United States Government Accountability Office

GAO

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

January 2005

WASTEWATER FACILITIES

Experts' Views on How Federal Funds Should Be Spent to Improve Security

GAO-05-165

January 2005

WASTEWATER FACILITIES

Experts' Views on How Federal Funds Should Be Spent to Improve Security

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-165, a report to the Committee on Environment and Public Works, U.S. Senate

Why GAO Did This Study

Since the events of September 11, 2001, the security of the nation's drinking water and wastewater infrastructure has received increased attention from Congress and the executive branch. Wastewater facilities in the United States provide essential services to residential, commercial, and industrial users by collecting and treating wastewater and discharging it into receiving waters. These facilities, however, may possess certain characteristics that terrorists could exploit either to impair the wastewater treatment process or to damage surrounding communities and infrastructure.

GAO was asked to obtain experts' views on (1) the key security-related vulnerabilities affecting the nation's wastewater systems, (2) the activities the federal government should support to improve wastewater security, and (3) the criteria that should be used to determine how any federal funds are allocated to improve security, and the best methods to distribute these funds. GAO conducted a systematic, Web-based survey of 50 nationally recognized experts to seek consensus on these key wastewater security issues.

EPA expressed general agreement with the report, citing its value as the agency works with its partners to better secure the nation's critical wastewater infrastructure.

www.gao.gov/cgi-bin/getrpt?GAO-05-165. To view the full product, including the scope and methodology, click on the link above. For more information, contact John B. Stephenson at (202) 512-3841 or stephensonj@gao.gov.

What GAO Found

Experts identified the collection system's network of sewer lines as the most vulnerable asset of a wastewater utility. Experts stated that the sewers could be used either as a means to covertly gain access to surrounding buildings or as a conduit to inject hazardous substances that could impair a wastewater treatment plant's capabilities. Among the other vulnerabilities most frequently cited were the storage and transportation of chemicals used in the wastewater treatment process and the automated systems that control many vital operations. In addition, experts described a number of vulnerabilities not specific to particular assets but which may also affect the security of wastewater facilities. These vulnerabilities include a general lack of security awareness among wastewater facility staff and administrators, interdependencies among various wastewater facility components leading to the possibility that the disruption of a single component could take down the entire system, and interdependencies between wastewater facilities and other critical infrastructures.

Experts identified several key activities as most deserving of federal funds to improve wastewater facilities' security. Among those most frequently cited was the replacement of gaseous chemicals used in the disinfection process with less hazardous alternatives. This activity was rated as warranting highest priority for federal funding by 29 of 50 experts. Other security-enhancing activities most often rated as warranting highest priority included improving local, state, and regional collaboration (23 of 50 experts) and supporting facilities' efforts to comprehensively assess their vulnerabilities (20 of 50 experts).

When asked how federal wastewater security funds should be allocated among potential recipients, the vast majority of experts suggested that wastewater utilities serving critical infrastructure (e.g., public health institutions, government, commercial and industrial centers) should be given highest priority (39 of 50). Other recipients warranting highest priority included utilities using large quantities of gaseous chemicals (26 of 50) and utilities serving areas with large populations (24 of 50). Experts identified direct federal grants as the most effective method to distribute the funds, noting particular circumstances in which a matching contribution should be sought from recipients. Specifically, a matching requirement was often recommended to fund activities that benefit individual utilities. Grants with no matching requirements were often recommended for activities that should be implemented more quickly and would benefit multiple utilities. The other funding mechanisms experts mentioned most frequently included the federal Clean Water State Revolving Fund, loans or loan guarantees, trust funds, and tax incentives.

Contents

Appendixes

Figures

Abbreviations

AMSA	Association of Metropolitan Sewerage Agencies
AMWA	Association of Metropolitan Water Agencies
CWSRF	Clean Water State Revolving Fund
DHS	Department of Homeland Security
EPA	Environmental Protection Agency
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
ISAC	Information Sharing and Analysis Center
LEL	lower explosive level
MGD	million gallons per day
POTW	publicly owned treatment works
SCADA	Supervisory Control and Data Acquisition
VA	vulnerability assessment
VSAT	Vulnerability Self Assessment Tool

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

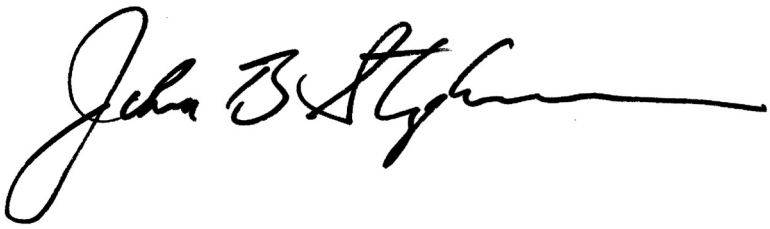
January 31, 2005

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 wastewater security, including the potential vulnerabilities of wastewater systems; activities that most warrant federal support to mitigate the risk of terrorism; and the criteria that the experts believe should be used to determine how any federal funds are allocated among recipients to improve their security and the methods the experts suggest should be used to distribute these funds.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. 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 contact me at (202) 512-3841 or stephensonj@gao.gov or my Assistant Director, Steve Elstein, at (202) 512-6515 or elsteins@gao.gov. Major contributors to this report are listed in appendix II.



John B. Stephenson
Director, Natural Resources
and Environment

Executive Summary

Purpose

Like safe drinking water, properly treated wastewater is critical to modern life. Wastewater utilities across the country have long been engaged in activities to ensure the health and safety of their customers and to comply with regulatory requirements to prevent harmful pollutants from being released into the nation's waters. Since the events of September 11, 2001, the security of the nation's water infrastructure against terrorist threats has received greater attention by Congress and executive branch agencies. While more federal resources have been directed toward drinking water security than wastewater security, some maintain that wastewater systems, like drinking water systems, also possess vulnerabilities that could be exploited. It has been alleged, for example, that the numerous storm drains, manholes, and sewers that make up a community's wastewater collection systems' network of sewers could be used to covertly place explosives beneath a major population center or to introduce substances that may damage a wastewater treatment plant's process. Such events could result in loss of life, destruction of property, and harm to the environment.

In 2003, Congress considered legislation that would have provided funds to, among other activities, assess the vulnerability of wastewater facilities, make physical security improvements, and conduct research. Since then, the wastewater industry has expressed its desire for a strong federal contribution to help meet its security needs. To inform further deliberations on this topic, as agreed with the Chairman and Ranking Minority Member of the Senate Committee on Environment and Public Works, this report identifies experts' views on (1) the key security-related vulnerabilities affecting the nation's wastewater systems, (2) specific activities the federal government should support to improve wastewater security, and (3) the criteria that should be used to determine how any federal funds are allocated among recipients to improve their security and the methods that should be used to distribute these funds.

To address these issues, GAO identified 50 recognized experts from the wastewater community and surveyed them using a Web-based Delphi process. The Delphi methodology is a systematic process for obtaining individuals' views on a question or problem of interest and seeking consensus if possible. In selecting experts for the expert panel, GAO sought individuals who are widely recognized as possessing expertise on one or more key aspects of wastewater security. GAO also sought to achieve balance in representation from key federal agencies, state or local agencies, industry and nonprofit organizations, academia, and water

utilities of varying sizes. A detailed description of GAO's methodology is presented in chapter 1.

Background

Wastewater systems vary by size and other factors, but all include a collection system and treatment facility. Collection systems are generally widely dispersed geographically and have multiple access points, including drains, catch basins, and manholes, most of which are not monitored. This underground network of sewers and pumping stations moves the wastewater away from its point of origination to the treatment plant. Typical wastewater treatment facilities use a series of physical, biological, and chemical processes to treat wastewater. Chemicals used in this process, most notably chlorine, are often stored on site at the treatment plant. Wastewater systems have become increasingly computerized and rely on the use of automated controls to monitor and operate them.

Nationwide, more than 16,000 publicly owned wastewater systems serve more than 200 million people, or about 70 percent of the nation's total population. About 500 large public wastewater systems provide service to 62 percent of the sewered population. To help address the security needs of the wastewater sector, EPA, since 2002, has provided more than $10 million to help address the security needs of the wastewater sector. A large portion of this funding has been awarded to nonprofit technical support and trade organizations to develop tools and training on conducting vulnerability assessments to reduce utility vulnerabilities, on planning for and practicing response to emergencies and incidents, and for research on a variety of security topics.

Wastewater utilities have had a history of openness with the communities they serve by sharing, among other things, alerts of scheduled maintenance activities and information about the quality of water that is released back into the environment. Many utilities also provide detailed information about their location, design, and treatment processes. The September 11 attacks, however, have led many wastewater utilities to reassess their openness to the general public and their ability to guarantee safe and reliable services to their customers and communities. In December 2003, the President issued Homeland Security Presidential Directive-7, which designated EPA as the lead agency to address water infrastructure security. EPA has worked with other organizations, such as the Water Environment Research Foundation, the Association of Metropolitan Sewerage Agencies, the Water Environment Federation, and the American Society of Civil Engineers, to conduct research, provide guidance and, importantly, to offer

training on how to assess wastewater facilities' vulnerabilities. Unlike drinking water facilities, wastewater utilities are not required by law to complete these "vulnerability assessments."

Results in Brief

GAO's panel of experts identified five key wastewater assets as most vulnerable to terrorist attacks: the collection systems' network of sewers, treatment chemicals, key components of the treatment plant, pumping stations, and control systems. Among these assets, 42 of the 50 experts listed the collection systems' network of sewers as a key vulnerability. Experts explained that adversaries could use this network of pipes to gain access to intended targets within the service area, convey hazardous substances that might destroy points along the system, or incapacitate the wastewater treatment process. In addition, 32 of 50 experts identified process chemicals used in wastewater treatment as a key vulnerability. Of particular concern is the accidental or intentional release of gaseous chlorine, used for disinfection processes, which can burn eyes and skin, inflame the lungs, and cause death if inhaled.

Experts identified 11 key actions when asked to identify and set priorities for the security-enhancing activities most deserving of federal support. Three were particularly noteworthy because they were given a rating of highest priority by a substantial number of the experts. The first activity was the replacement of gaseous chemicals used in wastewater treatment with less hazardous alternatives. Experts viewed this action as critical to reduce the vulnerability of systems that rely heavily upon gaseous chlorine in their treatment processes. Several experts noted that because replacing chlorine could be prohibitively expensive for many wastewater utilities, replacement was a particularly strong candidate for federal support. For example, the change to sodium hypochlorite can require approximately $12.5 million for new equipment and increase annual chemical costs from $600,000 for gaseous chlorine to over $2 million for sodium hypochlorite. The second activity cited was improving local, state, and regional efforts to coordinate responses in advance of a potential terrorist threat. According to the experts, enhanced partnerships among these entities can yield significant benefits to wastewater utilities including an increased ability to monitor critical infrastructure and facilities, improved understanding of agency roles and responsibilities, and faster response time to deal with potential security breaches. Finally, the third activity cited was completing vulnerability assessments for individual wastewater systems. Experts viewed these assessments as key steps toward informing stakeholders

about wastewater system vulnerabilities and countermeasures, and taking steps to implement appropriate countermeasures.

In identifying and setting priorities for the types of utilities that should receive federal funds to improve wastewater security, 39 of the 50 experts gave a rating of highest priority to utilities serving critical infrastructure. These utilities provide service to institutions that serve as hubs for government activity; commercial and industrial centers such as cities' financial districts, power plants, and airports; and public health institutions, such as major medical centers and hospitals. Just over half of the experts rated utilities using large quantities of gaseous chemicals as warranting highest priority for federal funds. Several pointed out that, if these chemicals were released to the atmosphere while being transported to the treatment plant or while stored on site, evacuations might be needed, and personal injuries or fatalities might result. Also receiving widespread support by the experts were utilities serving areas with large populations. Fewer experts recommended highest or high priority for utilities serving entities that have symbolic value or that serve medium or small populations.

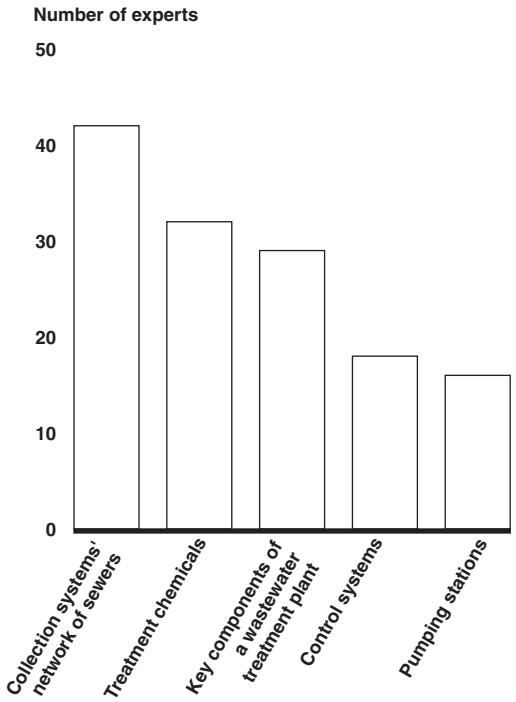
The experts overwhelmingly favored direct federal grants as the best method to distribute federal funds to potential recipients. They also specified instances in which some type of match by recipients would be particularly appropriate. Relatively fewer experts recommended the use of trust funds or the Clean Water State Revolving Fund, particularly for upgrades that need to be implemented quickly. Other mechanisms receiving support from at least some experts included loans or loan guarantees, and tax incentives for private utilities.

Principal Findings

Key Vulnerabilities

Figure 1 summarizes the 50 experts' identification of which wastewater system components were among the systems' top five vulnerabilities.

Figure 1: Key Wastewater System Vulnerabilities Identified by Experts



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

Collection systems' network of sewers. Forty-two of the 50 experts named the collection systems' network of sanitary, storm, and combined sewers. Several noted that sewers make underground travel from a point of entry to a potential target almost undetectable. Many also suggested that adversaries could use the collection system as an underground transport system—without ever physically entering the system—for explosive or toxic agents. For example, several experts explained, an adversary could pour a highly toxic chemical into the sewer that could destroy the biological agents vital to the treatment process.

Treatment chemicals. Thirty-two experts identified treatment chemicals used in wastewater treatment. Most experts singled out chlorine gas as a major chemical of concern. Chlorine is extremely volatile and requires specific precautions for its safe transport, storage, and use. As experts commented, although railroad tanker cars are designed to avoid leakage in the event of a derailment, and withstand a bullet from a normal handgun or rifle, one expert concluded that the "use of explosives to cause a rupture is

well within the skill set of a terrorist." Such an attack along a congested transportation corridor could have catastrophic public health and safety impacts.

Key components of the treatment plant. Twenty-nine experts identified the components of the main wastewater treatment facility. Typical facilities use multiple treatment processes before discharging the effluent back to the environment, with each stage of the process serving an integral role. Experts explained that damage to one or more of these processes could result in inadequately treated wastewater, thereby contaminating drinking water sources, harming the environment, and causing significant economic damage. While many experts expressed concern for the security of the entire treatment plant, several identified the headworks, where wastewater carried through the collection system first enters the plant, as particularly vulnerable to attack.

Pumping stations. Sixteen of the 50 experts identified pumping stations, which are often used to move sewage to the treatment plant when gravity alone is not sufficient, as among the top vulnerabilities. As one expert explained, destroying or disabling a pumping station could cause the collection system to overflow raw sewage into the streets, and into surface waters, and back up sewage into homes and businesses. Experts explained that the remoteness and geographic distribution of pumping stations, and their lack of continuous surveillance, make them particularly vulnerable.

Control systems. Eighteen experts cited the automated Supervisory Control and Data Acquisition (SCADA) systems, which serve functions ranging from storing and processing data to monitoring system conditions and controlling vital system operations. These systems can be vulnerable because of loose security in the control rooms at some plants, and remote access to SCADA through the Internet, among other reasons. One expert described a breach of cyber security in Australia which caused the release of thousands of gallons of raw sewage.

In addition to the vulnerabilities associated with specific system components, experts identified several overarching issues that compromise the integrity of systems' physical assets and their operations. Chief among them are (1) a general lack of security awareness within the wastewater sector; (2) interdependencies among components of the wastewater system, opening the possibility that a failure of any individual component could bring down the entire system (e.g., undermining the automated control system could cause numerous components to fail); and

(3) interdependencies between the wastewater system and other critical infrastructure that could fail, such as electric power supplies.

Security-Enhancing Activities That Most Warrant Federal Support

Three security-enhancing activities were most often cited by the experts as warranting "highest" priority for federal support:

Replacing gaseous chemicals used in wastewater treatment with less hazardous alternatives. Well over half of experts surveyed (29 of 50) rated the replacement of gaseous chemicals at wastewater treatment facilities with less hazardous alternatives as warranting highest priority for federal funding. Fourteen more experts rated this activity as a "high" priority. Experts asserted that wastewater systems carrying out treatment processes using gaseous forms of chemicals, particularly chlorine, inherently make themselves targets for terrorist attack. According to several experts, some communities and utilities currently using gaseous chemical treatment processes are interested in converting to an alternative treatment technology, but financial costs associated with conversion remain prohibitive. According to EPA, hypochlorite compounds tend to have higher operating costs than chlorine gas.[1] Nonchlorine-based technologies, such as ozone and ultraviolet light, tend to have higher capital costs than chlorine gas, according to a study prepared for the U.S. Army.[2] Another expert suggested that reducing the size of containers used to transport and store gaseous chemicals could help to mitigate the problem. This approach is being implemented by a facility where gaseous chlorine is now stored in 1-ton containers—a significant reduction in size from the larger 90-ton railroad car-sized containers the utility previously employed.

Improving local, state, and regional collaboration efforts. Twenty-three of 50 experts rated efforts to improve local, state, and regional collaboration efforts as warranting highest priority for federal funding. Fifteen more experts rated this activity as a high priority. As one expert noted, wastewater facilities are often disconnected from other key entities that participate in emergency planning and response, and the facilities instead

[1]*EPA Wastewater Technology Fact Sheet, Chlorine Disinfection*, EPA 832-F-99-062, September 1999.

[2]*Disinfection Technologies for Potable Water and Wastewater Treatment: Alternatives to Chlorine Gas*, Pacific Northwest National Laboratory, July 1998.

conduct these critical activities without an appreciation of the need to coordinate with other key players. An expert identified the nonprofit California Utilities Emergency Association as an example of an effective provider of communications, training, mutual aid coordination, and simulation exercises to participating utilities.

Completing vulnerability assessments for individual wastewater systems. Twenty of 50 experts rated the completion of vulnerability assessments as warranting highest priority for federal funding. Fourteen others rated this activity as a high priority. Experts suggested that vulnerability assessments enable wastewater utilities to identify and understand their systems' vulnerabilities and take steps to implement appropriate countermeasures. As such, they characterized these assessments as a logical first step in determining how best to spend funds to improve security.

In addition to these three activities, experts cited eight other activities as warranting high priority for federal funding: (1) training utility employees on how best to conduct vulnerability assessments and improve the security culture among employees; (2) improving national communication efforts between utilities and key entities responsible for homeland security; (3) installing early warning systems in collection systems to monitor for or detect sabotage; (4) hardening physical assets of treatment plants and collection systems; (5) strengthening operations and personnel procedures; (6) increasing research and development efforts aimed at improving threat detection, assessment, and response capabilities; (7) developing voluntary wastewater security standards and guidance documents; and (8) strengthening cyber security and SCADA systems.

Key Allocation Criteria and Distribution Methods for Federal Funding

GAO asked its expert panel for its views on the appropriate criteria for determining which utilities should receive federal funds, should Congress and the administration agree to provide such support. The most frequently cited criteria included the following:

Utilities serving critical infrastructure. Thirty-nine of the 50 experts accorded highest funding priority to utilities serving critical infrastructure. An additional 10 experts believed these utilities warranted a high priority. These utilities provide service to institutions that serve as hubs for government activity, to commercial and industrial centers, and to public health institutions. Many experts noted in particular that systems serving heavy commercial and industrial customers are critical to the country's

economic stability, and that a major or sustained disruption could have severe economic and/or public health consequences. One noted, for example, that a sustained shutdown in the computer chip manufacturing sector, caused by the loss of a wastewater treatment plant, could cost the economy millions of dollars per day.

Utilities using large quantities of gaseous chemicals. Citing the enormous risks posed by gaseous chemicals, just over half of the experts (26 of 50) recommended highest funding priority to help utilities convert from these chemicals to safer alternatives. An additional 18 rated these utilities as warranting a high priority for federal funds. Some experts cautioned, however, that if funds are used by utilities merely to convert to less hazardous chemicals (e.g., sodium hypochlorite), then the federal government may be perceived as rewarding these utilities at the expense of utilities that are considering much safer alternatives.

Utilities serving large populations. Almost half of the experts (24 of 50) gave highest priority to utilities serving areas with large populations. Seventeen additional experts rated these utilities as warranting a high priority for federal funds. Many experts shared the view that providing financial and technical assistance to the largest treatment plants would protect the greatest number of people. One expert pointed to EPA's 2000 Clean Water Needs Survey, which indicated that 62 percent of the nation's sewered population is served by about 500 of the largest wastewater treatment facilities. Furthermore, a number of experts suggested that terrorists often seek to maximize the number of people killed or injured by their attacks, and are, therefore, more likely to target the systems in large metropolitan areas that serve many customers.

GAO also asked its expert panel for their ratings of how effective each method would be for distributing federal funds to potential recipients. Among the mechanisms they recommended:

Direct grants. Direct federal grants were the most favored funding mechanism, with 34 of the 50 experts indicating that direct federal grants to utilities would be "very effective" in allocating federal funds. An additional 12 experts indicated that they would be at least "somewhat effective." Several experts commented that grants are preferable because they are more likely to result in safety improvements and other desired changes more quickly. Experts also offered the following opinions on situations in which it would be appropriate to offer a grant with or without a required match from the recipient:

- Many favored grants without a matching requirement for activities that benefit multiple utilities. Specific actions include conducting research and development to improve detection, assessment, and response capabilities; developing voluntary wastewater security standards and guidance; completing vulnerability assessments; and providing training to utility security personnel on how best to conduct vulnerability assessments and improve the security culture.

- Many favored cost-shared grants for activities that benefit individual utilities, such as establishing improved operation and personnel procedures (e.g., conducting background checks on new employees); installing early warning systems in collection systems to monitor for or detect sabotage; improving cyber security; and hardening physical assets through such actions as building fences and installing or upgrading locks.

Clean Water State Revolving Fund. Five experts cited the Clean Water State Revolving Fund as a very effective funding mechanism, and 35 others cited it as somewhat effective. Some experts expressed the view that the fund can leverage appropriated funds and, thereby, assist more facilities than direct grants. But several others expressed reservations about using the fund for security enhancement, including one who said that it "was not originally established to deal with security-related projects . . . the program either needs to [be] fixed to deal with security issues or a separate program needs to be created specifically for security projects." According to one expert, unless additional security-related monies were added to existing fund levels, the use of the fund for security would divert much needed funding away from the kind of critical infrastructure investments that have long been the fund's primary objective.

Loans or loan guarantees. Only one expert indicated that loans or loan guarantees would be very effective, although 34 others agreed that they would be somewhat effective. One expert pointed out that loans would "allow the community to amortize the costs over 20 years," while another commented that a low interest loan could provide some incentive and needed capital to implement security programs. Others cautioned, however, that while loans would have a smaller impact on the federal budget than grants, many local governments are already carrying a heavy debt load for capital improvements, making it difficult for them to take on significant additional debt without affecting their bond ratings.

Making Key Security Decisions in the Face of Uncertainty

To date, the federal government's role in promoting wastewater security has been limited primarily to supporting various training activities on how to complete vulnerability assessments and emergency response plans and several research projects. However, legislation supporting an expanded federal role, including a substantially greater financial commitment, has been proposed in the past and may be considered again in the future.

Should such funds be 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 target of an attack (i.e., a large but well-protected facility versus a smaller but less-protected facility); the nature of an attack (cyber, physical, chemical, biological, radiological), and its timing. The experts on GAO's panel have taken these uncertainties into account in deriving their own judgments about these issues. These views, while not unanimous, suggested some degree of consensus on a number of key issues.

GAO recognizes that such sensitive decisions ultimately must take into account a variety of political, equity, and other considerations. It believes they should also 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 these results as information for the decision-making process that Congress and the administration will likely go through as they seek to determine how best to use limited financial resources to reduce the vulnerability to the nation's wastewater utilities.

Agency Comments and Our Evaluation

GAO 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 Ground Water and Drinking Water, its Office of Homeland Security, and other relevant offices. The comments expressed general agreement with the content of the report and noted that the results will be useful as the agency continues to work with its partners to better secure the nation's critical wastewater infrastructure. EPA also offered specific technical comments and suggestions, which have been incorporated as appropriate.

Introduction

Wastewater systems in the United States provide essential services to residential, commercial, and industrial users by collecting and treating wastewater and discharging it into receiving waters. In light of the events of September 11, 2001, Congress and the executive branch have placed increased attention on improving the security of the nation's water infrastructure—including wastewater systems—to protect against future terrorist threats. While more federal resources have been directed toward drinking water security than wastewater security, some maintain that wastewater systems, like drinking water systems, also possess vulnerabilities that could be exploited. The unique characteristics and components these systems possess provide for the efficient collection, treatment, and disposal of wastewater—functions that are vital to the health of the general public and the environment. However, many of these same characteristics and components have been identified as potential means for carrying out a terrorist attack. A terrorist could seek to impair a wastewater system's treatment process, to use a wastewater system to carry out an attack elsewhere, or some combination of both.

Documented accidents and intentional acts highlight the destruction that arises from an attack on a wastewater system. For example, in June 1977 in Akron, Ohio, an intentional release of naptha, a cleaning solvent, and alcohol into a sewer by vandals at a rubber manufacturing plant caused explosions 3.5 miles away from the plant, damaging about 5,400 feet of sewer line and resulting in more than $10 million in damage.

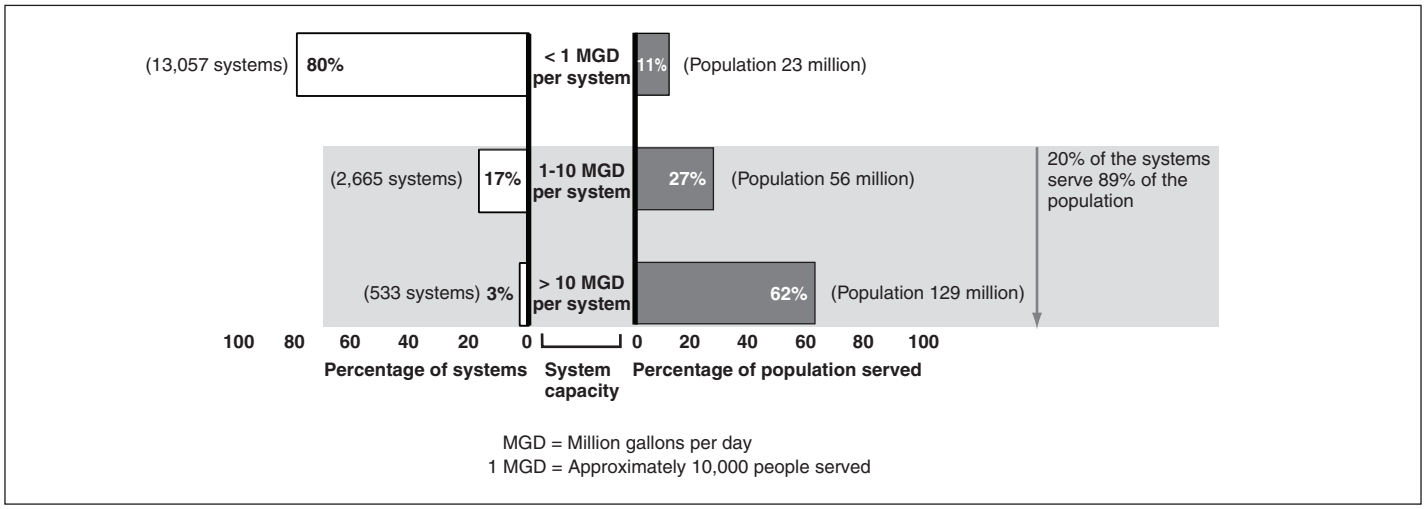
The Nation's Wastewater Systems and the Populations They Serve

A majority of the nation's wastewater is treated by publicly owned treatment works (POTW) that serve a variety of customers, including private homes, businesses, hospitals, and industry. These POTWs discharge treated water into surface waters and are regulated under the Clean Water Act. Nationwide, there are over 16,000 publicly owned wastewater treatment plants, approximately 800,000 miles of sewers, and 100,000 major pumping stations. This infrastructure serves more than 200 million people, or about 70 percent of the nation's total population. The remainder is served by privately owned utilities or by on-site systems, such as septic tanks. This report addresses both public and private wastewater systems.

Though outnumbered by the small systems, the relative handful of large wastewater systems serve the great majority of people. As depicted in figure 2, only 3 percent of the nation's total wastewater systems (approximately 500 systems) provide service to 62 percent of the

populations served by POTWs. Each of these systems treats more than 10 million gallons per day (MGD) of wastewater.

Figure 2: System Size by Population (POTW by system size and population served)



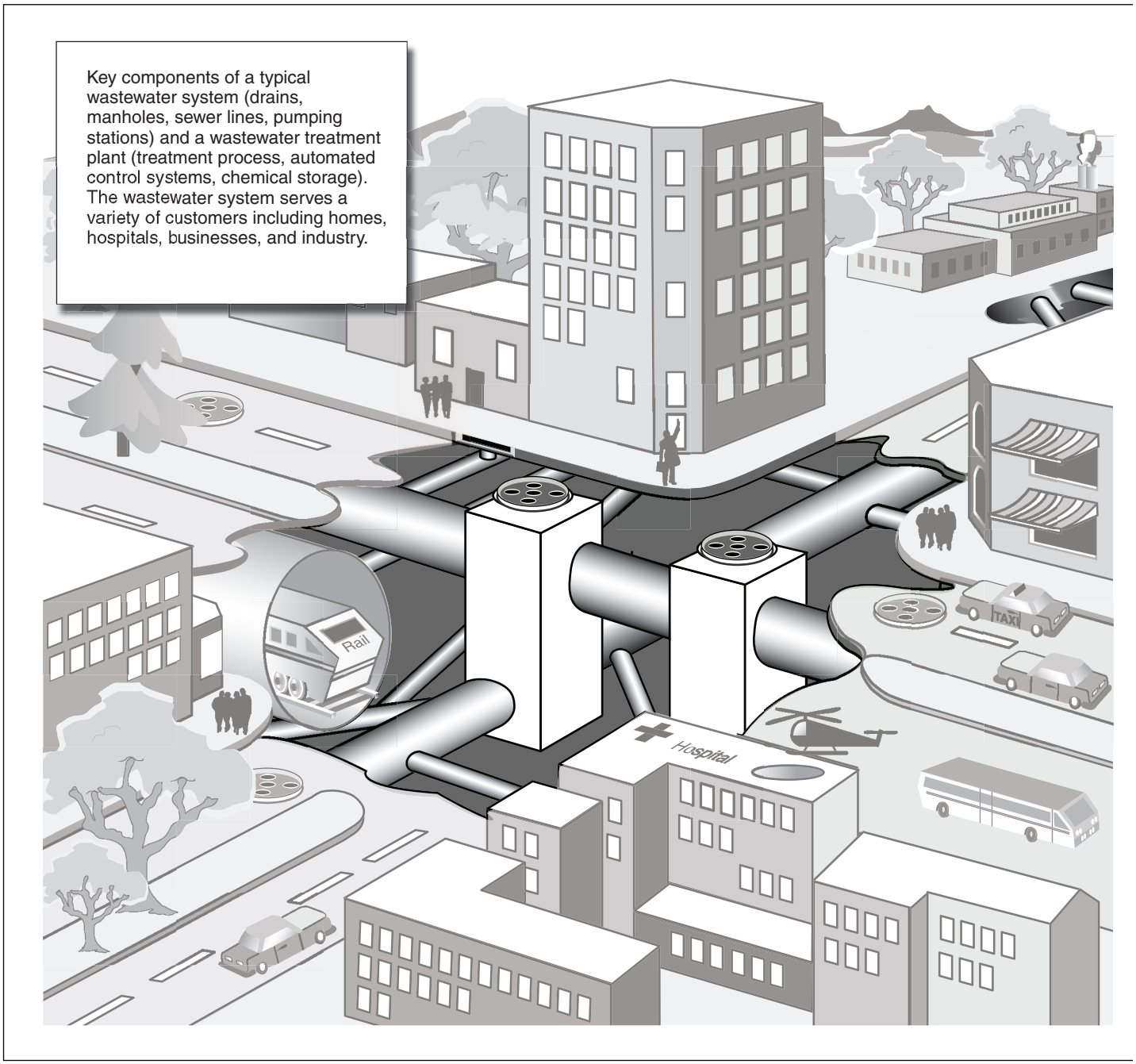
Source: EPA.

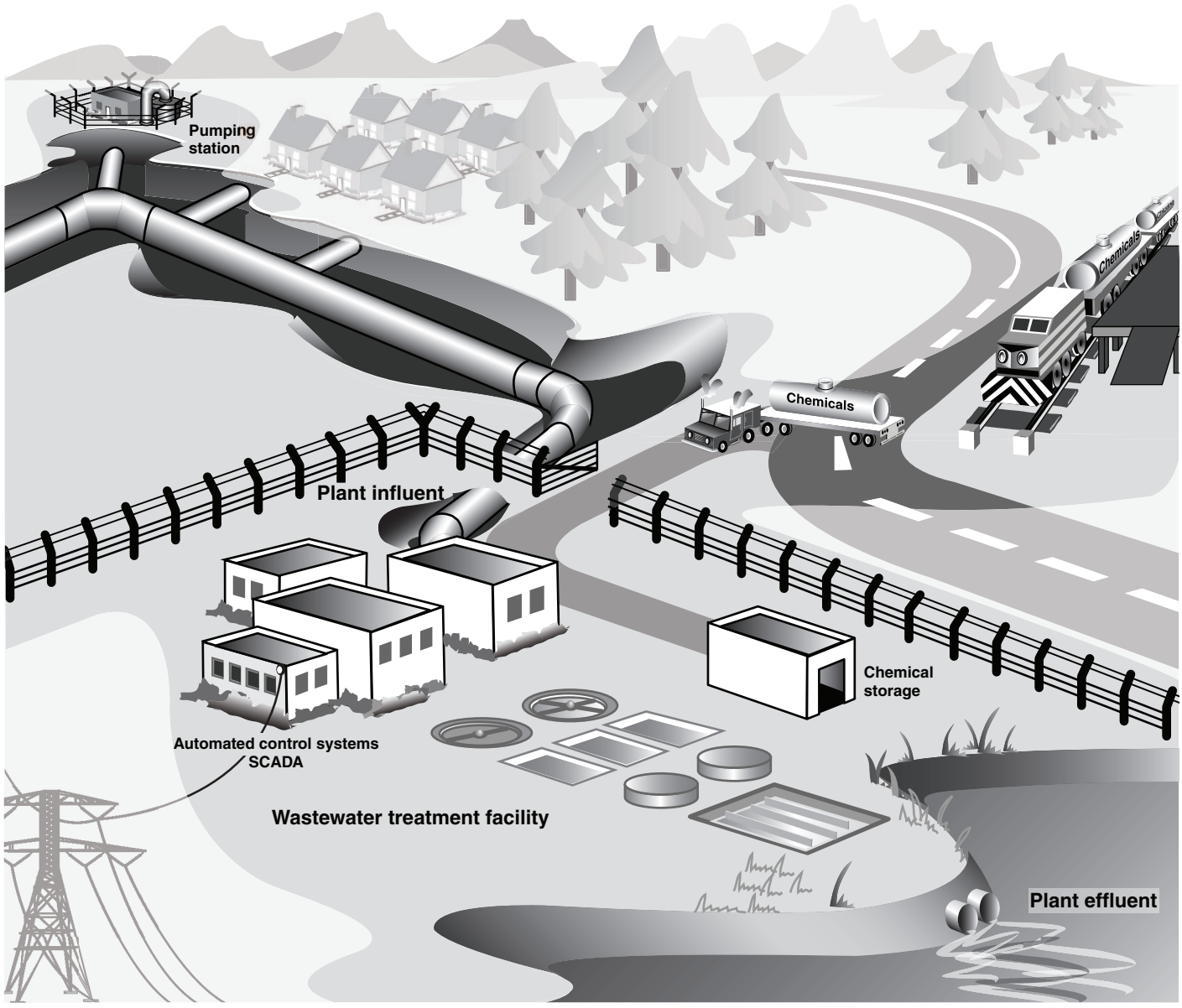
Key Components of a Typical Wastewater System

Wastewater systems vary by size and other factors but, as illustrated in figure 3, all include a collection system and treatment facility.

[This page left intentionally blank.]

Figure 3: Components of a Typical Community Wastewater System




Pumping station
Chemicals
Chemicals
Plant influent
Chemical storage
Automated control systems
SCADA
Wastewater treatment facility
Plant effluent

Source: GAO.

Collection System

The underground network of sewers includes both sanitary and storm water collection lines that may range from 4 inches to greater than 20 feet in diameter. Storm water lines tend to be large in diameter in order to accommodate a variety of precipitation events. Some of the nation's older cities have combined sanitary and storm water lines. Sewers are connected to all buildings and streets within typical communities through indoor plumbing and curb drains.

Most systems were designed for easy and frequent access to facilitate maintenance activities. Access for these purposes is usually conducted through manholes that are typically located approximately every 300 feet. Many collection systems rely on gravity to maintain the flow of sewage through the pipes toward the treatment plant. However, the geographic expanse of a collection system, both in size and topography, may impede the flow. For this reason, collection systems may depend on pumping stations to lift the flow to gain elevation for continued gravity flow until the wastewater reaches the wastewater treatment plant.

The Wastewater Treatment Plant

Once the wastewater enters the treatment plant (influent) through the collection system, the treatment process removes contaminants such as organic material, dirt, fats, oils and greases, nitrogen, phosphorus, and bacteria. The influent typically undergoes several stages of treatment before it is released. Primary treatment includes the removal of larger objects, such as rags, cans, or driftwood, through a screening device or a grit removal system, and solids are removed through sedimentation. Secondary treatment includes a biological process that consumes pollutants, as well as final sedimentation. Some facilities also use tertiary treatment to remove nutrients and other matter even further. Following secondary or tertiary treatment, the wastewater is disinfected to destroy harmful bacteria and viruses. Disinfection is often accomplished with chlorine, which is stored on-site at the wastewater treatment plant. The collection and treatment process is typically monitored and controlled by a Supervisory Control and Data Acquisition (SCADA) system, which allows utilities to control such things as the amount of chlorine needed for disinfection.

Government and Industry Have Recently Sought to Improve Security

In December 2003, the President issued Homeland Security Presidential Directive-7 (HSPD-7), which established a national policy for federal departments and agencies to identify and set priorities for the nation's critical infrastructures and to protect them from terrorist attacks. HSPD-7 established the Environmental Protection Agency (EPA) as the lead federal agency to oversee the security of the water sector, both drinking water and wastewater. Presidential Decision Directive 63 had done so earlier in May 1998, with a focus primarily on drinking water. Based on the 1998 directive, EPA and its industry partner, the Association of Metropolitan Water Agencies (AMWA) established a communication system, the Water Information Sharing and Analysis Center (Water ISAC). The Water ISAC was designed to provide real-time alerts of possible terrorist activity and access to a library of information and contaminant databases to water utilities throughout the nation. In fiscal year 2004, Congress appropriated $2 million for the Water ISAC, which today serves more than 1,000 users from water and wastewater systems. In November 2004, the Water ISAC launched a free security advisory system known as the Water Security Channel to distribute federal advisories on security threats via e-mail to the water sector.

EPA recently established a Water Security Working Group to advise the National Drinking Water Advisory Council (NDWAC) on ways to address several specific security needs of the sector. The working group is made up of 16 members selected on the basis of experience, geographic location, and their unique drinking water, wastewater, or security perspectives. It represents a diverse collection of drinking water and wastewater utilities of all sizes, state and local public health agencies, and environmental and rate-setting organizations. The group's charge includes making recommendations to the full council by the spring of 2005 that identify features of an active and effective security program and ways to measure the adoption of these practices. The working group is also charged with identifying incentives for the voluntary adoption of an active and effective security program in the water and wastewater sector.

The Department of Homeland Security (DHS) is also seeking to enhance communication between critical infrastructure sectors, like the water sector, with the government. The Homeland Security Information Network (HSIN) is being developed to provide the water sector with a suite of information and communication tools to share critical information both within the sector, across other sectors, and with DHS. According to DHS, these information and collaboration tools will facilitate the protection,

stability, and reliability of the nation's critical water infrastructure and provide threat-related information to law enforcement and emergency managers on a daily basis. A Water Sector Coordinating Council established by the department with representative members of the water sector community is charged with identifying information and other needs of the sector, including the appropriate use of and the relationships among ISAC, the Water Security Channel, and HSIN. According to a DHS official, the department is also assembling a Government Coordinating Council made up of federal, state, and local officials to assess impacts across critical infrastructure sectors, including the water sector.

While federal law does not address wastewater security as comprehensively as it addresses drinking water security,[1] wastewater utilities have taken steps, both in concert with EPA and on their own, to protect their critical components. Since 2002, EPA has provided more than $10 million to help address the security needs of the wastewater sector. A large portion of this funding has been awarded to nonprofit technical support and trade organizations including the Association of Metropolitan Sewerage Agencies (AMSA) and the Water Environment Federation to develop tools and training on conducting vulnerability assessments to reduce utility vulnerabilities and on planning for and practicing response to emergencies and incidents. Also, according to EPA, because of the relationship between the drinking water and wastewater sectors, much of the work and funding that has been allocated for drinking water security also directly benefits the wastewater sector. The Water Environment Research Foundation, for instance, has been conducting research on cyber security, real-time monitoring, the effects of contaminants on treatment systems, and other topics that could benefit both sectors. In addition, EPA has supported the development of a variety of resource documents for utilities such as guidance on addressing threats and security product guides for evaluating available technologies and has offered additional technical support to small systems.

[1]The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (the Bioterrorism Act of 2002), Pub. L. No. 107-188, required *drinking water systems* serving more than 3,300 people to complete vulnerability assessments by June 2004. According to EPA officials, many combined systems—those providing both drinking and wastewater services—have voluntarily completed vulnerability assessments for both. The act further required those systems to prepare or revise an emergency response plan incorporating the results of the vulnerability assessment within 6 months after completing the assessment.

To assist in the completion of vulnerability assessments, AMSA with EPA funding cited above, developed technical assistance documents and software including the Vulnerability Self Assessment Tool (VSAT) that are available free of charge to water and wastewater systems. The VSAT methodology and software offers utilities a structured approach for assessing their vulnerabilities and establishing a risk-based approach to taking desired actions.

Even though the wastewater industry has not been required by law to undertake the security measures undertaken by drinking water utilities, many in the industry maintain that enhanced security must be pursued. They note, however, that the implementation of security measures imposes additional financial costs on a sector that is already experiencing difficulty in meeting the financial challenges of an aging infrastructure. Accordingly, the industry has sought federal assistance through the congressional appropriations process. In 2003, Congress responded by considering legislation that would have authorized $200 million for use in making grants to wastewater utilities to conduct vulnerability assessments and implement security improvements, $15 million for technical assistance for small systems, and $5 million over 5 years for refinement to vulnerability assessment methodologies.

Objectives, Scope, and Methodology

As requested by 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 wastewater systems?
- What specific activities should the federal government support to improve wastewater security?
- What are the criteria that should be used to determine how federal funds are allocated among recipients to improve wastewater security, and how should the funds be distributed?

It was outside the scope of this review to ascertain the desirability of using federal funds to support wastewater security or to compare the merits of federal support of the wastewater industry with others such as the electric power or transportation industries. Rather, we sought to obtain expert

advice on how best to use federal funds to improve wastewater security, should Congress agree that they should be appropriated for this purpose.

To obtain information on these three questions, we conducted a three-phase Web-based survey of 50 experts on wastewater security. We identified these experts from a list of more than 100 widely recognized experts in one or more key aspects of wastewater 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, preparedness, engineering, epidemiology, public policy, security, wastewater treatment, risk assessment, water infrastructure, bioterrorism, and public health).

In addition, we sought experts from (1) key federal organizations (e.g., DHS, EPA, and National Science Foundation); (2) key state and local agencies, including health departments and environmental protection departments; and (3) key industry and nonprofit organizations such as AMSA, Environmental Defense, Water Environment Federation, and the Water Environment Research Foundation; and (4) water utilities serving populations of varying sizes. Of the approximately 70 experts we contacted, 50 agreed to participate and complete all three phases of our survey. A list of the 50 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 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 adapted the method to use on 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, allowing us to obtain a broad range of opinions.

For each phase in our three-phase Delphi process, we posted a questionnaire on GAO's survey Web site. 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 survey's first phase, we asked a series of open-ended questions. We pretested these questions with officials from the wastewater utility industry, nonprofit research groups, and a federal agency. Responses were content analyzed to provide the basis for the questions asked in the subsequent phases. Phase 2 questions were close-ended and asked experts to rate the relative priority or effectiveness of the Phase 1-identified security activities, allocation criteria, and funding mechanisms. Experts were also invited to provide narrative comments.

During the third phase, we provided experts with aggregate group results from Phase 2, along with their own individual answers to the Phase 2 questionnaire. Experts were asked to compare the group results with their own individual answers and to use this information as a basis for reconsidering their answers and revising their individual responses, if so desired.

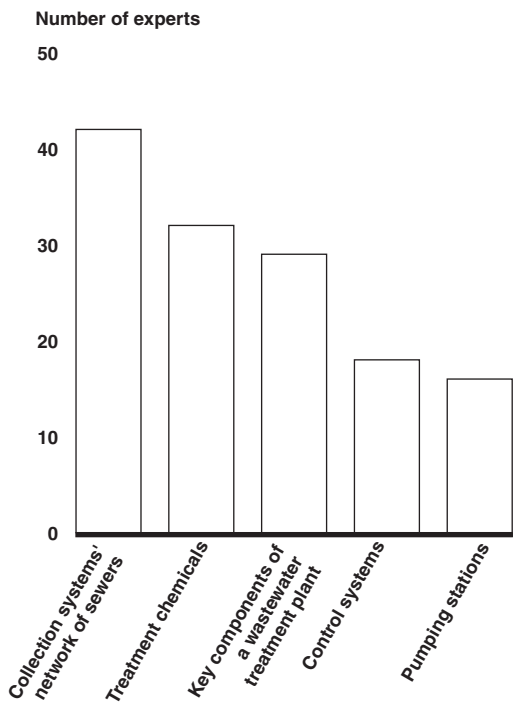
In addition to the information obtained from our expert panel, we obtained documentation from representatives of professional organizations, such as the National Academy of Sciences, the Water Environment Research Foundation, and AMSA. We also held interviews with EPA on the agency's wastewater security programs. During our interviews, we asked officials to provide information on program operations, policies, guidance, and funding levels. We also received training on VSAT from the Water Environment Federation, which was supported by AMSA, and attended specialized conferences addressing water security by the American Water Works Association and other organizations.

We conducted our work from January 2004 through December 2004 in accordance with generally accepted government auditing standards.

Experts Identified Key Vulnerabilities That Could Compromise Wastewater Security

Experts responding to our survey identified five key physical assets of wastewater systems as among the most vulnerable to terrorist-related attacks: (1) the collection systems' network of sewers, which includes underground sanitary, stormwater and combined sewer lines; (2) treatment chemicals, primarily chlorine, which are used to disinfect wastewater; (3) key components of the wastewater treatment plant, such as its headworks, where the raw sewage first enters the treatment plant; (4) control systems, used to control plant operations; and (5) pumping stations along the collection system, which lift or pump wastewater to allow gravity flow to help move sewage to the treatment plant (see fig. 4). Of these assets, experts ranked the collection systems' network of sewers and treatment chemicals as the most vulnerable.

Figure 4: Key Wastewater System Vulnerabilities Identified by Experts



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

Experts also identified overarching vulnerabilities that could compromise the overall integrity of the systems' security. These vulnerabilities include (1) a general lack of security awareness within the wastewater sector; (2)

interdependencies among components of the wastewater system, opening the possibility that a failure of any individual component could bring down the entire system; and (3) interdependencies between the wastewater system and other critical infrastructure that could fail, such as electric power supplies.

In general, our panel of experts' observations were consistent with those of major organizations that have conducted research on wastewater system vulnerabilities. Among these organizations are the Water Environment Federation and the Association of Metropolitan Sewerage Agencies.

Experts Identified Five Key Vulnerabilities

The five assets experts considered most vulnerable included the collection systems' network of sewer lines, treatment chemicals, key components of the wastewater treatment plant, control systems, and pumping stations.

Collection Systems' Network of Sewers

Forty-two of the 50 experts we surveyed identified the collection systems' network of sanitary, storm, and combined sewer lines as among the top five terrorist-related vulnerabilities of wastewater systems. Experts explained that adversaries could use the network of sewers to (1) covertly gain access to intended targets within the service area or to (2) convey hazardous or flammable substances that may cause explosions at points along the system or cause harm to the wastewater treatment system or process.

As some experts explained, gaining access to buildings or other intended targets could be accomplished covertly using sewer networks. Sewers make underground travel from a point of entry to a potential target almost undetectable. Entering the sewer system is relatively easy, due to the large number of access points, such as manholes, that may or may not be protected. Moreover, some sewers, particularly those in older cities, may be large enough for people and even trucks to covertly pass through—often beneath some of the most heavily populated and critical areas—and gain access to potential targets, such as government and financial districts. Sewer lines range in size from 4 inches to greater than 20 feet in diameter. One expert explained:

> Access controls to important installations, such as perimeter fencing, can be countered by a terrorist gaining access to the facility unseen by using the underground collectors. Once access is gained, any activity could then occur—target reconnaissance or surveillance,

planting of conventional explosives or weapons of mass destruction, hostage taking, [or] theft of critical documents and items.

Many experts also suggested that adversaries could use the collection system as an underground transport system—without ever physically entering the system—for explosive or toxic agents. These substances could be inserted into the system through storm drains, manholes, or household drains. Several experts explained that with prior knowledge of a system's gravity flow, an adversary could calculate the precise timing and location of an explosion or calculate the amount of a substance that might be necessary to disable or destroy the biological processes of a wastewater treatment plant.

However, even without precise knowledge about a system, significant damage can occur as a result of underground sewer explosions. These explosions may also damage natural gas or electric lines often co-located with sewers. One expert cited the effects of an unintentional explosion that occurred in 1981 in Louisville, Kentucky, where thousands of gallons of a highly flammable solvent, hexane, spilled into the sewer lines from a local processing plant. The fumes created an explosive mixture that was eventually ignited by a spark from a passing car. The result was a series of explosions that collapsed a 12-foot diameter pipe and damaged more than 2 miles of streets. While no one was seriously injured, sewer line repairs took 20 months, followed by several more months to repair the streets. A more serious incident occurred in Guadalajara, Mexico, when a gasoline leak into a sewer, in April 1992, caused explosions that killed 215 people, injured 1,500 others, damaged 1,600 buildings, and destroyed 1.25 miles of sewer. The explosion created craters as deep as 24 feet and as large as 150 feet in diameter. Another alarming incident was an intentional release of a cleaning solvent (naptha) and alcohol into a sewer that caused explosions 3.5 miles away from the source and damaged about 5,400 feet of sewer line. This June 1977 incident in Akron, Ohio, by vandals at a rubber manufacturing plant resulted in more than $10 million in damage.

Adversaries may also use the system to convey substances that disable the treatment process. For example, as one expert explained, an adversary could introduce a highly toxic chemical into the sewer that could damage the biological processes involved in treatment. Several experts warned that disabling the treatment process could cause the release of improperly treated sewage, placing the receiving water in jeopardy and potentially harming human health and the environment. In February 2002, such an incident occurred in Hagerstown, Maryland, when chemicals from an

unknown source entered the wastewater treatment plant and destroyed the facility's biological treatment process. This incident resulted in the discharge of millions of gallons of partially treated sewage into a major tributary of the Potomac River, less than 100 miles from a water supply intake for the Washington, D.C., metropolitan area.

Wastewater Treatment Chemicals

Thirty-two of the 50 experts we surveyed identified process chemicals used in wastewater treatment as among the top five terrorist-related wastewater system vulnerabilities. Wastewater treatment facilities use a variety of chemicals, including chlorine, sulfur dioxide, and ammonia during the treatment process. Most experts singled out chlorine gas as a major chemical of concern because it is an extremely volatile and hazardous chemical that requires specific precautions for its safe transport, storage, and use.

Chlorine is a disinfectant that is commonly used in the treatment process before treated water (effluent) is discharged into local waterways. However, if chlorine, which is stored and transported as a liquefied gas under pressure, is accidentally released into the atmosphere, it quickly turns into a potentially lethal gas. Because gaseous chlorine is heavier than air, the cloud it forms tends to spread along the ground. Consequently, accidental or intentional releases of chlorine could be extremely harmful to those in the immediate area. Exposures to chlorine could burn eyes and skin, inflame the lungs, and could be deadly if inhaled. One expert pointed out that accidental releases of chlorine gas have occurred numerous times and that a deliberate release would be relatively feasible. The expert further explained that many wastewater plants have been converting from chlorine gas to alternative disinfection methods for various reasons, including the risk of a release.

Recognizing that chlorine gas releases pose threats to the public and the environment, EPA requires, among other things, that any facility storing at least 2,500 pounds of chlorine gas submit a risk management plan; as of December 2004, EPA estimates that about 1,200 plants fit this category. The plan includes an estimate of the potential consequences to surrounding communities of hypothetical accidental "worst-case" chemical releases from their plants. These estimates include the residential population

located within the range of a toxic gas cloud produced by a "worst-case" chemical release, called the vulnerable zone.[1]

Several experts stated that a terrorist could use chlorine gas as a weapon, either at a wastewater plant that is in close proximity to a specific target population, or through theft and use at another location. In fact, on September 11, 2001, railroad tanker cars filled with toxic chemicals including chlorine sat at a treatment plant across the river from the Pentagon as it was being attacked. At that time, the population within the plant's vulnerable zone was 1.7 million people. Within weeks after September 11, this facility converted to an alternative disinfection method. Other facilities have also eliminated the use of chlorine gas, choosing instead chlorine-based technologies (e.g., sodium hypochlorite, calcium hypochlorite, mixed oxidant generation) or nonchlorine-based technologies (e.g., ozone and ultraviolet light). However, as one expert noted, several dozen wastewater treatment plants in heavily populated areas continue to use large amounts of chlorine gas.

In addition to concerns over on-site chlorine storage, experts were also concerned about the safe transport of chemicals to treatment facilities. Chlorine is delivered to facilities via railways and highways and in various container sizes ranging from 1-ton cylinders to 90-ton railroad cars (see figs. 5 and 6). As experts noted, although rail tank cars are designed to avoid leakage in the event of a derailment, and the containers can theoretically withstand a bullet from a normal handgun or rifle, one expert concluded that the "use of explosives to cause a rupture is well within the skill set of a terrorist."

[1]EPA's requirements for "worst-case" release analysis tend to result in consequence estimates that are significantly higher than what is likely to actually occur. For example, "worst case" release analysis does not take into account active mitigation measures facilities often employ to reduce the consequences of releases.

Figure 5: Chlorine Delivery Truck

Source: Withheld. Photograph used with permission.

Figure 6: Chlorine Railroad Car

Source: Withheld. Photograph used with permission.

Such an attack along a congested transportation corridor could have severe public health and safety impacts. One expert said that before converting from chlorine to alternative disinfection methods, a major wastewater treatment plant in Washington, D.C., received its chlorine supply via rail shipments that traversed through the center of the city, close to the U.S.

Capitol Building and across two military installations before reaching its final destination. Derailments of chlorine could have major impacts in small communities as well, as occurred in Alberton, Montana, in April 1996. One of the five tankers that derailed ruptured and reportedly released more than 60 tons of chlorine. Subsequently, a toxic plume of chlorine gas crossed the Clark Fork River, a major interstate, and surrounding residences. An estimated 1,000 people were evacuated, 350 people were hospitalized, and one person died.

Key Components of the Treatment Plant

In addition to the vulnerability of chemicals stored at a wastewater treatment plant, experts also listed the key process components of the treatment plant as vulnerable. Specifically, more than half of the experts (29 of 50) identified one or more of these components as among the top five vulnerabilities. One expert explained that, historically, security was not a consideration in site selection or design of these facilities. While many utilities planned for natural disasters or vandalism, it was only after September 11, that many utilities have considered how best to protect against potential terrorist attacks.

While experts expressed concern over the security of the entire treatment plant, several identified the headworks as a component that is particularly vulnerable to attack, as well as critical to the treatment process. This unit is part of a plant's primary treatment process, where wastewater carried through the collection system first enters the treatment plant. It is here that large objects, such as cans, wood, and plastics are removed from the wastewater stream. These structures may be open to the atmosphere and, according to one expert, are easy to attack. Experts explained that sabotage of the headworks could affect the proper working order of subsequent treatment processes and could cause the immediate interruption of the collection system, potentially restricting or completely blocking wastewater flow. As one expert noted, restricted flow would could cause backups through the collection system, and the stagnant wastewater would become a public health hazard within hours, either through physical contact or through cross-contamination of drinking water supplies.

Control Systems

Control systems were also listed as a key vulnerability by 18 of the 50 experts. Many wastewater systems are increasingly relying on the use of these control systems, including Supervisory Control and Data Acquisition (SCADA) networks, to serve functions ranging from storing and processing

data to monitoring the system's condition and controlling its operation. The primary role of SCADA systems is to monitor and control dispersed assets from a central location. According to one expert, "The backbone for process control is the SCADA system." The expert explained that several factors contribute to the vulnerability of these controls, including typically nonsecured process control rooms at treatment plants, remote access to SCADA, and shared passwords between multiple users.

Experts generally explained that an attack on these systems could interfere with critical operations. For example, one expert explained that an adversary could use SCADA systems to introduce either dangerously high or inadequate levels of chemicals; reduce biological treatment levels; or cause remote points along the collection system to fail. Although some facilities could operate their systems manually should the automated system fail or be compromised, others do not have the personnel or equipment to do so. For example, as one expert noted, large valves in modern plants are now typically operated electronically and seldom used manual operation components (see fig. 7).

Figure 7: Pump Operated through Remote Automated Systems

Source: Withheld. Photograph used with permission.

While SCADA networks offer operators increased flexibility and efficiency by controlling processes remotely, they were not designed with security in mind. The security of these systems is, therefore, often weak.[2] According to our experts, while many facilities take advantage of their system's flexibility, they often do not provide the necessary training on cyber security or implement security measures such as rotating passwords or securing network connections. Experts also explained that penetration of

[2]Department of Energy. 21 Steps to Improve Cyber Security of SCADA Networks. http\\www.eq.doe.gov/pdfs/21stepbooklet.pdf (Downloaded July 1, 2004).

SCADA systems, particularly those that may be nonencrypted and accessed via the Internet, offers a particularly easy point of access and control of a wastewater system. One expert provided an example of a breach in cyber security in 2000 when such a system in Australia was attacked, causing the release of thousands of gallons of raw sewage. While the actions were not an act of terrorism, they illustrate how a computer or cyber-related attack could be used to disrupt wastewater treatment.

Pumping Stations

Sixteen of the 50 experts identified pumping stations, which are components that help convey sewage to the wastewater treatment plant, as among the top vulnerabilities. One expert explained that destroying or disabling a pumping station could cause the collection system to overflow raw sewage into the streets and into surface waters and to back up sewage into homes and businesses. The expert added that adverse effects on public health and the environment are likely if the target pump station pumps several million gallons per day of wastewater. Another expert explained, that within a service area, one pumping station has the capacity to pump 25 million gallons of wastewater per day.

Experts explained that the remoteness and geographic distribution of pumping stations, and their lack of continuous surveillance, make them particularly vulnerable (see fig. 8). However, as one expert noted, should these stations be disabled or destroyed, alternatives such as “pump-around schemes,” where sewage flow is diverted and rerouted, can often be implemented within a few days or weeks.

Figure 8: Pumping Station

Source: Withheld. Photograph used with permission.

Overarching Vulnerabilities Affecting Overall Wastewater System Security

In addition to the physical assets identified as among the greatest vulnerabilities of wastewater systems, some experts also identified vulnerabilities that may affect the overall security of the nations' wastewater systems. First, they pointed out that wastewater utilities generally do not have a security culture because they are often more focused on operational efficiency and may, therefore, be reluctant to add security procedures and access control elements to their operations. For example, one expert noted the ease with which many types of individuals (employees, contractors, and visitors) and vehicles typically enter wastewater treatment plant facilities. As this expert pointed out, some facilities do not check to ensure that individuals entering the property have legitimate reasons for being there. This expert also raised a concern about

the lack of inspection of incoming truckloads at some wastewater treatment plants. An adversary could exploit this lack of security by delivering contaminants or explosives to destroy the treatment process or the entire facility. In addition to securing entrance checkpoints, two experts suggested there is little background screening of utility employees. One expert noted, "People with criminal records, falsified educational credentials, and other serious liabilities might be hired by utilities that fail to thoroughly check their backgrounds. The result can be intentional acts of terrorism on a utility."

Second, experts pointed to interdependencies *among* all major wastewater assets within the treatment system. The system as a whole relies on the proper working order of all its components to treat a community's wastewater. One expert explained that, because treatment plants are less able to recover from an attack, they may have a higher level of security than other assets, such as the collection system. However, because collection and treatment are part of one integrated system, securing one asset does not ensure that the system as a whole is more protected. For example, gates and fences around the main treatment plant may stop an adversary from coming onto the physical property, but it will not prevent a harmful agent from entering the facility through the collection system—an event that could destroy the facility's entire secondary treatment process.

Third, experts identified interdependencies *between* wastewater systems and other critical infrastructures. As several experts explained, disruptions in electric power, cyber systems, and transportation of treatment chemicals can result in a failure of wastewater treatment systems. One expert cautioned that the interruption of the power grid could render the wastewater plant useless, noting, "Several hours without power would cause the biological treatment process to halt and wastewater would back up on the collection system." Such an event occurred in 2003, when a major power failure caused treatment plants in Cleveland, Ohio, to release at least 60 million gallons of raw untreated wastewater into receiving waters. Without electric power, operators had no other option but to bypass treatment and directly discharge the untreated sewage into Lake Erie or the Cuyahoga River and other tributaries.

Conversely, there are instances in which other infrastructure and activities may depend on treated wastewater to properly function. For example, in some parts of the country, effluent is reclaimed and used as cooling water for power generation, to recharge groundwater, or to water outdoor landscapes. One expert noted that wastewater treated at a plant in the arid

Western United States is reclaimed and used to provide the only cooling source for a nuclear power plant that provides power for much of that region. According to the same expert, the immobilization of this treatment plant could, within a certain number of days, disable the nuclear plant, causing a major, multistate power outage.

Experts Identified Wastewater Security-Enhancing Activities That Warrant Federal Support

Experts most frequently identified 11 specific activities to improve wastewater security as deserving high priority for federal support (see fig. 9). Three activities are particularly noteworthy because they were given a rating of highest priority by a substantial number of the experts. These activities include the following:

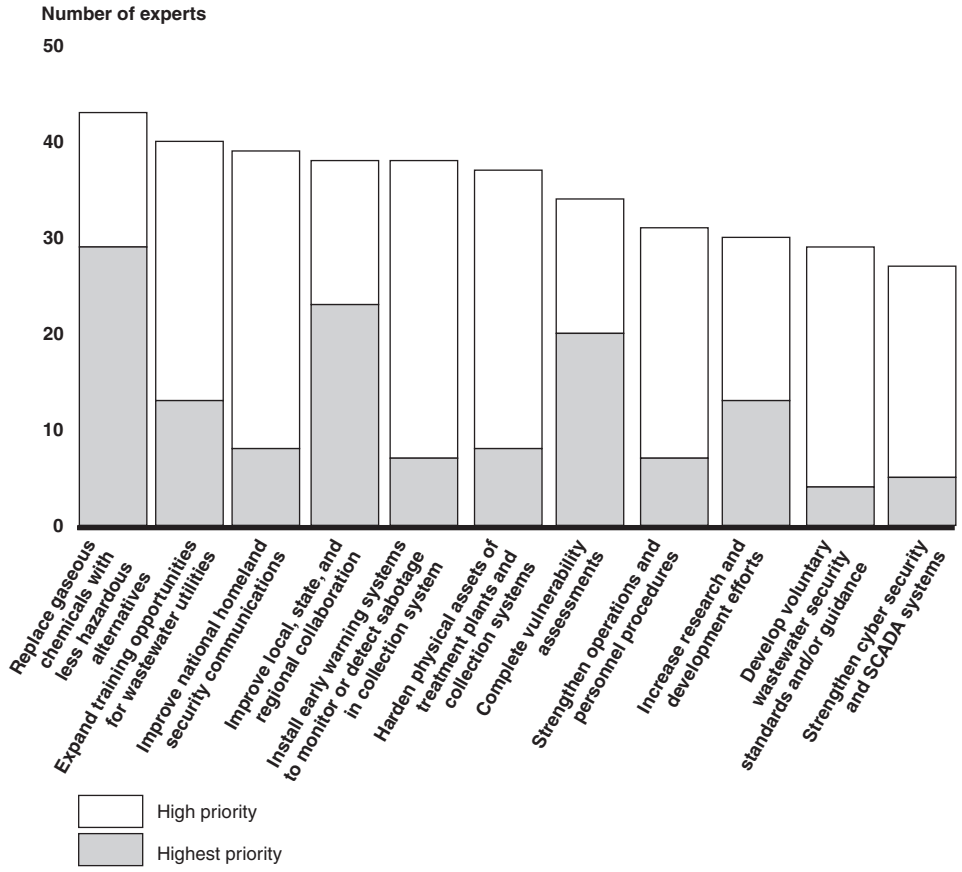
- *Replacing gaseous chemicals used in wastewater treatment with less hazardous alternatives.* Experts viewed these actions as essential to reduce the vulnerability inherent in systems that rely upon the transport, storage, and use of potentially hazardous materials such as gaseous chlorine in their treatment processes. Several experts noted that replacement could be cost prohibitive for many wastewater utilities and that it, therefore, warranted federal support.

- *Improving local, state, and regional collaboration efforts.* Experts identified the development of strong working relationships among utilities and public safety agencies as critical to protecting wastewater infrastructure and system customers from potential threats. Some experts also noted that enhanced partnerships among these groups would result in improved response capabilities should a wastewater system be attacked.

- *Completing vulnerability assessments for individual wastewater systems.* Experts cited these as necessary for utilities to understand their security weaknesses, to identify appropriate countermeasures, and to implement risk reduction strategies in a logical, coordinated manner.

The remaining eight activities experts frequently rated as warranting high or highest priority for federal funding include (1) providing training to utility employees related to conducting vulnerability assessments and improving the security culture among employees; (2) improving national communication efforts between utilities and key entities responsible for homeland security; (3) installing early warning systems in collection systems to monitor for or detect sabotage; (4) hardening physical assets of treatment plants and collection systems; (5) strengthening operations and personnel procedures; (6) increasing research and development efforts toward improving threat detection, assessment, and response capabilities; (7) developing voluntary wastewater security standards and guidance documents; and (8) strengthening cyber security and Supervisory Control and Data Acquisition (SCADA) systems.

Figure 9: Experts' Views on Wastewater Security Activities Most Deserving of Federal Support



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

Replace Gaseous Chemicals with Less Hazardous Alternatives

Over half of the experts surveyed (29 of 50) rated the replacement of gaseous chemicals at wastewater treatment facilities with less hazardous alternatives as warranting highest priority for federal funding. Another 14 experts rated this activity as high priority. Experts reported that wastewater systems carrying out treatment processes using gaseous forms of chemicals, particularly chlorine, make themselves targets for terrorist attack. However, as one expert noted, changing disinfection technologies effectively devalues these facilities as targets for "weaponization" of their existing infrastructure.

Several experts noted that some communities and utilities currently using gaseous chemical treatment processes have expressed interest in converting to an alternative treatment technology, but the financial costs associated with conversion remain prohibitive. However, one stated that replacing gaseous chemical treatment technology can actually result in certain offsetting cost savings. For example, the Blue Plains Wastewater Treatment Plant in Washington, D.C., employed around-the-clock police units prior to replacing its chlorine gas treatment process. Following conversion to a less hazardous treatment technology, Blue Plains found that it could reduce this security posture. In addition, the utility was able to reduce the need for certain emergency planning efforts and regulatory paperwork.

Experts suggested alternative treatment technologies such as sodium hypochlorite (a solution of dissolved chlorine gas in sodium hydroxide) and ultraviolet disinfection. These alternative processes have been implemented at several facilities throughout the United States, including Washington, D.C.; Atlanta, Georgia; Philadelphia, Pennsylvania; Cincinnati, Ohio; Jacksonville, Florida; and Harahan, Louisiana. The change, for an individual plant, to sodium hypochlorite may require approximately $12.5 million for new equipment and increase annual chemical costs from $600,000 for gaseous chlorine to over $2 million for sodium hypochlorite.[1]

Another expert suggested that reducing the size of containers used to transport and store gaseous chemicals could also prove an effective deterrent to terrorism. This approach is being implemented by a treatment plant in the Western United States, where gaseous chlorine is now stored in 1-ton canisters—a significant reduction in size from the larger 90-ton railroad tanker car size containers the utility previously employed (see fig. 10).

[1] http://c3.org/chlorine-issues/disinfection/water-disinfection.html

Figure 10: One-Ton Canisters of Chlorine Gas Stored at a Wastewater Treatment Plant

Source: Withheld. Photograph used with permission.

Improve Local, State, and Regional Collaboration Efforts

Twenty-three of 50 experts rated efforts to improve local, state, and regional collaboration as warranting highest priority for federal funding. Fifteen more experts rated this activity as high priority. Several experts noted the importance of establishing strong working relationships among utilities, local and state law enforcement agencies, fire departments, and other first response agencies in advance of a potential emergency situation. Many added that enhanced partnerships among these entities can yield significant benefits to wastewater utilities including an increased ability to monitor critical infrastructure and facilities, improved understanding of

agency roles and responsibilities, and faster response time to deal with potential security breaches.

According to one expert, significant personnel and other resources devoted to emergency response are theoretically available to the wastewater sector. These resources include law enforcement agencies, fire departments, public health care facilities, environmental authorities, and other nonprofit and commercial entities. However, the expert noted that wastewater facilities remain largely disconnected from these entities, and wastewater facilities' efforts for emergency response planning are, therefore, often undertaken independently. Consequently, emergency response teams do not gain a full understanding or appreciation of the unique challenges inherent in maintaining a utility's wastewater treatment capability.

This lack of collaboration perpetuates the community's idea that "sewers lead to [a] magical place where [materials] simply 'go away' without consequence," one expert suggested. The expert added that this misperception is demonstrated by a failure of some in the medical response community to adequately plan for proper disposal of waste resulting from decontamination efforts of a chemical, biological, or radiological event. Directly discharging such material to the wastewater influent stream could significantly damage or destroy the wastewater treatment process.

Collaboration among local, state, and regional agencies should include periodic field and "tabletop" exercises to establish and reevaluate the roles, capabilities, and responsibilities of agencies that would respond to a terrorist event, according to one expert. Another identified the nonprofit California Utilities Emergency Association, an entity to which most utilities in that state belong, as an effective provider of communications, training, mutual aid coordination, and simulation exercises. The expert also cited the San Francisco Bay Area Security Information Collaborative as a successful example of regional collaboration in which participating water utilities coordinate communications, responses, and emergency planning.

The Environmental Protection Agency (EPA) has provided funding for training on emergency response for wastewater utilities through agreements with the Wastewater Operator State Environmental Training Program, the Water Environment Federation, and other organizations. Through the Department of Homeland Security's Office of Domestic Preparedness, EPA has funded emergency response table-top exercise training to the nation's larger wastewater utilities.

Complete Vulnerability Assessments

Twenty of 50 experts rated the completion of vulnerability assessments as warranting highest priority for federal funding. Fourteen other experts rated this activity as high priority. Vulnerability assessments help water utilities evaluate their susceptibility to potential threats and identify corrective actions to reduce or mitigate the risk of serious consequences from vandalism, insider sabotage, or terrorist attack. One expert explained that this process enables a utility to evaluate its terrorist-related vulnerabilities and begin to implement security enhancement plans that directly address those identified vulnerabilities. Another added that the assessments also present useful findings that should be incorporated into a utility's emergency response plan and that they enable an active process for updating and exercising those plans.

The Bioterrorism Act of 2002 required vulnerability assessments for drinking water utilities serving more than 3,300 people but did not include a comparable requirement for wastewater utilities. To foster the completion of vulnerability assessments among wastewater utilities, EPA has funded the development of vulnerability assessment methodologies and provided training to wastewater utilities. EPA has encouraged wastewater utilities to use methodologies such as those provided by the National Environmental Training Center for Small Communities, on security and emergency planning, and the Vulnerability Self Assessment Tool (VSAT), developed and released by the Association of Metropolitan Sewerage Agencies. The VSAT methodology and accompanying software provide an interactive framework for utilities of all sizes to analyze security vulnerabilities to both manmade threats and natural disasters, evaluate potential countermeasures for these threats, and enhance response capability in the event of an emergency situation. This methodology has been continually updated and improved; VSAT Version 3.1 is currently available to utilities. Through EPA support, the Water Environment Federation has provided extensive training of the VSAT tool free of charge to wastewater utility operators and others involved in environmental protection, public safety, and security.

Expand Training Opportunities for Wastewater Utility Operators and Administrators

Thirteen of the 50 experts rated the expansion of training opportunities for utility personnel as warranting highest priority for federal funding, and an additional 27 experts suggested this activity warranted a high priority. According to experts, creating a security-minded culture among wastewater utilities is critical to building awareness of security vulnerabilities and implementing appropriate countermeasures.

In particular, experts noted that wastewater system operators and administrators need to become better educated about the importance of focusing on security and emergency preparedness issues. Several experts suggested that managers should have a full understanding of potential types of terrorist attacks and the systems or mechanisms that could preclude or mitigate these events. They added that other parties, including boards of directors of wastewater systems, mayors, and city councils need to be made aware of potential threats to wastewater systems and the impact a terrorist event could have upon a facility. One expert stated that successful development of security awareness among those associated with wastewater systems could mean the difference between simply installing security systems and actually becoming secure.

Experts also stated that additional *technical* training for operators is necessary to ensure the security of wastewater systems. One noted that this type of training could avert a catastrophe by enabling a wastewater operator to recognize a pending disaster as early as possible. Another expert stated that increased technical training, particularly for smaller wastewater utilities, is necessary to ensure that funds for physical security enhancements are used to their maximum potential, thus achieving maximum benefit for the wastewater utility. One expert also suggested that devoting funding toward increased technical training will provide wastewater utility employees with the skills necessary for developing comprehensive vulnerability assessments and implementing emergency response plans before a terrorist attack.

Since 2002, EPA has provided more than $10 million to help address the security needs of the wastewater sector. A large portion of this funding has been awarded to nonprofit technical support and trade organizations to develop tools and training on conducting vulnerability assessments to reduce utility vulnerabilities and on planning for and practicing response to emergencies and incidents.

Improve National Communication Efforts between Utilities and Key Entities Responsible for Homeland Security

While only 8 of 50 experts rated efforts to improve communications between utilities and federal entities responsible for homeland security as warranting highest priority for federal funding, well over half of the experts surveyed (31 of 50) rated this activity as high priority. One expert stated that it is essential to develop an effective communications strategy that involves the broad range of stakeholders responsible for ensuring wastewater security. Another emphasized that wastewater utilities need timely and useful information from federal authorities about increased threat levels and protective actions that should be implemented.

To improve national communications, EPA provided a grant to AMWA to develop the Water Information Sharing and Analysis Center (Water ISAC). The Water ISAC is a secure, Internet-based subscription service that provides time-sensitive information and expert analysis on threats to both wastewater and drinking water systems. It serves as a key link in the flow of water security information among utilities and federal homeland security, intelligence, law enforcement, public health, and environmental agencies.

However, according to some experts, Water ISAC does not sufficiently ensure adequate communication between federal agencies and utilities. One stated that despite a high reliance upon Water ISAC by drinking water utilities, this communication vehicle has proven inadequate for meeting the needs of the broad range of stakeholders involved in protecting drinking water security. This expert added that the Water ISAC needs to be better developed if it is to be an essential part of a communications strategy for the wastewater sector. Another expert noted that several water utilities have avoided the Water ISAC because of the subscription fees associated with the service. In the fall of 2004, the Water ISAC announced a new communication tool known as Water Security Channel. The Water Security Channel is a password protected site that electronically distributes federal advisories regarding threat information to the water sector. Water Security Channel is a service that is free of charge to any wastewater or drinking water utility that wishes to participate.

For its part, the Department of Homeland Security is implementing its Homeland Security Information Network (HSIN) initiative, which will provide a real-time, collaborative flow of threat information to state and local communities, as well as to individual sectors. According to the department, this network will be the only tool available that provides collaborative communications between first responders, emergency

services, the government (local, state, and federal) and other sectors on a real-time basis. In addition, the department has established a Water Sector Coordinating Council to identify information and other needs of the sector, including the appropriate use and the relationships among the Water ISAC, the Water Security Channel, and HSIN.

Install Early Warning Systems in Collection Systems to Monitor for or Detect Sabotage

Seven of 50 experts rated the installation of early warning systems in collection systems to monitor for or detect sabotage as warranting highest priority for federal funding, and an additional 31 experts rated this activity as a high priority. A device these experts frequently mentioned to achieve some degree of monitoring and detection for explosive substances is the lower explosive level (LEL) meter, which can be inserted into manholes and connected to central computers. One expert claimed LEL meters have significantly improved response time in mitigating the potential for structural damages resulting from explosions within the wastewater collection system.

One expert also noted that disabling the biological processes occurring at a wastewater treatment plant would require a large amount of toxic compounds to be inserted into the collection system, but several experts stated that this possibility remains of concern because of the open access collection systems afford. Many experts suggest that additional research is needed to develop early warning technologies that can sense the presence and concentration of these types of toxic compounds in the collection system and relay that information electronically to treatment operators.

Harden Physical Assets of Treatment Plants and Collection Systems

Eight of 50 experts rated physical hardening of treatment plants and collection systems as warranting highest priority for federal funding and an additional 29 experts rated this activity as high priority. Experts stated that physically securing the perimeter of the treatment plants and pumping stations with fences, locks, security cameras, alarm systems, motion detection systems, and other physical barriers can protect critical treatment components from direct attack or sabotage (see figs. 11 and 12). One expert noted that the more difficulty terrorists encounter in trying to reach critical targets in a wastewater system, the less frequently attacks will be attempted, and the lesser the impact will be if and when these attempts succeed. Furthermore, improvements to perimeter defenses surrounding wastewater treatment systems not only deter terrorist intruders but also restrict access by vandals, contributing toward improved

reliability of electronic surveillance systems. As one expert pointed out, physical hardening of assets can largely be accomplished with hardware that requires only minimal maintenance and replacement cost once installed.

Figure 11: Electronically-Controlled Security Gate

Source: Withheld. Photograph used with permission.

Figure 12: Security Camera and Infrared Motion Detectors

Source: Withheld. Photograph used with permission.

Other experts suggested that actions are needed to provide redundant capabilities to wastewater treatment systems. According to experts, additional power, pumping, and collection bypass systems would provide more reliable treatment capacity that would benefit the public not only in the event of terrorism but also during nonterrorist events (e.g., natural disasters, weather-related events, or interrelated infrastructure failures).

Such actions could ensure that wastewater systems maintain full treatment capabilities during a variety of unforeseen catastrophic events.

Although one expert claimed that protecting the several hundred miles of sewers in a large urban system is virtually impossible, other experts suggested that design improvements and physical alterations could limit access to collection systems. Some experts suggested securing manhole covers with maintenance-friendly lockdown mechanisms. In addition, one expert suggested improving engineering designs for wastewater systems in ways that reduce vulnerability risks posed by infrastructure cross-connections with other water systems.

Strengthen Operations and Personnel Procedures

Seven of 50 experts rated the strengthening of operations and personnel procedures at wastewater systems as warranting highest priority for federal funding, and an additional 24 experts rated this activity as a high priority. For example, one expert suggested that a highly efficient background check system should be available to water utilities to get accurate information on new and existing employees, contractors, and others who are working at vital facilities, such as wastewater treatment plants. This expert noted that access to such systems is afforded to airport administrators and certain law enforcement entities but is largely inaccessible to water utilities.

Another expert stated that wastewater utilities need procedures to ensure the security of collection system maps and drawings, while also allowing reasonable access to them by contractors and developers. The expert suggested maps could be electronically stored and password protected with a regularly changed password. Another expert suggested that all employees and visitors have identification badges with photographs and electronic strips or sensors that regulate points of access allowed by the badge.

Increase Research and Development Efforts to Improve Detection, Assessment, and Response Capabilities

Thirteen of 50 experts rated expanded research and development efforts to improve detection, assessment, and response capabilities for wastewater systems as warranting highest priority for federal funding, and an additional 17 experts suggested this activity warranted a high priority. One expert stated that new technologies are needed in the wastewater sector to better protect physical assets by providing reliable surveillance and detection capabilities with a minimal need for on-site, around-the-clock

security personnel. According to another expert, technologies currently in development for drinking water utilities could potentially be adapted for use by wastewater utilities. These technologies would need to detect hazardous chemical, biological, or radioactive contaminants while operating in the harsh environment of common, everyday contaminants found in sewage. Also, improved computer mapping systems tracking the course and speed of sewage flow could greatly enhance emergency response activities including evacuations, dilutions of harmful substances that have been introduced to the sewage flow, and venting of volatile materials.

EPA's Office of Research and Development has recently funded research that is intended to address many of these needs. According to an official with EPA's Water Security Division, while these efforts have been primarily directed toward drinking water security research, some of EPA's research findings can be applied to wastewater security. EPA has also developed a water security research and technical support action plan that outlines various research and technical support needs that the water industry and other stakeholders have identified. The plan also proposes specific projects to address these needs, and EPA has begun work on some of these projects in collaboration with the Water Environment Research Foundation and the American Water Works Association Research Foundation. These nonprofit research organizations have received funding to address a variety of wastewater security research projects, such as assessing new security technologies to detect and monitor contaminants and prevent security breaches. According to EPA, other issues being addressed include public health protection, vulnerability and protection of water and wastewater infrastructure, and communication in the event of deliberate attacks or natural disasters.

Develop Voluntary Wastewater Security Standards and Guidance Documents

Four of 50 experts rated the development of voluntary wastewater security standards and guidance documents as warranting highest priority for federal funding, and half of the experts surveyed (25 of 50) gave this activity a high priority rating. Experts identified options including development and issuance of voluntary standards for security of wastewater facilities (including design standards), a peer review process to evaluate the quality of wastewater utilities' vulnerability assessments and emergency response plans, and creation of a secure Web site that disseminates lessons learned by utilities throughout the various phases and processes related to protecting wastewater security.

One expert suggested that developing government standards for the security of all new facilities would help increase the overall ability of wastewater systems to withstand threats. The expert stated such standards should lay out minimum protection standards and provide a framework of threats utilities should consider when completing vulnerability assessments. Another expert suggested that, because water utilities seek guidance from the federal government on whether their individual treatment plants are secure, one option, in lieu of site visits by EPA, might be a peer review process of vulnerability assessments and emergency response plans across wastewater utilities. Development of a secure Web site for wastewater utilities that includes lessons learned from assessments, planning, training, and incident responses could also provide valuable guidance for wastewater utilities, one expert noted.

EPA recently commissioned a study by the National Drinking Water Advisory Council's Water Security Working Group to address some of these needs. The group's charge is to identify: (1) the features of an active and effective security program for drinking water and wastewater utilities; (2) incentives that would encourage water utilities to implement features of the security program; and (3) ways to measure the extent of utility implementation of the security program. In addition, in September 2003, EPA gave funding to the American Society of Civil Engineers to develop voluntary security standards for drinking water, wastewater, and stormwater utilities, which were released in December 2004 as interim standards. A training module is planned for spring 2005.

Strengthen Cyber Security and SCADA Systems

Five of 50 experts rated efforts to improve cyber security and SCADA systems as warranting highest priority for federal funding, and an additional 22 experts gave this activity a high priority rating. According to one expert, measures should be taken to minimize access to these systems by improving the security capabilities of hardware systems and software applications, as well as by implementing appropriate information technology security policies at wastewater utilities.

One other expert suggested the federal government invest in programs designed to create, accelerate, and deploy minimally acceptable cyber security standards for all automated systems where a compromising event could place a surrounding population at risk. This expert noted that the need for cyber security standards is not limited exclusively to wastewater systems, but stated that the particular needs and characteristics of these utilities should be considered as these standards are developed.

Experts Identified Key Allocation Criteria and Funding Mechanisms for Addressing Wastewater Security Needs

Numerous wastewater utilities have begun to address security concerns by completing vulnerability assessments or by undertaking security upgrades. To date, most security initiatives have been financed by reallocating funds from other important utility activities or embedding security into ongoing operations. According to industry representatives, utilities may ultimately have no choice but to pass these costs along to their customers through rate increases. Given the cost of these security actions, however, many in the utility industry believe federal assistance through the congressional appropriations process is warranted. Experts do not all agree that the wastewater industry as a whole should receive funding priority, noting that other sectors such as electricity or transportation may warrant higher priority. Indeed, while the vast majority of our experts did support federal funds for security for wastewater utilities, some voiced dissenting opinions on the matter.

Nonetheless, should Congress and the administration agree to a request for funds, 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 (1) the types of utilities that should receive funding priority and (2) the most effective mechanisms for directing these funds to potential recipients. Overall, we found a high degree of consensus on the following:

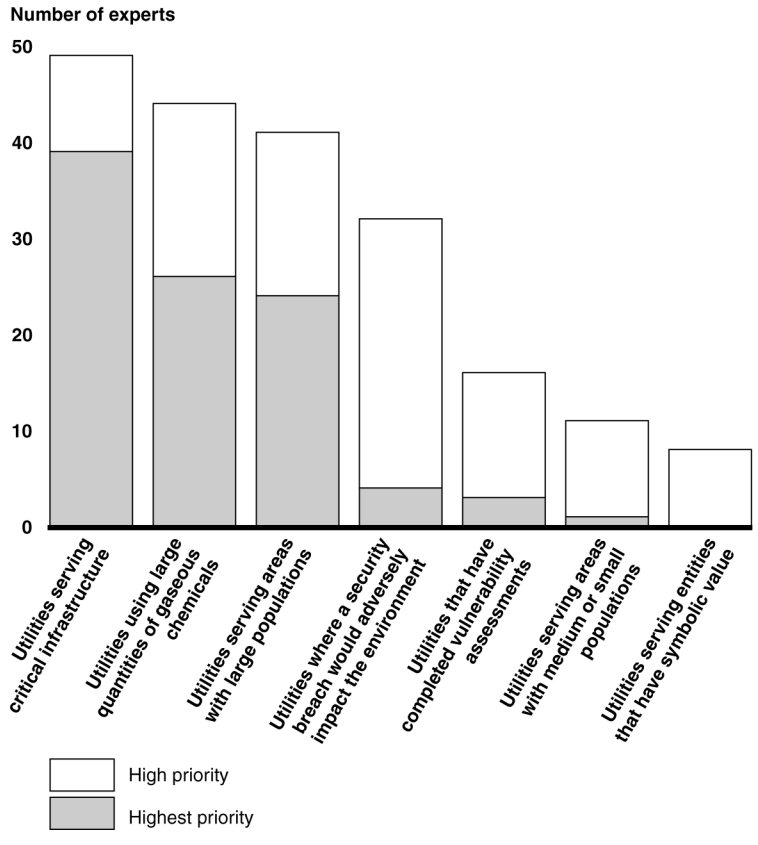
- Thirty-nine of the 50 experts indicated that utilities serving critical infrastructure (including government, commercial, industrial, and public health centers) should be given highest priority for federal funding. Half of the experts gave utilities using large quantities of gaseous chemicals a rating of highest priority while just under half of the experts gave the same rating to utilities serving large populations.

- Direct federal grants are the most favored funding mechanism, with many experts indicating the circumstances in which such grants should or should not include matching funds from the recipient. Many favored direct grants without a matching requirement for a wide variety of planning and coordination activities, such as completing vulnerability assessments, conducting training, and developing standards and guidance. Cost-shared grants were favored for activities that benefit individual utilities, such as strengthening operation and personnel procedures, installing early warning systems in collection systems, and hardening physical assets.

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 critical infrastructure including government, commercial, industrial, and public health centers; (2) using large quantities of gaseous chemicals; (3) serving areas with large populations; (4) where a security breach would adversely impact environmental resources (e.g., receiving waters); (5) having completed vulnerability assessments; (6) serving areas with medium or small populations; and (7) serving buildings, monuments, parks, tourist attractions or other entities that have symbolic value (see fig. 13).

Figure 13: Experts' Views on Which Characteristics of Wastewater Utilities Should Be Used to Set Priority for Federal Funds



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

Utilities Serving Critical Infrastructure

More than three quarters of the experts (39 of 50) gave utilities serving critical infrastructure a highest priority rating. An additional 10 experts gave these utilities a rating of high priority. These utilities provide service to institutions that serve as hubs for government activity; commercial and industrial centers, such as a city's financial district, power plants, or major airports; and public health institutions, such as major medical centers and hospitals. As one expert commented, "while every wastewater system is a potential target, it seems prudent to assume that the larger the system or the criticality of facilities served, the greater the potential impact and hence the more likely the target." Most experts shared this view, including one who said the highest priority should go to "the impact the loss of the treatment facility would have on other vital services" such as providing cooling water for a nuclear or steam generating power plant.

Some experts said that systems with heavy commercial and industrial usage are critical to the country's economic stability, and any major or sustained disruption could have severe economic as well as public health consequences. For example, one expert pointed out that critical industrial customers such as the computer chip manufacturing sector could cost the economy millions per day should a shutdown be caused by the loss of a wastewater treatment plant.

Utilities Using Large Quantities of Gaseous Chemicals

More than half of the experts (26 of 50) gave a rating of highest priority for funding of utilities using large quantities of gaseous chemicals. An additional 18 experts rated these utilities as warranting a high priority for federal funds. Some experts pointed out that many wastewater treatment plants use large quantities of elemental chlorine and other toxic materials which, if released to the atmosphere on-site or during transport to the site, would necessitate widespread evacuations, and possibly cause injuries and fatalities.

Several experts pointed out that the Environmental Protection Agency's (EPA) Risk Management Planning program requires industrial facilities that use threshold amounts of certain extremely hazardous substances to self-identify their worst-case chemical release scenarios. An expert cautioned, however, that funds should not be provided to utilities for converting to *less* hazardous chemicals (e.g., sodium hypochlorite) when other utilities have already or are currently looking at disinfection options that could pose *little or no* security worker risk, or public health risks.

Utilities Serving Areas with Large Populations

Almost half of the experts (24 of 50) gave a rating of highest priority to utilities serving areas with large populations. Seventeen additional experts rated these utilities as warranting a high priority for federal funds. Many experts shared the view that providing financial and technical assistance to the largest treatment plants would protect the greatest number of people. One expert pointed to EPA's 2000 Clean Water Needs Survey, which indicated that about 70 percent of the nation's sewered population is served by the 3,500 largest wastewater facilities (out of a total of 16,000 facilities). Each of these facilities maintains a flow that is greater than 1 million gallons per day. Thus, this expert concluded, funding the largest plants provided benefits to the greatest number of people. Finally, a number of experts suggested that because terrorists are likely to seek to maximize the number of people killed or injured by their attacks, they may try to strike systems serving many customers in large metropolitan areas.

Utilities Where a Security Breach Would Adversely Impact Environmental Resources

While only four experts gave a rating of highest priority to utilities where a security breach would adversely impact environmental resources, 28 of the experts rated these utilities as warranting a high priority. Several experts pointed out the potential for a negative impact on the environment and public health if raw sewage overflows into receiving bodies of water. One expert commented that many wastewater treatment plants discharge highly treated effluent to rivers upstream of the intakes to water treatment plants serving downstream cities. Damage to these wastewater treatment plants could cause the discharge of raw sewage that would be only partially diluted before it reached the intakes of the downstream drinking water treatment plants. Experts also cited significant potential effects on the environment. Some mentioned that the discharge of untreated sewage could impact beaches, critical habitats, or fisheries, causing economic damage in addition to negative environmental and public health effects.

Utilities That Have Completed Vulnerability Assessments

Three of the experts gave a highest priority rating to utilities that have completed vulnerability assessments (VAs). An additional 18 experts gave these utilities a high priority rating. Some experts said that only utilities that have completed VAs should be given federal funding. Other experts pointed out that there should be federal funding for those utilities that have not yet completed VAs so that they can complete this key task. As one expert commented, a key benefit of conducting a vulnerability assessment of a wastewater system is that it allows the areas of the greatest need to be identified.

Properly conducted, a vulnerability assessment brings in all the necessary divisions within a plant including operations, information technology, management, and external forces such as fire departments and local police. Should a plant demonstrate that it has conducted such an assessment, that plant would be much more likely to use federal funding efficiently, this expert added.

Utilities Serving Areas with Medium or Small Populations

Eight of the 50 experts rated utilities serving areas with medium or small populations as a high priority for federal funding. An additional 27 experts rated these utilities as a medium priority. One expert pointed out that such facilities are least able to afford security enhancements or acquire the security expertise and, therefore, may be in need of federal support.

The relatively small number of experts giving a high or highest priority rating for utilities serving areas with medium or small populations may not fully reflect the concern among some experts for the safety of these utilities. For example, some who gave a higher priority rating to utilities serving areas with large populations suggested that the need for federal support should be an important associated criterion, regardless of system size. Accordingly, these experts said that some funding could be justified for both large and small populations based on need. One expert favored a bifurcated focus with one effort seeking to ensure minimal levels of security for all utilities, and another expert favored more intensive efforts focusing on systems serving larger populations.

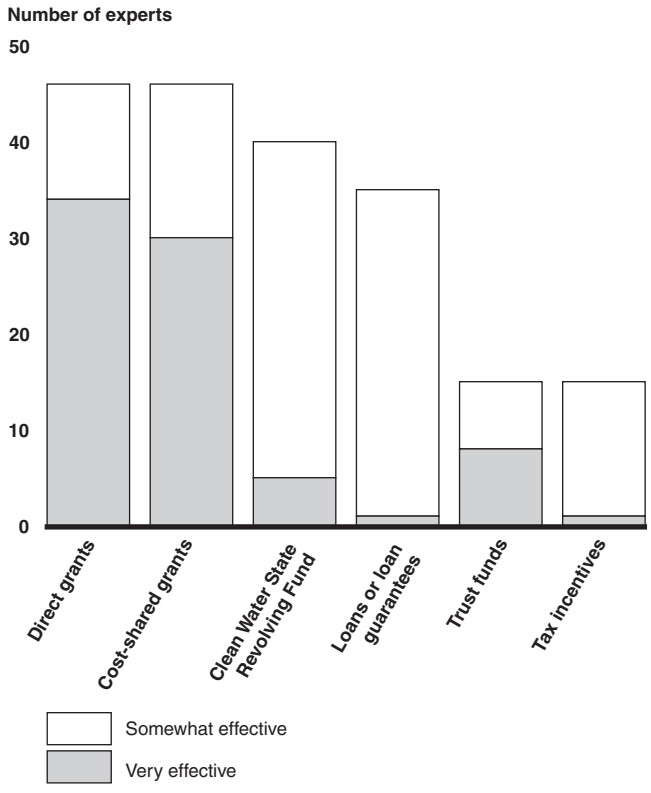
Utilities Serving Entities That Have Symbolic Value

Only one expert gave a highest priority rating to utilities serving buildings, monuments, parks, tourist attractions, or other entities that have symbolic value. An additional 10 experts rated these utilities as warranting a high priority. One expert commented that terrorists have already shown that they want to cause serious economic damage by disrupting tourism. Another noted that terrorists have also targeted cities that have stadiums, convention centers, and other attractions where large numbers of people gather.

Funding Mechanisms Recommended for Distributing Federal Funds

When we asked the experts to identify how best to distribute federal funds that may be made available to utilities to address wastewater security, they overwhelmingly indicated that direct federal grants to utilities would be the most effective mechanism. The experts also indicated that grants in which some type of match is required of recipients would be effective. Relatively fewer experts indicated that the use of trust funds or the Clean Water State Revolving Fund, particularly for upgrades to be implemented in the short term, would be effective. Other mechanisms that were rated as less effective included loans, or loan guarantees, and tax incentives for private utilities. Figure 14 shows how experts rated six different mechanisms for funding wastewater security.

Figure 14: Experts' Views on Mechanisms for Funding Wastewater Security



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

Direct Federal Grants

Thirty-four of the 50 experts indicated that direct federal grants to the utility would be very effective in allocating federal funds. An additional 12 said these mechanisms would be somewhat effective in doing so.

Experts expressed a variety of views regarding how best to implement these grants. For example, some cautioned that a grant program for wastewater security should be solely dedicated to the protection of the wastewater infrastructure, rather than being consolidated together with other programs, such as grants for enhancing homeland security. One said that, contrary to the way grant programs usually operate, utilities should be allowed to apply for grants during project implementation or even after the project is completed. This could reward those who were proactively addressing their security needs. Among other suggestions, one expert said that EPA and the Department of Homeland Security (DHS) should collaborate on allocating these grant funds. This expert stated that "EPA has technical knowledge about facility operations that is especially important and DHS has grant funds for homeland security that could be quickly made available until Congress approves a special allocation." Some experts also commented that direct grants are preferable because they are more likely to result quickly in safety improvements and other desired changes.

Experts also offered opinions on situations in which it would be appropriate to offer a grant without requiring a matching contribution from the recipient. Many, for example, favored direct grants with no match for activities that benefit multiple utilities, or which should be addressed in the near term. Such actions would include conducting research and development to improve detection, developing voluntary wastewater security standards and guidance, completing vulnerability assessments, and providing training to utility security personnel on how best to conduct vulnerability assessments and improve the security culture.

Grants with Matching Requirement (Cost-Shared Grants)

Thirty of the 50 experts indicated that grants with a matching requirement (cost-shared grants) would be very effective as a mechanism for providing funds to wastewater utilities. An additional 16 rated such grants as somewhat effective.

Experts generally favored cost-shared grants for activities that benefit individual utilities. For example, 38 of the 50 experts indicated that cost-shared grants were best for strengthening operation and personnel

procedures, such as securing sewer maps and conducting background checks on new employees. Almost three-quarters of the experts (36 of 50) indicated that cost-shared grants were also best for installing early warning systems in collection systems to monitor for or detect sabotage. Similarly, 32 of the 50 experts indicated that recommended cost-shared grants would be best for improving cyber security and for activities required to harden physical assets, such as building fences, installing locks, and securing manhole covers.

Clean Water State Revolving Fund

The Clean Water State Revolving Fund (CWSRF) is an EPA-administered program that provides grants to the states to allow them to assist publicly owned wastewater utilities. States, in turn, use the funds to provide loans to participating wastewater utilities to assist them in making infrastructure improvements needed to protect public health and ensure compliance with the Clean Water Act. Five experts indicated that the CWSRF would be a very effective funding mechanism to improve wastewater security. An additional 35 indicated that it would be somewhat effective.

According to an EPA Fact Sheet, states may use the CWSRF to assist utilities in completing a variety of security-related actions, such as vulnerability assessments, contingency plans, and emergency response plans. In addition, the EPA Fact Sheet identifies other infrastructure improvements that may be eligible for CWSRF funds, such as the conversion from gaseous chemicals to alternative treatment processes, installation of fencing or security cameras, securing large sanitary sewers and installing tamper-proof manholes.[1] Some experts said that the advantage of the CWSRF is its ability to leverage appropriated federal funds, thereby enabling it to assist more facilities than direct federal grants.

A number of experts, however, expressed caution about relying heavily on the CWSRF to support security enhancements. Several questioned whether the CWSRF was appropriate in an environment where quick, emergency-related decisions were needed, noting that the administrative process in applying for and receiving the funds can be lengthy. Another noted that the CWSRF "was not originally established to deal with security-related projects," and that the program therefore "either needs to [be] fixed to deal

[1]Environmental Protection Agency, Fact Sheet, "Use of the Clean Water State Revolving Fund to Implement Security Measures at Publicly-owned Wastewater Treatment Works," (Washington, D.C., 2003).

with security issues or a separate program needs to be created specifically for security projects." Another expert noted that unless additional security-related monies were added to existing CWSRF levels, it would divert much needed funding away from the kind of critical infrastructure investments that have been the CWSRF's primary purpose.

Loans or Loan Guarantees

Loans are a disbursement of funds by the government to a nonfederal borrower under a contract that requires the repayment of such funds with or without interest. Loan guarantees represent a nonfederal loan to which a federal guarantee is attached.[2] Only one expert indicated that loans and loan guarantees would be very effective mechanisms for providing federal support for wastewater security. An additional 34, however, indicated they would be somewhat effective. Generally, these experts cited the primary advantage of loans or loan guarantees as offering communities the option to amortize security-related costs over an extended period of time, while minimizing the overall cost to the federal treasury. Another expert commented that a low interest loan could provide some incentive and needed capital to implement security programs.

A number of experts, however, expressed reservations. One cautioned that the establishment of any federal loan program to support wastewater security needs should not come at the expense of federal support for the CWSRF, given the critical infrastructure needs that already depend on it for support. Another questioned the value of loans to utilities already strapped for funds, noting that "while loans have less impact on the federal government, many wastewater utilities and local governments generally carry a heavy debt load for capital improvements, and they cannot add significant additional debt that could affect their bond ratings."

Trust Funds

Federal trust funds are accounting mechanisms used to link receipts (from particular taxes or other sources) that by law have been dedicated for a specific purpose or program, such as for infrastructure improvement. For example, such a mechanism is in place for the transportation sector through the Highway Trust Fund. Eight experts indicated that trust funds would be a very effective mechanism for distributing funds for the wastewater security sector. An additional 7 said they would be somewhat

[2]"A Glossary of Terms Used in the Federal Budget Process," (Washington, D.C., 1993) 40, 50.

effective. However, almost half of the experts (24 of 50) indicated that they either had no opinion on this subject or that trust funds were "neither effective nor ineffective."

Experts raised a number of issues as to how the trust fund concept would be implemented. A key consideration was whether the fund would be dedicated solely to wastewater security needs, or be part of a broader fund that serves other wastewater infrastructure needs.[3] One expert suggested that, if wastewater security needs have to compete with the broader range of the wastewater industry's infrastructure needs, they may not receive sufficient priority to be funded adequately. Another expert suggested that a trust fund should be supported annually by the federal government and local wastewater utilities, and administered in a manner similar to the former Wastewater Construction Grants program that funded wastewater construction. This expert indicated that the fund should be used exclusively for enhancing wastewater security.

Tax–Based Incentives

Federal tax-based incentives may include new tax credits for spending on security improvements and the existing exemptions from federal income tax of interest income from state and local government bonds. One expert indicated that tax incentives are very effective, and an additional 14 said they are somewhat effective. Notably, 20 experts indicated that tax-based incentives would be very ineffective—a result due in part to the fact that most wastewater utilities are publicly owned and operated and would, therefore, not benefit from tax-based incentives, like tax credits that would be used to reduce federal income tax.

Nonetheless, some experts said that for the smaller proportion of privately owned systems, tax-based incentives could be beneficial and particularly efficient. One expert noted, for example, that "in those cases where the wastewater treatment facility is privately owned, nothing succeeds as well as tax incentives." Recognizing the diversity of wastewater systems, this expert stated further that the owners know their utility better than anyone

[3]The Water Infrastructure Network, a coalition of groups representing the interests of the water and wastewater industry, has advocated the establishment of a trust fund to support a broad range of water and wastewater infrastructure needs. Some experts on our panel suggested that should this type of mechanism be established, it should be structured in a way that supports the industry's security needs.

and are best able to achieve results in a more cost effective way, if they are incentivized.

Conclusions

To date, the federal government's role in promoting wastewater security has been limited primarily to supporting various training activities on completing vulnerability assessments and emergency response plans and several research projects addressing how contaminants affect treatment systems and other areas. However, legislation supporting an expanded federal role, including a substantially greater financial commitment, has been proposed in the past and may be considered again in the future.

Should such funds be 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 target of an attack (i.e., a large but well-protected facility versus a smaller but less-protected facility); the nature of an attack (cyber, chemical, biological, radiological); and its timing. The experts on our panel have taken these uncertainties into account in deriving their own judgments about these issues. These views, while not unanimous, suggest some degree of consensus on a number of key issues.

We recognize that such sensitive decisions ultimately must take into account a variety of political, equity, and other considerations. We believe they should also consider the judgments of the nation's most experienced individuals on these matters, such as those included on this panel. It is in this context that we offer these results as an input into the decision-making process that Congress and the administration will likely go through as they seek to determine how best to use limited financial resources to reduce the vulnerability to the nation's wastewater utilities.

Participating Experts on Wastewater Security Panel

Expert	Affiliation
Doug Abbott	Maryland Center for Environmental Training
Mark Anderson	Virginia Department of Health
Carol Andress	Environmental Defense
Clifford Arnett	Columbus Water Works
Curt Baranowski	U.S. Environmental Protection Agency
Jeanette Brown	Stamford Water Pollution Control Authority/American Academy of Environmental Engineers
Leonard Casson	University of Pittsburgh
William Conlon	Parsons Brinckerhoff Quade & Douglas, Inc.
Joseph Cotruvo	Joseph Cotruvo & Associates, LLC
James Covel	Upper Occoquan Sewage Authority
Paula Dannenfeldt	Association of Metropolitan Sewerage Agencies
Shuki Einstein	IDC Architects
Richard Fox	Camp Dresser & McKee, Inc.
Suzanne Goss	JEA Electric, Water & Sewer
Neil Grigg	Colorado State University
Michael Gritzuk	City of Phoenix, Water Services Department
Charles Haas	Drexel University
Gail Hackney	Pima Community College
Rick Hahn	R. Hahn & Company, Inc.
Alan Hais	U.S. Environmental Protection Agency
Miriam Heller	National Science Foundation
Richard Holstein	Tetra Tech, Inc.
John Hoornbeek	National Environmental Training Center for Small Communities
Alan Ispass	CH2M Hill
David Jenkins	University of California, Berkeley
Patrick Karney	CH2M Hill (formerly with Metropolitan Sewer District of Greater Cincinnati)
Bruce Larson	American Water
Cecil Lue-Hing	Cecil Lue-Hing & Associates, Inc.
Michael Luers	Snyderville Basin Water Reclamation District
Michael Marcotte	City of Houston, Department of Public Works and Engineering (formerly with District of Columbia Water and Sewer Authority)
John Masek	ABS Consulting

(Continued From Previous Page)

Expert	Affiliation
Paul Orum	Working Group on Community Right-to-Know
Rebecca Parkin	George Washington University Medical Center
Jay Pimpare	U.S. Environmental Protection Agency
Roy Ramani	Water Environment Research Foundation
Daniel Rees	Scientech, LLC
Joan Rose	Michigan State University
H.J. “Bud” Schardein	Louisville/Jefferson County Metropolitan Sewer District
Tom Segars	Miami-Dade Water and Sewer Department
Jim Sullivan	Water Environment Federation
Richard Sustich	University of Illinois at Urbana-Champaign (formerly with Metropolitan Water Reclamation District of Greater Chicago)
James Thomson	Jason Consultants International
Mike Traubert	Arizona Department of Environmental Quality
William Wallace	Rensselaer Polytechnic Institute
Mike Wallis	East Bay Municipal Utility District
Chuck Weber	Prince William County Service Authority
David Weinberg	U.S. Department of Homeland Security
Gary Westerhoff	Malcolm Pirnie, Inc.
Gary Yoshida	Sanitation Districts of Los Angeles County
Rae Zimmerman	New York University

Source: GAO.

Questions and Responses to the Final Questionnaire for the Expert Panel

The body of this report generally identifies which options received the most favorable responses from the expert panel as to how federal funds can best be spent to improve wastewater security (i.e., which activities were viewed as warranting "highest" or "high" funding priority). The table below provides the full range of responses (e.g., "highest priority" to "lowest priority") by the experts to these questions. The tables also indicate the number of experts in each case that responded with "no opinion" or "no response."

Survey Question: What funding priority do you think each of the following security activities should be given?

	Priority for Funding						
Security-Enhancing Activities	**Highest Priority**	**High Priority**	**Medium Priority**	**Low Priority**	**Lowest Priority**	**No Opinion**	**No Response**
Replace Gaseous Chemicals Used in Wastewater Treatment with Less Hazardous Alternatives	29	14	2	5	0	0	0
Improve Local, State, and Regional Collaboration Efforts	23	15	12	0	0	0	0
Complete Vulnerability Assessments	20	14	15	0	1	0	0
Expand Training Opportunities for Wastewater Utility Operators and Administrators	13	27	9	0	1	0	0
Improve National Communications Between Utilities and Homeland Security Entities	8	31	8	1	2	0	0
Install Early Warning Systems to Monitor or Detect Sabotage	7	31	6	4	2	0	0
Harden Physical Assets of Treatment Plants and Collection Systems	8	29	9	4	0	0	0
Strengthen Operations and Personnel Procedures	7	24	17	1	1	0	0
Increase Research and Development Efforts to Improve Detection, Assessment, and Response Capabilities	13	17	15	3	2	0	0
Develop Voluntary Wastewater Security Standards and Guidance Documents	4	25	13	3	5	0	0
Improve Cyber Security and SCADA	5	22	21	1	0	0	1

Note: Table gives the number of experts (out of 50) who indicated each rating.
Source: GAO analysis of experts' survey responses.

Survey Question: What priority should be given to each of the following criteria when allocating federal funds for addressing wastewater security?

	Priority for Allocation of Federal Funds						
Allocation Criteria for Addressing Security Needs	**Highest Priority**	**High Priority**	**Medium Priority**	**Low Priority**	**Lowest Priority**	**No Opinion**	**No Response**
Utilities Serving Critical Infrastructure	39	10	0	1	0	0	0
Utilities Using Large Quantities of Gaseous Chemicals	26	18	1	3	0	1	1
Utilities Serving Areas With Large Populations	24	17	6	2	0	0	1
Utilities Where a Security Breach Would Adversely Impact Environmental Resources	4	28	14	3	0	0	1
Utilities that have Completed Vulnerability Assessments	3	13	21	5	1	1	6
Utilities Serving Buildings, Monuments, Parks, Tourist Attractions, or Other Entities that have Symbolic Value	1	10	29	4	5	0	1
Utilities Serving Areas with Medium or Small Populations	0	8	27	13	1	1	0

Note: Table gives the number of experts (out of 50) who indicated each rating.
Source: GAO analysis of experts' survey responses.

Survey Question: Assuming there is a federal role in funding wastewater security, how effective or ineffective would each of the following funding mechanisms be?

	Effectiveness or Ineffectiveness of Funding Mechanisms						
Funding Mechanisms for Distributing Federal Funds	**Very Effective**	**Somewhat Effective**	**Neither Effective nor Ineffective**	**Somewhat Ineffective**	**Very Ineffective**	**No Opinion**	**No Response**
Direct Grants	34	12	0	3	1	0	0
Cost-Shared Grants	30	16	0	2	0	2	0
Clean Water State Revolving Funds	5	35	5	2	0	3	0
Loans or Loan Guarantees	1	34	11	3	0	1	0
Trust Funds	8	7	10	5	6	14	0
Tax Incentives	1	14	5	5	20	4	1

Note: Table gives the number of experts (out of 50) who indicated each rating.
Source: GAO analysis of experts' survey responses.

Survey Question: **We recognize that different funding mechanisms may be used for different security activities. Considering the funding mechanisms and security activities addressed in this questionnaire, which funding method do you believe would be the best for each of the security activities?**

	Funding Mechanisms for Distributing Federal Funds						
Security-Enhancing Activities	Direct Grants	Cost-Shared Grants	Clean Water State Revolving Funds	Loans or Loan Guarantees	Trust Funds	Tax Incentives	No Response
Replace Gaseous Chemicals Used in Wastewater Treatment with Less Hazardous Alternatives	11	26	10	0	0	0	3
Improve Local, State, and Regional Collaboration Efforts	27	12	1	1	2	0	7
Complete Vulnerability Assessments	28	10	5	1	1	0	5
Expand Training Opportunities for Wastewater Utility Operators and Administrators	28	12	2	2	0	0	6
Improve National Communications Between Utilities and Homeland Security Entities	8	28	5	1	2	0	6
Install Early Warning Systems to Monitor or Detect Sabotage	3	36	3	2	1	0	5
Harden Physical Assets of Treatment Plants and Collection Systems	1	32	11	2	0	0	4
Strengthen Operations and Personnel Procedures	4	38	1	2	0	0	5
Increase Research and Development Efforts to Improve Detection, Assessment, and Response Capabilities	35	8	2	1	0	0	4
Develop Voluntary Wastewater Security Standards and Guidance Documents	30	7	6	1	1	0	5
Improve Cyber Security and SCADA	2	32	8	2	2	0	4

Note: Table gives the number of experts (out of 50) who indicated each rating.
Source: GAO analysis of experts' survey responses.

GAO Contacts and Staff Acknowledgments

GAO Contacts

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

Staff Acknowledgments

In addition to the individuals named above, important contributions were made by Ulana Bihun, Christopher R. Durbin, Lynn Musser, and Diane B. Raynes. Katherine M. Raheb and Carol Herrnstadt Shulman also made key contributions.

GAO's Mission

The Government Accountability 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 GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

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. Government Accountability 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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548