

# Coordinating Efforts to Secure American Public Water Supplies

Tim De Young and Adam Gravley

*It has long been recognized that among public utilities, water supply facilities offer a particularly vulnerable point of attack to the foreign agent, due to the strategic position they occupy in keeping the wheels of industry turning and in preserving the health and morale of the American populace.*

J. Edgar Hoover

First director of the FBI, shortly before the Japanese attack on Pearl Harbor (1941)

Recent media reports claim that Taliban forces in Afghanistan, employing a warfare tactic used in ancient Rome, placed dead animals in community wells to pollute the water supplies of recalcitrant villages. Closer to home and months before the September 11 attacks, the FBI alerted water utilities across the nation that it had received a signed threat, later determined to be a hoax, that an identified terrorist group intended to disrupt water operations in twenty-eight U.S. cities. Just one month after the tragic events of September 11, a spokesman for the East Bay Municipal Utility District in California reported that thieves had stolen several maps describing the water supply infrastructure for twenty-two San Francisco Bay Area cities, including Oakland and Berkeley, along with a tool used to open water valves.

Shortly thereafter, Environmental Protection Agency (EPA) Administrator Christine Todd Whitman assured the American public that the likelihood of a biological or chemical attack on U.S. water supplies is extremely small because of increased security and in light of the so-called dilution effect, whereby an extremely large quantity of any known pollutant would be required to contaminate an entire system. At about the same time, EPA issued a white paper providing guidance to water utilities on immediate steps to take to enhance security. Agencies have stepped up training on how to assess vulnerability, the FBI has issued advice to every law enforcement agency in the country of steps

*Mr. De Young is a shareholder in the Albuquerque office of Modrall Sperling Roehl Harris & Sisk, P.A. and is a vice chair of the Section's Water Resources Committee. He may be reached at tjd@modrall.com. Mr. Gravley is a partner in the Seattle office of Preston Gates and Ellis, LLP and is also a vice chair of the Section's Water Resources Committee. He may be reached at adamg@prestongates.com.*

that can be taken to detect and prevent threats to water systems, and several bills have appeared in the U.S. Congress promising millions of dollars to protect the nation's critical water supply infrastructures.

How secure are our public water supplies? How likely is an attack and how much destruction could result? Are water service providers taking necessary precautions? Do they have adequate resources to respond to the threat? What will an effective response cost, both financially and in terms of restrictions on freedom of information and the public's right to know? Will the patchwork quilt of private, quasi-public, and public water supply systems inhibit or even prevent the implementation of sufficient safeguards? Will this diverse system need to be reformed to allow a coordinated and effective response? Should federal security standards apply to all water systems? In the aftermath of September 11, an impressive array of public agencies, private utilities, and industry trade groups are striving to answer these complex and difficult questions.

To assist these efforts, this article first briefly describes the risks involved, including the possibilities for deliberate attacks and the areas of vulnerability. As part of this analysis, we characterize the potential "targets," the water systems that constitute the complex and highly fragmented infrastructure of America's water supply systems. We then survey the initial institutional responses with a particular focus on the challenges and obstacles. Finally, we identify and discuss potential liability and related legal and policy issues that will need to be addressed as the struggle to protect public water supplies continues.

## *What Are the Risks?*

*One wacko who understands hydraulics and (has) access to a drum of toxic chemicals could inflict serious damage to a water supply in a neighborhood or pressure zone without detection pretty quickly in most communities.*

Gay Porter DeNileon, journalist and member  
National Critical Infrastructure Protection  
Advisory Group (2001)

*It would take large amounts of contaminants to threaten the safety of a city water system. Because of increased security at water reservoirs and*

*other facilities around the country—and because people are being extra vigilant as well—we believe it would be very difficult for anyone to introduce the quantities needed to contaminate an entire system.*

Governor Christine Todd Whitman  
EPA Administrator (2001)

Opinions vary on the susceptibility of public water supplies to terrorist attacks as well as the likelihood of such attacks. There is far less dispute about the needs of water utility customers. Water users require sufficient quantities, adequate pressure, and a reliable, uninterrupted supply of potable water. Deliberate acts that undermine any of these requirements could have devastating impacts on human health and safety, as well as on the economy. Destruction of key operating system components, such as storage facilities, could jeopardize water quality and quantity. Less obviously, a well-placed bomb could cause severe flooding resulting in loss of human life, property damage, and unacceptable costs to the natural environment. Reduced water pressure could, in turn, undermine firefighting efforts. Adequate water quantity and quality is not only required to protect public health, clean water is essential for certain key industries to produce power, process food, and manufacture essential products.

As a result of the anthrax scare, public attention understandably has been focused on biological or chemical weapons. However, physical attacks on water system components pose a more likely and therefore more significant threat to public water supplies. Physical attacks could include the destruction or release of chlorine and other hazardous chemicals used for water treatment. The release of chlorine gas could be deadly within the immediate area of the treatment facility, but the interruption or alteration in the supply of chemicals to the treatment plant preventing disinfection might have more widespread impacts. For any type of physical attack, damages will increase to the extent that alternative water sources are not available.

Because many water systems are governed by highly sophisticated computer systems, much damage could be done by simply destroying or altering computerized controls. The threat of cyber attacks on automated systems used by water utilities should not be underestimated. A hacker hypothetically could modify water quality detection systems, steal sensitive information, and prevent or disrupt water deliveries. In recent years, EPA and other agencies and groups have sponsored workshops to prevent cyber attacks. Such outreach is likely to increase.

As reflected in EPA Administrator Whitman's comments to Congress, experts generally believe that the so-called dilution effect will prevent the successful introduction of a toxic chemical or microbiological agent unless massive quantities are used. Two researchers, Jonathan Tucker and Amy Sands, conducted an exhaustive literature search and found only one documented

death in the U.S. due to intentional water contamination. (Their article, "An Unlikely Threat," was published in the July/August 1999 issue of the *Bulletin of the Atomic Scientists*.) Moreover, nearly all known biological warfare weapons are most effective via aerosol application. Chemicals intentionally introduced for water disinfection historically have posed more of a health threat than acts of chemical or biological sabotage. Since September 11, there have not been any specific threats against any American water supplies, according to the American Water Works Association (AWWA), a trade group with 57,000 members.

If there is one lesson to be learned from September 11, however, it is that even the most unlikely events can occur with devastating results. The particular method used by the terrorists on that date—using hijacked commercial airliners as weapons against buildings—was unprecedented. While it is encouraging to know that few successful attacks on public water supplies have occurred, for the same reason past experience will not help us predict future attacks. While it may be relatively easy to protect water sources and treatment plants from contamination, extensive distribution systems provide multiple access points. For example, if a pollutant is injected into the end of a water line at a higher pressure than the pipe's existing pressure, then the pollutant could enter the system unless there is backflow protection. Some water utility officials believe that the leading threat to the nation's water supply may be the use of backflow pressure to introduce poisons into local water distribution systems.

Unfortunately, some infectious agents and a few biotoxins are unaffected by chlorination. Not surprisingly, the Centers for Disease Control and Prevention is increasing research on the waterborne viability and resistance to disinfection of various agents including smallpox, botulinum toxin, and hemorrhagic fever viruses. At this time, little is known about the extent of risk posed by these materials.

Security measures obviously should be designed to prevent attacks, but continuous monitoring and rapid response capabilities also must be developed. In any event, physical attacks on water systems, including computers, would appear to constitute the primary threat.

### *Increased Security May Further Stress the Aging Water Supply Infrastructure*

*To think of water infrastructure as integrated on a national level is simply inaccurate. It is, in fact, many thousands of separate infrastructures across the country, with vastly different histories and needs.*

Peter Cook, Executive Director  
National Association of Water Companies (2001)

American water supply systems range from massive, well-known federal and state irrigation, flood control, and drinking water projects down to part-time

single well systems providing water during the tourist season at a campground. EPA estimates that approximately 170,000 public water supply systems provide water to more than 250 million Americans including about 54,000 community water systems and more than 20,000 noncommunity water systems serving schools, factories, and other facilities with their own supplies. The sheer number of public, private, and quasi-public systems poses a significant challenge to any attempt to implement a coordinated, effective response to the threats of terrorism. Beyond the numbers, the realities of the existing infrastructure include unprotected reservoirs, systems with inadequate or no treatment capabilities, minimal real-time quality and pressure monitoring, open distribution systems, aging infrastructure, limited resources, stricter quality standards, and significant growth in demand.

An appropriate response to the terrorist attacks should be a renewed focus on the increasing inadequacy of the nation's water supply systems. The U.S. Census Bureau has documented a 9 percent increase in the number of water-consuming Americans in the 1990s and an 80 percent increase since 1950. Moreover, the number of water users is predicted to grow from more than 270 million in 2000 to an estimated 390 million in 2050. A recent AWWA report estimates that to respond to increasing demand more than \$250 billion may be needed over the next thirty years simply to replace worn-out components. This estimate does not include the costs of refurbishing wastewater infrastructure, compliance with new drinking water standards, or improving security. A study by the Water Infrastructure Network in 2000 similarly estimates that \$23 billion per year is needed for the next twenty years just to preserve current health standards and replace crumbling infrastructure. Making needed improvements to aging water supply infrastructure in and of itself will be expensive. The emerging consensus that increased security also is required exacerbates the problem.

On the one hand, security concerns may act as a catalyst to increase spending on crumbling infrastructure. As systems are rebuilt and expanded, security protection can be incorporated during the design process. On the other hand, securing funds for water supply systems may be a zero-sum game in which basic infrastructure improvements and security compete for funds. It does not make much sense to have secure water systems which otherwise are unable to meet the requirements of water users. First, low-cost security measures should receive

top priority and, second, preference should be given to the renovation of basic infrastructure.

It should not be necessary to start from scratch to secure water supply systems, however. All large systems, and many small ones, have implemented emergency response plans. Because most plans primarily address accidental spills and natural disasters, intentional acts can be addressed as such plans are updated. Fortunately, guidance and tools are being developed both by trade organizations and federal agencies as discussed in the following section.

### *Initial Institutional Responses to Protect Water Supplies*

Protection of public water supplies is central to governmental efforts to increase the nation's security and preparedness following September 11. The immediate response for water supplies has focused on three areas: information and communication, research and training, and risk assessment and response planning. Because much remains to be learned about the scope of potential threats and the vulnerability of existing systems, the specific elements of a long-term program remain unknown.

Initial responses of the federal government and national trade organizations are encouraging. The national strategy appears to properly emphasize the need to coordinate efforts of numerous executive departments, federal agencies, state and local governments, water supply associations, and other private entities. A veritable alphabet soup of governmental agencies and industry associations has assumed responsibility for water supply protection programs. See sidebar, page 149. As a result, success will largely turn on the ability of these

entities to coordinate their efforts effectively.

The Bush administration has emphasized the need for coordination in its designation of public water supply as a key infrastructure following September 11. On October 16, 2001, President Bush established the Critical Infrastructure Protection Board to coordinate protection programs to secure information systems and physical assets in water, along with seven other critical infrastructure sectors. Exec. Order No. 13,231, 66 Fed. Reg. 53,063 (2001). The Critical Infrastructure Protection Board's efforts are to be funneled through the Office of Homeland Security established eight days earlier by the President. Exec. Order No. 13,228, 66 Fed. Reg. 51,812 (Oct. 8, 2001).

The federal government began to focus on protecting the nation's water supplies and infrastructure from

---

*Low-cost security measures should receive top priority and second preference should be the renovation of basic infrastructure.*

---

potential terrorist attacks relatively recently. In 1998, the Clinton administration issued Presidential Decision Directives (PDD) on combating terrorism and critical infrastructure protection that set forth key elements of a policy to protect critical infrastructures, including water supply, from physical and cyber attacks. PDD 63 designated EPA as the lead agency for the water supply sector and provided for a private-sector counterpart. Initial water supply protection steps taken by the Bush administration appear to build upon, rather than replace or duplicate, the policy and organizational structure established by the Clinton administration. EPA continues to be the lead agency and other offices created by PDD 63 were retained. Building on the existing framework seems logical and efficient in light of the urgency created by September 11.

The Critical Infrastructure Protection Board communicates with the private sector and state and local governments through the National Infrastructure Protection Center and the Critical Infrastructure Assurance Office. Housed within the FBI, the National Infrastructure Protection Center serves as the national focal point for threat assessment, warning, investigation, and response to attacks on critical infrastructures. The Critical Infrastructure Assurance Office's mission is to integrate plans for separate industry sectors into a national plan, assist federal agency analyses of critical infrastructure dependencies, and promote national education and awareness programs. The directors of the Critical Infrastructure Assurance Office and the National Infrastructure Protection Center serve as members of the Critical Infrastructure Protection Board. The relationship between these offices and their ongoing activities will be developed further over the coming months.

The federal government lacks the resources to communicate directly with each of the nation's approximately 54,000 community water systems. The Clinton administration encouraged public-private partnerships to reduce vulnerability to attacks and initiated mechanisms for two-way communication and information-sharing with water industry groups. In 1998, EPA designated the Association of Metropolitan Water Agencies as the private-sector liaison to the federal government for water supply protection. This industry organization, along with the AWWA and other groups, continues to have significant responsibility for developing and implementing water supply security programs under the Bush administration. For example, EPA recently provided grant funding to the Association of Metropolitan Water Agencies to further develop an information-sharing and analysis center to help disseminate security information and knowledge among drinking water utilities.

The Association of Metropolitan Water Agencies heads up another coordinating group, the Critical Infrastructure Protection Advisory Group. Other members of this advisory group include the Association of State

## Key Agencies and Organizations in Water Security Issues

*Environmental Protection Agency (EPA)* is the lead agency for coordinating drinking water supply security programs.

*Critical Infrastructure Protection Board* is organized under the Office of Homeland Security to coordinate a protection program to secure information systems and physical assets in water and seven other critical infrastructure sectors.

*Critical Infrastructure Protection Advisory Group* coordinates efforts and communications within the water supply utility sector and is led by the Association of Metropolitan Water Agencies.

*Critical Infrastructure Assurance Office* integrates separate industry sector protection into a national plan, assists federal agency analyses of critical infrastructure dependencies, and promotes national education and awareness programs.

*National Infrastructure Protection Center* exists under the FBI to serve as the national focal point for threat assessment, warning, investigation, and response to attacks on critical infrastructures.

*American Water Works Association (AWWA)* is the largest scientific and educational association representing drinking water supply professionals, with approximately 57,000 individual members and 42,000 water utility members.

*Association of Metropolitan Water Agencies* is a trade association, which has been appointed by EPA as the water-sector liaison to the federal government. It leads the Critical Infrastructure Protection Advisory Group.

*National Association of Water Companies* is a 200-member association of private and investor-owned drinking water utilities.

*Sandia National Laboratories* is a Department of Energy research facility based in Albuquerque, New Mexico.

Drinking Water Administrators, AWWA, National Association of Water Companies, and other water supply organizations. The current goals of this group are to promote water supply vulnerability assessments and emergency procedures for response and recovery, oversee development of an information-sharing and analysis center, and suggest areas for continued research and development.

Substantively, individual water supply systems have been encouraged to take action in three key areas: prevention, detection, and response. Heightened security at all access points is the first step in prevention. Utilities have increased basic prevention measures such as checking identification, locking gates and doors, and verifying alarm systems are in place and in working order. These relatively low-cost measures can do much to deter physical attacks. Current efforts also encourage water utilities to update or complete vulnerability assessments to identify preventative measures needed for a particular system. Many local water supply systems have emergency response plans in place, but these plans tend to focus on natural disasters. An unresolved issue is the proper balance between the public's right to know and the need to limit disclosure to enhance security.

Beginning in November 2001, EPA, with the assistance of AWWA and Sandia National Laboratories, began holding training sessions to help water supply utilities assess vulnerabilities and develop measures to reduce the risk of attacks. The initial training sessions have focused on the 340 largest water systems that serve populations of 100,000 or more people. The AWWA Research Foundation and Sandia National Laboratories are also leading research efforts to develop a program and technical tools to assess water infrastructure vulnerabilities for use by all utilities.

Although the costs of initial security measures and vulnerability assessments may be minimal, many water systems will need to spend significant amounts to implement long-term security measures. For example, the City of Seattle provides water to 1.3 million people and has nine uncovered, in-city reservoirs each storing 7 million to 68 million gallons of treated drinking water. Under federal regulation, new reservoirs are required to be covered. Pursuant to a negotiated regulatory order, however, Seattle is not required to cover its nine uncovered reservoirs until 2020. In the aftermath of September 11, the Seattle City Council is considering accelerating the reservoir-covering program as part of a comprehensive security enhancement program. The cost of covering one reservoir ranges from \$2 million to \$12 million.

The Seattle example also illustrates the likely competition between making improvements to aging water supply infrastructure versus spending limited funds on security. Seattle constructed the uncovered reservoirs between 1901 and 1958. Typical of large water supply

utilities, Seattle built major parts of its current system decades ago when concerns about terrorist attacks were not present. An increasing number of these facilities need replacement. The nation's water systems face an estimated funding gap of \$11 million per year merely to replace aging pipes and meet the current requirements of the Safe Drinking Water Act. Although the level of additional funding required to address security requirements for capital improvements is just beginning to be studied, it is sure to be large. As the national economy continues to struggle, there is unlikely to be adequate funding to address both immediate security needs and long-term infrastructure needs.

**R**ecommended or required security measures raise a significant risk of creating an unfunded federal mandate for water supply systems. Even the initial rush to require vulnerability assessments and update emergency response plans may be underfunded. The Association of Metropolitan Water Agencies has estimated that \$94 million will be needed to conduct physical vulnerability assessments for the roughly 740 large water systems that serve more than 50,000 people and that \$55 million is needed to update and improve emergency plans for these large systems. This does not even include the costs of conducting vulnerability assessments and updating the response plans of smaller systems.

As part of a recent \$40 billion supplemental appropriation for disaster assistance and antiterrorism initiatives, President Bush initially proposed to allocate \$34 million to EPA to fund drinking water vulnerability assessments, about one-third of the amount needed. The President's budget did not include any funds for emergency response plans. In November, the House Appropriations Committee recommended the appropriation of \$110 million for vulnerability assessments. H.R. 3338, 107th Cong. (2001). In December, Congress approved a version of the bill that would provide approximately \$90 million for EPA to spend on various counterterrorism initiatives, including water system vulnerability assessments.

Congress also is working on a range of proposed legislative measures to address potential biological attacks and the costs to fully assess and implement water supply security measures. These proposals are evolving as they move through the legislative process, and new bills are in preparation, but the following leading proposals as of December 2001 highlight the extent of congressional interest.

The Senate approved a bill in December focusing on the immediate concerns for basic security measures at drinking water and wastewater facilities. S. 1608, 107th Cong. (2001). The program would authorize EPA to provide \$50 million for short-term projects such as security staffing; intrusion alert systems; fencing, lighting, and increased visibility around facilities; closed-circuit television monitoring; and training programs. Although \$50

million is a relatively small amount for a federal grants program, this would only fund the lowest-cost measures.

Congress is also starting to address water security research. The House of Representatives and the Senate Environment and Public Works Committee approved the Water Infrastructure Security and Research Development Act. H.R. 3178, 107th Cong. (2001); S. 1593, 107th Cong. (2001). This bill would authorize EPA to provide \$12 million annually to support water security research by the AWWA Research Foundation, universities, and national laboratories. This amount may be inadequate because significant research is needed to prevent, detect or respond to physical or cyber threats including biological, chemical, and radiological contamination. Projects developing programs or tools to disseminate information and research results also would be eligible to compete for this limited funding. Although such legislation would enable antiterrorism research to become a higher priority for EPA, the level of funding should be increased.

Indeed, three current bills propose higher levels of funding. First, the Bioterrorism Protection Act of 2001 proposes a \$7 billion package including \$246 million in 2002 for water and wastewater systems. H.R. 3255, 107th Cong. (2001). The bill would authorize EPA to provide \$66 million for vulnerability assessments, \$55 million for emergency response planning, \$60 million for basic security enhancements, \$80 million for cyber security, and \$3 million for research. Again, the amount for research appears to be inadequate.

A key problem with this bill and other proposals involving EPA assistance to water systems involves effective distribution of funds. EPA historically has used the State Revolving Fund under the Safe Drinking Water Act to distribute federal funds to water supply utilities. However, the necessary paperwork can be complicated and particularly frustrating to smaller systems with limited staff resources. In addition, several states restrict the distribution of such funds to certain types of utilities. Assuming EPA continues as the funding agency, its effective, fair, and timely distribution of grant funds seems unlikely. Absent some other funding method, EPA should implement a streamlined process to distribute monies quickly and fairly.

In contrast, a different bill, the proposed Homeland Security Block Grant Act, would provide \$3 billion directly to cities, counties, and states. S. 1737, 107th Cong. (2001). Activities eligible for assistance include physical and cyber security for water systems, security planning, and communication and notification systems. By using the block grant approach, this proposal would provide a more direct and timely funding mechanism and give more flexibility to local communities.

A major bill that has passed the House would be problematic for water supply utilities because it could create an unfunded mandate. The Public Health Security and Bioterrorism Response Act of 2001 proposes

\$120 million for water supply system vulnerability assessments and emergency response planning. H.R. 3448, 107th Cong. (2001). Each of the approximately 8,000 community water systems that serve more than 3,300 persons would be required to assess the vulnerability of its facilities to a terrorist attack or any other act intended to substantially disrupt the ability to provide a safe and reliable supply of drinking water. Water systems are then required to prepare or update emergency response plans to incorporate the results of the vulnerability assessment. In addition to proposing insufficient funding for the initial vulnerability assessment and planning phase, the mandate of H.R. 3448 would likely cause systems to incur significant additional expenses on an ongoing basis. The counterpart bioterrorism bill passed by the Senate does not authorize funds for water system assessments or planning. S. 1765, 107th Cong. (2001).

Congress should fully fund the initial security response without creating any new mandates and then proceed to address the long-term capital needs of our nation's water infrastructure. Specifically, Congress should immediately provide funds for basic physical and cyber security steps, vulnerability assessments, emergency response planning, communication networks, and research. To speed distribution of money to water systems, Congress should use a direct grant program to cities and states instead of an indirect program like the State Revolving Fund. After the results of vulnerability assessments and research efforts become known, Congress can revisit water supply security threats and determine whether a second phase of federal assistance or involvement is warranted.

### *Unresolved Legal and Policy Issues*

Balancing the objectives of freedom of information and the public's right to know with the need for national security is one of the most important challenges to address in the post-September 11 era. This challenge is directly applicable to water supply systems. On October 12, 2001, for example, the U.S. Government Printing Office issued an order directing all 335 federal depository libraries to destroy copies of a CD-ROM containing an electronic database issued by the U.S. Geological Survey in 1999. The action has caused an ongoing debate about the extent to which publicly available information will be restricted on national security grounds. The database, "Source-Area Characteristics of Large Public Surface-Water Supplies in the Conterminous United States," contains no analysis of system vulnerabilities. The federal government removed the database, however, apparently because it provided locations of critical water supply infrastructure. Interestingly, the database merely compiled previously published information but its electronic, comprehensive format apparently was considered to be too attractive to would-be terrorists.

Similar efforts to remove sensitive information from government websites and public libraries are ongoing. The destruction of sensitive information already made available to the public is a questionable tactic not only because the information has already been released but because legitimate users may be deprived access to useful information. Instead of destroying information, it would be better to restrict access to information that creates a genuine security risk if disclosed, such as emergency response plans. Fortunately, the technology for encryption and password protection is sufficiently advanced to protect sensitive information and should be employed. At the same time, what does and does not constitute a security threat must be determined, keeping in mind both the tendency of criminals to shift their targets in response to security measures and the need to allow for freedom of information to the extent possible.

A second issue concerns the liability of water utilities. Our review of the initial institutional responses to terrorist threats suggests that there has been little consideration of this issue. Because of limited experience, the extent to which utilities could be held liable for terrorist attacks is largely unknown. Following the 1993 bombing of the World Trade Center, hundreds of lawsuits were filed against the New York Port Authority claiming personal injury, wrongful death, property damage, and damages for business interruption. While many of the liabilities were based on claims of negligence, claims were also made based on premises liability and contract. Lawsuits inevitably will arise in the aftermath of September 11 to the extent that victim compensation relief is insufficient. Similar lawsuits can be expected when water supplies or infrastructure are sabotaged. For many water utilities, a large award could undermine their financial ability to continue providing needed services. Even a claim could affect a utility's bond rating. While it is beyond the scope of this article to present a thorough legal analysis of potential liability, the key features of the problem are highlighted below.

Generally, utilities would be sued under negligence theories. From a policy perspective, it could be argued that making water utilities liable for damages caused by terrorist attacks may encourage utilities to take necessary steps to prevent such attacks. On the other hand, many water utilities simply do not have the resources to act as insurers for its customers or to address all conceivable threats. Ironically, legal actions may arise from attempts to make public water supplies more secure. For example, EPA's recently issued guidelines detail the security measures water utilities are advised to implement immediately. If a particular utility fails to implement some or all of these measures or does so in a negligent manner, then the utility arguably should be liable for consequential damages. In the numerous jurisdictions where comparative negligence applies, a utility theoretically could be held liable for some portion of

the damages upon a showing of minimal negligence. There appears to be little case law directly on point but a number of courts have held that a water distributor is not an insurer with respect to the condition of its infrastructure and is therefore not liable for damages except on a showing of negligence.

Many, but clearly not all, water providers may be protected from some liability claims under the doctrine of sovereign immunity. For those private utilities with no such protection, increased insurance protection may be advisable. Post-September 11, the availability of insurance against acts of terrorism may in turn be more problematic. Even where the doctrine of sovereign immunity applies, there is generally no protection for negligent operations or maintenance of facilities. Moreover, ordinances or service contract disclaimers of liability have not barred recovery in many cases. In any event, a coordinated federal response would not appear to be possible due to the considerable variations across the states in both tort claims act provisions and applicable case law. Striking the proper balance between insulating water utilities from liability and protecting water consumers from terrorist attacks therefore may best be resolved at the state or local level.

Securing drinking water and supply systems against possible terrorism will not be easy, inexpensive, or without controversy. However, the immediate response is promising. Building on an existing organizational scheme of federal agencies and water industry associations, the initial tasks are to identify and assess risks, plan how to prevent and respond to attacks, and develop or improve communication networks. Congress should quickly and directly provide funds to water systems to carry out the initial response steps without attaching any new mandates, and consider later whether an increased federal role in local water supply would help.

Keeping the longer-term mission on course will require sustained effort and hard choices. Congress and state legislatures will be asked to narrow freedom of information laws in many areas and clarify legal responsibility for injury caused by terrorist actions, including water supply and other key infrastructure sectors. Government agencies, water industry organizations, and local water systems will increasingly need to work together to develop and share information and balance increased protection with continued local control. It is the local water suppliers that are ultimately responsible for providing safe and reliable drinking water, but they oversee a declining infrastructure base. Federal funding is needed to address the growing backlog of capital requirements in addition to implementing security measures. Modern water supply systems are fundamental to public, environmental, and economic health. Our national response to September 11 should include a commitment to renew neglected cornerstones of our homeland's foundation. 