access alternative sources of water. Finally, one expert suggested that water could be shared across interconnected utility systems if one system experienced a suspension of service. This individual stated that there is so much excess capacity in the systems that many utilities could supply their own needs and another system of a similar size.

EPA's preliminary cost estimate for interconnectivity research, such as contingency planning for alternative sources of water, is about $2.6 million. Among other things, the agency intends to develop case studies that describe how utilities and populations can share water, how truck-mounted and portable water facilities can be designed and implemented during crises, and how redundancy in water systems can better ensure sustained and consistent water supplies. The agency's work in this area has been complemented by other projects that use computer modeling to simulate water flows in distribution systems.

## Conclusions

EPA's Strategic Plan on Homeland Security sets forth the goal that "by 2005, unacceptable security risks at water utilities across the country will be significantly reduced through completion of appropriate vulnerability assessments; design of security enhancement plans; development of emergency response plans; and implementation of security enhancements." The plan further commits to providing federal resources to help accomplish these goals as funds are appropriated.

Key judgments about which recipients should get funding priority, and how those funds should be spent, will have to be made in the face of great uncertainty about the likely targets of attacks, the nature of attacks (whether physical, cyber, chemical, biological, or radiological), and the timing of attacks. The experts on our panel have had to consider these uncertainties in deriving their own judgments about these issues. These judgments, while not unanimous on all matters, suggested a high degree of consensus on a number of key issues.

We recognize that such sensitive decisions must ultimately take into account political, equity, and other considerations. But we believe they should also consider the judgments of the nation's most experienced

individuals regarding these matters, such as those included on our panel. It is in this context that we offer the results presented in this report as information for Congress and the Administration to consider as they seek the best way to use limited financial resources to reduce threats to the nation's drinking water supply.

## Recommendation for Executive Action

We recommend that, as EPA refines its efforts to help drinking water utilities reduce their vulnerability to terrorist attacks, the Administrator of the EPA 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.

# Participating Experts on Drinking Water Security Panel

| | |
|---|---|
| Gregory Baecher | University of Maryland |
| Pete Baxter | Jane's Information Group |
| Kevin Bennett | Federal Bureau of Investigation, National Infrastructure Protection Center |
| Paul Bennett | New York City Department of Environmental Protection |
| Frank Blaha | American Water Works Association Research Foundation |
| Jennifer Brower | RAND |
| Liz Casman | Carnegie Mellon University |
| Jeff Danneels | Sandia National Laboratories |
| Rolf Deininger | University of Michigan |
| John Ditmars | Argonne National Laboratory |
| David Dobbins | Black & Veatch Company |
| Jane Downing | U.S. Environmental Protection Agency |
| Wayne Einfeld | Sandia National Laboratories |
| James H. Fetzer | Tennessee Valley Authority |
| Tim Gablehouse | Gablehouse and Eppel |
| Gregg Grunenfelder | Washington State Department of Health |
| Eugene Habiger | San Antonio Water System |
| Todd Humphrey | Portland Water Bureau |
| Gerald Iwan | Connecticut Department of Public Health |
| Steve Jackson | U.S. Department of the Interior, Bureau of Reclamation |
| Brian Jenkins | RAND |
| Janet Jensen | U.S. Department of Defense, U.S. Army, Aberdeen Proving Grounds |
| Dennis Juranek | U.S. Department of Health and Human Services, Centers for Disease Control and Prevention |
| Michael Keegan | National Rural Water Association |
| Dave Lawrence | Wisconsin Rural Water Assocation |
| Vanessa Leiby | Association of State Drinking Water Administrators |
| Carrie Lewis | Milwaukee Water Department |
| John McLaughlin | Brown and Caldwell |

| | |
|---|---|
| Christine L. Moe | Emory University |
| Erik Olson | National Resources Defense Council |
| Julian Palmore | University of Illinois |
| Janet Pawlukiewicz | U.S. Environmental Protection Agency |
| E.L. Quarantelli | University of Delaware |
| Brian Ramaley | Newport News Waterworks |
| Alan Roberson | American Water Works Association |
| Ken Rubin | PA Consultants |
| Leonard Shabman | Resources for the Future |
| Jim Shell | Metropolitan Washington Council of Governments |
| Kimberly Shoaf | University of California at Los Angeles |
| David Spath | California Department of Health Services |
| Mic Stewart | Metropolitan Water District of Southern California |
| Billy Turner | Columbus Water Works |
| Ray Yep | Santa Clara Valley Water District |

# GAO Contacts and Staff Acknowledgments

## GAO Contacts

John Stephenson, (202) 512-3841
Steve Elstein, (202) 512-6515

## Acknowledgments

In addition to the individuals named above, important contributions were made by Don Cowan, Lynn Musser, Diane Raynes, and Aaron Shiffrin. Charles Bausell, Brandon Haller, Katherine M. Raheb, and Carol Shulman also made key contributions.

## GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

## Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

## Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

**United States**
**General Accounting Office**
**Washington, D.C. 20548-0001**

**Official Business**
**Penalty for Private Use $300**

**Address Service Requested**

**Presorted Standard**
**Postage & Fees Paid**
**GAO**
**Permit No. GI00**